COMMUTATIVE ALGEBRA

OREN BECKER

This introductory set of notes is based on a 24-lecture Part III (master's level) course I taught at the University of Cambridge during Michaelmas terms 2022–2024, with some modifications. If you happen to spot any errors or have suggestions, I'd be grateful if you reached out to me at oren.becker@gmail.com.

Some sections draw on the classic *Introduction to Commutative Algebra* by Atiyah and Macdonald, and for the part on Tensor Products, I found inspiration in two excellent sets of notes by Keith Conrad, available at: https://kconrad.math.uconn.edu/blurbs/.

Contents

1. A concise review of rings and modules

Unless stated otherwise, we use the term *ring* for a commutative (i.e. $ab = ba$) unital (i.e. $1 \in A$) ring A.

Nevertheless, here's a important noncommutative ring: For an abelian group M, let $\operatorname{End} M$ be the ring of group endomorphisms of M (i.e. group homomorphisms $M \to M$), with pointwise addition, and where the ring multiplication is given by composition of functions.

Recall that a homomorphism $R \to S$ of unital rings is required to send $1_R \mapsto 1_S$.

Definition 1.1. An R-module M (R a ring) is an abelian group $(M, +)$ together with a fixed ring homomorphism $\rho\colon R \to \operatorname{End} M$ (called the *structure homomorphism*).

For $r \in R$ and $m \in M$, we write $rm \coloneqq (\rho(r))m$. Then:

(1) $r(m_1 + m_2) = (\rho(r))(m_1 + m_2) = (\rho(r)m_1) + (\rho(r)m_2) = rm_1 + rm_2$ (since $\rho(r)\colon M \to M$ is a group homomorphism)
(2) $(r_1 + r_2)m = \rho(r_1 + r_2)m = (\rho(r_1) + \rho(r_2))m = r_1m + r_2m$ (since $\rho\colon R \to \operatorname{End} M$ is a ring homomorphism)

(3) etc.

Note:

(1) For a field k, a k-module is the same thing as a k-vector space.
(2) Every abelian group M has a unique structure of a $\mathbb{Z}$-module (because there is exactly one ring homomorphism $\mathbb{Z} \to \operatorname{End} M$). So a $\mathbb{Z}$-module is the same as an abelian group.
(3) An R-submodule of an R-module M is an additive subgroup $N \subset M$ such that $rN \subset N$ for all $r \in R$.
(4) Every ring R is an R-module in a natural way (where $\rho\colon R \to \operatorname{End} R$ is given by $\rho(r)r' = rr'$).
(5) For a subset S of an R-module M, the R-submodule of M generated by S is the intersection of all R-submodules of M that contain S. Equivalently, it is the set of sums of the form $\sum_{i=1}^{n} r_i x_i$, $n \geq 0$, $r_i \in R$, $x_i \in S$ (these are called R-linear combinations of the elements of S; note that each such sum has finitely many terms).
(6) An *ideal* of the ring R is the same thing as an R-submodule of R.

For an ideal I of R, we can form the quotient ring R/I. As an abelian group, this is just the group quotient R/I. The multiplication is given by $(r_1 + I)(r_2 + I) = r_1 r_2 + I$ (note that the product set $\{(r_1 + x_1)(r_2 + x_2) \mid x_1, x_2 \in I\}$ is contained in $r_1 r_2 + I$, but the inclusion might be proper, unlike the case of a quotient group G/N, $N \lhd G$, where the product set of $g_1 N$ and $g_2 N$ is always equal to $g_1 g_2 N$; it is true, however, that $r_1 r_2 + I$ is the unique coset of I that contains the product set above). Note that a subset I of R is an ideal if and only if there is a ring S and a ring homomorphism $R \to S$ whose kernel is I.

2. Chain conditions

Definition 2.1. An R-module M is *noetherian* if one (hence both) of the following conditions holds:

(1) Every ascending chain of submodules $M_1 \subset M_2 \subset \dots$ of M stabilizes (i.e., for some $n \geq 1$, $M_{n'} = M_n$ for all $n' \geq n$).
(2) Every nonempty set Σ of submodules of M has a maximal element (i.e., an element of Σ not contained in any other element of Σ).

An R-module M is *artinian* if it satisfies (1) above, but with "ascending" replaced by "descending" (i.e. $M_1 \supset M_2 \supset \dots$). Equivalently, M is artinian if it satisfies (2) above, but with "maximal" replaced by "minimal".

The equivalence of the two conditions above is proved using the axiom of choice (or some weak form of it). Noetherian modules have one more equivalent characterization, which I personally prefer to use most of the time:

Lemma 2.2. *An R-module M is noetherian if and only if every submodule of M is finitely generated.*

In particular, every noetherian module is finitely generated. The converse is false: Every ring R is finitely generated as an R-module (by the single element 1_R), and in particular this is true for the polynomial ring $R = \mathbb{Z}[T_1, T_2, \ldots]$. Let M be the submodule of R generated by $T_1, T_2, \ldots$ (consisting of all polynomials with constant term 0). Any finite subset S of M is contained in the submodule $M' = R \cdot T_1 + \ldots + R \cdot T_\ell$ for some $\ell \geq 0$ because each polynomial in S involves finitely many variables. But M' (which is just the submodule of R generated by $T_1, \ldots, T_\ell$) does not contain $T_{\ell+1}$, and thus S does not generate M.

Definition 2.3. A ring R is *noetherian* (resp. *artinian*) if R, regarded as an R-module, is noetherian (resp. artinian).

Equivalently, one may define a noetherian (resp. artinian) ring by taking Definition 2.1, and replacing the word submodule by the word ideal.

Example 2.4.

1. $\mathbb{Z}$-modules:
   - (a) $\mathbb{Z}$, as a $\mathbb{Z}$-module, is noetherian, but not artinian.
   - (b) The $\mathbb{Z}$-module $\mathbb{Z}\big[\frac{1}{2}\big]/\mathbb{Z}$ is artinian, but not noetherian (this requires some thought). Here $\mathbb{Z}\big[\frac{1}{2}\big] = \big\{\frac{a}{2^m} \mid a, m \in \mathbb{Z}\big\}$.
2. Rings:
   - (a) $\mathbb{Z}$, as a ring, is noetherian, but not artinian.
   - (b) Every artinian ring is noetherian. In fact, a ring R is artinian if and only if R is noetherian of Krull dimension zero (see later).

Recall that another name for a homomorphism of R-modules is an *R-linear map*.

Definition. Let R be a ring. A sequence

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

of R-modules $(M_i)_{i\in\mathbb{Z}}$ and R-linear maps $(f_i \colon M_{i-1} \to M_i)_{i\in\mathbb{Z}}$ is *exact* if $\operatorname{im} f_i = \ker f_{i+1}$ for all $i \in \mathbb{Z}$.

A *short exact sequence* (*SES*) is an exact sequence of the form:

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{p} L \longrightarrow 0$$

Remark 2.5. In a SES as above:

1. The left and right maps are necessarily the zero maps.
2. Thus i is injective and p is surjective.
3. Thus $N \cong i(N)$ and $L \cong M/i(N)$ as R-modules.

Lemma 2.6. *Let*

$$0 \to N \to M \to L \to 0$$

be a short exact sequence of R-modules. Then M is noetherian (resp. artinian) if and only if both N and L are noetherian (resp. artinian).

Corollary 2.7. *If M_1 and M_2 are noetherian (resp. artinian) R-modules then $M_1 \oplus M_2$ is noetherian (resp. artinian).*

Proof. Apply Lemma 2.6 to the SES:

$$0 \longrightarrow M_1 \overset{m_1 \mapsto (m_1,0)}{\longrightarrow} M_1 \oplus M_2 \overset{(m_1,m_2) \mapsto m_2}{\longrightarrow} M_2 \longrightarrow 0$$

□

Note that the corollary can be applied repeatedly a finite number of times to deduce that $M_1 \oplus \ldots \oplus M_n$ is a noetherian (resp. artinian) R-module whenever $M_1, \ldots, M_n$ are noetherian (resp. artinian).

Two observations:

(1) **R-linear maps from R:** For an R-linear map $\varphi\colon R \to M$ we have $\varphi(r) = \varphi(r \cdot 1) = r\varphi(1)$. So $\varphi(r) = rm$ for $m = \varphi(1)$. On the other hand, $r \mapsto rm'$ is an R-linear map for all $m' \in M$.

(2) The universal property of the direct sum: For R-modules $(M_t)_{t\in T}$ (T any set), consider the direct sum $\bigoplus_{t\in T} M_t$ and the natural embeddings $\rho_t\colon M_t \to \bigoplus_{t\in T} M_t$ (recall that each element of $\bigoplus_{t\in T} M_t$ is zero in all but finitely many coordinates, by definition). Then for any R-module N and R-linear maps $\varphi_t\colon M_t \to N$ there is exactly one homomorphism $\varphi\colon \bigoplus_{t\in T} M_t \to N$ such that $\varphi \circ \rho_t = \varphi_t$ for all $t \in T$. In other words, specifying an R-linear map $\bigoplus_{t\in T} M_t \to N$ is equivalent to specifying a collection of R-linear maps $(M_t \to N)_{t\in T}$.

(3) Combining the two observations above, we see that R-linear maps $\varphi\colon R^{\oplus \ell} \to M$ are exactly the maps of the form $(r_1, \ldots, r_\ell) \mapsto \sum_{i=1}^{\ell} r_i m_i$ for fixed $m_1, \ldots, m_\ell$. If φ is surjective then M is finitely generated (by $\varphi(1,0,\ldots,0), \ldots, \varphi(0,\ldots,0,1)$). Conversely, if N is an R-module generated by finitely many elements $n_1, \ldots, n_k \in N$ then there is a surjective R-linear map $R^{\oplus k} \to N$ given by $(r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i n_i$.

To summarize, a "finitely generated R-module" is the same as "an R-module that admits a surjective R-linear map from $R^{\oplus \ell}$ for some integer $\ell \geq 0$", i.e. "a quotient module of $R^{\oplus \ell}$ for some integer $\ell \geq 0$ (up to isomorphism)".

(4) In general, an R-module isomorphic to $R^{\oplus S}$ (i.e., the direct sum of $|S|$ copies of R, where S is finite or infinite) is called a *free* R-module. By the discussion above, we see that it is easy to produce

homomorphisms from a free R-module to any other R-module (just choose a homomorphism for each coordinate).

Equivalently, an R-module M is free if it has a free basis (i.e., a subset $B \subset M$ such that every $x \in M$ is equal to $\sum_{i=1}^{\ell} r_i x_i$, $\ell \geq 0$, $0 \neq r_i \in R$, $x_i \in B$ in a unique way).

(5) For a field k, the theorem "every k-vector space has a basis" is equivalent to "every k-module is free". In particular, the k-module $k^{\mathbb{N}}$ (of all $\mathbb{N}$-indexed tuples with entries in k) is isomorphic to $k^{\oplus S}$ for some set S (the proof that every vector space has a basis requires some form of the axiom of choice, so the isomorphism $k^{\mathbb{N}} \cong k^{\oplus S}$ is somewhat mysterious).

Proposition 2.8. *Let R be a noetherian (resp. artinian) ring. Then every finitely generated R-module M is noetherian (resp. artinian).*

Proof. By the observations above, M is a quotient of $R^{\oplus \ell}$ for some $\ell \geq 1$. But R is a noetherian R-module, and so $R^{\oplus \ell}$ is noetherian, and thus so is its quotient M (and similarly for the artinian case). □

In particular, a finitely generated module over a noetherian ring is noetherian[1]. A deeper (and still true) statement is Hilbert's basis theorem (see below): every finitely generated algebra over a noetherian ring is noetherian. But what is an algebra?

Definition 2.9. An R-algebra is a ring A equipped with a fixed ring homomorphism $\rho \colon R \to A$.

For $r \in R$ and $x \in A$, we write $rx \coloneqq \rho(r)x$.

So specifying an R-algebra is superficially similar to specifying an R-module, with two major differences: We start with a ring A (rather than a mere abelian group M), and then we fix a ring homomorphism $R \to A$ (rather than $R \to \operatorname{End} M$).

So, every R-algebra is also an R-module: Take an R-algebra A, whose structural homomorphism is $\rho \colon R \to A$. Then the map $R \to \operatorname{End}(R, +)$ given by $r \mapsto (x \mapsto \rho(r)x)$ is a ring homomorphism, making A into an R-module.

Note that every ring A is a $\mathbb{Z}$-algebra in exactly one way (because there is exactly one ring homomorphism $\mathbb{Z} \to A$).

It is sometimes notationally convenient to notice that $\rho(r) = r \cdot 1_A$ in the notation of Definition 2.9 (Proof: $\rho(r) = \rho(r) \cdot 1_A = r \cdot 1_A$). This allows us to declutter the notation by not naming the ring homomorphism $R \to A$ when taking about an algebra).

[1] So, a ring R is noetherian if and only if every submodule of every finitely generated R-module is again finitely generated (check!)

A subalgebra of an R-algebra A is a subring $B \subset A$ such that $rx \in B$ for all $r \in R$ and $x \in B$. Note that is implies that B contains the image of R in A (i.e. all elements of the form $r \cdot 1_A$). For a subset S of an R-algebra A, the subalgebra B of A generated by S is the intersection of the subalgebras of A that contain S. Equivalently B consists of all elements of the form $p(x_1, \ldots, x_m)$, $m \geq 0$, where $p \in R[T_1, \ldots, T_m]$ (i.e., p is a polynomial in the variables $T_1, \ldots, T_m$ with coefficients in R) and $x_1, \ldots, x_m \in S$.

Example 2.10. Let k be a field and consider the polynomial ring $A = k[T_1, \ldots, T_m]$. Then A is a k-algebra and a k-module (in the natural ways). But A is a finitely generated k-algebra (generated by $T_1, \ldots, T_m$), but not a finitely generated k-module (prove!).

A further clarification: Let A be an R-algebra and S a subset of A. Then the R-submodule of A generated by S is the set of elements of the form $p(x_1, \ldots, x_m)$, $m \geq 0$, where $p \in R[T_1, \ldots, T_m]$ has degree 1 and no constant term and $x_1, \ldots, x_m \in S$ (whereas the subalgebra generated by S consists of elements of the same form, but with no restriction on the polynomial p).

Remark 2.11. First, recall that $\{0\}$ is a ring (called the zero ring). It is the only ring where $1 = 0$ (prove!), and there is no ring homomorphism from $\{0\}$ to any nonzero ring. Now to the remark itself: For a k-algebra $A \neq \{0\}$, where k is a field, the structural ring homomorphism $\rho\colon k \to A$ must send $1 \mapsto 1$. Thus $1 \notin \ker \rho$, and so $\ker \rho$ is an ideal of k that does not contain 1. But k has only two ideals: $\{0\}$ and k. So $\ker \rho = \{0\}$, i.e. ρ is injective. In particular, a nonzero k-algebra contains a copy of k (embedded in A in a particular way via ρ).

Definition 2.12. For R-algebras A and B, with structural homomorphisms $\rho_A\colon R \to A$ and $\rho_B\colon R \to B$, an R-algebra homomorphism $A \to B$ is a ring homomorphism $\varphi\colon A \to B$ such that $\varphi \circ \rho_A = \rho_B$.

(so, an R-algebra homomorphism is a ring homomorphism between R-algebras that sends $r \cdot 1_A \mapsto r \cdot 1_B$ for each $r \in R$).

Equivalently, φ is an R-algebra homomorphism if and only if φ is an R-linear map such that $\varphi(1_A) = 1_B$ and $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$ for all $a_1, a_2 \in A$ (check!).

Exercise 2.13. Some people wrongly say that a nonzero algebra over a field k is just a "ring that contains k". Give them an example that shows that their definition does not allow to capture the notion of a k-algebra homomorphism as in Definition 2.12. **Hint:** Make $\mathbb{C}$ into a $\mathbb{C}$-algebra in two different ways, and then check if the identity map $\mathbb{C} \to \mathbb{C}$ is a $\mathbb{C}$-algebra homomorphism, where the domain and range and $\mathbb{C}$-algebras in different ways.

For a ring R, the polynomial R-algebra $R[T_1, \dots T_n]$ has the following universal property: For every R-algebra A and elements $a_1, \dots, a_n \in A$, there is exactly one R-algebra homomorphism $R[T_1, \dots, T_n] \to A$ that sends $T_i \mapsto a_i$ for all $1 \leq i \leq n$. This works even if there are infinitely many variables (remember that each polynomial involves finitely many variables). Thus, it is easy to produce homomorphisms from $R[T_1, \dots, T_n]$ to any other R-algebra (which is similar to the way it is easy to produce homomorphisms from a free R-module to any other R-module).

We say that an algebra A is noetherian (resp. artinian) if A, as a ring, is noetherian (resp artinian).

Theorem 2.14 (Hilbert's basis theorem)**.** *Every finitely generated algebra over a noetherian ring is noetherian.*

Proof. Let R be a noetherian ring. By the observations above, it suffices to prove that the polynomial algebra $R[T_1, \dots, T_n]$ is noetherian. Since $R[T_1, \dots, T_n] \cong R[T_1, \dots, T_{n-1}][T_n]$, it suffices to show that the univariate polynomial algebra $R[T]$ is noetherian, and then proceed by induction.

Let $\mathfrak{a}$ be an ideal of $R[T]$. For $i \geq 0$, write $\mathfrak{a}(i) = \left\{c_0 \mid c_0 T^i + \dots + c_i T^0 \in \mathfrak{a}, c_0, \dots, c_i \in R\right\}$ (this set consists exactly of the leading coefficients of all degree-i polynomials in $\mathfrak{a}$, toegether with 0). Then $\mathfrak{a}(i) \subset \mathfrak{a}(i+1)$ and $\mathfrak{a}(i)$ is an ideal of B for all $i \geq 0$ (check!). Since R is noetherian, the sequence $\mathfrak{a}(0) \subset \mathfrak{a}(1) \subset \dots$ stabilizes, say, $\mathfrak{a}(m') = \mathfrak{a}(m)$ for some $m \geq 0$ and all $m' \geq m$, and each ideal $\mathfrak{a}(i)$, $i \geq 0$, is generated by some finite subset $\{r_{i,1}, \dots, r_{i,n_i}\}$ of R. By the definition of $\mathfrak{a}(i)$, there is $f_{i,j} \in \mathfrak{a}$ such that $f_{i,j} = r_{i,j}T^i + \{\text{terms of degree} < i \text{ in } T\}$. Let $\mathfrak{b}$ be the ideal of $R[T]$ generated by the finite set $\{f_{i,j} \mid 0 \leq i \leq m, 1 \leq j \leq n_i\}$. So $\mathfrak{b}(i) = \mathfrak{a}(i)$ for all $i \geq 0$ (check!). We claim that $\mathfrak{a} = \mathfrak{b}$.

By construction, $\mathfrak{b} \subset \mathfrak{a}$. If $\mathfrak{a} \neq \mathfrak{b}$, take $f \in \mathfrak{a} \setminus \mathfrak{b}$ of least degree, and denote $i = \deg f$. Since $\mathfrak{b}(i) = \mathfrak{a}(i)$, there is $g \in \mathfrak{b}$ such that $\deg(f - g) < i$, and thus $f - g \in \mathfrak{b}$ (by the minimality of i, and since $f - g \in \mathfrak{a}$). Thus $f = (f - g) + g \in \mathfrak{b}$, a contradiction. □

Remark 2.15. It is a completely general fact that if a finitely generated ideal I of a ring A is generated by a subset S of A then there is a finite subset S_0 of S that generates I (prove!).

Now, take a field k. Take a subset S of $k[T_1, \dots, T_n]$, generating an ideal I. The set V of simultaneous zeros in k^n of the polynomials in S is equal to the set of simultaneous zeros in k^n of the polynomials in I (check!). But I is finitely generated (by Hilbert's basis theorem), and thus V is also the set of simultaneous zeros of some finite subset S_0 of S. This means that if we start from the empty set, and add to it the elements of S one by one, we will see that the set of simultaneous zeros in k^n shrinks and shrinks, but at a certain finite step it stabilizes (no longer shrinks). In particular, every infinite system of polynomial equations is equivalent to a finite subsystem of polynomial equations.

Exercise 2.16. We have seen that every finitely generated module over a noetherian (resp. artinian) ring is noetherian (resp. artinian). We have also seen that every finitely generated algebra over a noetherian ring is noetherian. But is every finitely generated algebra over an artinian ring artinian?

Remark 2.17 (Groebner bases). **[Non-examinable]** Let k be a field and consider the polynomial algebra $k[T_1, \dots, T_n]$. For two monomials $T_1^{\alpha_1} \cdots T_n^{\alpha_n}$ and $T_1^{\beta_1} \cdots T_n^{\beta_n}$, we say that $T_1^{\alpha_1} \cdots T_n^{\alpha_n} \succ T_1^{\beta_1} \cdots T_n^{\beta_n}$ if $\alpha_1 + \cdots + \alpha_n > \beta_1 + \cdots + \beta_n$ or ($\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ but $(\alpha_1, \dots, \alpha_n)$ is larger than $(\beta_1, \dots, \beta_n)$ lexicographically). Using $\succ$, we can talk about the *leading monomial* of a polynomial $f \in k[T_1, \dots, T_n]$. Now, for an ideal $I = (f_1, \dots, f_\ell)$ of $k[T_1, \dots, T_n]$, one may consider two sets: $A = \mathrm{LM}(I)$, the set of leading monomials elements of I, and B, the set of monomials divisible by the leading monomial of at least one of $f_1, \dots, f_\ell$. Clearly $B \subset A$. If $B = A$, we say that $f_1, \dots, f_\ell$ is a *Groebner basis* of I (a notion invented by Buchberger). It is a theorem that every ideal in $k[T_1, \dots, T_n]$ has a finite Groebner basis, and that every Groebner basis of I generates I. This is a more complicated way to prove Hilbert's basis theorem (for finitely generated algebras over a field), but Groebner bases are useful on their own for making computations. There is an algorithm (Buchberger's algorithm) that takes a generating set for I as input and generates a Groebner basis for I. Example applications: Given ideals $I = (f_1, \dots, f_\ell)$ and $J = (g_1, \dots, g_k)$ of $k[T_1, \dots, T_n]$, can you find a generating set for $I \cap J$? What about determinng if a given $h \in k[T_1, \dots, T_n]$ belongs to I? There are algorithms in terms of Groebner bases to solve these problems (and many other computational problems in commutative algebra, related to dimension, projections, and more). We don't have time for this, but much of the theory is quite elementary.

3. Tensor products

Literature: There two sets of fantastic lecture notes on tensor products on Keith Conrad's website at https://kconrad.math.uconn.edu/blurbs/. They cover more than is covered here. I've drawn inspiration from these notes for some parts of the presentation in this chapter.

3.1. **Tensor products of modules.** Let M and N be R-modules. Informally, the tensor product $M \otimes_R N$ is an R-module consisting of all formal sums $\sum_{i=1}^k m_i \otimes n_i$, $m_i \in M$, $n_i \in N$, with the identifications:

(1) $m \otimes n_1 + m \otimes n_2 = m \otimes (n_1 + n_2)$.
(2) $m_1 \otimes n + m_2 \otimes n = (m_1 + m_2) \otimes n$.

(3) $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$ $(r \in R)$.

First note that $0 \otimes n = 0(1 \otimes n) = 0$, and similarly $m \otimes 0 = 0$ for all $m \in M$ and $n \in N$.

When the ring R is clear from the context, we shall write $M \otimes N$ to mean $M \otimes_R N$.

Example 3.1.

(1) Consider $\mathbb{Z}/2$ and $\mathbb{Z}/3$ as $\mathbb{Z}$-modules. In $\mathbb{Z}/2 \otimes \mathbb{Z}/3$ we have

$$a \otimes b = (3a) \otimes b = a \otimes (3b) = a \otimes \underbrace{0}_{0 \cdot 0} = 0 \cdot (a \otimes 0) = 0 \otimes 0 \ ,$$

so $\mathbb{Z}/2 \otimes \mathbb{Z}/3$ must be the $\mathbb{Z}$-module $\{0 \otimes 0\}$.

(2) Let k be a field, and consider two finite dimensional k-vector spaces V, W. We shall see that $\dim_k V \otimes W = \dim_k(V) \cdot \dim_k(W)$.

Recall that a map $f \colon V \times W \to U$, for R-modules V, W, U, is R-bilinear if $v \mapsto f(v, w_0) \colon V \to U$ and $w \mapsto f(v_0, w)$ are R-linear (i.e., homomorhpisms of R-modules) for all $v_0 \in V$, $w_0 \in W$.

Definition 3.2. Let M, N be R-modules. Write $\mathcal{F}$ for the free R-modules on $M \times N$ (i.e. $\mathcal{F} \cong R^{\oplus(M \times N)}$, with basis $\{e_{m,n} \mid (m,n) \in M \times N\}$). The *tensor product* of M and N is $M \otimes_R N \coloneqq \mathcal{F}/K$, where K is the R-submodule of $\mathcal{F}$ generated by the union of:

(1) $\{e_{m,n_1} + e_{m,n_2} - e_{m,n_1+n_2} \mid m \in M, n_1, n_2 \in N\}$.
(2) $\{e_{m_1,n} + e_{m_2,n} - e_{m_1+m_2,n} \mid m_1, m_2 \in M, n \in N\}$.
(3) $\{re_{m,n} - e_{rm,n} \mid r \in R, m \in M, n \in N\}$.
(4) $\{re_{m,n} - e_{m,rn} \mid r \in R, m \in M, n \in N\}$.

The image of $e_{m,n} \in \mathcal{F}$ in $M \otimes N$ is denoted $m \otimes n$. We have an R-bilinear map $i_{M \otimes N} \colon M \times N \to M \otimes N$ given by $i_{M \otimes N}(m,n) = m \otimes n$.

The elements of $M \otimes N$ are sometimes called *tensors*, and the elements of the form $m \otimes n$, $m \in M$, $n \in N$ are called *pure tensors*. By construction, we see that the pure tensors generate $M \otimes N$. But not every element of $M \otimes N$ is pure (in general).

Note: The pure tensors certainly generate $M \otimes_R N$ as an R-module by construction. So every $x \in M \otimes_R N$ can be written in the form $x = \sum_{i=1}^{\ell} r_i(m_i \otimes n_i) = \sum_{i=1}^{\ell} (r_i m_i) \otimes n_i$ $(r_i \in R, m_i \in M, n_i \in N)$. So the pure tensors generate $M \otimes_R N$ even as a $\mathbb{Z}$-module (i.e. as an abelian group).

Proposition 3.3 (The universal property of a tensor product)**.** *For R-modules M and N, the pair $(M \otimes N, i_{M \otimes N})$ satisfies the following universal property: For every R-module L and R-bilinear map $f \colon M \times N \to L$, there* *is exactly one R-linear map $h\colon M \otimes N \to L$ such that $f = h \circ i_{M\otimes N}$, i.e. the following diagram commutes:*

$$\begin{tikzcd}
M \times N \arrow[r, "i_{M\otimes N}"] \arrow[dr, "f"'] & M \otimes N \arrow[d, dashed, "\exists! h"] \\
 & L
\end{tikzcd}$$

Proof. Write $\{e_{m,n} \mid (m,n) \in M \times N\}$ for the standard basis of $\mathcal{F} = R^{\oplus M\times N}$. Take an R-bilinear $f\colon M \times N \to L$. The condition $f = h \circ i_{M\otimes N}$ is equivalent to $h(m \otimes n) = f(m,n)$ for all $(m,n) \in M \times N$. Thus there is at most one such h since $\{m \otimes n \mid m \in M, n \in N\}$ generates $M \otimes N$. But such h really does exist because, for K as in Definition 3.2, the map $R^{\oplus(M\times N)} \to L$ extending the law $e_{m,n} \mapsto f(m,n)$ vanishes on all of the generators of K since f is R-bilinear, and thus this law vanishes on K, and thus factors through $M \otimes N$ to give $h\colon M \otimes N \to L$ as required. □

I like thinking of the universal property of the tensor product in challenge-solution terminology: You challenge $M \otimes N$ with some R-blinear map $f\colon M \times N \to L$ and you are guaranteed a unique solution $h\colon M \otimes N \to L$ to the equation $f = h \circ i_{M\otimes N}$ (where h is an R-linear map).

Remark 3.4. The universal property of the tensor product of R-modules M, N can also been seen as a bijection between sets for every R-module C:

$$\mathrm{Bilin}_R(M \times N, L) \xrightarrow{\sim} \mathrm{Hom}_R(M \otimes_R N, L) \ .$$

The LHS is the set of R-bilinear maps $M \times N \to L$, the RHS is the set of R-linear maps $M \otimes_R N \to L$, and the bijection takes a bilinear map $f\colon M \times N \to L$ to the unique R-linear map $h\colon M \otimes_R N \to L$ such that $f = h \circ i_{M\otimes N}$, i.e. $f(m,n) = h(m \otimes n)$ for all $(m,n) \in M \times N$.

Proposition 3.5. *For R-modules M, N, if a pair (T, j), T an R-module and $j\colon M \times N \to T$ an R-bilinear map, satisfies the universal property from Proposition 3.3, then there is exactly one R-module isomorphism $\varphi\colon M \otimes N \to T$ such that $\varphi \circ i_{M\otimes N} = j$ (in particular, $M \otimes N \cong T$ as R-modules by the isomorphism sending $m \otimes n \mapsto j(m,n)$).*

Proof. Challenge $M \otimes N$ with the R-bilinear map $j\colon M \times N \to T$ to obtain the solution $\varphi\colon M \otimes N \to T$ such that $j = \varphi \circ i_{M\otimes N}$.

Now challenge T with the R-bilinear map $i_{M\otimes N}\colon M \times N \to M \otimes N$ to obtain the solution $\psi\colon T \to M \otimes N$ such that $i_{M\otimes N} = \psi \circ j$.

Consider the composite map $\psi \circ \varphi$. Then $(\psi \circ \varphi) \circ i_{M\otimes N} = \psi \circ j = i_{M\otimes N}$. In other words, $\psi \circ \varphi\colon M \otimes N \to M \otimes N$ is a solution when challenging $M \otimes N$ with the R-bilinear map $i_{M\otimes N}\colon M \times N \to M \otimes N$.

But the identity map $\mathrm{id}_{M\otimes N}$ is also a solution to the same challenge. So by the uniquness of the solution, $\psi \circ \varphi = \mathrm{id}_{M\otimes N}$.

Similarly, $\varphi \circ \psi = \mathrm{id}_T$. Thus ψ and φ are isomorphisms. The uniqueness of φ (among R-linear maps such that $\varphi \circ i_{M\otimes N} = j$) is clear (why?) □

To prove that an element $\sum_{i=1}^{\ell} m_i \otimes n_i$ of a tensor product $M \otimes N$ is equal to 0 we can try to play with the bilinearity relations (see the example above with $\mathbb{Z}/2 \otimes \mathbb{Z}/3$). The following proposition also shows us how to prove that an element of $M \otimes N$ is not zero by constructing a single incriminating R-bilinear map.

Proposition 3.6. *Let M, N be R-modules. Then $\sum_{i=1}^{\ell} m_i \otimes n_i = 0$ in $M \otimes N$ if and only for every R-module L and R-bilinear map $f\colon M \times N \to L$ we have $\sum_{i=1}^{\ell} f(m_i, n_i) = 0$.*

Proof. Assume that $\sum_{i=1}^{\ell} m_i \otimes n_i = 0$. Let $f\colon M \times N \to L$ be an R-bilinear map, L an R-module. Then $f = h \circ i_{M\otimes N}$ for some R-linear map $h\colon M \otimes N \to L$, and so $\sum_{i=1}^{\ell} f(m_i, n_i) = \sum_{i=1}^{\ell} h(m_i \otimes n_i) = h\Big(\sum_{i=1}^{\ell} m_i \otimes n\Big) = h(0) = 0$.

Now, assume that $\sum_{i=1}^{\ell} m_i \otimes n_i \neq 0$. Then $\sum_{i=1}^{\ell} i_{M\otimes N}(m_i, n_i) = \sum_{i=1}^{\ell} m_i \otimes n_i \neq 0$. □

Example 3.7. For R-modules M and N, $M \otimes N$ is generated (as an R-module) by the pure tensors $\{m \otimes n \mid (m, n) \in M \times N\}$. If M (resp. N) is generated as an R-module by a subset $S \subset M$ (resp. $T \subset N$) then $M \otimes N$ is generated by $\{s \otimes t \mid (s, t) \in S \times T\}$.

Take a field k and $m, n \geq 0$. Write $\{e_1, \dots, e_m\}$ and $\{f_1, \dots, f_n\}$ for the standard bases of k^m and k^n, respectively. By the preceding paragraph, $k^m \otimes k^n$ is spanned (over k) by $\mathcal{B} = \{e_i \otimes f_j\}_{i,j}$. In fact, $\mathcal{B}$ is a basis for $k^m \otimes k^n$ (over k). Indeed, assume that $\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij}(e_i \otimes f_j) = 0$, $\alpha_{ij} \in k$. Consider projection maps $\pi_a\colon k^m \to k$ and $p_b\colon k^n \to k$ from the a-th and b-th coordinates (respectively). Then $T\colon k^m \times k^n \to k$ given by $T(v, w) = \pi_a(v)p_b(w)$ is a k-bilinear map. By Lemma 3.6, $\sum_{i=1}^{m} \sum_{j=1}^{n} T(\alpha_{ij} e_i, f_j) = 0$. But the LHS is equal to $\alpha_{a,b}$, which proves that $\mathcal{B}$ is k-linearly independent. So $k^m \otimes_k k^n \cong k^{mn}$. The same reasoning shows that $R^m \otimes_R R^n \cong R^{mn}$ for any ring. In fact, the same reasoning shows that for all (possibly infinite) sets I, J, the R-module $R^{\oplus I} \otimes_R R^{\oplus J}$ is free with basis $\{e_i \otimes e_j \mid i \in I, j \in J\}$.

Now take $\mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2$ for example. This tensor product contains infinitely many pure tensors (these are all elements of the form $v \otimes w$, $v, w \in \mathbb{R}^2$, by definition). Some sums in $\mathbb{R}^2 \otimes \mathbb{R}^2$ are equal to pure tensors even if they don't seem so at first:

$$3(e_1 \otimes e_1) + 4(e_1 \otimes e_2) + 6(e_2 \otimes e_1) + 8(e_2 \otimes e_2)$$

is in fact pure since it is equal to

$$(e_1 + 2e_2) \otimes (3e_1 + 4e_2)\ .$$

But some (most, in some senses) elements of $\mathbb{R}^2 \otimes \mathbb{R}^2$ are not pure. The basis $\{e_i \otimes e_j\}_{i,j}$ of $\mathbb{R}^2 \otimes \mathbb{R}^2$ will be helpful in order to show that. Every pure tensor is of the form ($\alpha, \beta, \gamma, \delta \in \mathbb{R}$):

$$(\alpha e_1 + \beta e_2) \otimes (\gamma e_1 + \delta e_2)$$

and thus has the special form:

$$(\alpha\gamma)(e_1 \otimes e_1) + (\alpha\delta)(e_1 \otimes e_2) + (\beta\gamma)(e_2 \otimes e_1) + (\beta\delta)(e_2 \otimes e_2)$$

(notice that $(\alpha\gamma, \alpha\delta)$ and $(\beta\gamma, \beta\delta)$ are linearly dependent). So, for example, the following tensor is not pure in $\mathbb{R}^2 \otimes \mathbb{R}^2$:

$$1 \cdot (e_1 \otimes e_1) + 2 \cdot (e_1 \otimes e_2) + 3 \cdot (e_2 \otimes e_1) + 4 \cdot (e_2 \otimes e_2)$$

(you will be asked to think about this more generally and thoroughly in the example sheet).

Example 3.8 (Warning)**.** Consider the $\mathbb{Z}$-modules $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, and the submodule $2\mathbb{Z}$ of $\mathbb{Z}$. In $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, we have $2 \otimes (1 + 2\mathbb{Z}) = 2(1 \otimes (1 + 2\mathbb{Z})) = 1 \otimes (2 + 2\mathbb{Z}) = 0$.

This computation is invalid in $(2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. In fact, in this tensor product, we have $2 \otimes (1 + 2\mathbb{Z}) \neq 0$. To see this, define a $\mathbb{Z}$-bilinear map $b\colon 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by $b(2x, y + 2\mathbb{Z}) = xy + 2\mathbb{Z}$ (check bilinearity!). Then $b(2, 1 + 2\mathbb{Z}) \neq 0$, and so $2 \otimes (1 + 2\mathbb{Z}) \neq 0$.

So, the notation $2 \otimes (1 + 2\mathbb{Z})$ is somewhat misleading. We must remember which tensor product we are working in! And it's wrong to naively view $(2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ as a submodule of $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ (for the same reason).

Remark 3.9. The other direction does work: if M' and N' are submodules of M and N (respectively) and $\sum m_i \otimes n_i = 0$ in $M' \otimes N'$, then $\sum m_i \otimes n_i = 0$ also in $M \otimes N$ (prove!).

Proposition 3.10. *Assume that $\sum_{i=1}^{\ell} m_i \otimes n_i = 0$ in $M \otimes N$. Then there are finitely generated R-modules $M' \subset M$ and $N' \subset N$ such that the same expression $\sum_{i=1}^{\ell} m_i \otimes n_i = 0$ is true in $M' \otimes N'$.*

Proof. In the notation of Definition 3.2, we have $\sum_{i=1}^{\ell} e_{m_i,n_i} \in K$ and thus

$$\sum_{i=1}^{\ell} e_{m_i,n_i} = \sum_{j=1}^{n} k_i \tag{3.1}$$

where $\{e_{m,n}\}_{(m,n)\in M\times N}$ is the standard basis of $\mathcal{F} = R^{\oplus(M\times N)}$, and each k_i is one of the generators of K as listed in Definition 3.2. The expressions for the k_i, as in Definition 3.2, involve finitely many elements $m'_1, \dots, m'_r \in M$ on the left sides of the pure tensors, and finitely many elements $n'_1, \dots, n'_r \in N$ on the right sides. Thus, (3.1) holds when interpreted in $R^{\oplus(M' \times N')}$, and so, construction $M' \otimes_R N'$ as in Definition 3.2 the desired conclusion follows. □

Corollary 3.11. *Let A and B be torsion-free abelian groups*[2]*. Then $A \otimes_{\mathbb{Z}} B$ is a torsion-free abelian group.*

Proof. Assume that 1

$$n \sum_{i=1}^{\ell} a_i \otimes b_i = 0 \tag{3.2}$$

in $A \otimes_{\mathbb{Z}} B$ ($n \in \mathbb{N}$). By Proposition 3.10 there are finitely generated subgroups A' of A and B' of B such that (3.2) holds if interpretted in $A' \otimes B'$. But A' and B' are torsion-free finitely generated abelian groups, and thus $A' \cong \mathbb{Z}^k$ and $B' \cong \mathbb{Z}^\ell$ for some $k, \ell \geq 0$. Thus $A' \otimes_{\mathbb{Z}} B' \cong \mathbb{Z}^{k\ell}$ is torsion free, and so

$$\sum_{i=1}^{\ell} a_i \otimes b_i = 0 \tag{3.3}$$

when interpretted in $A' \otimes_{\mathbb{Z}} B'$. But then (3.3) also holds in $A \otimes B$ (this direction always works, going from being zero in the tensor product of the submodules to that of the modules - think about it!). Thus $A \otimes_{\mathbb{Z}} B$ is torsion free. □

Another thing to note is how the base ring can affect the tensor product. For example, consider the tensors products $\mathbb{C}^2 \otimes_{\mathbb{R}} \mathbb{C}^3$ and $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3$ (where $\mathbb{C}^n$ is viewed as an $\mathbb{R}$-module in the natural way). First, $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3 \cong \mathbb{C}^6$ as we've seen (which is 12-dimensional over $\mathbb{R}$). But $\mathbb{C}^2 \otimes_{\mathbb{R}} \mathbb{C}^3 \cong \mathbb{R}^4 \otimes_{\mathbb{R}} \mathbb{R}^6 \cong \mathbb{R}^{24}$. This makes sense: We expect $\mathbb{C}^2 \otimes_{\mathbb{R}} \mathbb{C}^3$ to be larger than $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3$ because $\mathbb{R}$ is smaller than $\mathbb{C}$, and so we are making fewer identifications in $\mathbb{C}^2 \otimes_{\mathbb{R}} \mathbb{C}^3$, e.g. in $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3$ we have $(2i, 3i) \otimes (4,5,6) = i((2,3) \otimes (4,5,6)) = ((2,3) \otimes i(4,5,6))$, but this is wrong in $\mathbb{C}^2 \otimes_{\mathbb{R}} \mathbb{C}^3$, where we are only allowed to move real scalars around.

Proposition 3.12. *Let M, N, P be R-modules. Then there are natural isomorphisms (stated in parentheses only for pure tensors, but remember that in general not all tensors are pure):*

1. ***Commutativity:*** $M \otimes_R N \to N \otimes_R M$ $(m \otimes n \mapsto n \otimes m)$
2. ***Associativity:*** $(M \otimes_R N) \otimes_R P \to M_R \otimes (N \otimes_R P) \to M \otimes_R N \otimes_R P$ *(where the rightmost term is defined using R-trilinear maps).* $((m \otimes n) \otimes p \mapsto m \otimes (n \otimes p) \mapsto m \otimes n \otimes p)$

[2] Recall that an abelian group A is torsion free if $na \neq 0$ for all $0 \neq n \in \mathbb{Z}$ and $0 \neq a \in A$.

(3) ***Distributivity:*** $(\bigoplus_i M_i) \otimes_R P \to \bigoplus_i (M_i \otimes_R P)$.
$((m_i)_i \otimes p \mapsto (m_i \otimes p)_i)$

(4) ***Identity element:*** $R \otimes_R M \to M$
$(r \otimes m \mapsto rm)$

(5) ***Quotients:*** *For submodules $M' \subset M$, $N' \subset N$, $(M/M') \otimes_R (N/N') \to (M \otimes_R N)/L$, where L is the R-submodule of $M \otimes_R N$ generated by $\{m' \otimes n \mid (m', n) \in M' \times N\} \cup \{m \otimes n' \mid (m, n') \in M \times N'\}$.*
$((m + M') \otimes (n + N') \mapsto m \otimes n + L)$

Proof. This will be in the example sheet. Here we just show the distributivity. One way to proceed would be to show that $\bigoplus_{i \in I}(M_i \otimes P)$ satisfies the universal property of $\left(\bigoplus_{i \in I} M_i\right) \otimes P$, and the use Proposition 3.5. We will proceed in another way.

Define an R-bilinear map $\left(\bigoplus_{i \in I} M_i\right) \times P \to \bigoplus_{i \in I}(M_i \otimes P)$ by letting $\left((m_i)_{i \in I}, p\right) \mapsto (m_i \otimes p)_{i \in I}$. This bilinear map gives rise, by the universal property of $\left(\bigoplus_{i \in I} M_i\right) \otimes P$, to an R-linear map $\varphi\colon \left(\bigoplus_{i \in I} M_i\right) \otimes P \to \bigoplus_{i \in I}(M_i \otimes P)$ given on pure tensors by

$$\varphi\big((m_i)_{i \in I} \otimes p\big) = (m_i \otimes p)_{i \in I} \ .$$

In the other direction, for each i, define a bilinear map $M_i \times P \to \left(\bigoplus_{i \in I} M_i\right) \otimes P$ by letting $(m, p) \mapsto e_i(m) \otimes p$ (here we write $e_i(m) \in \bigoplus_{i \in I} M_i$ for the element with m in the i-th entry and 0 elsewhere). By the universal property of $M_i \otimes P$, this bilinear map gives rise to an R-linear map $\psi_i\colon M_i \otimes P \to \left(\bigoplus_{i \in I} M_i\right) \otimes P$ given on pure tensors by

$$\psi_i(m \otimes p) \mapsto (e_i(m)) \otimes p \ .$$

Now we use the universal property of the direct sum that says that we can gather all of the ψ_i into one homomorphism $\psi\colon \bigoplus_{i \in I}(M_i \otimes P) \to \left(\bigoplus_{i \in I} M_i\right) \otimes P$ satisfṫying

$$\psi\big((m_i \otimes p)_{i \in I}\big) = (m_i)_{i \in I} \otimes p \ .$$

Finally, we have

$$(\psi \circ \varphi)\big((m_i)_{i \in I} \otimes p\big) = \psi\big((m_i \otimes p)_{i \in I}\big) = (m_i)_{i \in I} \otimes p \ .$$

Since the pure tensors $(m_i)_{i \in I} \otimes p$ generate $\left(\bigoplus_{i \in I} M_i\right) \otimes P$ as an R-module, this means that $\psi \circ \varphi = \mathrm{id}_{\left(\bigoplus_{i \in I} M_i\right) \otimes P}$. In the other direction, we have

$$(\varphi \circ \psi)\big((m_i \otimes p)_{i \in I}\big) = \varphi\big((m_i)_{i \in I} \otimes p\big) = (m_i \otimes p)_{i \in I} \ .$$

But elements of the form $(m_i \otimes p)_i$ (i.e. elements of $\bigoplus_{i \in I}(M_i \otimes P)$ which are pure tensors in each coordinate) generate $\bigoplus_{i \in I}(M_i \otimes P)$. Thus φ and ψ are isomorphisms of R-modules. □

Remark 3.13. Note that the distributivity property above implies immediately that for a field k, $k^n \otimes k^m = \left(\bigoplus_{1\leq i\leq n} k\right) \otimes \left(\bigoplus_{1\leq j\leq m} k\right) \cong \bigoplus_{i,j} \left(\underbrace{k \otimes k}_{\cong k}\right) \cong k^{nm}$ as we've seen earlier $k \otimes k \cong k$ follows from the Identity Element property in Proposition 3.12). This shows that $R^n \otimes R^m \cong R^{nm}$ for any ring R (and in fact, so does our previous proof of $k^n \otimes k^m \cong k^{nm}$).

Remark 3.14. From the Quotient property in Proposition 3.12, for ideals I and J of R, we have

$$R/I \otimes_R R/J \cong R/(I+J)$$

via an R-module isomorphism sending $(r_1 + I) \otimes (r_2 + J) \mapsto r_1 r_2 + (I + J)$. The isomorphism in the other direction is given by $r + (I + J) \mapsto (r + I) \otimes (r + J)$. Thus, the kernel of the map $R \to R/I \otimes_R R/J$, $r \mapsto r((1 + I) \otimes (1 + J))$ is $I + J$. Compare this to the kernel of $R \to R/I \times R/J$, which is $I \cap J$. In general there is no description of the product ideal IJ of R in terms of a kernel of a nice map (recall that IJ is the ideal of R generated by the set of all elements of the form xy, $x \in I$, $y \in J$).

3.1.1. *Tensor products of R-linear maps.* The following proposition serves as the definition of the tensor product $f \otimes g$ of R-linear maps f and g.

Proposition 3.15. *For R-linear maps $f\colon M \to M'$ and $g\colon N \to N'$ there is exactly one R-linear map $(f \otimes g)\colon M \otimes N \to M' \otimes N'$ such that*

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n) \qquad \forall (m, n) \in M \times N$$

Proof. If such a homomorphism exists then it is unique because the pure tensors generate $M \otimes N$ as an R-module. To prove the existence, consider the R-bilinear map $b\colon M \times N \to M' \otimes N'$ given by $b(m, n) = f(m) \otimes g(n)$ (check that this is an R-bilinear map!). By the universal property of $M \otimes N$ we obtain an R-linear map $M \otimes N \to M' \otimes N'$ as desired. □

Exercise 3.16. Show that $(f \otimes g) \circ (h \otimes i) = (f \circ h) \otimes (g \circ i)$ for R-linear maps $M_1 \xrightarrow{h} M_2 \xrightarrow{f} M_3$ and $N_1 \xrightarrow{i} N_2 \xrightarrow{g} N_3$ (check by evaluating on pure tensors).

Example 3.17 (Kronecker Product)**.** Let $T\colon k^a \to k^b$ and $S\colon k^c \to k^d$ be k-linear maps (k a field). To simplify the notation, write e_i (resp. f_i) for the vector with 1 on the i-th coordinate and 0 elsewhere in k^a or k^c (resp. k^b or k^d). Write $[T]$ and $[S]$ for the matrices representing T and S w.r.t. these standard bases. Then

$$\begin{aligned}(T\otimes S)(e_i\otimes e_j) &= (Te_i)\otimes(Se_j)\\ &= \left(\sum_{\ell=1}^{b}[T]_{\ell i}f_\ell\right)\otimes\left(\sum_{t=1}^{d}[S]_{tj}f_t\right)\\ &= \sum_{\ell,t}[T]_{\ell i}[S]_{tj}\cdot f_\ell\otimes f_t\end{aligned}$$

Now order the k-basis $\{e_i\otimes e_j\}$ of $k^a\otimes k^c$ as follows: $e_1\otimes e_1,\dots,e_1\otimes e_c,e_2\otimes e_1,\dots,e_2\otimes e_c,\dots e_a\otimes e_c$ and similarly for the basis $\{f_\ell\otimes f_t\}$ of $k^c\otimes k^d$. Representing $T\otimes S$ according to these ordered bases we have a block matrix representation:

$$[T\otimes S]=\begin{pmatrix}[T]_{11}[S] & \cdots & [T]_{1a}[S]\\ \vdots & \ddots & \vdots\\ [T]_{b1}[S] & \cdots & [T]_{ba}[S]\end{pmatrix}\in M_{bd\times ac}(k)\ .$$

The resulting matrix is called the Kronecker product of the matrices $[T]$ and $[S]$.

Proposition 3.18. *Let $f\colon M\to M'$ and $g\colon N\to N'$ be R-linear maps. Then*

(1) If f and g are R-module isomorphisms then so is $f\otimes g$.
(2) If f and g are surjective then so is $f\otimes g$.

Proof. (1) In this case $f^{-1}\otimes g^{-1}$ is a two-sided inverse for $f\otimes g$ and an R-linear map.

(2) The image of $f\otimes g$ is an R-submodule of $M'\otimes_R N'$, and so it suffices to show that this image contains every pure tensor of $M'\otimes_R N'$, but this is clear. □

What about injectivity?

Example 3.19. Consider the function $f\colon\mathbb{Z}\to\mathbb{Z}$ such that $f(x)=px$, and the identity map $\mathrm{id}\colon\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$. Both are injective $\mathbb{Z}$-linear maps. But

$$(f\otimes\mathrm{id})(a\otimes b)=(pa)\otimes b=a\otimes\left(\underbrace{pb}_{=0}\right)=0\ ,$$

that is, $f\otimes\mathrm{id}\colon\underbrace{\mathbb{Z}\otimes_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z})}_{\cong\mathbb{Z}/p\mathbb{Z}}\to\underbrace{\mathbb{Z}\otimes_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z})}_{\cong\mathbb{Z}/p\mathbb{Z}}$ is the zero map, which is not injective.

3.2. **Tensor products of algebras.** Let B, C be algebras over a ring R. Considering B, C as R-modules, we can construct the module $B \otimes C$. We can make the module $B \otimes C$ into a ring by defining $(b \otimes c)(b' \otimes c') = (bb') \otimes (cc')$, and extending R-linearly. Since there can be more than one way to write a tensor as a sum of pure tensors, we must show that this is indeed well defined.

(1) **The multiplication map on $B \otimes_R C$:**
  (a) We have an R-linear isomorphism $f\colon (B \otimes C) \otimes (B \otimes C) \to (B \otimes B) \otimes (C \otimes C)$ given by $(b_1 \otimes c_1) \otimes (b_2 \otimes c_2) \mapsto (b_1 \otimes b_2) \otimes (c_1 \otimes c_2)$.
  (b) We also have the multiplication maps $B \times B \to B$ and $C \times C \to C$, sending $(b_1, b_2) \mapsto b_1 b_2$ and $(c_1, c_2) \mapsto c_1 c_2$.
  (c) Both are R-bilinear, and so give rise to R-linear maps $m_B\colon B \otimes B \to B$ and $m_C\colon C \otimes C \to C$, given on pure tensors by $m_B(b_1 \otimes b_2) = b_1 b_2$ and $m_C(c_1 \otimes c_2) = c_1 c_2$.
  (d) So, we have an R-bilinear map $(B \otimes B) \times (C \otimes C) \to B \otimes C$ satisfying $(b_1 \otimes b_2, c_1 \otimes c_2) \mapsto b_1 b_2 \otimes c_1 c_2$.
  (e) This gives rise to an R-linear map $g\colon (B \otimes B) \otimes (C \otimes C) \to B \otimes C$ satisfying $(b_1 \otimes b_2) \otimes (c_1 \otimes c_2) \mapsto b_1 b_2 \otimes c_1 c_2$.
  (f) The composite map $g \circ f\colon (B \otimes C) \otimes (B \otimes C) \to B \otimes C$ is R-linear and satisfies $(b_1 \otimes c_1) \otimes (b_2 \otimes c_2) \mapsto b_1 b_2 \otimes c_1 c_2$.
  (g) This gives rise to an R-bilinear map $m\colon (B \otimes C) \times (B \otimes C) \to B \otimes C$ satifying $(b_1 \otimes c_1, b_2 \otimes c_2) \mapsto b_1 b_2 \otimes c_1 c_2$.
  (h) This m is our multiplication map.
  (i) This multiplication is distributive since m is bilinear. Verifying the rest of the ring axioms is left to the reader.

(2) **Making $B \otimes_R C$ into an R-algebra:**
  (a) $B \otimes C$ is a B-algebra via the ring homomorphism $b \mapsto b \otimes 1\colon B \to B \otimes C$.
  (b) $B \otimes C$ is a C-algebra via the ring homomorphism $c \mapsto 1 \otimes c\colon B \to B \otimes C$.
  (c) Since B and C are R-algebras, we have their structure ring homomorphisms $R \to B$ and $R \to C$.
  (d) Overall, we obtain to ring homomorphisms $R \to B \otimes C$: $r \mapsto r \otimes 1$ and $r \mapsto 1 \otimes r$.
  (e) They are identical: $r \otimes 1 = r(1 \otimes 1) = 1 \otimes r$.
  (f) So, $B \otimes C$ is an R-algebra via the ring homomorphism $R \to B \otimes C$ sending $r \mapsto r(1 \otimes 1)$. Note that in general $r(1 \otimes 1)$ is equal to both $r \otimes 1$ and $1 \otimes r$, but not to $r \otimes r$.

Warning: There seems to a mistake in Atiyah–Macdonald regarding how to make the ring $B \otimes_R C$ into an R-algebra.

Lemma 3.20 (Upgrading an R-linear map to a R-algebra homomorphism)**.** *Let $f\colon A \to B$ be an R-linear map between R-algebras, R a ring. Let $S \subset A$ be a set generating A as an R-module. Assume that $f(1_A) = 1_B$ and $f(a_1a_2) = f(a_1)f(a_2)$ for all $a_1, a_2 \in S$. Then f is an R-algebra homomorphism.*

Proof. The map f is additive and $f(1_A) = 1_B$. Also, $f(r \cdot 1_A) = r \cdot f(1_A) = r \cdot 1_B$ since f is R-linear. It remains to show that f is multiplicative:

$$\begin{aligned} f\left(\left[\sum_{i=1}^{n} r_i a_i\right] \cdot \left[\sum_{j=1}^{n} r'_j a'_j\right]\right) &= \sum_{i,j} r_i r'_j f\big(a_i a'_j\big) \\ &= \sum_{i,j} r_i r'_j f(a_i) f\big(a'_j\big) \\ &= \left[\sum_{i} r_i f(a_i)\right]\left[\sum_{j} r'_j f\big(a'_j\big)\right] \\ &= f\left(\sum_i r_i a_i\right) f\left(\sum_j r'_j a'_j\right) \end{aligned}$$

for $n \geq 0$, $r_i, r'_i \in R$, $a_i, a'_j \in S$. □

Now, if A and B are R-algebras, generated as R-modules by S_A and S_B respectively, then $A \otimes_R B$ is generated as an R-module by $\{a \otimes b \mid a \in S_A, b \in S_B\}$ (this is just a subset of the set of pure tensors, but it already generates). Thus:

Corollary 3.21. *Let A, B and C be R-algebras (R a ring). Let S_A and S_B be generating sets for A and B, respectively, as R-modules. Let $f\colon A \otimes_R B \to C$ be an R-linear map such that $f(a_1a_2 \otimes b_1b_2) = f(a_1 \otimes b_1)f(a_2 \otimes b_2)$ for all $a_1, a_2 \in S_A$ and $b_1, b_2 \in S_B$, and $f(1_A \otimes 1_B) = 1_C$. Then f is a homomorphism of R-algebras.*

Example 3.22. Consider the R-algebras $R[X_1, \dots, X_n]$ and $R[T_1, \dots, T_r]$ (polynomial algebras over R). We wish to find an R-algebra isomorphism

$$\varphi\colon R[X_1, \dots, X_n] \otimes_R R[T_1, \dots, T_r] \xrightarrow{\sim} R[X_1, \dots, X_n, T_1, \dots, T_r] \ .$$

As R-modules, both sides are free with a R-free basis of cardinality $\aleph_0$. So they are isomorphic in many ways as R-modules, but we wish to have an R-algebra isomorphism. We know that the LHS has the following free basis over R: the set of all pure tensors $a \otimes b$ where $a \in R[X_1, \dots, X_n]$ and

$b \in R[T_1, \dots, T_r]$ are monomials[3]. So we have an R-module isomorphism φ given on this basis by $\varphi(a \otimes b) = ab$ (check that it sends an R-basis to an R-basis). We have $\varphi(1 \otimes 1) = 1$. For monomials $a_1, a_2 \in R[X_1, \dots, X_n]$ and $b_1, b_2 \in R[T_1, \dots, T_r]$, we have $\varphi(a_1 a_2 \otimes b_1 b_2) = a_1 a_2 b_1 b_2 = a_1 b_1 a_2 b_2 = \varphi(a_1 \otimes b_1)\varphi(a_2 \otimes b_2)$. So φ is an R-algebra isomorphism by the corollary (see also Example 3.26 below, where this is done in a different way).

Now, let's take ideals I and J of $R[X_1, \dots, X_n]$ and $R[T_1, \dots, T_r]$, respectively. Using the Quotients part of Proposition 3.12, we have an R-linear isomorphism

$$R[X_1, \dots, X_n]/I \otimes_R R[T_1, \dots, T_r]/J \overset{\sim}{\to} (R[X_1, \dots, X_n] \otimes_R R[T_1, \dots, T_r])/L \ ,$$

where L is the submodule generated by

$$\{p \otimes q \mid p \in I, q \in R[T_1, \dots, T_r]\} \cup \{g \otimes h \mid g \in R[X_1, \dots, X_n], h \in J\} \ .$$

Under the isomorphism φ from the previous paragraph, L is mapped onto the ideal $I^e + J^e$ of $R[X_1, \dots, X_n, T_1, \dots, T_r]$ (where I^e is the extension of I to $R[X_1, \dots, X_n, T_1, \dots, T_r]$, i.e. the ideal of $R[X_1, \dots, X_n, T_1, \dots, T_r]$ generated by I). Thus,

$$R[X_1, \dots, X_n]/I \otimes_R R[T_1, \dots, T_r]/J \cong R[X_1, \dots, X_n, T_1, \dots, T_r]/(I^e + J^e) \ .$$

.

For example,

$$\mathbb{C}[X, Y, Z]/(f, g) \otimes \mathbb{C}[W, U]/(h) \cong \mathbb{C}[X, Y, Z, W, U]/(f, g, h)$$

as $\mathbb{C}$-algebras, by an isomorphism sending a pure tensor $(p + (f, g)) \otimes (q + (h))$ to $pq + (f, g, h)$.

Remark 3.23. **[non-examinable]** In algebraic geometry, the calculation above shows that the product variety $\underbrace{V(f,g)}_{\subset \mathbb{A}^3_{\mathbb{C}}} \times \underbrace{V(h)}_{\subset \mathbb{A}^2_{\mathbb{C}}}$ (over $\operatorname{Spec} \mathbb{C}$) is isomorphic to $\underbrace{V(f,g,h)}_{\subset \mathbb{A}^5_{\mathbb{C}}}$. The tensor product of algebras helps us understand what topology (and further structure) to put on a product of varieties (or schemes).

As we've seen before, for R-algebras A and B, we have ring homomorphisms $i_A \colon A \to A \otimes_R B$ and $i_B \colon B \to A \otimes_R B$ given by $i_A(a) = a \otimes 1$ and $i_B(b) = 1 \otimes b$. Now:

Proposition 3.24 (The universal property of the tensor product of algebras)**.** *Let A, B be R-algebras. Then:*

[3] In these notes, a *monomial* is a product of powers of the variables, without a scalar coefficient. To refer to a product of a scalar and a monomial we shall use the term *term*.

(1) *For every R-algebra C and R-algebra homomorphisms $f_1\colon A \to C$ and $f_2\colon B \to C$ there is exactly one R-algebra homomorphism $h\colon A \otimes_R B \to C$ such that $f_1 = h \circ i_A$ and $f_2 = h \circ i_B$.*

(2) *For every triplet (Q, j_A, j_B) of R-algebra Q and R-algebra homomorphisms $j_A\colon A \to Q$ and $j_B\colon B \to Q$ that satisfies the universal property of $(A \otimes_R B, i_A, i_B)$ as in (1), there is exactly one R-algebra homomorphism $\varphi\colon A \otimes_R B \to Q$ such that $j_A = \varphi \circ i_A$ and $j_B = \varphi \circ i_B$.*

Proof. (1) Take C, f_1 and f_2 as in the statement. The uniqueness of h as in the statement follows from the fact that $A \otimes_R B$ is generated as an R-algebra by $\{a \otimes 1 \mid a \in A\} \cup \{1 \otimes b \mid b \in B\}$. Regarding the existence of h: Define an R-bilinear map $A \times B \to C$ sending $(a, b) \mapsto f_1(a)f_2(b)$. By the universal property of $A \otimes_R B$ as an R-module there is an R-linear map $h\colon A \otimes_R B \to C$ such that $h(a \otimes b) = f_1(a)f_2(b)$. Clearly $f_1 = h \circ i_A$ and $f_2 = h \circ i_B$. It remains to show that h is an R-algebra homomorphism. First, $h\left(\underbrace{1_{A\otimes_R B}}_{=1_A \otimes 1_B}\right) = 1_C$. Second, for $a_1, a_2 \in A$ and $b_1, b_2 \in B$, we have

$$\begin{aligned} h(a_1a_2 \otimes b_1b_2) &= f_1(a_1a_2)f_2(b_1b_2) \\ &= [f_1(a_1)f_2(b_1)] \cdot [f_1(a_2)f_2(b_2)] \\ &= h(a_1 \otimes b_1)h(a_2 \otimes b_2) \end{aligned}$$

and thus h is an R-algebra homomorphism by Corollary 3.21, applied with $S_A = A$ and $S_B = B$ (we're taking the entire modules as the generating sets).

(2) Left to the reader. □

Remark 3.25. **[non-examinable]** In category-theoretic terms, Proposition 3.24 says that the category of R-algebras has coproducts, and that they are given by tensor products. Being a coproduct just means satisfying the universal property as in Proposition 3.24. Some coproducts in other categories: In the category of sets the coproduct is the disjoint union, in groups it is the free product, in R-modules it is the direct sum.

Example 3.26. We reanalyze Example 3.22. We can show that there is an R-algebra isomorphism

$$\varphi\colon R[X_1, \dots, X_n] \otimes_R R[T_1, \dots, T_r] \xrightarrow{\sim} R[X_1, \dots, X_n, T_1, \dots, T_r]$$

by showing that the RHS is the coproduct of $R[X_1, \dots, X_n]$ and $R[T_1, \dots, T_r]$ (and then invoking Proposition 3.24(2)). First we define R-algebra homomorphisms

$$j_A\colon R[X_1, \dots, X_n] \to R[X_1, \dots, X_n, T_1, \dots, T_r]$$

and

$$j_B\colon R[T_1,\dots,T_r]\to R[X_1,\dots,X_n,T_1,\dots,T_r]$$

in the natural ways. Now take R-algebra homomorphisms $f_1\colon R[X_1,\dots,X_n]\to C$ and $f_2\colon R[T_1,\dots,T_r]\to C$ for some R-algebra C. For an R-algebra homomorphism

$$h\colon R[X_1,\dots,X_n,T_1,\dots,T_r]\to C\ ,$$

satisfying $f_1=h\circ j_A$ and $f_2=h\circ j_B$ is equivalent to satisfying $h(X_i)=f_1(X_i)$ and $h(T_j)=f_2(T_j)$. There is exactly one such h by the universal property of the polynomial algebra $R[X_1,\dots,X_n,T_1,\dots,T_r]$. This shows that φ as desired exists by Proposition 3.24(2), and also that $\varphi(p\otimes q)=pq$ (notice how this proposition not only tells us that there is an isomorphism, but also gives us the formula for it on pure tensors). The isomorphism

$$R[X_1,\dots,X_n]/I\otimes_R R[T_1,\dots,T_r]/J\xrightarrow{\sim}R[X_1,\dots,X_n,T_1,\dots,T_r]/(I^e+J^e)$$

can be constructed in a similar way.

Some further properties (easy to prove):

(1) If $f\colon A\to A'$ and $g\colon B\to B'$ are R-algebra homomorphisms then so is $f\otimes g\colon A\otimes B\to A'\otimes A$ (we saw that it is an R-linear map).
(2) Many of our R-linear maps are R-algebra homomorphisms (By Corollary 3.21, it suffices to check that $1\mapsto 1$ and to check multiplicativity on a set of R-module generators):
  (a) $R/I\otimes_R R/J\cong R/(I+J)$.
  (b) $A\otimes_R B\cong B\otimes_R A$.
  (c) $A\otimes_R(B\times C)\cong(A\otimes_R B)\times(A\otimes_R C)$.
  (and thus also $A\otimes_R B^n\cong(A\otimes_R B)^n$.
  (d) $(A\otimes_R B)\otimes_R C\cong A\otimes_R(B\otimes_R C)$.

3.3. **Restriction and extension of scalars.**

3.3.1. *Modules: Restriction and extension of scalars.* Let $f\colon R\to S$ be a ring homomorphism, and let M be an S-module. Then M is an R-module via the action $rm:=f(r)m$ for all $r\in R$, $m\in M$ (in other words, if $\rho\colon S\to\operatorname{End}M$ is the structural homomorphism of M as an S-module, we let $\rho\circ f\colon R\to\operatorname{End}M$ be the structural homomorphism of M as an R-module). Making an S-module into an R-module is this way is called *restriction of scalars*. Example: For the usual embedding $f\colon\mathbb{R}\to\mathbb{C}$ and the $\mathbb{C}$-module $\mathbb{C}^n$, we obtain the $\mathbb{R}$-module $\mathbb{R}^{2n}$ by restriction of scalars.

In the other direction, we have *extension of scalars*: Keep the ring homomorphism $f\colon R\to S$. Take an S-module M and an R-module N. Then M is also an R-module (by restriction of scalars via f), and so we may form the tensor product $M\otimes_R N$. We shall now give $M\otimes_R N$ the structure of an

S-module. In many situations one takes $M = S$ and considers $S \otimes_R N$, but we shall require the more general setting.

The S-module structure on $M \otimes_R N$ is given on pure tensors by

$$s(m \otimes n) = (sm) \otimes n \qquad \forall s \in S \quad m \in M \quad n \in N \ .$$

We need to check that this is indeed well defined and makes $M \otimes_R N$ into an S-module:

(1) Fix $s \in S$. We have an R-bilinear map $M \times N \to M \otimes_R N$ given by $(m, n) \mapsto (sm) \otimes n$. By the universal property of $M \otimes_R N$, this bilinear map gives rise to an R-linear map $h_s \colon M \otimes_R N \to M \otimes_R N$ satisfying $h_s(m \otimes n) = (sm) \otimes n$ for all $s \in S$, $m \in M$, $n \in N$.

(2) Define a function $\varphi \colon S \to \operatorname{End}(M \otimes_R N)$ by setting $\varphi(s) = h_s$. Here, as usual, $\operatorname{End}(M \otimes_R N)$ stands for the ring of endomorphisms of $M \otimes_R N$ as an abelian group (h_s is an R-module endomorphism, so certainly also a $\mathbb{Z}$-module endomorphism). It remains to show that φ is a ring homomorphism, but this is clear (check!).

Example 3.27.

(1) We already know the R-module isomorphism $S \otimes_R R \xrightarrow{\sim} S$ given by $s \otimes r \mapsto sr$. It is in fact an S-module isomorphism since $s'(s \otimes r) = (s's) \otimes r \mapsto (s's)r = s'(sr)$. In particular $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R} \xrightarrow{\sim} \mathbb{C}$ as $\mathbb{C}$-modules.

(2) For an S-module M and R-modules N_i, $i \in I$, we know an R-module isomorphism $M \otimes_R \bigoplus_{i \in I} N_i \mapsto \bigoplus_{i \in I}(M \otimes_R N_i)$. Again it can be easily verified that this is an S-module isomorphism. In particular, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \xrightarrow{\sim} \mathbb{C}^n$ as $\mathbb{C}$-modules.

(3) **Restrict and then extend:** Take the $\mathbb{C}$-module $\mathbb{C}^n$. Restrict scalars to $\mathbb{R}$ and obtain $\mathbb{R}^{2n}$. Extend scalars to $\mathbb{C}$ and obtain $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^{2n} \cong \mathbb{C}^{2n}$.

(4) **Extend and then restrict:** Take the $\mathbb{R}$-module $\mathbb{R}^n$. Extend scalars to $\mathbb{C}$ and obtain $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$. Restrict scalars to $\mathbb{R}$ and obtain $\mathbb{R}^{2n}$.

(5) Take the $\mathbb{Z}$-module $\mathbb{Z}^n$. Extend scalar to $\mathbb{Z}/n\mathbb{Z}$ and obtain $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong (\mathbb{Z}/n\mathbb{Z})^n$ (this is a perfectly valid extension of scalars, even if it's not what the common people associate with the word extension).

The extensions in the example above are all of the form $S \otimes_R N$ for some R-module N (and an ambient ring homomorphism $f \colon R \to S$), where we sought to understand the S-module structure of $S \otimes_R N$. Here's an example of the form $M \otimes_R N$ where M is an S-module different from S: What is the $\mathbb{C}$-module structure on $\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell$ (i.e. is there a nicer expression for this?). First, we have an $\mathbb{R}$-module isomorphism

$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong \mathbb{R}^{2n} \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong \mathbb{C}^{n\ell}$$

where the second isomorphism follows from the equality of dimensions over $\mathbb{R}$. Now, surely we can guess how to choose the isomorphism such that $\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong \mathbb{C}^{n\ell}$ becomes a $\mathbb{C}$-module isomorphism (and then verify that it is indeed one). But, instead, we shall use the following proposition. It says, in particular, that if we're going to tensor $\mathbb{R}^\ell$ with the $\mathbb{C}$-module $\mathbb{C}^n$ (necessarily tensoring over $\mathbb{R}$) to obtain a $\mathbb{C}$-module (via the extension of scalars construction), we can first prepare $\mathbb{R}^\ell$ by extending scalars to $\mathbb{C}$ (obtaining $\mathbb{C} \otimes \mathbb{R}^\ell \cong \mathbb{C}^\ell$), and then tensor the resulting $\mathbb{C}$-module with $\mathbb{C}^n$ (tensoring over $\mathbb{C}$!). That is:

$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong \mathbb{C}^n \otimes_{\mathbb{C}} \left(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell\right) \cong \mathbb{C}^n \otimes_{\mathbb{C}} \mathbb{C}^\ell \cong \mathbb{C}^{nl}$$

(and this is a $\mathbb{C}$-module isomorphism by the following proposition). More generally, the proposition breaks a "complicated" extension of scalars $M \otimes_R N$ (M an S-module, N an R-module) into two steps: a simpler extension of scalars, $S \otimes_R N$, followed by an ordinary tensor product of S-modules.

Proposition 3.28. *Let M be an S-module, N an R-module. Then*

$$M \otimes_R N \cong M \otimes_S (S \otimes_R N)$$

as S-modules, where the isomorphism sends $m \otimes n \mapsto m \otimes (1 \otimes n)$ (and in the other direction $(sm) \otimes n \leftarrow\!\shortmid m \otimes (s \otimes n)$).

Proof. **One of the questions in the example sheet is to prove this statement (or just read the proof below).**

We will construct S-linear maps in both directions and verify that they are inverses. Define an R-bilinear map $M \times N \to M \otimes_S (S \otimes_R N)$ sending $(m, n) \mapsto m \otimes (1 \otimes n)$. By the universal property of $M \otimes_R N$, there is an R-linear map $\varphi \colon M \otimes_R N \to M \otimes_S (S \otimes_R N)$ such that $\varphi(m \otimes n) = m \otimes (1 \otimes n)$. In fact, φ is also an S-linear map:

$$\varphi\left(\underbrace{s(m \otimes n)}_{=(sm)\otimes n}\right) = (sm) \otimes (1 \otimes n) = s \underbrace{(m \otimes (1 \otimes n))}_{=\varphi(m \otimes n)}$$

(it suffices to check this on pure tensors).

Now we define an S-linear map in the other direction in several steps. Fix $m \in M$. Define an R-bilinear map $S \times N \to M \otimes_R N$ sending $(s, n) \mapsto (sm) \otimes n$. By the universal property of $S \otimes_R N$ there is an R-linear map $H_m \colon S \otimes_R N \to M \otimes_R N$ such that $H_m(s \otimes n) = (sm) \otimes n$. Unfix $m \in M$. Define an S-bilinear map $M \times (S \otimes_R N) \to M \otimes_R N$ sending $(m, x) \mapsto H_m(x)$ (verify S-bilinearity carefully!). By the universal property of $M \otimes_S (S \otimes_R N)$, there is an S-linear map $\psi \colon M \otimes_S (S \otimes_R N) \to M \otimes_R N$ such that $\psi(m \otimes (s \otimes n)) = H_m(s \otimes n) = (sm) \otimes n$.

Take a pure tensor $m \otimes n \in M \otimes_R N$. Then

$$\begin{aligned}(\psi \circ \varphi)(m \otimes n) &= \psi(m \otimes (1 \otimes n)) \\ &= H_m(1 \otimes n) \\ &= m \otimes n\end{aligned}$$

and thus $\psi \circ \varphi = \mathrm{id}_{M \otimes_R N}$ (it suffices to check on the pure tensors since they generate $M \otimes_R N$ as an R-module, a fortiori as an S-module).

Take a pure tensor $m \otimes \left(\underbrace{\sum_{i=1}^{\ell} s_i \otimes n_i}_{=:x} \right) \in M \otimes_S (S \otimes_R N)$. Then

$$\begin{aligned}(\varphi \circ \psi)(m \otimes x) &= \varphi(H_m(x)) \\ &= \varphi\left(\sum_{i=1}^{\ell} s_i m \otimes n_i\right) \\ &= \sum_{i=1}^{\ell} \underbrace{(s_i m) \otimes (1 \otimes n_i)}_{=m \otimes (s_i \otimes n_i)} \\ &= m \otimes \underbrace{\sum_{i=1}^{\ell} s_i \otimes n_i}_{=x} \ .\end{aligned}$$

Thus $\varphi \circ \psi = \mathrm{id}_{M \otimes_S (S \otimes_R N)}$ and so φ and ψ are S-module isomorphisms. □

The following theorem is an analogue of Theorem 3.12 in the extension of scalars setting.

Theorem 3.29. *Take S-modules M, M' and R-modules N, N' (and some fixed ring homomorphism $R \to S$). Then there are S-module isomorphisms (all sending pure tensors to their obvious images):*

(1) $M \otimes_R N \xrightarrow{\sim} N \otimes_R M$.
(2) $(M \otimes_R N) \otimes_R N' \xrightarrow{\sim} M \otimes_R (N \otimes_R N')$.
(notices that the LHS involves two extension of scalars, while the RHS involves one)
(3) $(M \otimes_R N) \otimes_S M' \xrightarrow{\sim} M \otimes_S (N \otimes_R M')$.
(4) $M \otimes_R \left(\bigoplus_{i \in I} N_i\right) \cong \bigoplus_{i \in I}(M \otimes_R N_i)$
(where N_i is an R-module).

Proof. I suggest you plug in $R = \mathbb{R}$, $S = \mathbb{C}$, $M = \mathbb{C}^n$, $M' = \mathbb{C}^{n'}$, $N = \mathbb{R}^{\ell}$ and $N' = \mathbb{R}^{\ell'}$ just to get a feeling for what each statement means.

You can certainly prove this statement by yourself at this point. I will skip most of the proof. Let's just do (3) using the associativity of $\otimes_S$ (when not mixed with $\otimes_R$) and using Proposition 3.28:

$$\begin{aligned}(M \otimes_R N) \otimes_S M' &\cong (M \otimes_S (N \otimes_R S)) \otimes_S M' \\ &\cong M \otimes_S \left((N \otimes_R S) \otimes_S M'\right) \\ &\cong M \otimes_S \left(N \otimes_R M'\right)\end{aligned}$$

□

The following corollary shows what happens when you take a tensor product of R-modules and apply $S\otimes_R$ to it (e.g. what is $\mathbb{C} \otimes_{\mathbb{R}} \left(\mathbb{R}^\ell \otimes_{\mathbb{R}} \mathbb{R}^k\right)$ as a $\mathbb{C}$-module? Although this example is easy actually).

Corollary 3.30. *Let N, N' be R-modules (as usual, there's some fixed ring homomorphism $R \to S$). Then there is an S-module isomorphism*

$$S \otimes_R \left(N \otimes_R N'\right) \cong (S \otimes_R N) \otimes_S \left(S \otimes N'\right)$$

sending $s \otimes (n \otimes n') \mapsto s((1 \otimes n) \otimes (1 \otimes n'))$.

Proof. By Theorem 3.29(2) and Proposition 3.28, we have S-module isomorphisms

$$\begin{aligned}S \otimes_R \left(N \otimes_R N'\right) &\cong (S \otimes_R N) \otimes_R N' \\ &\cong (S \otimes_R N) \otimes_S (S \otimes_R N)\end{aligned}$$

with the isomorphisms sending pure tensors in a way that matches the statement. □

For example (of Corollary 3.30), as $\mathbb{C}$-modules:

$$\begin{aligned}\mathbb{C} \otimes_{\mathbb{R}} \left(\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell\right) &\cong (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n) \otimes_{\mathbb{C}} \left(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell\right) \\ &\cong \mathbb{C}^n \otimes_{\mathbb{C}} \mathbb{C}^\ell \\ &\cong \mathbb{C}^{n\ell}\end{aligned}$$

We already knew that because, as $\mathbb{C}$-modules

$$\mathbb{C} \otimes_{\mathbb{R}} \left(\underbrace{\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell}_{\cong \mathbb{R}^{n\ell}}\right) \cong \mathbb{C}^{n\ell}$$

but now we have a new way to think about this. Note that in Corollary 3.30 we are discussing a simple extension of scalars, i.e. $S\otimes_R$. The corollary is not true for $M\otimes_R$ for a general S-module M: Indeed (verify using what we've learned), $\mathbb{C}^n \otimes_{\mathbb{R}} \left(\mathbb{R}^m \otimes_{\mathbb{R}} \mathbb{R}^\ell\right) \cong \mathbb{C}^{nm\ell}$ as $\mathbb{C}$-modules, while $(\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^m) \otimes_{\mathbb{C}} \left(\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell\right) \cong \mathbb{C}^{n^2 m\ell}$ as $\mathbb{C}$-modules, a contradiction if $n \geq 2$.

Applying Corollary 3.30 repeatedly one can also see that $S \otimes_R (N_1 \otimes_R \cdots \otimes_R N_\ell) = (S \otimes_R N_1) \otimes_S \cdots \otimes_S (S \otimes_R N_\ell)$.

Remark 3.31. An imporant feature of extension of scalars is that it acts on morphisms and not only on modules. If $f\colon N \to N'$ is an R-linear map and M is an S-module (as usual, some ring homomorphism $R \to S$ lives in the background), then $\mathrm{id}_M \otimes f\colon M \otimes_R N \to M \otimes_R N'$, which we already know is an R-linear map, is an S-linear map. Indeed,

$$(\mathrm{id}_M \otimes f)\left(\underbrace{s(m \otimes n)}_{=(sm)\otimes n}\right) = \underbrace{(sm) \otimes f(n)}_{s(m \otimes f(n))} = s(\mathrm{id}_M \otimes f)(m \otimes n)\ .$$

As an example, take a linear map $T\colon \mathbb{R}^n \to \mathbb{R}^m$ and tensor it with the identity map $\mathrm{id}_\mathbb{C}\colon \mathbb{C} \to \mathbb{C}$. If $e_1, \ldots, e_n$ and $f_1, \ldots, f_m$ are $\mathbb{R}$-bases of $\mathbb{R}^n$ and $\mathbb{R}^m$, respectively, then $1 \otimes e_1, \ldots, 1 \otimes e_n$ and $1 \otimes f_1, \ldots, 1 \otimes f_m$ are $\mathbb{C}$-bases of $\underbrace{\mathbb{C} \otimes_\mathbb{R} \mathbb{R}^n}_{\cong \mathbb{C}^n}$ and $\underbrace{\mathbb{C} \otimes_\mathbb{R} \mathbb{R}^m}_{\cong \mathbb{C}^m}$, respectively. Now, write $[T]$ for T represented according to these $\mathbb{R}$-bases. Then

$$\begin{aligned}(\mathrm{id}_\mathbb{C} \otimes T)(1 \otimes e_i) &= 1 \otimes Te_i \\ &= 1 \otimes \sum_{\ell=1}^m [T]_{\ell i} f_j \\ &= \sum_{\ell=1}^m [T]_{\ell i}(1 \otimes f_j)\ ,\end{aligned}$$

and so the matrix representing T according to the $\mathbb{C}$-bases above is exactly $[T]$ (interpreted as a matrix with complex entries that all happen to be real).

3.3.2. *Algebras: Restriction and extension of scalars.* Given two R-algebras A and B, we constructed a new R-algebra $A \otimes_R B$ with the structure map $R \to A \otimes B$ given by $r \mapsto \rho(r) \otimes 1$ (where $\rho\colon R \to A$ is the structure ring homomorphism of A as an R-algebra). But $A \otimes_R B$ is also an A-algebra via $a \mapsto a \otimes 1$, and a B-algebra via $b \mapsto 1 \otimes b$. So the R-algebra structure on $A \otimes_R B$ is given by taking either the A- or B- algebra structure on $A \otimes_R B$ and restricting scalars to R (the result will be the same).

Example 3.32. We construct a $\mathbb{C}$-algebra homomorphism

$$\varphi\colon \mathbb{C} \otimes_\mathbb{R} (\mathbb{R}[T_1, \ldots, T_n]) \xrightarrow{\sim} \mathbb{C}[T_1, \ldots, T_n]$$

The $\mathbb{R}$-bilinear map $\mathbb{C} \times \mathbb{R}[T_1, \ldots, T_n] \to \mathbb{C}[T_1, \ldots, T_n]$ given by $(z, p) \mapsto zp$ gives rise to an $\mathbb{R}$-linear map $\varphi\colon \mathbb{C} \otimes_\mathbb{R} \mathbb{R}[T_1, \ldots, T_n] \to \mathbb{C}[T_1, \ldots, T_n]$. In fact, φ is $\mathbb{C}$-linear (check!). Next, we show that φ is a $\mathbb{C}$-module isomorphism. Indeed, by Theorem 3.29(4), $\mathbb{C} \otimes_\mathbb{R} (\mathbb{R}[T_1, \ldots, T_n])$ is a free $\mathbb{C}$-module with basis $\{1 \otimes m \mid m \text{ is a monomial in } T_1, \dots, T_n\}$. On the other hand, $\mathbb{C}[T_1, \dots, T_n]$ is a free $\mathbb{C}$-module with a basis consisting the set of monomials in $T_1, \dots, T_n$. So φ is a $\mathbb{C}$-module isomorphism because it sends a basis bijectively onto a basis. It is left to check that φ is a $\mathbb{C}$-algebra homomorphism (and thus an isomorphism, because we already know that φ is bijective). This is easy to verify using Corollary 3.21. We can write φ^{-1} explicitly: $\varphi^{-1}\Big(\sum_{e=(e_1,\dots,e_n)\in\mathbb{Z}^n_{\geq 0}} z_e T_1^{e_1} \cdots T_n^{e_n}\Big) = \sum_{e=(e_1,\dots,e_n)\in\mathbb{Z}^n_{\geq 0}} z_e \otimes T_1^{e_1} \cdots T_n^{e_n}$, where $z_e \in \mathbb{C}$ (the sum is finite, i.e. almost all z_e are zero, because elements of $\mathbb{C}[T_1, \dots, T_n]$ are polynomials). In the same way, we have an S-algebra isomorphism $S \otimes_R R[T_1, \dots, T_n] \xrightarrow{\sim} S[T_1, \dots, T_n]$ w.r.t. any ring homomorphism $f \colon R \to S$. The isomorphism sends $s \otimes p \mapsto s\tilde{f}(p)$, where $\tilde{f}(p)$ results from p by applying f to each coefficient.

Some additional features (again, it suffices to check multiplicativity on pure tensors):

(1) Proposition 3.28 has an analogue for algebras: For an R-algebra A and an S-algebra B, we have an S-algebra structure on $A \otimes_R B$ (via B, as we've seen), and an S-algebra isomorphism

$$A \otimes_R B \cong (A \otimes_R S) \otimes_S B \ ,$$

i.e. we are breaking a complicated extension of scalars $A \otimes_R B$ into a simpler one $A \otimes_R S$, followed by a tensor product of S-algebras.

(2) Corollary 3.30 also extends: For R-algebras A and B, we have an S-algebra isomorphism

$$S \otimes_R (A \otimes_R B) \cong (S \otimes_R A) \otimes_S (S \otimes_R B)$$

sending $s \otimes (a \otimes b) \mapsto s((1 \otimes a) \otimes (1 \otimes b))$.

3.4. **Exactness properties of the tensor product.**

3.4.1. *The tensor-with-M functor is right exact.* Fix an R-module M. We have a functor T_M from the category of R-modules to itself, taking an R-module N to $T_M(N) \coloneqq M \otimes_R N$, and taking an R-linear map $f \colon N \to N'$ to $T_M(f) \coloneqq \mathrm{id}_N \otimes f$ (the term functor means that T_M acts both on the objects and the morphisms of the category of R-modules, and that it sends identity morphisms to identity morphisms and respects the composition of morphisms).

We aim to show that if

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

is an exact sequence of R-modules, and M any R-module, then

$$M \otimes A \xrightarrow{\mathrm{id}_M \otimes f} M \otimes B \xrightarrow{\mathrm{id}_M \otimes g} M \otimes C \longrightarrow 0$$

is an exact sequence. In other words, we want to show that T_M is a *right-exact functor*. We proceed in several steps, but first - an application.

Remark 3.33.

(1) What can we say about $M \otimes_R (P/Q)$ for R-modules M, P, Q (Q a submodule of P)? Consider the exact sequence

$$Q \xrightarrow{\iota} P \xrightarrow{\pi} P/Q \longrightarrow 0$$

where ι and π are the inclusion and quotient maps, respectively. Since $T_M(\cdot)$ is right exact (see Proposition 3.37 below), we have an exact sequence

$$M \otimes Q \overset{\mathrm{id}_M \otimes \iota}{\longrightarrow} M \otimes P \overset{\mathrm{id}_M \otimes \pi}{\longrightarrow} M \otimes (P/Q) \longrightarrow 0 \ .$$

That is, $\mathrm{id}_M \otimes \pi$ is surjective, and its kernel is $K := (\mathrm{id}_M \otimes \iota)(M \otimes Q)$, i.e. K is the submodule of $M \otimes P$ generated by $\{m \otimes q \mid m \in M, q \in Q\}$ (as discussed earlier, the map $\mathrm{id}_M \otimes \iota$ does not have to be injective). Thus, we have an R-linear isomorphism

$$\varphi\colon (M \otimes P)/\underbrace{(\mathrm{id}_M \otimes \iota)(M \otimes Q)}_{=K} \overset{\sim}{\longrightarrow} M \otimes (P/Q)$$

such that $\varphi((m \otimes p) + K) = m \otimes (p + Q)$, and so $\varphi^{-1}(m \otimes (p + Q)) = (m \otimes p) + K$.

(2) Now, consider R-algebras S and T, and an ideal I of T. We study $S \otimes_R (T/I)$. The first part of this remark gives us an R-linear isomorphism $\psi\colon S \otimes_R (T/I) \cong (S \otimes_R T)/J$, $J = (\mathrm{id}_S \otimes \iota)(S \otimes_R I)$. In fact, while the first part only guaranteed that J is an R-submodule of $S \otimes_R T$, it is in fact an ideal of $S \otimes_R T$, generated by $\{1 \otimes x \mid x \in I\}$ (check!), and ψ is an S-algebra isomorphism. In other words, J is the ideal of $S \otimes_R T$ generated by the image of I under the ring homomorphism $T \to S \otimes_R T$ given by $t \mapsto 1 \otimes t$.

(3) For example, $\mathbb{C} \otimes_{\mathbb{R}} (\mathbb{R}[T_1, \ldots, T_n]/I) \cong (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[T_1, \ldots, T_n])/J \cong \mathbb{C}[T_1, \ldots, T_n]/I^e$ as $\mathbb{C}$-algebras, where I^e is the extension of I to $\mathbb{C}[T_1, \ldots, T_n]$, i.e. the ideal of $\mathbb{C}[T_1, \ldots, T_n]$ generated by I (we used the result of Example 3.32).

Definition 3.34. For R-modules Q and P, let $\mathrm{Hom}_R(Q, P)$ be the set of R-linear maps $Q \to P$, equipped with the R-module structure where the addition is pointwise addition of functions, and the R-action is given by

$$(rf)(x) = r(f(x)) \qquad \forall r \in R \ f \in \mathrm{Hom}_R(Q, P) \ x \in Q$$

(check that rf is in $\mathrm{Hom}_R(Q, P)$ and that $\mathrm{Hom}_R(Q, P)$ is an R-module).

Fix R-modules Q, P. Then we have two new functors from the category of R-modules to itself:

$$\operatorname{Hom}_R(Q, \cdot)$$
$$\operatorname{Hom}_R(\cdot, P)$$

These are defined for an R-linear map $f\colon M \to N$ by:

$$\operatorname{Hom}_R(Q, M) \overset{\operatorname{Hom}_R(Q,f)}{\longrightarrow} \operatorname{Hom}_R(Q, N)$$

is given by $\varphi \mapsto f_*(\varphi) \coloneqq f \circ \varphi$, and

$$\operatorname{Hom}_R(N, P) \overset{\operatorname{Hom}_R(f,P)}{\longrightarrow} \operatorname{Hom}_R(M, P)$$

is given by $\varphi \mapsto f^*(\varphi) \coloneqq \varphi \circ f$.

Notice how $\operatorname{Hom}_R(\cdot, P)$ reverses the direction of the morphism. For this reason we say that $\operatorname{Hom}_R(\cdot, P)$ is a *contravariant* functor (while $\operatorname{Hom}(Q, \cdot)$ and T_M are *covariant* functors).

The following proposition is easy to prove (see Example Sheet 2):

Proposition 3.35 (The Hom functors are left exact)**.**

(1) *If*

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

is an exact sequence of R-module then so is

$$0 \longrightarrow \operatorname{Hom}_R(Q, A) \xrightarrow{f_*} \operatorname{Hom}_R(Q, B) \xrightarrow{g_*} \operatorname{Hom}_R(Q, C)\ .$$

(2) *If*

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

is an exact sequence of R-module then so is

$$0 \longrightarrow \operatorname{Hom}_R(C, P) \xrightarrow{g^*} \operatorname{Hom}_R(B, P) \xrightarrow{f^*} \operatorname{Hom}_R(A, P)\ .$$

Lemma 3.36. *Consider R-linear maps*

$$A \xrightarrow{f} B \xrightarrow{g} C \tag{3.4}$$

such that for every R-module P, the following sequence is exact:

$$\operatorname{Hom}_R(C, P) \xrightarrow{g^*} \operatorname{Hom}_R(B, P) \xrightarrow{f^*} \operatorname{Hom}_R(A, P)\ . \tag{3.5}$$

Then (3.4) *is exact.*

Proof. First plug in $P = C$. By the exactness of (3.5), $0 = f^*(g^*(\mathrm{id}_C)) = g \circ f$. That is, $\operatorname{im} f \subset \ker g$.

Now plug[4] in $P = B/\operatorname{im} f$, and consider the quotient map $h\colon B \to B/\operatorname{im} f$. Clearly $h \in \ker f^*$, and thus the exactness of (3.5) implies that there is $e \in \operatorname{Hom}_R(C, B/\operatorname{im} f)$ such that $e \circ g = h$. Thus, $\ker g \subset \ker h = \operatorname{im} f$. □

For R-modules M, N, L, we have already seen a bijection

$$\operatorname{Hom}_R(M \otimes_R N, L) \xrightarrow{\sim} \operatorname{Bilin}_R(M \times N, L)$$

which reflects the universal property of $M \otimes_R N$: Each R-bilinear map $M \times N \to L$ corresponds to a single R-linear map $M \otimes_R N \to L$ (write to yourself what the bijections are in both directions). But

$$\operatorname{Bilin}_R(M \times N, L) \xrightarrow{\sim} \operatorname{Hom}_R(N, \operatorname{Hom}_R(M, L))$$

by a bijection sending an R-bilinear map $b\colon M \times N \to L$ to

$$n \mapsto (m \mapsto b(m, n))$$

(convince yourself that this is a well defined bijection). All, in all, we have a bijection

$$\operatorname{Hom}_R\left(\underbrace{M \otimes_R N}_{=T_M(N)}, L\right) \xrightarrow{\sim} \operatorname{Hom}_R(N, \operatorname{Hom}_R(M, L)) \ . \tag{3.6}$$

(in category theoretic language, the fact that this set bijection is natural[5] in both arguments implies that $T_M(\cdot)$ and $\operatorname{Hom}_R(M, \cdot)$ form an *adjoint pair*, with $T_M(\cdot)$ being the left adjoint, and $\operatorname{Hom}_R(M, \cdot)$ the right adjoint).

Proposition 3.37. *Let M be an R-module. Then the functor T_M is right exact.*

Proof. Take an exact sequence of R-modules:

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

Let P be an R-module. Apply $\operatorname{Hom}_R(\cdot, P)$ and then $\operatorname{Hom}_R(M, \cdot)$ to obtain the exact sequence (see Proposition 3.35):

$$0 \to \operatorname{Hom}_R(M, \operatorname{Hom}_R(C, P)) \to \operatorname{Hom}_R(M, \operatorname{Hom}_R(B, P)) \to \operatorname{Hom}_R(M, \operatorname{Hom}_R(A, P))$$

But by (3.6), this sequence is isomorphic to the following sequence (to be completely formal, one needs to draw a little commutative diagram here, representing an isomorphism of sequences):

$$0 \to \operatorname{Hom}_R(M \otimes C, P) \to \operatorname{Hom}_R(M \otimes B, P) \to \operatorname{Hom}_R(M \otimes A, P) \ ,$$

[4] $B/\operatorname{im} f$ is called the *cokernel* of f, denoted by $\operatorname{coker} f$.

[5] Whatever that means (we will only mention category theoretic notions in passing in this course).

so the latter sequence is exact. Since this is true for every R-module P, Lemma 3.36 implies that

$$M \otimes A \to M \otimes B \to M \otimes C \to 0$$

is exact. □

Remark 3.38. **[Non-examinable]** The general principle here is that a left adjoint functor is right exact, and a right adjoint functor is left exact. The more general principle is that a left adjoint functor is continuous (commutes with limits of categorical diagrams), and a right adjoint functor is cocontinuous (commutes with colimits). This is relevant to exact sequences because kernels are limits and cokernels colimits. The natural isomorphism $M \otimes (A \oplus B) \cong (M \otimes A) \oplus (M \otimes B)$ is another instance of this phenomenon: The direct sum is the coproduct (and so, a colimit) in the category of R-modules, and T_M is cocontinuous, and thus tensoring before or after taking a direct sum gives the same result (up to a natural isomorphism).

Warning: It sometimes happens that

$$A \to B \to C$$

is an exact sequence of R-modules, but

$$M \otimes A \to M \otimes B \to M \otimes C$$

isn't (i.e. the extra → 0 on the right is crucial for the preservation of exactness by T_M). See the following example (but first, if you think about it for a second, a functor that preserves all exact sequences of length 3 must preserve all exact sequences, so we really did not expect T_M to do that).

Example 3.39. Consider the exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \overset{x \mapsto 2x}{\longrightarrow} \mathbb{Z} \ .$$

Tensoring with $\mathbb{Z}/2\mathbb{Z}$ (by which we mean as usual that we tensor the objects with $\mathbb{Z}/2\mathbb{Z}$ and the morphisms with $\mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$), we have

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \overset{\mathrm{id}_{\mathbb{Z}/2\mathbb{Z}} \otimes (x \mapsto 2x)}{\longrightarrow} \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \ ,$$

which is equivalent to

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \overset{x+2\mathbb{Z} \mapsto 2x+2\mathbb{Z}}{\longrightarrow} \mathbb{Z}/2\mathbb{Z} \ ,$$

which is not exact.

We take this opportunity to introduce the notion of a morphism of sequences using the example above. We have a diagram

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \arrow[r, "(a+2\mathbb{Z})\otimes b \mapsto (a+2\mathbb{Z})\otimes(2b)"] \arrow[d, "(a+2\mathbb{Z})\otimes b \mapsto ab+2\mathbb{Z}"] & \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \arrow[d, "(a+2\mathbb{Z})\otimes b \mapsto ab+2\mathbb{Z}"] \\
0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "x+2\mathbb{Z} \mapsto 2x+2\mathbb{Z}"] & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

where each square commutes (i.e. the composition of right and down is equal to the composition of down and right). This is an instance of a *commutative diagram.*

The notion of composition of morphisms of sequences is defined in the obvious way. An isomorphism of sequences is a morphism that has a two-sided inverse. Equivalently, an isomorphism of sequences is a morphism of sequences where all the vertical arrows are isomorphisms (check that the two defintions are equivalent). This notion of an isomorphism is the one we need in order to think of two sequences as essentially the same.

3.4.2. *Flat modules - a first encounter.*

Definition 3.40. An R-module M is *flat* if for every R-linear map $f\colon N \to N'$, if f is injective then so is $\mathrm{id}_M \otimes f$.

Example 3.41.

(1) Example 3.39 shows exactly that the $\mathbb{Z}$-module $\mathbb{Z}/2$ is not flat: tensoring the injective map $\mathbb{Z} \xrightarrow{x \mapsto 2x} \mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z}$ results in the zero map $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

(2) Free modules are flat: If $f\colon M \to M'$ is an injective R-linear map then $\mathrm{id}_{R^{\oplus I}} \otimes f\colon R^{\oplus I} \otimes M \to R^{\oplus I} \otimes M'$ is equivalent to the map $M^{\oplus I} \to M'^{\oplus I}$ the sends $(m_i)_{i\in I} \mapsto (f(m_i))_{i \in I}$, which is certainly injective (the equivalence is in the sense of an isomorphism of sequences as defined above). In the example sheet you will prove a generalization: Projective modules are flat.

(3) **The base ring matters:** Notice that $\mathbb{Z}/2\mathbb{Z}$ is flat as a $\mathbb{Z}/2\mathbb{Z}$-module (a very special case of a free module), but not as a $\mathbb{Z}$-module.

(4) A generalization of the first example: An R-module M is *torsion free* if $rm \neq 0$ whenever $r \in R$ is not a zero divisor and $m \neq 0$ (this generalizes the notion of a torsion-free abelian group, i.e. $\mathbb{Z}$-module, noting that in $\mathbb{Z}$ the only zero divisor is 0).

Flat modules are torsion free: Assume that M is not torsion free. Then there is $r_0 \in R$, not a zero divisor, and $0 \neq m_0 \in M$, such that $r_0 m_0 = 0$. Now, the map $\mu_{r_0}\colon R \to R$ given by $\mu_{r_0}(r) = r_0 r$ is injective since r_0 is not a zero divisor. But $\mathrm{id}_M \otimes \mu_{r_0}\colon M \otimes R \to M \otimes R$,

$m \otimes r \mapsto \underbrace{m \otimes (r_0 r)}_{=(r_0 m)\otimes r}$ is not injective because it sends $m_0 \otimes 1$ to 0, while $m_0 \otimes 1 \neq 0$ because under the isomorphism $M \otimes R \cong R$, $m \otimes r \mapsto rm$, $m_0 \otimes 1$ is mapped to $m_0 \neq 0$.

(5) A special case of the previous point: If $(0) \subsetneq I \subsetneq R$ is an ideal of an integral domain R then $M = R/I$ is not a flat R-module. Indeed, M is not a torsion-free R-module: Take $0 \neq r \in I$. Then r is not a zero divisor since R is an integral domain, but the map $m \mapsto rm \colon M \to M$ is the zero map, while M is not the zero module.

Proposition 3.42 (Characterization of flat modules)**.** *Let M be an R-module. The following are equivalent:*

1. *T_M preserves the exactness of all exact sequences.*
2. *T_M preserves the exactness of short exact sequences*[6]*.*
3. *M is flat (i.e. preserves the exactness of exact sequences of the form $0 \to N' \to N$).*
4. *M is "flat for finitely generated R-modules": If $N \xrightarrow{f} N'$ is injective and N, N' are finitely generated R-modules, then $M \otimes_R N \overset{\mathrm{id}_M \otimes f}{\longrightarrow} M \otimes_R N$ is injective.*

Proof. Clearly (1)⇒(2)⇒(3)⇒(4) [why (2)⇒(3)?].

(2)⇒(1) **[in class I will draw a nice diagram]** Assume that $A \xrightarrow{f} B \xrightarrow{g} C$ is exact. Consider the following short exact sequences:

$$0 \longrightarrow \ker f \longrightarrow A \xrightarrow{f} \operatorname{im} f \longrightarrow 0$$

$$0 \longrightarrow \underbrace{\ker g}_{=\operatorname{im} f} \longrightarrow B \xrightarrow{g} \operatorname{im} g \longrightarrow 0$$

$$0 \longrightarrow \operatorname{im} g \longrightarrow C \longrightarrow C/\operatorname{im} g \longrightarrow 0$$

Applying $M \otimes (\cdot)$ to each sequence, exactness is preserved:

$$0 \longrightarrow M \otimes \ker f \longrightarrow M \otimes A \overset{\mathrm{id}_M \otimes f}{\longrightarrow} M \otimes \operatorname{im} f \longrightarrow 0 \tag{3.7}$$

$$0 \longrightarrow M \otimes \underbrace{\ker g}_{=\operatorname{im} f} \longrightarrow M \otimes B \overset{\mathrm{id}_M \otimes g}{\longrightarrow} M \otimes \operatorname{im} g \longrightarrow 0 \tag{3.8}$$

$$0 \longrightarrow M \otimes \operatorname{im} g \longrightarrow M \otimes C \longrightarrow M \otimes C/\operatorname{im} g \longrightarrow 0 \tag{3.9}$$

Consider the sequence

$$M \otimes A \overset{\mathrm{id}_M \otimes f}{\longrightarrow} M \otimes B \overset{\mathrm{id}_M \otimes g}{\longrightarrow} M \otimes C \tag{3.10}$$

[6] Recall: A short exact sequence is an exact sequence of the form $0 \to N' \to N \to N'' \to 0$.

Then

$$\begin{aligned}\operatorname{im}(M\otimes A\to M\otimes B) &= \operatorname{im}(M\otimes A\to M\otimes \operatorname{im} f\to M\otimes B)\\ &= \operatorname{im}(M\otimes \operatorname{im} f\to M\otimes B)\end{aligned}$$

because $M\otimes A\to M\otimes \operatorname{im} f$ is surjective by the exactness of (3.7) at $M\otimes \operatorname{im} f$. But now

$$\operatorname{im}\left(M\otimes \underbrace{\operatorname{im} f}_{=\ker g}\to M\otimes B\right) = \ker(M\otimes B\to M\otimes \operatorname{im} g)$$

by the exactness of (3.8) at $M\otimes B$. And now,

$$\ker(M\otimes B\to M\otimes \operatorname{im} g) = \ker\left(\underbrace{M\otimes B\to M\otimes \operatorname{im} g\to M\otimes C}_{=M\otimes B\to M\otimes C}\right)$$

because $M\otimes \operatorname{im} g\to M\otimes C$ is injective by the exactness of (3.9) at $M\otimes \operatorname{im} g$. This shows that (3.10) is exact.

(3)⇒(2): Follows since T_M is right exact (Proposition 3.37).

(4)⇒(3): **I suggest trying to prove this yourself before reading the proof below**.

Take an injective R-linear map $f\colon N\to N'$, and take $\sum m_i\otimes n_i\in \ker(\mathrm{id}_M\otimes f\colon M\otimes N\to M\otimes N')$. Then

$$\sum m_i\otimes f(n_i)=0 \tag{3.11}$$

(in $M\otimes N'$).

Let N_0 be the submodule of N generated by the n_i.

By Proposition 3.10, there are finitely generated submodules M_0 of M and N_0' of N' such that (3.11) holds in $M_0\otimes N_0'$. Then (3.11) also holds in $M_0\otimes (N_0'+f(N_0))$.

Consider $\mathrm{id}_{M_0}\otimes(f\mid_{N_0})\colon M_0\otimes N_0\to M_0\otimes(N_0'+f(N_0))$. Then $\sum m_i\otimes n_i$, as an element $M_0\otimes N_0$, is sent to 0, and thus (4) implies that $\sum m_i\otimes n_i=0$ in $M_0\otimes N_0$. Thus $\sum m_i\otimes n_i=0$ also in $M\otimes N$. □

Proposition 3.43 (Extension of scalars preserves flatness)**.** *Let $f\colon R\to S$ be a ring homomorphism, and take a flat R-module M. Then $S\otimes_R M$ is a flat S-module.*

Proof. Let $g\colon N\to N'$ be an injective S-linear map. We have a commutative diagram

$$\begin{tikzcd}
(S\otimes_R M)\otimes_S N \arrow[r, "\mathrm{id}_{S\otimes_R M}\otimes g"] \arrow[d, "(s\otimes m)\otimes n\mapsto m\otimes(sn)"] & (S\otimes_R M)\otimes_S N' \arrow[d, "(s\otimes m)\otimes n'\mapsto m\otimes(sn')"] \\
M\otimes_R N \arrow[r, "\mathrm{id}_M\otimes g"] & M\otimes_R N'
\end{tikzcd}$$

The commutativity of the diagram is clear (just follow with pure tensors). The vertical arrows are S-module isomorphisms by Proposition 3.28. Thus, the injectivity of the bottom arrow implies the injectivity of the top arrow by basic diagram chasing[7]. □

Remark 3.44. The non-left-exactness of T_M for a non-flat module M seems like a caveat, but it also opens the door to a very rich study of modules via tools of homological algebra.

Remark 3.45. **[non-examinable]** If you want to know more about flat modules, your next steps could be to learn the following:

(1) Note that for every ideal I of R and R-module M, we have a surjective R-linear map $I \otimes_R M \to IM$, $i \otimes m \mapsto im$, where IM is the submodule of M generated by $\{im \mid i \in I, m \in M\}$.
   (a) **Proposition A:** M is flat if and only if this R-linear map $I \otimes_R M \to IM$ is also injective for every finitely generated ideal I of M.
   (b) Clearly, this condition is necessary for flatness: The inclusion $I \hookrightarrow R$ is R-linear and injective, and tensoring with id_M gives the map above, which much also be injective if M is flat.

(2) A second worthy goal is to learn enough homomological algebra to understand the following proposition:
   (a) **Proposition B:** The map $I \otimes M \to IM$ above is injective if and only if $\mathrm{Tor}_1(R/I, M) = 0$.
   (b) Proposition B can be used to prove Proposition A.

3.5. Further examples of tensor products.

Example 3.46. For $x \otimes y \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$, we have

$$x \otimes y = \left(n\frac{x}{n}\right) \otimes y = \frac{x}{n} \otimes \underbrace{ny}_{=0}$$

and so $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$. What properties of the abelian groups $\mathbb{Q}$ and $\mathbb{Z}/n\mathbb{Z}$ did we use?

(1) $A = \mathbb{Q}$ is a divisible group (i.e. for all $n \geq 1$ and $a \in A$ there is $a' \in A$ such that $na' = a$).

(2) $B = \mathbb{Z}/n\mathbb{Z}$ is a torsion group (i.e. every element of B has finite order).

[7] The chase in this case: Start with $x \in (S \otimes_R M) \otimes_B N$ such that going right makes it 0. So going right then down also brings x to 0. Thus going down and then right brings x to 0. The injectivity of the bottom row implies that just going down brings x to 0. But the left arrow is an S-module isomorphism, and thus $x = 0$.

So, $A \otimes_{\mathbb{Z}} B = 0$ whenever A is a divisible group[8] and B is an abelian torsion group. Now, $\mathbb{Q}/\mathbb{Z}$ is a torsion divisible group, and thus

$$(\mathbb{Q}/\mathbb{Z})^{\otimes 2} = 0 \ .$$

On the other hand:

Proposition 3.47. *If $M \neq 0$ is a finitely generated R-module then $M^{\otimes n} \neq 0$ for all $n \geq 1$.*

Proof. See the example sheet. □

Above, we referred to the tensor power $M^{\otimes n}$. More generally, one may form a tensor product $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ of R-modules. It is defined similarly to the case $n = 2$. We have $M_1 \otimes (M_2 \otimes M_3) \cong M_1 \otimes M_2 \otimes M_3 \cong (M_1 \otimes M_2) \otimes M_3$ naturally (which can be used to prove the associativity of the tensor product). Also, $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ is characterized by a universal property in terms of R-multilinear maps, analogous to the universal property of $M \otimes N$ in terms of bilinear maps. We will not spell out the precise definition because it is a trivial generalization, but you are expected to understand what the definition is (or read somewhere).

Example 3.48. Let V be a $\mathbb{Q}$-vector space. Then we know that $\mathbb{Q} \otimes_{\mathbb{Q}} V \cong V$ by the isomorphism $x \otimes v \mapsto xv$. Notice that every tensor in $\mathbb{Q} \otimes_{\mathbb{Q}} V$ is pure:

$$\sum x_i \otimes v_i = \sum 1 \otimes x_i v_i = 1 \otimes \sum x_i v_i \ .$$

What about $\mathbb{Q} \otimes_{\mathbb{Z}} V$? Is every tensor still pure? We are only allowed to move elements of $\mathbb{Z}$ across the $\otimes$ sign, but still we have an affirmative answer (below $a_i, b_i \in \mathbb{Z}$):

$$\begin{aligned} \sum \frac{a_i}{b_i} \otimes v_i &= \sum \frac{1}{b_i} \otimes a_i v_i \\ &= \sum \frac{1}{b_i} \otimes \frac{a_i b_i}{b_i} v_i \\ &= \sum 1 \otimes \frac{a_i}{b_i} v_i \\ &= 1 \otimes \sum \frac{a_i}{b_i} v_i \ . \end{aligned}$$

So what is $\mathbb{Q} \otimes_{\mathbb{Z}} V$ (here we restrict scalars from $\mathbb{Q}$ to $\mathbb{Z}$ on V, and then extend scalars to $\mathbb{Q}$ again)? The $\mathbb{Z}$-bilinear map $\mathbb{Q} \times V \to V$ sending $(x, v) \mapsto xv$ gives rise to a $\mathbb{Z}$-linear map $\varphi \colon \mathbb{Q} \otimes_{\mathbb{Z}} V \to V$ such that $\varphi(x \otimes v) = xv$. Clearly φ is surjective and sends nonzero pure tensors to nonzero elements. But every tensor in $\mathbb{Q} \otimes_{\mathbb{Z}} V$ is pure, and thus φ is injective, that is, an isomorphism of $\mathbb{Z}$-modules (check that it is also an isomorphism of $\mathbb{Q}$-modules).

[8] Divisible groups are abelian by definition.

The proof above generalizes trivially to show that[9] $\operatorname{Frac}(R) \otimes_R V \cong V$ as $\operatorname{Frac}(R)$-modules whenever R is an integral domain and V is a $\operatorname{Frac}(R)$-module. We can even generalize further:

Proposition 3.49. *Let R be an integral domain and V a* $\operatorname{Frac} R$*-module. Let $M \neq 0$ be an R-submodule of* $\operatorname{Frac} R$*. Then $M \otimes_R V \cong V$ as R-modules by an isomorphism sending $m \otimes v \mapsto mv$.*

Proof. See the example sheet. You can still prove that all tensors are pure, but this is a bit more subtle. Then injectivity follows easily. It is also less clear than before why the map is surjective, so a short explanation is required. □

Example 3.50. Consider $R = \mathbb{Z}\big[\sqrt{-5}\big]$ (so $\operatorname{Frac} R = \mathbb{Q}\big(\sqrt{-5}\big)$), and an ideal I of $\mathbb{Z}\big[\sqrt{-5}\big]$ (so I is a $\mathbb{Z}\big[\sqrt{-5}\big]$-submodule of $\mathbb{Q}\big(\sqrt{-5}\big)$). If I is principal then[10] $R \cong I$ as R-modules, and thus certainly $I \otimes_R \operatorname{Frac} R \cong R \otimes_R \operatorname{Frac} R \cong \operatorname{Frac} R$.

For a nonprincipal ideal I of R, we have $R \ncong I$ as R-modules because R can is generated as an R-module by 1_R, while I cannot be generated by a single element. For example $I = \big(2, 1 + \sqrt{-5}\big)$ is nonprincipal (proof omitted; if you really want to you can use the field norm of $\mathbb{Q}\big(\sqrt{-5}\big)/\mathbb{Q}$ to prove this). But still we have $\big(2, 1 + \sqrt{-5}\big) \otimes_{\mathbb{Z}[\sqrt{-5}]} \mathbb{Q}\big(\sqrt{-5}\big) \cong \mathbb{Q}\big(\sqrt{-5}\big)$ by Proposition 3.49.

Remark 3.51. The argument in Example 3.48 raises the question of whether an R-linear map $f\colon M \otimes_R N \to L$ that is injective on pure tensors must be injective. The answer is negative. You will be asked to consider this question in the example sheet.

Example 3.52. We have a nice R-module isomorphism $M \otimes_R \bigoplus_{i \in I} M_i \xrightarrow{\sim} \bigoplus_{i \in I} M \otimes_R M_i$ given by $m \otimes (m_i)_{i \in I} \mapsto (m \otimes m_i)_{i \in I}$. The same formula also gives an R-linear map $M \otimes_R \prod_{i \in I} M_i \longrightarrow \prod_{i \in I} M \otimes_R M_i$, which in general is not an isomorphism. Let's see an example where these two R-modules are not even isomorphic. On one hand, $\prod_{n \geq 1} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} = 0$ (why?). On the other hand $\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$ is not the zero module. Indeed, take an element $x \in \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$ of infinite order (say $x = (1, 1, 1, \dots)$). Write $\langle x \rangle$ for the subgroup of $\prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$ generated by x. Then $\mathbb{Q} \otimes_{\mathbb{Z}} \underbrace{\langle x \rangle}_{\cong \mathbb{Z}} \cong \mathbb{Q} \neq 0$.

But $\mathbb{Q}$ is a flat $\mathbb{Z}$-module (see later, or prove directly), and so tensoring the inclusion $\langle x \rangle \hookrightarrow \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$ with $\mathbb{Q}$ results in an embedding of the nonzero module $\mathbb{Q} \otimes_{\mathbb{Z}} \langle x \rangle$ in $\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$.

[9] Here $\operatorname{Frac} R$ is the field of fractions of an integral domain R.

[10] In general, for a principal ideal $I = (x)$ of a ring R, we have a surjective R-linear map $R \to I$, $r \mapsto rx$, which is also injective when R is a domain and $x \neq 0$.

Example 3.53. What is $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$? First, as an $\mathbb{R}$-module, the right copy of $\mathbb{C}$ has an $\mathbb{R}$-basis $\{1, i\}$. Treating $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ as an extension of scalars of the right copy from $\mathbb{R}$ to $\mathbb{C}$, we see that $\{1 \otimes 1, 1 \otimes i\}$ is a $\mathbb{C}$-basis for $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

Furthermore, we have $\mathbb{C}$-algebra homomorphisms

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &\cong \mathbb{C} \otimes_{\mathbb{R}} \big(\mathbb{R}[T]/\big(T^2+1\big)\big) \\ &\cong \mathbb{C}[T]/((T-i)(T+i)) \\ &\cong \mathbb{C}[T]/(T-i) \times \mathbb{C}[T]/(T+i) \\ &\cong \mathbb{C} \times \mathbb{C} \end{aligned}$$

(the third equality used the Chinese Remainder Theorem, see the example sheet). What is the isomorphism?

$$\begin{aligned} \Bigg(\underbrace{a+bi}_{=:x}\Bigg) \otimes \Bigg(\underbrace{c+di}_{=:y}\Bigg) &\mapsto (a+bi) \otimes \big(c + dT + \big(T^2+1\big)\big) \\ &\mapsto \underbrace{(a+bi)(c+dT)}_{ac+bdiT+ibc+Tad=:P} + \big(T^2+1\big) \\ &\mapsto (P + (T-i), P + (T+i)) \\ &\mapsto ((ac-bd) + i(bc+ad), (ac+bd) + i(bc-ad)) \\ &= (xy, x\overline{y}) \ . \end{aligned}$$

What are the elements of $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ that are mapped to $(1,0)$ and $(0,1)$? Recall that as a $\mathbb{C}$-module, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is of dimension 2, with basis $\Bigg\{\underbrace{1 \otimes 1}_{=v_1}, \underbrace{1 \otimes i}_{=v_2}\Bigg\}$. We take $\alpha, \beta \in \mathbb{C}$, and compute our isomorphism $\varphi \colon \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathbb{C} \times \mathbb{C}$:

$$\underbrace{\alpha v_1 + \beta v_2}_{=\alpha\otimes 1+\beta\otimes i} \mapsto \underbrace{(\alpha, \alpha) + (\beta i, -\beta i)}_{=(\alpha+\beta i, \alpha-\beta i)} \tag{3.12}$$

and thus

$$\begin{aligned} &\underbrace{\frac{1}{2}v_1 - \frac{i}{2}v_2}_{=:u_1} \mapsto (1,0) \\ &\underbrace{\frac{1}{2}v_1 + \frac{i}{2}v_2}_{=:u_2} \mapsto (0,1) \ . \end{aligned}$$

In other words, the basis $\{u_1, u_2\} = \left\{\frac{1}{2} \otimes 1 - \frac{i}{2} \otimes i, \frac{1}{2} \otimes 1 + \frac{i}{2} \otimes i\right\}$ makes the multiplication in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ very simple:

$$(\alpha_1 u_1 + \beta_1 u_2)(\alpha_2 u_1 + \beta_2 u_2) = (\alpha_1\alpha_2)u_1 + (\beta_1\beta_2)u_2 \ .$$

Indeed,

$$\begin{aligned}(\alpha_1 u_1 + \beta_1 u_2)(\alpha_2 u_1 + \beta_2 u_2) &= \varphi^{-1}\left(\underbrace{\varphi(\alpha_1 u_1 + \beta_1 u_2)}_{=(\alpha_1,\beta_1)}\underbrace{\varphi(\alpha_2 u_1 + \beta_2 u_2)}_{=(\alpha_2,\beta_2)}\right)\\ &= \varphi^{-1}(\alpha_1\alpha_2, \beta_1\beta_2)\\ &= (\alpha_1\alpha_2)u_1 + (\beta_1\beta_2)u_2\ .\end{aligned}$$

The somewhat alert yet not fully alert reader might find the following "contradiction": If in (3.12) we write $\alpha(1\otimes 1)+\beta(1\otimes i) = 1\otimes\alpha + 1\otimes\beta i$ and compute, we get a different result, but there should only be one answer to the question of where $\alpha(1\otimes 1)+\beta(1\otimes i)$ is sent! The answer is that $A \coloneqq \mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ is a tensor product over $\mathbb{R}$, and as such we are only allowed to move scalars from $\mathbb{R}$ across the $\otimes$ symbol. When we decided to take the right copy of the $\mathbb{R}$-algebra $\mathbb{C}$ and extend scalars to $\mathbb{C}$, we have made a decision to let the base ring $\mathbb{C}$ act on the left side of pure tensors. If we make a similar construction $B \coloneqq \mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ where we think of the left copy as an $\mathbb{R}$-module and extend scalars to $\mathbb{C}$ from the right, then the set-theoretic identity map $A \to B$ is an $\mathbb{R}$-module isomorphism, but not a $\mathbb{C}$-linear map (however, there is a $\mathbb{C}$-algebra isomorphism, which is..). Note that the issue is not unique to algebras, it's an issue with modules in general: Making $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ into a $\mathbb{C}$-module via the left or right copies of $\mathbb{C}$ results in different modules (in the sense that the set-theoretic identity map is not a $\mathbb{C}$-linear map from $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ defined the first way to $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ defined the second way).

Remark 3.54. **[Non-examinable]** One can classify all $\mathbb{C}$-algebra homomorphisms $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}$. Every such homomorphism is $\mathbb{R}$-linear and thus corresponds to an $\mathbb{R}$-bilinear maps $\mathbb{C}\times\mathbb{C}\to\mathbb{C}$. These are all of the form $(x,y)\mapsto T(x)S(y)$ where T,S are $\mathbb{R}$-linear maps $\mathbb{C}\to\mathbb{C}$. Thus, each $\mathbb{R}$-linear maps $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}$ send $x\otimes y\mapsto T(x)S(y)$ for T,S as above. For such an $\mathbb{R}$-linear map to be a $\mathbb{C}$-algebra homomorphism it is necessary that $x\otimes 1\mapsto x$, and so $T=\mathrm{id}_{\mathbb{C}}$. So, what does it take for a map $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}$ satisfying $x\otimes y\mapsto xS(y)$ to be a $\mathbb{C}$-algebra homomorphism? Since $(1\otimes y_1)(1\otimes y_2) = 1\otimes(y_1y_2)$, we must have $S(y_1y_2)=S(y_1)S(y_2)$. Similarly $S(1)=1$. So $S\colon\mathbb{C}\to\mathbb{C}$ is a ring homomorphism (and also $\mathbb{R}$-linear). An $\mathbb{R}$-linear map $\mathbb{C}\to\mathbb{C}$ sending $1_{\mathbb{C}}\mapsto 1_{\mathbb{C}}$ must be the identity on $\mathbb{R}$. A ring homomorphism $\mathbb{C}\to\mathbb{C}$ fixing $\mathbb{R}$ elementwise must send $i\in\mathbb{C}$ to a root of T^2+1. The only such $\mathbb{R}$-linear maps are the identity and conjugation on $\mathbb{C}$. So $x\otimes y\mapsto xy$ and $x\otimes y\mapsto x\overline{y}$ are the only $\mathbb{C}$-algebra homomorphisms $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}$. We can pack them into a single $\mathbb{C}$-algebra homomorphism $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}\times\mathbb{C}$, $x\otimes y\mapsto(xy,x\overline{y})$. This map is surjective. Surjetivity will always hold when you take a commutative $\mathbb{C}$-algebra A, $\dim_{\mathbb{C}} A<\infty$, and a collection of distinct $\mathbb{C}$-algebra homomorphisms, and pack them like this. You can think about this directly. I think about it as a special case of the Artin–Wedderburn Theorem (from the not-necessarily-commutative world). In our case, the $\mathbb{C}$-linear surjective map is between $\mathbb{C}$-vector spaces of the same dimension (i.e. dimension 2), and so it is an isomorphism. In fact, in general, if you use all $\mathbb{C}$-algebra homomorphisms $A \to \mathbb{C}$, you will have an isomorphism if and only if the only nilpotent element in A is 0 (if A has a nonzero nilpotent element then the number of $\mathbb{C}$-algebra homomorphisms $A \to \mathbb{C}$ is smaller than $\dim_{\mathbb{C}} A$).

4. Localization

Definition 4.1. A multiplicative subset of the ring R is a subset $S \subset R$ such that $1 \in S$ and $ab \in S$ whenever $a, b \in S$.

The *multiplicative closure* of a subset U of R is the intersection of all multiplicative subsets of R that contain U (equivalently, it is the set S of all elements of the form $\prod_{i=1}^{n} s_1 \cdots s_n$, $n \geq 0$, which automatically includes 1 by taking $n = 0$).

4.1. An overview of the basic idea.

If R is an integral domain, we know the construction of the field of fractions $\operatorname{Frac} R$ of R. We have a canonical ring homomorphism $R \to \operatorname{Frac} R$ sending $r \mapsto \frac{r}{1}$. Informally, we start from R and add inverses for all elements of the set $S = R \setminus \{0\}$. This set S is multiplicative because R is an integral domain. Here we generalize this construction: we will not assume that R is an integral domain, and we will add inverses for the elements of an arbitrary multiplicative subset $S \subset R$. The resulting ring will be denoted $S^{-1}R$, and we will have a canonical map $R \to S^{-1}R$, $r \mapsto \frac{r}{1}$, which will not always be injective (it will be injective if and only if S does not contain any zero divisor of R). We go even further: for an R-module M and a multiplicative subset S of R, we form the R-module $S^{-1}M$, consisting of elements of the form $\frac{m}{s}$, $m \in M$, $s \in S$. Then the ring $S^{-1}R$ is a special case of $S^{-1}M$, by looking at R as an R-module, but unlike the general case of $S^{-1}M$, in $S^{-1}R$ we also define multiplication that makes it into a ring and not just a module. It then turns out the $S^{-1}M$ is not just an R-module, but an $S^{-1}R$-module (i.e. the structure ring homomorphism $R \to \operatorname{End} S^{-1}M$ of $S^{-1}M$ as an R-module factors through the canonical map $R \to S^{-1}R$, $r \mapsto \frac{r}{1}$). Finally, we will see that the ring $S^{-1}R$ has a certain universal property: any ring homomorphism $R \to A$ sending each element of S to an invertible element of A factors uniquely via the canonical map $R \to S^{-1}R$. As usual with universal properties, $S^{-1}R$ will be shown to be the unique ring satisfying the universal property (up to isomorphism). One can easily define a similar universal property for an arbitrary subset

U of R rather than the multiplicative subset S of R, i.e. is there a ring B such that every homomorphism $R \to A$ sending each element of U to an invertible element of A factors uniquely through some fixed map $R \to B$? The answer turns out to be positive: the unique answer is to take $B = S^{-1}R$, where S is the multiplicative closure of U in R. In this sense, working with multiplicative subsets to begin with does not limit the generality. Another way to think about this, slightly less formally: in any ring A, if $a_1, a_2 \in A$ are both invertible, then so is their product a_1a_2, and so if you "add inverses" to a certain set $U \subset R$ of elements, you have to add inverses to all elements in the multiplicative closure S of U. Once we are done with the fundamentals reviewed above, we will see algebraic applications of localization. In other courses, such as Algebraic Geomtery, you will see geometric applications that explain, in particular, what local geometric information becomes accessible via localization.

4.2. **The construction and univeral property.**

Definition 4.2. Let S be a multiplicative subset of the ring R. Let M be an R-module. Consider the set of all pairs (m, s), $m \in M$, $s \in S$. Write $(m_1, s_1) \sim (m_2, s_2)$ if there is $u \in S$ such that $u(s_2m_1 - s_1m_2) = 0$. Then $\sim$ is an equivalence relation (see later). We write $\frac{m}{s}$ for the equivalence class of (m, s), and let $S^{-1}M = \left\{\frac{m}{s} \mid m \in M, s \in S\right\}$. We make the set $S^{-1}M$ into an abelian group by letting $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2m_1+s_1m_2}{s_1s_2}$, which is well defined (see later). We make the abelian group $S^{-1}M$ into an R-module by letting $r\frac{m}{s} = \frac{rm}{s}$, which is again well defined.

Consider R as an R-module. Then the R-module $S^{-1}R$ becomes a ring by letting $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$, which is well defined (see later).

The R-module $S^{-1}M$ is in fact an $S^{-1}R$-module via the action $\frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}$, which is well defined (see later).

Remark 4.3. For the reader who knows the construction of the field of fractions $\operatorname{Frac} R$ of an integral domain R, the only surprise in the definition above is probably the introduction of u in the definition of the equivalence class $\sim$. But it is easy to see that u is necessary: our point is to make u (and every other element of S) into an invertible element in the new ring $S^{-1}R$. But, regardless of localization, for any R-module M, invertible element $x \in R$ and $m \in M$, if $xm = 0$, then, letting x^{-1} act on both sides, we have $m = 0$. So u is necessary. The more surprising thing is that handling this particular issue in the definition of $\sim$ is sufficient in order to make $S^{-1}R$ and $S^{-1}M$ into a ring and a module (respectively), and to satisfy the universal property sketched in the overview.

From now on we shall use the term *unit* to refer to an invertible element of a ring. We turn to checking that the notions in Definition 4.2 are as promised (i.e. well defined, and give the structure of a module, ring, etc.). Let $S \subset R$ be a multiplicative subset and take an R-module M. First, we show that $\sim$ is an equivalence relation. It is clearly reflexive and symmetric. We show transitivity: Assume that $(m_1, s_1) \sim (m_2, s_2)$ and $(m_2, s_2) \sim (m_3, s_3)$. Then there $u, v \in S$ such that

$$u(s_2 m_1 - s_1 m_2) = 0 = v(s_3 m_2 - s_2 m_3) \ .$$

Multiplying the LHS by vs_3, the RHS by us_1, and adding the results up, we have:

$$uv(s_2 s_3 m_1 - s_1 s_3 m_2 + s_1 s_3 m_2 - s_1 s_2 m_3) \ ,$$

i.e.

$$uvs_2(s_3 m_1 - s_1 m_3) \ ,$$

and so $(m_1, s_1) \sim (m_3, s_3)$ because $uvs_2 \in S$ because S is multiplicative.

What is still left to prove?

(1) Addition in $S^{-1}M$ is well defined and makes $S^{-1}M$ into an abelian group (with $\frac{0}{1}$ as the zero element).
(2) Multiplication of a scalar $r \in R$ by $m \in M$ is well defined and makes $S^{-1}M$ into an R-module.
(3) Multiplication of $\frac{r_1}{s_2}$ and $\frac{r_2}{s_2}$ is well defined and makes R into a ring (with $\frac{1}{1}$ as the multiplicative identity).

These verifications are straightforward and are left to the reader and will be taken for granted from now on. Now:

(1) The map $R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$ is clearly a ring homomorphism.
(2) **Making $S^{-1}M$ into an $S^{-1}R$-module:** Write $\rho\colon R \to \operatorname{End} S^{-1}M$ for the structure ring homomorphism of the R-module $S^{-1}M$. Now, $\rho(s) = \left(\frac{x}{t} \mapsto \frac{sx}{t}\right)$ is a unit of $\operatorname{End} S^{-1}M$ for all $s \in S$ because it has the map $\frac{x}{t} \mapsto \frac{x}{st}$ as an inverse (verify that this map is in $\operatorname{End} S^{-1}M$). Thus, by the universal property of $S^{-1}R$ (see below) ρ factors through a unique ring homomorphism $\overline{\rho}\colon S^{-1}R \to \operatorname{End} S^{-1}M$ (i.e. $\rho(r) = \overline{\rho}\left(\frac{r}{1}\right)$), and $\overline{\rho}\left(\frac{r}{s}\right) = \left(\frac{m}{t} \mapsto \frac{\rho(r)(m)}{st}\right)$, that is, $\frac{r}{s} \cdot \frac{m}{t} = \frac{r \cdot m}{st}$ (again, the universal property will give this). The fact that the ring $\operatorname{End} S^{-1}M$ is generally not commutative will not pose a problem.

Here is the universal property of $S^{-1}R$. We will write $\iota_{S^{-1}R}\colon R \to S^{-1}R$ for the canonical ring homomorphism $\iota_{S^{-1}R}(r) = \frac{r}{1}$. It has the property that $\iota_{S^{-1}R}(s)$ is a unit of $S^{-1}R$ for all $s \in S$.

Proposition 4.4. *Let S be the multiplicative closure of a subset U of R. Then, for every ring B (unital, but not necessarily commutative) and ring* *homomorphism $f\colon R \to B$ such that $f(u)$ is a unit for all $u \in U$, there a unique ring homomorphism $h\colon S^{-1}R \to B$ such that $f = h \circ \iota_{S^{-1}R}$ (that is, $f(r) = h\big(\frac{r}{1}\big)$ for all $r \in R$). It is given by $h\big(\frac{r}{s}\big) = \big(f(s)\big)^{-1} f(r)$.*

Furthermore, if (A, j) is another pair of a ring A and a ring homomorphism $j\colon R \to A$ with the same universal property[11] *of $\big(S^{-1}R, \iota_{S^{-1}R}\big)$ as above, then we have an isomorphism $\varphi\colon S^{-1}R \to A$ given by $\varphi\big(\frac{r}{s}\big) = \big(j(s)\big)^{-1} j(r)$.*

Proof. Consider a ring homomorphism $f\colon R \to B$ as in the statement. First, note that since f sends the elements of U to units, it all sends the elements of the multiplicative closure S of U to units. Define a ring homomorphism $h\colon S^{-1}R \to B$ by letting $h\big(\frac{r}{s}\big) = \big(f(s)\big)^{-1} f(r)$. Then clearly $f(r) = h\big(\frac{r}{1}\big)$. Also, for h to be a ring homomorphism we must have $1 = h(1) = h\big(\frac{1}{s} \cdot \frac{s}{1}\big) = h\big(\frac{1}{s}\big) \underbrace{h\Big(\frac{s}{1}\Big)}_{=f(s)}$ and so $h\big(\frac{r}{s}\big) = h\big(\frac{1}{s}\big) \underbrace{h\Big(\frac{r}{1}\Big)}_{=f(r)} = \big(f(s)\big)^{-1} f(r)$, so there is no other way to define h. We still need to prove that h is a well defined ring homomorphism: Assume that $\frac{r_1}{s_1} = \frac{r_2}{s_2}$. Then there is $t \in S$ such that $ts_2r_1 = ts_1r_2$. Then $f(t)f(s_2)f(r_1) = f(t)f(s_1)f(r_2)$, and we can divide both sides by $f(t)f(s_1)f(s_2)$ because f sends the elements of S to units. So h is well defined. Checking that h is a ring homomorphism is now trivial.

Now to the uniqueness of $\big(S^{-1}R, \iota_{S^{-1}R}\big)$ as a pair satisfying a universal property. Assume that (A, j) as in the statement also satisfies the universal property. Challenging $S^{-1}R$ with j we obtain a ring homomorphism $\varphi\colon S^{-1}R \to A$ such that $j = \varphi \circ \iota_{S^{-1}R}$. Challenging A with $\iota_{S^{-1}R}$ we obtain a ring homomorphism $\psi\colon A \to S^{-1}R$ such that $\iota_{S^{-1}R} = \psi \circ j$. Thus $\psi \circ \varphi \circ \iota_{S^{-1}R} = \iota_{S^{-1}R}$. That is, $\psi \circ \varphi$ is the solution for challenging $S^{-1}R$ with $\iota_{S^{-1}R}$. But $\mathrm{id}_{S^{-1}R}$ is a solution to the same challenge, and so $\psi \circ \varphi = \mathrm{id}_{S^{-1}R}$. Similarly $\varphi \circ \psi = \mathrm{id}_A$, and so φ and ψ are isomorphisms. As for the formula for the isomorphism $\varphi\colon S^{-1}R \to A$: we have $j = \varphi \circ \iota_{S^{-1}R}$, which means that $\varphi\big(\frac{r}{1}\big) = j(r)$. As in the first paragraph, this forces $\varphi\big(\frac{r}{s}\big) = \big(j(s)\big)^{-1} j(r)$. □

We can express the universal property of the ring $S^{-1}R$ as a natural bijection: For every ring B,

$$\mathrm{Hom}_{\mathrm{Rings}}\big(S^{-1}R, B\big) \cong \big\{\varphi \in \mathrm{Hom}_{\mathrm{Rings}}(R, B) \mid \varphi(U) \subset B^\times\big\}$$

where $B^\times$ is the group of units (i.e. invertible elements) of B. The bijection sends $f\colon S^{-1}R \to B$ to the map $r \mapsto f\big(\frac{r}{1}\big)$.

Some properties of $S^{-1}R$ and the map $\iota = \iota_{S^{-1}R}\colon R \to S^{-1}R$ (S a multiplicative subset of R):

[11] That is, $j(u)$ is a unit of A for all $u \in U$, and every ring homomorphism $f\colon R \to B$ such that $f(u)$ is a unit for all $u \in U$ factors uniquely via j.

(1) An element $\frac{r}{s} \in S^{-1}R$ is $0 \Leftrightarrow \frac{r}{s} = \frac{0}{1} \Leftrightarrow$ There is $u \in S$ such that $ur = 0$.
(2) So $S^{-1}R = 0 \Leftrightarrow \frac{1}{0} = \frac{0}{1}$ in $S^{-1}R \Leftrightarrow 0 \in S$, and
(3) $\ker \iota = \{r \in R \mid \exists u \in S\ ur = 0\}$.
(4) In particular, $\ker \iota = 0 \Leftrightarrow S$ contains no zero divisors.
(5) ι is always an epimorphism, but usually not surjective.
Recall that a morphism $f\colon A \to B$ (in any category) is an epimorphism if $g \circ f = h \circ f$ implies $g = h$. For example, the embedding $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism because two ring homomorphisms from $\mathbb{Q}$ that agree on $\mathbb{Z}$ must agree on all of $\mathbb{Q}$. But clearly $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is not surjective. Similarly, if two ring homomorphisms from $S^{-1}R$ agree on $\operatorname{im} \iota_{S^{-1}R}$ then they must agree (check!).
Nevertheless, every surjective ring homomorphism is an epimorphism. Note that in the following categories, the epimorphisms are precisely the surjective morphisms: Sets, Groups, R-modules, topological spaces.

The following two examples of localizations are very important.

Example 4.5.

(1) Let $f \in R$. Then $S = \{f^n \mid n \geq 0\}$ is a multiplicative subset of R. The ring $S^{-1}R$ is denoted R_f. It is "R with f inverted" (and necessarily all powers of f are inverted too).
   (a) Example: $R = \mathbb{Z}$, $f = 2$. Then $R_f = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \geq 0\right\}$. This is the ring of dyadic rational numbers. It is isomorphic to the ring $\mathbb{Z}\left[\frac{1}{2}\right]$ (i.e., the subring of $\mathbb{Q}$ generated by $\mathbb{Z}$ and $\frac{1}{2}$, i.e. the image of the unique $\mathbb{Z}$-algebra homomorphism $\mathbb{Z}[T] \mapsto \mathbb{Q}$ sending $T \mapsto \frac{1}{2}$).
   Notational caveat: In some undergraduate texts, $\mathbb{Z}_n$ denotes a ring isomorphic to $\mathbb{Z}/n\mathbb{Z}$. I will only write $\mathbb{Z}/n\mathbb{Z}$ for this finite ring. But there's another problem: for a prime number p, $\mathbb{Z}_p$ commonly denotes the ring of p-adic integers, which is not the ring $\{p^n \mid n \geq 0\}^{-1}\mathbb{Z}$ discussed above. For this reason, when localizing $\mathbb{Z}$ using $S = \left\{n^\ell \mid \ell \geq 0\right\}$, I will write $\mathbb{Z}\left[\frac{1}{n}\right]$ instead of using the R_f notation.
   (b) R_f is the zero ring if and only if $0 \in \{f^n \mid n \geq 0\}$ if and only if f is a nilpotent element of R (we will use it later to provet that a certain ring element is nilpotent!).
(2) Let $\mathfrak{p}$ be a prime ideal of R. Then $S = R \setminus \mathfrak{p}$ is a multiplicative set (in fact, that's the definition of $\mathfrak{p}$ being prime). We let $R_\mathfrak{p} \coloneqq (R \setminus \mathfrak{p})^{-1}R$. The ring $R_\mathfrak{p}$ is called R *localized at* $\mathfrak{p}$.

(a) Example: Let p be a prime number. Then $\mathfrak{p} = (p)$ is a prime ideal of $\mathbb{Z}$, and we may localize $\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z} \quad p \nmid n \right\}$.

Proposition 4.6. *Let M be an R-module. Then $S^{-1}R \otimes_R M \xrightarrow{\sim} S^{-1}M$ as $S^{-1}R$-modules via an isomorphism sending $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$.*

Proof. Define an R-bilinear map $S^{-1}R \times M \to S^{-1}M$ sending $\left(\frac{r}{s}, m\right) \mapsto \frac{rm}{s}$. It gives rise to an R-linear map $\varphi\colon S^{-1}R \otimes M \to S^{-1}M$ such that $\varphi\left(\frac{r}{s} \otimes m\right) = \frac{rm}{s}$. It is clear that φ is surjective, and easy to check that it is $S^{-1}R$-linear (and not just R-linear). We now show that φ is injective. First, we show that every tensor $t = \sum_{i=1}^{\ell} \frac{r_i}{s_i} \otimes m_i$ in $S^{-1}R \otimes_R M$ is pure. Let $s = s_1 \cdots s_\ell$ and $t_i = \prod_{j \in \{1,\ldots,\ell\} \setminus \{i\}} s_j$. Then

$$\begin{aligned} t &= \sum_{i=1}^{\ell} \left(\frac{t_i}{s}\right) \otimes r_i m_i \\ &= \sum_{i=1}^{\ell} \frac{1}{s} \otimes t_i r_i m_i \\ &= \frac{1}{s} \otimes \sum_{i=1}^{\ell} t_i r_i m_i \ . \end{aligned}$$

Thus, it suffices to check injectivity on pure tensors of the form $\frac{1}{s} \otimes m$. If $\varphi\left(\frac{1}{s} \otimes m\right) = \frac{0}{1}$ then $\frac{m}{s} = \frac{0}{1}$, and thus $um = 0$ for some $u \in S$. Thus $\frac{1}{s} \otimes m = \frac{u}{us} \otimes m = \frac{1}{us} \otimes um = 0$. □

Let S be a multiplicative subset of R. We have defined $S^{-1}(\cdot)$ of an R-module M. We have seen that $S^{-1}R \otimes_R M \cong S^{-1}M$ as $S^{-1}R$-modules. But $S^{-1}R \otimes (\cdot)$ is a functor, acting not only on R-modules, but also on R-linear maps. So we can also make $S^{-1}(\cdot)$ into a functor, by defining $S^{-1}f$ in the way that makes the following diagram commute for every R-linear map $f\colon N \to N'$:

$$\begin{tikzcd} S^{-1}R \otimes_R N \arrow[r, "\mathrm{id}_{S^{-1}R} \otimes f"] \arrow[d, "\frac{r}{s} \otimes n \mapsto \frac{rn}{s}"] & S^{-1}R \otimes_R N' \arrow[d, "\frac{r}{s} \otimes n' \mapsto \frac{rn'}{s}"] \\ S^{-1}N \arrow[r, "S^{-1}f"] & S^{-1}N' \end{tikzcd}$$

There is just one way to define $S^{-1}f$ that makes this diagram commute (start from $S^{-1}N$, go up-right-down). That is $\frac{n}{s} \mapsto \frac{1}{s} \otimes n \mapsto \frac{1}{s} \otimes f(n) \mapsto \frac{f(n)}{s'}$. That is $\left(S^{-1}f\right)\left(\frac{n}{s}\right) = \frac{f(n)}{s}$. This is an $S^{-1}R$-linear map because we defined it as the composition of three $S^{-1}R$-linear maps. Since $S^{-1} \otimes_R (f \circ g) = \big(\left(S^{-1}R\right) \otimes f\big) \circ \big(\left(S^{-1}R\right) \otimes g\big)$, we have $S^{-1}(f \circ g) = \left(S^{-1}f\right) \circ \left(S^{-1}g\right)$.

Remark 4.7. **[non-examinable]** In category-theoretic terminology, we have shown that the functors $S^{-1}R \otimes_R (\cdot)$ and $S^{-1}(\cdot)$ (both from the category of R-modules to the category of $S^{-1}R$-modules) are *naturally isomorphic.* A natural isomorphism between functors is a collection of isomorphisms between objects, that satisfies a certain property as a collection. In our case, the natural isomorphism is $(\varepsilon_M)_M$ (M runs over all R-modules), where each $\varepsilon_M \colon S^{-1}R \otimes_R M \to S^{-1}M$ is an $S^{-1}R$-linear isomorphism, $\varepsilon_M\big(\frac{r}{s} \otimes m\big) = \frac{rm}{s}$, such that for every R-linear map $f \colon N \to N'$ the following diagram commutes:

$$\begin{tikzcd}
S^{-1}R \otimes_R N \arrow[r, "S^{-1}R\otimes f"] \arrow[d, "\varepsilon_N"] & S^{-1}R \otimes_R N' \arrow[d, "\varepsilon_{N'}"] \\
S^{-1}N \arrow[r, "S^{-1}f"] & S^{-1}N'
\end{tikzcd}$$

The commutativity of this diagram is clear because we defined $S^{-1}f$ in order for this diagram to commute, but this was a good opportunity to mention the notion of a natural isomorphism. A natural isomorphism is a special case of a natural transformation (where the ε_M are only required to be morphisms, not necessarily isomorphisms).

Remark 4.8. Take an R-algebra A. By the proposition above, we have an $S^{-1}R$-module isomorphism $S^{-1}R \otimes_R A \to S^{-1}A$, $\frac{r}{s} \otimes a \mapsto \frac{ra}{s}$. It is easy to check that this map sends $\frac{1}{1} \otimes 1 \mapsto \frac{1}{1}$ and respects multiplication, and so it is an $S^{-1}R$-algebra isomorphism. We also know that $S^{-1}R \otimes_R (\cdot)$ takes R-algebra homomorphisms to $S^{-1}R$-algebra homomorphisms. Since $S^{-1}(\cdot)$ of a morphism was defined via $S^{-1}R \otimes_R (\cdot)$, we deduce that $S^{-1}(\cdot)$ also takes an R-algebra homomorphism to an $S^{-1}R$-algebra homomorphism.

We've seen that restriction of scalars followed by extension of scalars does not, in general, result in the original module. However, the following lemma says that in the case of $S^{-1}R \otimes_R (\cdot)$, applied to an $S^{-1}R$-module M, the result is isomorphic to M as an $S^{-1}R$-module.

Lemma 4.9. *Let $S \subset R$ be a multiplicative subset. Let M be an $S^{-1}R$-module. Write $S^{-1}M$ for the module resulting from restricting scalars in M from $S^{-1}R$ to R, and then localizing with S. Then $M \xrightarrow{\sim} S^{-1}M$ as $S^{-1}R$-modules via a map sending $m \mapsto \frac{m}{1}$ (and $\frac{1}{s}m \mapsfrom \frac{m}{s}$). Equivalently, $M \xrightarrow{\sim} S^{-1}R \otimes_R M$ as $S^{-1}R$-modules via a map sending $m \mapsto 1 \otimes m$ (and $\frac{r}{s}m \mapsfrom \frac{r}{s} \otimes m$).*

Proof. The map $m \mapsto \frac{m}{1} \colon M \to S^{-1}M$ is $S^{-1}R$-linear. For $\frac{m}{s} \in S^{-1}M$, we have $\frac{1}{s}m \mapsto \frac{1}{s} \cdot m = \frac{m}{s}$, proving surjectivity. To prove injectivity: if $\frac{m}{1} = \frac{0}{1}$ in

$S^{-1}M$ then $um = 0$ in M for some $u \in S$. But M is an $S^{-1}R$-module, and so we deduce that $\underbrace{\frac{1}{u}um}_{=m} = 0$. □

We have seen that $S^{-1}R$ is characterized by a universal property. The same is true for $S^{-1}M$. We have an R-linear map $\iota_{S^{-1}M}\colon M \to S^{-1}M$ given by $\iota_{S^{-1}M}(m) = \frac{m}{1}$. The universal property can be expressed succintly as $\operatorname{Hom}_R(M, L) \cong \operatorname{Hom}_{S^{-1}R}\big(S^{-1}M, L\big)$ for every $S^{-1}R$-module L (with a natural isomorphism between the sets, see below):

Proposition 4.10. *Let S be a multiplicative subset of R, and let M be an R-module. Consider an R-linear map $f\colon M \to L$, where L is an $S^{-1}R$-module. Then there is a unique $S^{-1}R$-linear map $h\colon S^{-1}M \to L$ such that $f = h \circ \iota_{S^{-1}M}$.*

Furthermore if (T, j) is a pair of $S^{-1}R$-module T and R-linear map $j\colon M \to T$ satisfyng the same universal property, then $S^{-1}M \xrightarrow{\sim} T$ by the $S^{-1}R$-module isomorphism sending $\frac{m}{s} \mapsto \frac{1}{s}j(m)$.

Proof. Since the functors $S^{-1}(\cdot)$ and $S^{-1}R \otimes_R (\cdot)$ are naturally isomorphic, we can prove the claim for the pair $\big(S^{-1}R \otimes_R M, \iota\big)$, for the R-linear map, $\iota\colon M \to S^{-1}R \otimes_R M$, $\iota(m) = 1 \otimes m$ instead of the pair $\big(S^{-1}M, \iota_{S^{-1}M}\big)$. We have an R-linear map $f\colon M \to L$, L an $S^{-1}R$-module. Define $h = \mathrm{id}_{S^{-1}R} \otimes f\colon S^{-1}R \otimes_R M \to \underbrace{S^{-1}R \otimes_R L}_{\cong L}$ (where Lemma 4.9 was used). As a map into L, h is given by $h\big(\frac{r}{s} \otimes m\big) = \frac{r}{s}f(m)$. Then $h\left(\underbrace{\iota(m)}_{=1\otimes m}\right) = f(m)$ as desired. The uniqueness of the $S^{-1}R$-linear map h follows from the fact the tensors of the form $1 \otimes m$ generate $S^{-1}R \otimes_R M$ as an $S^{-1}R$-module.

The proof of the uniqueness of $\big(S^{-1}R \otimes_R M, \iota\big)$ is left to the reader. □

Recall that a functor that preserves all exact sequences of length 3 must preserve all exact sequences.

Proposition 4.11 (Exactness of $S^{-1}(\cdot)$)**.** *If $A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence of R-modules then so is $S^{-1}A \xrightarrow{S^{-1}f} S^{-1}B \xrightarrow{S^{-1}g} S^{-1}C$. Equivalently, $S^{-1}R \otimes_R (\cdot)$ is an exact functor from the category of R-modules to the category of $S^{-1}R$-modules. Equivalently, $S^{-1}R$ is a flat R-module*[12].

[12] It is clear that $S^{-1}R$ is a flat $S^{-1}R$-module since every ring is flat as a module over itself. Here we have a stronger statement. For example, $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

Proof. Clearly $\operatorname{im} S^{-1}f \subset \ker S^{-1}g$ because $\left(S^{-1}g\right) \circ \left(S^{-1}f\right) = S^{-1}\left(\underbrace{f \circ g}_{=0}\right)$. Now, take $\frac{b}{s} \in \ker S^{-1}g$. Then $\frac{g(b)}{s} = \frac{0}{1}$. That is, $\underbrace{ug(b)}_{=g(ub)} = 0$ for some $u \in S$, i.e. $ub \in \ker g = \operatorname{im} f$. Take $a \in A$ such that $f(a) = ub$. Then $\frac{b}{s} = \frac{f(a)}{us} = \left(S^{-1}f\right)\left(\frac{a}{us}\right) \in \operatorname{im} S^{-1}f$. □

Remark 4.12. Let S be a multiplicative subset of R. Let M be an R-module and N an R-submodule. Consider the inclusion map $\iota\colon N \hookrightarrow M$, and apply S^{-1}. The exactness of $S^{-1}(\cdot)$ implies that $S^{-1}N \to S^{-1}M$, $\frac{n}{s} \mapsto \frac{n}{s}$, is injective. It is convenient that the notation $\frac{n}{s}$ for an element of $S^{-1}N$ is the same as the notation for an element of $S^{-1}M$ whose numerator happens to be in N. So we shall treat $S^{-1}N$ as an $S^{-1}R$-submodule of M. Equivalently, the flatness of $S^{-1}R$ as an R-module implies that $\mathrm{id}_{S^{-1}R} \otimes N \to \mathrm{id}_{S^{-1}R} \otimes M$ is injective, and so we can think of elements of $S^{-1}R \otimes_R N$ (expressed as sums of pure tensors) as elements of $S^{-1}R \otimes_R M$. We've seen in Example 3.8, in the general case of a tensor product of submodules, that the situtation is not as nice in the absence of flatness.

Remark 4.13. For the next proposition, recall that for an R-module M and submodules N_1 and N_2, we write $N_1 + N_2$ for the submodule of M consisting of all elements of the form $n_1 + n_2$, $n_1 \in N_1$ and $n_2 \in N_2$. We have a surjective R-linear map $\varphi\colon N_1 \oplus N_2 \to N_1 + N_2$ sending $(n_1, n_2) \mapsto n_1 + n_2$ whose kernel is $\{(n, -n) \mid n \in N_1 \cap N_2\}$. Thus, we say that the sum $N_1 + N_2$ is *direct* if $N_1 \cap N_2 = \{0\}$ because then φ is an isomorphism. In this case, we refer to $N_1 + N_2$ as an *internal direct sum* (as opposed to the *external direct sum* $N_1 \oplus N_2$). More generally, a sum $N_1 + \cdots + N_\ell$ of submodules of M is *direct* if the natural surjective R-linear map $N_1 \oplus \cdots \oplus N_\ell \to N_1 + \cdots + N_\ell$ is injective (equivalently, $(N_1 + \cdots + N_i) \cap N_{i+1} = \{0\}$ for all $1 \leq i < \ell$). The sums in the following proposition are not assumed to be direct.

Proposition 4.14. *Let N, P be submodules of an R-module M. Then (see Remark 4.12 to recall why we can write $=$):*

(1) *$S^{-1}(N + P) = S^{-1}N + S^{-1}P$.*
(2) *$S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.*
(3) *$S^{-1}M/S^{-1}N \xrightarrow{\sim} S^{-1}(M/N)$ as $S^{-1}R$-modules by a map sending $\frac{m}{s} + S^{-1}N \mapsto \frac{m+N}{s}$ (and $\frac{m}{s} + S^{-1}N \leftarrow\!\shortmid \frac{m+N}{s}$).*

Proof. (1) The LHS consists of all elements of $S^{-1}M$ of the form $\frac{n+p}{s}$, $n \in N$, $p \in P$, $s \in S$, while the RHS consists of all elements of the form $\frac{n}{s_1} + \frac{p}{s_2}$. These sets are equal.

(2) If $x \in S^{-1}N \cap S^{-1}P$ then $x = \frac{n}{s_1} = \frac{p}{s_2}$, $n \in N$, $p \in P$, $s_1, s_2 \in S$. Hence, $u(s_2n - s_1p) = 0$ for some $u \in S$. So $w := \underbrace{us_2n}_{\in N} = \underbrace{us_1p}_{\in P}$ is in $N \cap P$, and thus $x = \frac{n}{s_1} = \frac{w}{us_1s_2} \in S^{-1}(N \cap P)$. The reverse inclusion is clear.

(3) Apply the exact functor S^{-1} to the short exact sequence

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

to obtain the exact sequence

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

Now $\big(S^{-1}\iota\big)\big(S^{-1}N\big)$ is exactly $S^{-1}N$, viewed as a submodule of $S^{-1}M$. Furthermore, the map $S^{-1}\pi$ sends $\frac{m}{s}$ to $\frac{m+N}{s}$. That is, the kernel of the map $S^{-1}M \to S^{-1}(M/N)$, $\frac{m}{s} \mapsto \frac{m+N}{s}$, is exactly $S^{-1}N$, and the result follows. □

Proposition 4.15. *Let S be a multiplicative subset of a ring R, and let M, N be R-modules. Then $S^{-1}M \otimes_{S^{-1}R} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_R N)$ as $S^{-1}R$-modules by a map sending $\frac{m}{s_1} \otimes \frac{n}{s_2} \mapsto \frac{m \otimes n}{s_1 s_2}$.*

In particular, if $\mathfrak{p}$ is a prime ideal of R then $M_\mathfrak{p} \otimes_{R_\mathfrak{p}} N_\mathfrak{p} \cong (M \otimes_R N)_\mathfrak{p}$.

Proof.

$$\big(S^{-1}R \otimes_R M\big) \otimes_{S^{-1}R} \big(S^{-1}R \otimes N\big) \cong S^{-1}R \otimes_R (M \otimes_R N)$$

as $S^{-1}R$-modules by Corollary 3.30, sending $\Big(\frac{r_1}{s_1} \otimes m\Big) \otimes \Big(\frac{r_2}{s_2} \otimes n\Big) \mapsto \frac{r_1 r_2}{s_1 s_2} \otimes (m \otimes n)$. Using the natural isomorphism $S^{-1}R \otimes_R M \to S^{-1}M$, $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$, the result follows. □

4.3. Extension and contraction under the localization map $R \to S^{-1}R$.

For a ring homomorphism $f\colon A \to B$, recall that:

(1) We have a contraction map $\mathfrak{b} \mapsto \underbrace{f^{-1}(\mathfrak{b})}_{=:\mathfrak{b}^c}$ ($\mathfrak{b}$ an ideal of B), and $\mathfrak{b}^c$ is an ideal of A.

(2) We have an extension map $\mathfrak{a} \mapsto \underbrace{(f(\mathfrak{a}))}_{=:\mathfrak{a}^e}$ ($\mathfrak{a}$ an ideal of A), i.e. $\mathfrak{a}^e$ is the ideal of B generated by the image of $\mathfrak{a}$ under f.

(3) For every prime ideal $\mathfrak{b}$ of B, the ideal $\mathfrak{b}^c$ is also prime[13].

(4) A *contracted ideal* of A is an ideal of the form $\mathfrak{b}^c$ for an ideal $\mathfrak{b}$ of B. An *extended ideal* of B is an ideal of the form $\mathfrak{a}^e$, $\mathfrak{a}$ an ideal of A.

(5) From Example Sheet 1:

[13] Indeed, the kernel of the composite map $A \xrightarrow{f} B \longrightarrow B/\mathfrak{b}$ is $\mathfrak{b}^c$, and so $A/\mathfrak{b}^c$ embeds in the integral domain $B/\mathfrak{b}$, and thus $A/\mathfrak{b}^c$ is an integral domain.

(a) An ideal $\mathfrak{a}$ of A is contracted $\Leftrightarrow$ $\mathfrak{a} = \mathfrak{a}^{ec}$ (while $\mathfrak{a} \subset \mathfrak{a}^{ec}$ holds for every $\mathfrak{a}$).

(b) An ideal $\mathfrak{b}$ of B is extended $\Leftrightarrow$ $\mathfrak{b} = \mathfrak{b}^{ce}$ (while $\mathfrak{b} \supset \mathfrak{b}^{ce}$ holds for every $\mathfrak{b}$).

(c) We have a bijective correspondence

$$\{ \text{ contracted ideals of } A\} \leftrightarrow \{ \text{ extended ideals of } B \ \}$$

given by $\mathfrak{a} \mapsto \mathfrak{a}^e$ and $\mathfrak{b}^c \hookleftarrow \mathfrak{b}$.

Let S be a multiplicative subset of R. Recall the localization map $R \to S^{-1}R$, $r \mapsto \frac{r}{1}$. Extensions and contractions will be taken below with respect to this map (denoted $()^e$ and $()^c$, respectively). We have explicit formulas for the extension and contraction under the localiztion map:

(1) **Extension:** For an ideal $\mathfrak{a}$ of R,

$$\mathfrak{a}^e = \underbrace{S^{-1}\mathfrak{a}}_{=\left\{\frac{a}{s}\in S^{-1}R \mid a\in\mathfrak{a},\ s\in S\right\}} .$$

The RHS is formed by thinking of $\mathfrak{a}$ as an R-submodule of R, and applying $S^{-1}(\cdot)$. The equality follows since both $\mathfrak{a}^e$ and $S^{-1}\mathfrak{a}$ are equal to the smallest ideal of $S^{-1}R$ containing $\left\{\frac{a}{1} \mid a \in \mathfrak{a}\right\}$ (check!).

(a) Thus $\mathfrak{a}^{ec} = \bigcup_{s\in S} \underbrace{(\mathfrak{a} : s)}_{=\{r\in R \mid rs\in\mathfrak{a}\}}$. Indeed, if r is in the RHS then $rs = a$ (in R) for some $s \in S$, $a \in \mathfrak{a}$, and thus $\frac{rs}{1} = \frac{a}{1}$ (in $S^{-1}R$), that is, $\frac{r}{1} = \underbrace{\frac{a}{s}}_{\in\mathfrak{a}^e}$, i.e. $r \in \mathfrak{a}^{ec}$. In the other direction, if r is in the LHS then $\frac{r}{1} = \frac{a}{s}$ (in $S^{-1}R$) for some $a \in \mathfrak{a}$, $s \in S$, and so $u(rs - a) = 0$ for some $u \in S$, and thus $rus = ua \in \mathfrak{a}$, and hence $r \in \left(\mathfrak{a} : \underbrace{us}_{\in S}\right)$.

(2) **Contraction:** For an ideal $\mathfrak{b}$ of $S^{-1}R$:

$$\mathfrak{b}^c = \left\{r \in R \mid \frac{r}{1} \in \mathfrak{b}\right\}$$

(this is just the definition).

(a) Thus $\mathfrak{b}^{ce} = \mathfrak{b}$: $\subset$ holds for every ring homomorphism (not just $R \to S^{-1}R$). Now, take $\frac{r}{s} \in \mathfrak{b}$. Then $\frac{r}{1} \in \mathfrak{b}$. Thus $r \in \mathfrak{b}^c$. Hence $\frac{r}{1} \in \mathfrak{b}^{ce}$. So $\frac{r}{s} \in \mathfrak{b}^{ce}$.

Below we will write $\operatorname{spec} R$ for the set of prime ideals of a ring R.

Proposition 4.16. *Consider the localization map $R \to S^{-1}R$, $r \mapsto \frac{r}{1}$ (which is a ring homomorphism). Then:*

(1) *Every ideal of $S^{-1}R$ is extended.*

(2) *An ideal $\mathfrak{a}$ of R is contracted if and only if the image $\overline{S}$ of S in $R/\mathfrak{a}$ contains no zero divisors.*

(3) $\mathfrak{a}^e = S^{-1}R$ *if and only if* $\mathfrak{a} \cap S \neq \emptyset$.

(4) *We have a bijection*

$$\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \operatorname{spec} S^{-1}R$$

given by $\mathfrak{p} \mapsto \mathfrak{p}^e$ *and* $\mathfrak{q}^c \mapsfrom \mathfrak{q}$.

Proof. 1) Follows since $\mathfrak{b} = \mathfrak{b}^{ce}$.

2) $\mathfrak{a}$ is contracted $\Leftrightarrow \underbrace{\mathfrak{a}^{ec}}_{=\bigcup_{s\in S}(\mathfrak{a}:s)} \subset \mathfrak{a} \Leftrightarrow \big(\underbrace{Sr \cap \mathfrak{a} \neq \emptyset}_{\Leftrightarrow (0+\mathfrak{a} \in \overline{S}\cdot(r+\mathfrak{a}))} \Rightarrow \underbrace{r \in \mathfrak{a}}_{\Leftrightarrow r+\mathfrak{a}=0+\mathfrak{a}} \big) \Leftrightarrow$ the image $\overline{S}$ of S in $R/\mathfrak{a}$ has no zero divisors.

3) If $\mathfrak{a} \cap S \neq \emptyset$, take $x \in \mathfrak{a} \cap S$. Then $\mathfrak{a}^e \ni \frac{x}{x} = 1$.
In the other direction, if $1 \in \mathfrak{a}^e$, then $\frac{1}{1} = \frac{a}{s}$ for some $a \in \mathfrak{a}$, $s \in S$, and thus $u(a-s) = 0$ for some $u \in S$, and so $\underbrace{us}_{\in S} = \underbrace{ua}_{\in \mathfrak{a}}$.

4) In general (for every ring homomorphism), the contraction of a prime ideal is a prime ideal. By (2), a prime ideal $\mathfrak{p}$ of R is contracted $\Leftrightarrow$ the image of S in $R/\mathfrak{p}$ contains no zero divisors $\Leftrightarrow \mathfrak{p} \cap S = \emptyset$ (since $R/\mathfrak{p}$ is an integral domain). Thus, $\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \cap S = \emptyset\}$ is the set of contracted prime ideals of R, and the contraction map $\mathfrak{q}^c \mapsfrom \mathfrak{q}\colon \operatorname{spec} R \leftarrow \operatorname{spec} S^{-1}R$ is in fact a map:

$$\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \cap S = \emptyset\} \leftarrow \operatorname{spec} S^{-1}R\ .$$

For $\mathfrak{q} \in \operatorname{spec} S^{-1}R$, we have $\mathfrak{q}^{ce} = \mathfrak{q}$ since every ideal of $S^{-1}R$ is extended. For $\mathfrak{p} \in \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \cap S = \emptyset\}$, we have $\mathfrak{p}^{ec} = \mathfrak{p}$ because $\mathfrak{p}$ is contracted as explained above. It remains to show that $\mathfrak{p}^e$ belongs to $\operatorname{spec} S^{-1}R$ (when $\mathfrak{p} \cap S = \emptyset$)[14]. By (3) we know that $\mathfrak{p}^e$ is a proper ideal of $S^{-1}R$. Now, take $\frac{x_1}{s_1}, \frac{x_2}{s_2} \in S^{-1}R$, $x_1, x_2 \in R$, $s_1, s_2 \in S$, such that $\frac{x_1x_2}{s_1s_2} \in \mathfrak{p}^e$. Then $\frac{x_1x_2}{s_1s_2} = \frac{p}{t}$ for some $p \in \mathfrak{p}$ and $t \in S$, and so $\underbrace{ut}_{\notin \mathfrak{p}} x_1x_2 = \underbrace{us_1s_2p}_{\in \mathfrak{p}}$ for some $u \in S$. Thus $x_1x_2 \in \mathfrak{p}$, and so $x_1 \in \mathfrak{p}$ or $x_2 \in \mathfrak{p}$, and hence $\frac{x_1}{s_1} \in \mathfrak{p}^e$ or $\frac{x_2}{s_2} \in \mathfrak{p}^e$. □

[14] In the lecture, I proved this in a different way. Many thanks to the student who suggested that it's shorter to argue directly. For completeness, here's the proof from the lecture: The strategy is to show that $\big(S^{-1}R\big)/\mathfrak{p}^e$ is an integral domain by showing that it embeds in $\operatorname{Frac}(R/\mathfrak{p})$. The composite map $R \to R/\mathfrak{p} \to \operatorname{Frac}(R/\mathfrak{p})$ sends every element of $S \subset R$ to an invertible element of $\operatorname{Frac}(R/\mathfrak{p})$, and thus gives rise to a ring homomorphism $\varphi\colon S^{-1}R \to \operatorname{Frac}(R/\mathfrak{p})$ given by $\frac{r}{s} \mapsto \frac{r+\mathfrak{p}}{s+\mathfrak{p}}$. We see that the image of φ is contained in the subring $\overline{S}^{-1}(R/\mathfrak{p})$ of $\operatorname{Frac}(R/\mathfrak{p})$, where $\overline{S}$ is the image of S in $R/\mathfrak{p}$. Take $\frac{r}{s} \in S^{-1}R$. Then $\frac{r}{s} \in \ker\varphi \Leftrightarrow \frac{r+\mathfrak{p}}{s+\mathfrak{p}} = \frac{0}{1}$ in $\overline{S}^{-1}(R/\mathfrak{p}) \Leftrightarrow$ there is $u + \mathfrak{p} \in \overline{S}$, $u \in S$, such that $(u+\mathfrak{p})(r+\mathfrak{p}) = 0 \Leftrightarrow ur \in \mathfrak{p}$ for some $u \in S \Leftrightarrow r \in \mathfrak{p}$ (since $\mathfrak{p}$ is prime and $u \notin \mathfrak{p}$). That is, $\ker\varphi = \big\{\frac{r}{s} \mid r \in \mathfrak{p}, s \in S\big\} = \mathfrak{p}^e$, and so φ induces a a ring embedding $\big(S^{-1}R\big)/\mathfrak{p}^e \hookrightarrow \operatorname{Frac}(R/\mathfrak{p})$.

To show an application, we introduce some important definitions.

Definition 4.17. The *radical* of an ideal I of R is $\sqrt{I} = \{r \in R \mid \exists n \geq 1 \;\; r^n \in I\}$.

Any radical (and in particular, the *nilradical* $\operatorname{nil} R \coloneqq \sqrt{(0)}$, consisting of all nilpotent elements of R) is an ideal of R: If $x^n \in I$ and $y^\ell \in I$ then $(x+y)^{n+\ell} \in I$ (since each term in the expansion of $(x+y)^{n+\ell}$ is $x^i y^j$ where $i \geq n$ or $j \geq \ell$). Thus $\sqrt{I}$ is closed under addition, and the rest of the proof is trivial. Note that $I \subset \sqrt{I}$. Note also that if $J \subset I$ are ideals of R then $\sqrt{I/J} = \sqrt{I}/J$ (check!).

Proposition 4.18. $\sqrt{I} = \bigcap_{I \subset \mathfrak{p} \in \operatorname{spec} R} \mathfrak{p}$.

Proof. If $x \in \sqrt{I}$ then $x^n \in I$ for some $n \geq 0$, and so $x^n \in \mathfrak{p}$ for every $\mathfrak{p} \in \operatorname{spec} R$ such that $I \subset \mathfrak{p}$, and thus $x \in \mathfrak{p}$ since $\mathfrak{p}$ is prime.

Now, assume that $x \in R$, $x \notin \sqrt{I}$. Then $I \neq R$, and so $R/I \neq 0$. Write $\overline{x}$ for the image of x in R/I, and consider the localized ring $\underbrace{(R/I)_{\overline{x}}}_{\{\overline{x}^n \mid n \geq 0\}^{-1}(R/I)}$. This ring is nonzero since $\overline{x}$ is not nilpotent (as $x \notin \sqrt{I}$), and so $(R/I)_{\overline{x}}$ has a prime ideal (because every nonzero ring has a maximal ideal). This prime ideal corresponds to a prime ideal of R/I, disjoint from $\{\overline{x}^n \mid n \geq 0\}$. Taking the preimage in R, we obtain a prime ideal $\mathfrak{p}$ of R, containing I and disjoint from $\{x^n \mid n \geq 0\}$, and in particular $x \notin \mathfrak{p}$. □

4.4. Local properties.

Definition 4.19. A ring R is *local* if R has exactly one maximal ideal $\mathfrak{m}$.

When introducing a local ring, we often write $(R, \mathfrak{m})$ to give a name $\mathfrak{m}$ to the unique maximal ideal of R.

Example 4.20. Let $\mathfrak{p} \in \operatorname{spec} R$, and consider $R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1} R$. Write $\mathfrak{p} R_{\mathfrak{p}}$ for the extension $\mathfrak{p}^e$ of $\mathfrak{p}$ to $R_{\mathfrak{p}}$. The prime ideals of $R_{\mathfrak{p}}$ are given (bijectively) by extensions of prime ideals of R contained in $\mathfrak{p}$. In particular, all prime ideals of $R_{\mathfrak{p}}$ are contained in $\mathfrak{p} A_{\mathfrak{p}}$. Thus, $(R_{\mathfrak{p}}, \mathfrak{p} R_{\mathfrak{p}})$ is a local ring. For example, $\mathbb{Z}_{(2)} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z},\; 2 \nmid b\right\}$ is a local ring whose unique maximal ideal is $(2)\mathbb{Z}_{(2)} = \left\{\frac{2a}{b} \mid a, b \in \mathbb{Z},\; 2 \nmid b\right\}$.

For every R-module M, $M_{\mathfrak{p}}$ is a module over the local ring $R_{\mathfrak{p}}$. The purpose of this section is to reduce problems concerning general modules to problems concerning modules over local rings. Later, we will develop tools to deal with modules over local rings (such as Nakayama's Lemma, which is useful for finitely generated modules over local rings).

Remark 4.21. It is instructive to contrast $R_{\mathfrak{p}}$ with $R/\mathfrak{p}$. The prime ideals of $R_{\mathfrak{p}}$ correspond to the prime ideals R that are contained in $\mathfrak{p}$. The prime ideals of $R/\mathfrak{p}$ correspond to the prime ideals of R that contain $\mathfrak{p}$. If $\mathfrak{q} \subset \mathfrak{p}$ are prime ideals of R, then the prime ideals of $R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$ correspond to the prime ideals of R between $\mathfrak{q}$ and $\mathfrak{p}$. The same can be said about[15] $(R/\mathfrak{q})_\mathfrak{p}$. In fact, we have a ring isomorphism $R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p} \to (R/\mathfrak{q})_\mathfrak{p}$, $\frac{r}{s} + \mathfrak{q}R_\mathfrak{p} \mapsto \frac{r+\mathfrak{q}}{s+\mathfrak{q}}$, since localiztion commutes with quotients. If we take $\mathfrak{p} = \mathfrak{q}$ we obtain the ring $\kappa(\mathfrak{p}) \coloneqq R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, which is a field since $\mathfrak{p}R_\mathfrak{p}$ is a maximal ideal of $R_\mathfrak{p}$. We call $\kappa(\mathfrak{p})$ the *residue field* of R at $\mathfrak{p}$. Equivalently, we may set $\kappa(\mathfrak{p}) = (R/\mathfrak{p})_\mathfrak{p} = \operatorname{Frac}(R/\mathfrak{p})$.

Proposition 4.22 (Being zero is a local property)**.** *For an R-module M, the following are equivalent:*

1. $M = 0$.
2. $M_\mathfrak{p} = 0$ *for each prime ideal* $\mathfrak{p}$ *of* R.
3. $M_\mathfrak{m} = 0$ *for each maximal ideal* $\mathfrak{m}$ *of* R.

Proof. (1)⇒(2)⇒(3) is clear. Assume (3). Take $m \in M$. Consider the anni hilator ideal $\operatorname{Ann}_R(m) = \{r \in R \mid rm = 0\}$. It suffices to show that $\operatorname{Ann}_R(M) = R$ because then $1 \in \operatorname{Ann}_R(M)$, i.e. $1 \cdot m = 0$, and so $M = 0$. So it suffices to prove that $\operatorname{Ann}_R(M)$ is not contained in any $\mathfrak{m} \in \operatorname{mspec} R$. Fix $\mathfrak{m} \in \operatorname{mspec} R$, and consider $M_\mathfrak{m} = 0$. There, $\frac{m}{1} = \frac{0}{1}$ and so $um = 0$ for some $u \in R \setminus \mathfrak{m}$, i.e. $u \in \operatorname{Ann}_R(m) \setminus \mathfrak{m}$ and so $\operatorname{Ann}_R(m) \nsubseteq \mathfrak{m}$. □

Remark 4.23. We shall require the following two observations regarding localization: Let $S \subset R$ be a multiplicative set, and $f \colon M \to N$ an R-linear map. Consider the exact sequence $0 \longrightarrow \ker f \longrightarrow M \xrightarrow{f} \operatorname{im} f \longrightarrow 0$. Since $S^{-1}(\cdot)$ is exact, $0 \longrightarrow S^{-1}(\ker f) \longrightarrow S^{-1}M \xrightarrow{S^{-1}f} S^{-1}(\operatorname{im} f) \longrightarrow 0$ is exact, and so:

1. $S^{-1}(\ker f) = \ker\bigl(S^{-1}f\bigr)$, and
2. $S^{-1}(\operatorname{im} f) = \operatorname{im}\bigl(S^{-1}f\bigr)$.

Proposition 4.24 (Exactness is a local property)**.** *For a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ of R-linear maps between R-modules, the following are equivalent:*

1. $A \xrightarrow{f} B \xrightarrow{g} C$ *is exact.*
2. $A_\mathfrak{p} \xrightarrow{f_\mathfrak{p}} B_\mathfrak{p} \xrightarrow{g_\mathfrak{p}} C_\mathfrak{p}$ *is exact for each prime ideal* $\mathfrak{p}$ *of* R.
3. $A_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} B_\mathfrak{m} \xrightarrow{g_\mathfrak{m}} C_\mathfrak{m}$ *is exact for each maximal ideal* $\mathfrak{m}$ *of* R.

Proof. (1) implies (2) since localization is an exact functor (Proposition 4.11), and clearly (2) implies (3).

[15] To be formal, we should write $(R/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$ for the localization of the ring $R/\mathfrak{q}$ at the prime ideal $\mathfrak{p}/\mathfrak{q}$, but we may also regard $R/\mathfrak{q}$ as an R-module, localize to $\mathfrak{p}$ to obtain the $R_\mathfrak{p}$-module $(R/\mathfrak{q})_\mathfrak{p}$, and define the ring structure on $(R/\mathfrak{q})_\mathfrak{p}$ in the natural way - the result is isomorphic to $(R/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$

Assume (3). Then $[\operatorname{im}(g \circ f)]_{\mathfrak{m}} = \operatorname{im}((g \circ f)_{\mathfrak{m}}) = \operatorname{im}(g_{\mathfrak{m}} \circ f_{\mathfrak{m}}) = 0$ for every $\mathfrak{m} \in \operatorname{mspec} R$. Thus $\operatorname{im}(g \circ f) = 0$ by Proposition 4.22, i.e. $g \circ f = 0$, namely $\operatorname{im} f \subset \ker g$. Now $(\ker g / \operatorname{im} f)_{\mathfrak{m}} \cong (\ker g)_{\mathfrak{m}} / (\operatorname{im} f)_{\mathfrak{m}} = (\ker g_{\mathfrak{m}})/(\operatorname{im} f_{\mathfrak{m}}) = 0$ for every $\mathfrak{m} \in \operatorname{mspec} R$, and thus $\ker g / \operatorname{im} f = 0$ by Proposition 4.22, i.e. $\operatorname{im} f = \ker g$. □

We have the following immediate corollary:

Proposition 4.25 (Injectivity and surjectivity are local properties)**.** *For an R-linear map $f \colon M \to N$, the following conditions are equivalent:*

(1) *$f \colon M \to N$ is injective.*
(2) *$f_{\mathfrak{p}} \colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every $\mathfrak{p} \in \operatorname{spec} R$.*
(3) *$f_{\mathfrak{m}} \colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for every $\mathfrak{m} \in \operatorname{mspec} R$.*

and similary for "surjective" instead of "injective".

Proposition 4.26 (Flatness is a local property)**.** *Let M be an R-module. Then TFAE:*

(1) *M is a flat R-module.*
(2) *$M_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \operatorname{spec} R$.*
(3) *$M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module for all $\mathfrak{m} \in \operatorname{mspec} R$.*

Proof. (1)⇒(2): We know that $M_{\mathfrak{p}} \cong R_{\mathfrak{p}} \otimes_R M$ as $R_{\mathfrak{p}}$-modules, and we know that extension of scalars preserves flatness (Proposition 3.43).

(2)⇒(3): Every maximal ideal is prime.

(3)⇒(1): Take an injective R-linear map $f \colon N \to P$. Take $\mathfrak{m} \in \operatorname{mspec} R$. Then $f_{\mathfrak{m}} \colon N_{\mathfrak{m}} \to P_{\mathfrak{m}}$ is injective since injectivity is a local property. Thus $f_{\mathfrak{m}} \otimes \operatorname{id}_{M_{\mathfrak{m}}} \colon N_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} \to P_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}}$ is injective by the assumption that $M_{\mathfrak{m}}$ is flat. So $(N \otimes_R M)_{\mathfrak{m}} \to (P \otimes_R M)_{\mathfrak{m}}$ is injective[16]. Since this is true for every $\mathfrak{m} \in \operatorname{mspec} R$, and since injectivity is a local property, we deduce that $N \otimes_R M \to P \otimes_R M$ is injective. □

Remark 4.27. One may ask: Is it always enough to verify local properties on maximal (rather than prime) ideals? The answer is yes for every reasonable property, where a property $\mathcal{P}$ of modules is reasonable[17] if the following always holds: (I) For every a ring R, if M and N are isomorphic R-modules, then M has $\mathcal{P}$ if and only if N has $\mathcal{P}$, and (II) For every pair of isomorphic rings $R' \xrightarrow{\sim} R$ and R-module M, if M has $\mathcal{P}$ as an R-module then M has $\mathcal{P}$ as an R'-module.

If you want to, prove that for a reasonable module property $\mathcal{P}$ and an R-module M, if $M_{\mathfrak{m}}$ has $\mathcal{P}$ for all $\mathfrak{m} \in \operatorname{mspec} R$ then M has $\mathcal{P}$. You can

[16] by the isomorphism $S^{-1}R \otimes_R (N \otimes_R M) \cong (S^{-1}R \otimes_R N) \otimes_{S^{-1}R} (S^{-1}R \otimes_R M)$, $S = R \setminus \mathfrak{m}$, and similarly for $P \otimes_R M$

[17] I haven't seen this terminology used outside this remark.

also define what it means for a property of linear maps to be reasonable (basically the same: say that R_1-linear maps $f\colon M_1 \to N_1$ and $g\colon M_2 \to N_2$ are isomorphic if the sequences $M_1 \xrightarrow{f} N_1$ and $M_2 \xrightarrow{g} N_2$ are isomorphic, and imitate reasonability for module properties).

Remark 4.28. A property that passes from M to $M_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{spec} R$ is called *localizable.* A property that holds for M whenever it holds for $M_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{spec} R$ is called *local-to-global.* So, a property is local if and only if it is both localizable and local-to-global.

Here's a famous example that illustrates the use of local properties. It will be stated and proved in the next example class. In a future example sheet, you will use this result to find an interesting example.

Proposition 4.29. ***[Covered in Example Class 2]*** *Let R be a ring such that:*

1. *$R_\mathfrak{m}$ is a noetherian ring for all $\mathfrak{m} \in \operatorname{mspec} R$.*
2. *$|\{\mathfrak{m} \in \operatorname{mspec} R \mid x \in \mathfrak{m}\}| < \infty$ for every $0 \neq x \in R$.*

Then R is noetherian[18].

Proof. Take an ideal $0 \neq \mathfrak{a}$ of R. We want to show that $\mathfrak{a}$ is finitely generated. It suffices to find a finitely generated ideal $\mathfrak{b} \subset \mathfrak{a}$ of R such that $\underbrace{\mathfrak{a}R_\mathfrak{m}}_{=\mathfrak{a}_\mathfrak{m}} = \underbrace{\mathfrak{b}R_\mathfrak{m}}_{\mathfrak{b}_\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{mspec} R$. Indeed, if that's the case then consider the inclusion map $\iota\colon \mathfrak{b} \hookrightarrow \mathfrak{a}$ (as an R-linear map between R-modules). We have that $\iota_\mathfrak{m}\colon \mathfrak{b}_\mathfrak{m} \to \mathfrak{a}_\mathfrak{m}$ is an equality (in particular, surjective) for all $\mathfrak{m} \in \operatorname{mspec} R$. Thus ι is surjective (as surjectivity is a local property), and so $\mathfrak{a} = \mathfrak{b}$, and thus $\mathfrak{a}$ is finitely generated.
Fix $0 \neq x \in \mathfrak{a}$. We partition $\operatorname{mspec} R$ as a union of 3 subsets:

$$M_1 = \{\mathfrak{m} \in \operatorname{mspec} R \mid x \notin \mathfrak{m}\}$$

$$M_2 = \{\mathfrak{m} \in \operatorname{mspec} R \mid x \in \mathfrak{m} \quad \mathfrak{a} \not\subset \mathfrak{m}\}$$

$$M_3 = \{\mathfrak{m} \in \operatorname{mspec} R \mid \mathfrak{a} \subset \mathfrak{m}\}$$

For $\mathfrak{m} \in M_1$, we have $(x) \not\subset \mathfrak{m}$ and $\mathfrak{a} \not\subset \mathfrak{m}$, and so $(x)R_\mathfrak{m} = R_\mathfrak{m} = \mathfrak{a}R_\mathfrak{m}$.
For $\mathfrak{m} \in M_2$, fix $x^{(\mathfrak{m})} \in \mathfrak{a} \setminus \mathfrak{m}$. Then $\big(x^{(\mathfrak{m})}\big) \not\subset \mathfrak{m}$ and $\mathfrak{a} \not\subset \mathfrak{m}$, and so $\big(x^{(m)}\big)R_\mathfrak{m} = R_\mathfrak{m} = \mathfrak{a}R_\mathfrak{m}$.
For $\mathfrak{m} \in M_3$, the ideal $\mathfrak{a}R_\mathfrak{m}$ is finitely generated (since $R_\mathfrak{m}$ is noetherian) by some $\frac{a_1}{s_1}, \dots, \frac{a_\ell}{s_\ell}$, $a_i \in \mathfrak{a}$, $s_i \in R \setminus \mathfrak{m}$. Then $\mathfrak{a}R_\mathfrak{m}$ is also generated by $\frac{a_1}{1}, \dots, \frac{a_\ell}{1}$.
Let $\mathfrak{a}^{(\mathfrak{m})} = \underbrace{(a_1, \dots, a_\ell)}_{\subset \mathfrak{a}}$. Then $\mathfrak{a}^{(\mathfrak{m})}R_\mathfrak{m} = \mathfrak{a}R_\mathfrak{m}$.

[18] There are non-noetherian rings A such that $A_\mathfrak{m}$ is noetherian for all $\mathfrak{m} \in \operatorname{mspec} A$. That is, the second condition cannot be dropped.

Let $\mathfrak{b} = \underbrace{(x)}_{\subset\mathfrak{a}} + \sum_{\mathfrak{m}\in M_2} \underbrace{\left(x^{(\mathfrak{m})}\right)}_{\subset\mathfrak{a}} + \sum_{\mathfrak{m}\in M_3} \underbrace{\mathfrak{a}^{(\mathfrak{m})}}_{\subset\mathfrak{a}}$. Then $\mathfrak{b}R_\mathfrak{m} = \mathfrak{a}R_\mathfrak{m}$ for all $\mathfrak{m} \in \operatorname{mspec} R$. By our hypothesis, M_2 and M_3 are finite sets (their union is the set of maximal ideals of R that contain x). Thus $\mathfrak{b}$ is the finite sum of finitely generated ideals, and so $\mathfrak{b}$ is finitely generated.

□

Example 4.30 (Freeness is not a local property)**.** An R-module M is *locally free* if $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module for all $\mathfrak{p} \in \operatorname{spec} R$. Take $R = \mathbb{C}\times\mathbb{C}$. Then[19], $\operatorname{spec} R = \left\{ \underbrace{\mathbb{C}\times\{0\}}_{=:\mathfrak{p}_1}, \underbrace{\{0\}\times\mathbb{C}}_{=:\mathfrak{p}_2} \right\}$. What is $R_{\mathfrak{p}_1}$? It is $S^{-1}(\mathbb{C}\times\mathbb{C})$ for $S = \mathbb{C}\times(\mathbb{C}\setminus\{0\})$. The ring homomorphism $\mathbb{C}\times\mathbb{C}\to\mathbb{C}$ given by $(x,y)\mapsto y$ maps all elements of S to units, and thus we have a ring homorphism $\varphi\colon R_{\mathfrak{p}_1}\to\mathbb{C}$, $\varphi\left(\frac{(x,y)}{(a,b)}\right) = \frac{y}{b}$. Clearly φ is surjective. Its kernel consists of all elements of the form $\frac{(x,0)}{(a,b)}$. But elements of the latter form are equal to $\frac{0}{1}$ since $\underbrace{(0,1)}_{\in S}\cdot(x,0) = 0$. Thus φ is an isomorphism, and $R_{\mathfrak{p}_1}\cong\mathbb{C}$ as rings. Similarly, $R_{\mathfrak{p}_2}\cong\mathbb{C}$. That is, R is locally a field (in fact, locally $\mathbb{C}$). Thus, every R-module is locally a vector space (in particular, locally free). If we can find one R-module M that is not free, then M will be locally free but not free.

Consider $M = \mathbb{C}\times\{0\}$. Then M is an ideal of R, and hence an R-module. But M is not free: For all $(x,0)\in M$ we have $(0,1)\cdot(x,0) = 0$, and so the empty set $\emptyset$ is the only R-linearly independent subset of M, but it clearly does not span M.

Remark 4.31. **[non-examinable]** It is more interesting to see an example of an integral domain R and a non-free locally free R-module M: The ideal $M = \left(2, 1+\sqrt{-5}\right)$ of the integral domain $R = \mathbb{Z}\left[\sqrt{-5}\right]$ is projective (since it is a direct summand of $R\oplus R$), and thus $M_\mathfrak{p}$ is a projective $R_\mathfrak{p}$-module for each $\mathfrak{p}\in\operatorname{spec} R$. But projective modules over local rings are free, and thus M is locally free. However, M is not free because it is an ideal of R which is not principal (we've seen that if $x\in A$ is not a zero divisor, A a ring, then $a\mapsto ax\colon A\to(x)$ is an R-linear isomorphism, and thus (x) is free of rank 1; it is clear that the ideal (0) of A is free of rank 0; it is a fact that these are the only examples of ideals of A that are free - can you prove this?).

[19] In general, the ideals in a finite product $\prod_{i=1}^n R_i$ of rings are exactly the subsets $\prod_{i=1}^n I_i$, where I_i is an ideal of R_i. The prime ideals of $\prod_{i=1}^n R_i$ are exactly $\prod_{i=1}^n I_i$ as above, where I_{i_0} is prime for one i_0, and $I_i = R_i$ for all $i\neq i_0$. You should prove this if you haven't seen this in a more basic course.

We have discussed local properties of modules. What about rings?

Example 4.32. A ring R is *reduced* if 0 is the only nilpotent element of R (i.e. $\sqrt{(0)} = (0)$ in R). You will show in the example sheet that if R is a ring such that $R_{\mathfrak{p}}$ is reduced for all $\mathfrak{p} \in \operatorname{spec} R$ then R is reduced. However, being an integral domain is not a local property of rings.

4.5. **The localiztion of a ring as a quotient.** Let S be the multiplicative closure of a subset U of R. We constructed $S^{-1}R$ as a set of equivalence classes. Here we give another construction satisfying the same universal property (thus the new construction is necessarily isomorphic to $S^{-1}R$).

Consider the R-algebra $R\big[\{T_u\}_{u\in U}\big]$. This is a polynomial R-algebra with one variable T_u for each element of U. Now consider the quotient

$$R_U = R\big[\{T_u\}_{u\in U}\big] / \underbrace{\big(\{uT_u - 1\}_{u\in U}\big)}_{=:I_U} .$$

This is the quotient of our R-algera by the ideal I_U generated by the elements of the form $uT_u - 1$, $u \in U$. The image $\overline{u}$ and $\overline{T_u}$ of u and T_u in R_U satisfy $\overline{u} \cdot \overline{T_u} = 1$. In this sense, R_U is obtained from R by "adding inverses" to the elements of U. We will see that $R_U \cong S^{-1}R$ as rings.

We have a ring homomorphism $\iota\colon R \to R_U$ sending $r \mapsto r + I_U$. Take a ring homomorphism $f\colon R \to A$ such that $f(u)$ is a unit for each $u \in U$. We want to show that there is exactly one ring homomorphism $h\colon R_U \to A$ that makes the following diagram commute:

$$\begin{tikzcd}
R \arrow[r, "\iota"] \arrow[dr, "f"] & R_U \arrow[d, dashed, "h"] \\
 & A
\end{tikzcd}$$

We can think of R_U and A as R-algebras via ι and f, respectively. Then, the diagram commutes if and only if the ring homomorphism h is an R-algebra homomorphism. We claim that there is exactly one R-algebra homomorphism $R_U \to A$. Indeed, an R-algebra homomorphism $R\big[\{T_u\}_{u\in U}\big] \to A$ is determined uniquely by the images of $\{T_u\}_{u\in U}$ (and must send $r \mapsto f(r)$ for all $r \in R$), while R-algebra homomorphisms $R_U \to A$ correspond to R-algebra homomorphisms $\Phi\colon R\big[\{T_u\}_{u\in U}\big] \to A$ that vanish on $\{uT_u - 1\}_{u\in U}$, i.e. $\Phi(T_u) = (\Phi(u))^{-1}$ for all $u \in U$, i.e. $\Phi(T_u) = (f(u))^{-1}$. There is exactly one such Φ since f is given. Thus there is exactly one R-algebra homomorphism $h\colon R_U \to A$. It is given by $h(p + I_U) = \Big(p \mid_{T_u \leftarrow (f(u))^{-1}}\Big)$ for all $p \in R\big[\{T_u\}_{u\in U}\big]$. Thus the pair (R_U, ι) satisfies the universal property of $\big(S^{-1}R, \iota_{S^{-1}R}\big)$, and so $R_U \cong S^{-1}R$ by a ring isomorphism sending

$p + I_U \mapsto p\,|_{T_u \leftarrow (f(u))^{-1}}$ and $r\prod_{i=1}^{\ell}(T_{u_i} + I_U) \mapsfrom \frac{r}{u_1 \cdots u_\ell}$. Clearly, this ring isomorphism is an R-algebra isomorphism (viewing R_U and $S^{-1}R$ as R-algebras via ι and $\iota_{S^{-1}R}$, respectively).

An important special case is when $U = \{u\}$ consists of a single element. Then $S = \{u^n \mid n \geq 0\}$ and we denote $S^{-1}R$ by R_u as before. We record our conclusion in this special case:

Lemma 4.33. *Let $u \in R$. Then*

$$\underbrace{R_u}_{:=\{u^n \mid n \geq 0\}^{-1}R} \xrightarrow{\sim} R[T]/(uT - 1)$$

by an R-algebra isomorphism sending $\frac{r}{u^n} \mapsto rT^n + (uT - 1)$ and $p\big(\frac{1}{u}\big) \mapsfrom p + (uT - 1)$, $p \in R[T]$.

Remark 4.34. For each of $M \otimes_R N$ and for $S^{-1}R$, we have constructions by means of a quotient of a huge object by another huge object. To construct $M \otimes_R N$ we took the quotient a huge free module by a huge submodule. In the case of $S^{-1}R$ we took (here in this subsection) the quotient of a huge polynomial algebra by a huge ideal. The quotient in each case was shown to satisfy a universal property. In these two cases, the universal properties were useful in order to understand morphisms from $M \otimes_R N$ and $S^{-1}R$ into other objects. But it is useful to have additional constructions of the same objects. In the case of $M \otimes_R N$, we studied a set of tools to understand $M \otimes_R N$ explicitly in special cases. In the case of $S^{-1}R$, we started in fact with the more explicit construction (in terms of equivalence classes on pairs). The explicit construction of $S^{-1}R$ allowed us, for example, to study extension and contraction of ideals for the localization map $R \to S^{-1}R$ (this would have been difficult to do directly using the universal property, which deals with morphisms from $S^{-1}R$ to other rings).

5. Nakayama's lemma

Nakayama's lemma is a simple yet powerful tool for studying finitely generated modules. It is particularly useful for finitely generated modules over local rings.

Proposition 5.1 (Cayley–Hamilton)**.** *Let M be a finitely generated R-module. Let $f \colon M \to M$ be an R-linear map. Let $\mathfrak{a}$ be an ideal of R such that*[20] *$f(M) \subset \mathfrak{a}M$. Then there is $n \geq 1$ and $a_1, \ldots, a_n \in \mathfrak{a}$ such that*

$$f^n + a_1 f^{n-1} + \cdots + a_n f^0 = 0$$

[20] $\mathfrak{a}M$ is the submodule of M generated by $\{am \mid a \in \mathfrak{a}, m \in M\}$

(an equality in $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$*, where* f^k *is* f *composed with itself* k *times).*

Proof. Take a generating set $\{m_1, \dots, m_n\}$ for the R-module M. Each element of $\mathfrak{a}M$ is an $\mathfrak{a}$-linear combination of $m_1, \dots, m_n$. Since $f(M) \subset \mathfrak{a}M$, we have

$$\begin{pmatrix} f(m_1) \\ \vdots \\ f(m_n) \end{pmatrix} = P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \tag{5.1}$$

for some matrix $P \in M_{n\times n}(R)$ with entries in $\mathfrak{a}$.

The R-module M is defined by some structure ring homomorphism $\rho\colon R \to \operatorname{End} M$. This makes $\operatorname{End} M$ into a (noncommutative) R-algebra. An R-algebra homomorphism $R[T] \to \operatorname{End} M$ is determined by the image of T, and every choice of image for T extends to an R-algebra homomorphism[21]. We send T to f. Thus M becomes an $R[T]$-module, where R acts on M as before, and $Tm = f(m)$ for all $m \in M$.

Then (5.1) can be written in the form:

$$T \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} . \tag{5.2}$$

That is, the matrix $Q := T \cdot I_n - P \in M_{n\times n}(R[T])$ satisfies $Q \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$, where $I_n \in M_{n\times n}(R[T])$ is the identity matrix. Multiplying both sides by the adjugate matrix $\operatorname{adj} Q$ on the left, we have $(\det Q) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$. Thus, $\left(\underbrace{\det Q}_{\in R[T]}\right) m = 0$ for all $m \in M$ (since $m_1, \dots, m_n$ generate the R-module M). In other words, the image of $\deg Q \in R[T]$ in $\operatorname{End} M$, obtained by substituting f for T, is the zero endomorphism. But $\det Q$ is a monic degree-n polynomial, where the coefficients of $T^0, \dots, T^{n-1}$ are in $\mathfrak{a}$ (since the entries of P are in $\mathfrak{a}$). □

[21] If we wanted to generate an R-algebra homomorphism $R[T_1, \dots, T_n] \to B$ for some non-commutative ring B, we would have to make sure that the images of $T_1, \dots, T_n$ commute. But with only one variable this is not an issue.

Corollary 5.2. *Let M be a finitely generated R-module, and let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{a}M = M$. Then there is $a \in \mathfrak{a}$ such that $am = m$ for all $m \in M$.*

Proof. Apply Proposition 5.1 with $f = \mathrm{id}_M$. Then $(1 + a_1 + \cdots + a_n)\,\mathrm{id}_M = 0$ in $\mathrm{End}_R(M)$, $a_i \in \mathfrak{a}$. Set $a = -(a_1 + \cdots + a_n)$. □

Definition 5.3. The *Jacobson radical* $J(R)$ of the ring R is the intersection of all maximal ideals of R.

Example 5.4.

(1) For a local ring $(R, \mathfrak{m})$, $J(R) = \mathfrak{m}$.
(2) $J(\mathbb{Z}) = \{0\}$ (0 is the only integer divisible by all prime numbers).

Proposition 5.5. *$x \in J(R)$ if and only if $1 - xy$ is a unit in R for all $y \in R$.*

Proof. If there is $y \in R$ such that $1 - xy$ is not a unit, then $1 \notin (1 - xy)$, and so $(1 - xy) \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R. If $x \in J(R)$ then $x \in \mathfrak{m}$ and so $\underbrace{x + (1 - xy)}_{=1} \in \mathfrak{m}$, a contradiction.

If $x \notin J(R)$ then $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R, and thus $\mathfrak{m} + (x) = R$, i.e. $t + xy = 1$ for some $t \in \mathfrak{m}$ and $y \in R$. Thus, $1 - xy = t \in \mathfrak{m}$, and so $1 - xy$ is not a unit. □

Proposition 5.6 (Nakayama's lemma)**.** *Let M be a finitely generated R-module, and $\mathfrak{a} \subset J(R)$ an ideal of R such that $\mathfrak{a}M = M$. Then $M = 0$.*

Proof. By Corollary 5.2, there is $a \in J(R)$ such that $am = m$ for all $m \in M$, i.e. $(1 - a)m = 0$. By Proposition 5.5, $1 - a$ is a unit of R, and thus $m = 0$ (for all $m \in M$). □

Corollary 5.7. *Let M be a finitely generated R-module, $N \subset M$ a submodule, $\mathfrak{a} \subset J(R)$ an ideal of R such that $\mathfrak{a}M + N = M$. Then*[22] *$N = M$.*

Proof. We have $\mathfrak{a}(M/N) = \left(\underbrace{\mathfrak{a}M + N}_{=M}\right)/N = M/N$, and so $M/N = 0$ by Proposition 5.6. □

As you can see, the larger the Jacobson radical - the more useful Nakayama's lemma is. It is most useful for a local ring $(R, \mathfrak{m})$ since $J(R) = \mathfrak{m}$ is very large. You will study further applications of Nakayama's lemma in Example Sheet 3, and also later in the course. For example, you will be asked to prove that if M is a finitely generated module over a local ring $(R, \mathfrak{m})$ and

[22] I remember this corollary as "$J(R)M$ is small when M is finitely generated". It is small in the sense that $J(R)M + P$ will never be all of M if P is a proper submodule of M.

$\{x_1 + \mathfrak{m}M, \dots, x_n + \mathfrak{m}M\}$ is a spanning set for the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, then $\{x_1, \dots, x_n\}$ generates M. This is useful because often vector spaces are easier to understand than more general modules.

6. Integral and finite extensions (Part I)

Definition 6.1. Let A be an R-algebra. An element $x \in A$ is *integral over R* (or *R-integral*) if there is a monic polynomial $f \in R[T]$ such that $f(x) = 0$.

Recall that $x \in A$ is R-algebraic if there is a polynomial (not necessarily monic) $f \in R[T]$ such that $f(x) = 0$. So every integral element is algebraic.

Example 6.2.

(1) If K is a field and A is a K-algebra, then $x \in A$ is K-integral if and only if x is K-algebraic.

(2) Later we will show that:

  (a) The set of $\mathbb{Z}$-integral elements in $\mathbb{Q}$ is exactly $\mathbb{Z}$. But all elements of $\mathbb{Q}$ are $\mathbb{Z}$-algebraic (indeed, for $a, \underbrace{b}_{\neq 0} \in \mathbb{Z}$, $\frac{a}{b}$ is a root of $bT - a \in \mathbb{Z}[T]$).

  (b) The set of $\mathbb{Z}$-integral elements in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

  (c) The set of $\mathbb{Z}$-integral elements of $\mathbb{Q}(\sqrt{5})$ is $\underbrace{\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]}_{\supsetneq \mathbb{Z}[\sqrt{5}]}$.

Definition. An R-module M is *faithful* if the structural ring homomorphism $R \to \operatorname{End} M$ of M is injective (i.e. for every $0 \neq r \in R$ there is $m \in M$ such that $rm \neq 0$).

Example 6.3. If $R \subset A$ are rings then A is an R-algebra, and so A is also an R-module. In fact, A is a faithful R-module: If $0 \neq r \in R$ then $r \cdot 1_A = r \neq 0$.

Lemma 6.4. *Let $R \subset A$ be rings and $x \in A$. Considering $R[x] \subset A$, we see that A is also an $R[x]$-module. Then x is R-integral if and only if there is $M \subset A$ such that both of the following condition hold:*

i) *M is a faithful $R[x]$-submodule of A, i.e.,*

  (a) *M is an R-submodule of A.*

  (b) *$xM \subset M$.*

  (c) *For all $0 \neq p \in R[x]$ there is $m \in M$ such that $pm \neq 0$.*

ii) *M is finitely generated as an R-module.*

Proof. First, assume that (i) and (ii) hold. Since $xM \subset M$, we have an R-linear map $f\colon M \to M$, $f(m) = xm$. Since M is finitely generated over R,

Cayley–Hamilton gives us:

$$f^n + r_1 f^{n-1} + \ldots + r_n f^0 = 0 \qquad (\text{in } \operatorname{End}_R M) \tag{6.1}$$

for some $r_1, \ldots, r_n \in R$, $n \geq 1$. Take any $m \in M$ and evaluate both sides of (6.1) at m:

$$\big(x^n + r_1 x^{n-1} + \cdots + r_n x^0\big)m = 0\ . \tag{6.2}$$

Since (6.2) holds for all $m \in M$, and since M is faithful as an $R[x]$-module, this means that

$$x^n + r_1 x^{n-1} + \cdots + r_n x^0 = 0\ ,$$

that is, x is R-integral.

In the other direction, assume that x is R-integral. Then $x^n + r_1 x^{n-1} + \ldots + r_n x^0 = 0$ for some $n \geq 1$ and $r_1, \ldots, r_n \in R$. Thus, the finitely generated R-submodule $M = \operatorname{span}_R\{x^0, \ldots, x^{n-1}\}$ of A satisfies $xM \subset M$ (since $x \cdot x^{n-1} = -\big(r_1 x^{n-1} + \ldots + r_n x^0\big)$). That is, M is an $R[x]$-submodule of A. Furthermore, M is a faithful $R[x]$-module because $\underbrace{1_A}_{=x^0} \in M$ and $p \cdot 1_A = p \neq 0$ for all $0 \neq p \in R[x]$. □

Definition 6.5. Let A be an R-algebra.

(1) A is *integral* (over R) if every $a \in A$ is R-integral.
(2) A is *finite* (over R) if A is finitely generated as an R-module.

Proposition 6.6. *Let A be an R-algebra. The following conditions are equivalent:*

i) *A is a finitely generated integral R-algebra.*
ii) *A is generated as an R-algebra by a finite set of R-integral elements.*
iii) *A is a finite R-algebra.*

Proof. (i) ⇒ (ii): Clear.

(ii) ⇒ (iii): Let $\alpha_1, \ldots, \alpha_m \in A$ be R-integral elements that generate A as an R-algebra. Then $A = \operatorname{span}_R\{\alpha_1^{e_1} \cdots \alpha_m^{e_m} \mid e_i \geq 0\}$. Since each α_i is R-integral, we have

$$\alpha_i^{n_i} + r_{i,1}\alpha_i^{n_i - 1} + \ldots + r_{i,n_i}\alpha_i^0 = 0$$

for some $n_i \geq 1$, $r_{i,1}, \ldots, r_{i,n_i} \in R$ (for each $1 \leq i \leq m$). Thus $\alpha_i^{n_i} \in \operatorname{span}_R\Big\{\alpha_i^{n_i-1}, \ldots, \alpha_i^0\Big\}$. Hence (check!) $\alpha_1^{e_1} \cdots \alpha_m^{e_m} \in \operatorname{span}_R \underbrace{\Big\{\alpha_1^{f_1} \cdots \alpha_m^{f_m} \mid 0 \leq f_i \leq n_i - 1\Big\}}_{=:S}$ for all $e_1, \ldots, e_m \geq 0$. Thus the finite set S generates A as an R-module.

(iii) ⇒ (i): Since A is finitely generated as an R-module, it is also finitely generated as an R-algebra (by the same generating set). It remains to show that every $\alpha \in A$ is R-integral. Write $\rho\colon R \to A$ for the structure homomorphism of A as an R-algebra, and consider its image $\rho(R) \subset A$ and the subring $(\rho(R))[\alpha]$ of A. Then A is a $(\rho(R))[\alpha]$-module. In fact, $1 \in A$ and so A is a faithful $(\rho(R))[\alpha]$-module (as discussed above), finitely generated as an R-module, and thus α is $\rho(R)$-integral by Lemma 6.4 (and hence α is R-integral: check!). □

Proposition 6.7. *Let A be an R-algebra, and let $\mathcal{O}$ be the set of R-integral elements of A. Then $\mathcal{O}$ is an R-subalgebra of A.*

Proof. If $x, y \in \mathcal{O}$ then the R-subalgebra generated by $\{x, y\}$ is R-integral by Proposition 6.6[(ii)⇒(i)]. Thus $x + y, xy \in \mathcal{O}$ and $\{r \cdot 1_A\}_{r\in R} \subset \mathcal{O}$. So $\mathcal{O}$ is an R-subalgebra of A. □

Proposition 6.8 (Transitivity of finiteness and integrality)**.** *Let $A \subset B \subset C$ be rings.*

i) *If C is finite over B and B is finite over A, then C is finite over A.*
ii) *If C is integral over B and B is integral over A, then C is integral over A.*

Proof. (i) Write $C = \operatorname{span}_B\{\gamma_1, \dots, \gamma_n\}$, $\gamma_i \in C$, $n \geq 1$, and $B = \operatorname{span}_A\{\beta_1, \dots, \beta_\ell\}$, $\beta_i \in B$, $\ell \geq 1$. Take $c \in C$. Then $c = b_1\gamma_1 + \cdots + b_n\gamma_n$, $b_i \in B$, and $b_i = a_{i,1}\beta_1 + \cdots + a_{i,\ell}\beta_\ell$, $a_i \in A$. So $c = \sum_{i=1}^n \sum_{j=1}^\ell a_{ij}\gamma_i\beta_j$. So $C = \operatorname{span}_A\{\gamma_i\beta_j \mid i \leq n,\ j \leq \ell\}$, and thus C is finite over A.

(ii) Let $c \in C$. We need to show that c is A-integral. There is a monic polynomial $f = T^n + b_1T^{n-1} + \cdots + b_nT^0 \in B[T]$, $n \geq 1$, $b_i \in B$, such that $f(c) = 0$. Then $f \in \underbrace{A[b_1, \dots, b_n]}_{=:A'}$, and so c is integral over A'. By Proposition 6.6[(ii)⇒(iii)], $A'[c]$ is finite over A', and A' is finite over A. Thus $A'[c]$ is finite over A by (i). Thus c is integral over A by Proposition 6.6[(iii)⇒(i)]. □

Definition 6.9. Let A be a ring.

(1) If $A \subset B$ (rings):
   (a) The *integral closure*[23] of A in B is $\overline{A} = \{b \in B \mid b \text{ is integral over } A\}$.
   (b) A is *integrally closed* in B if $\overline{A} = A$.
(2) If A is an integral domain:
   (a) The *integral closure* of A is the integral closure of A in $\operatorname{Frac} A$.
   (b) A is *integrally closed* if A is integrally closed in $\operatorname{Frac} A$.

Example 6.10. $\mathbb{Z}[\sqrt{5}]$ is not integrally closed because $\alpha = \frac{(1+\sqrt{5})}{2} \in \underbrace{\mathbb{Q}\left(\sqrt{5}\right)}_{=\operatorname{Frac}(\mathbb{Z}[\sqrt{5}])} \setminus \mathbb{Z}[\sqrt{5}]$ is a root of $T^2 - T - 1$, and is thus $\mathbb{Z}[\sqrt{5}]$-integral.

[23] By Proposition 6.7, $\overline{A}$ is an A-subalgebra of B.

However, $\mathbb{Z}$ and $k[T_1, \ldots, T_n]$ are integrally closed by the following proposition.

Proposition 6.11. *Every unique factorization domain*[24] *is integrally closed.*

Proof. Let A be a UFD. Take $x \in \operatorname{Frac}(A) \setminus A$. Then $x = \frac{a}{b}$ for $a, b \in A$, $b \neq 0$**,** such that $p \mid b$, $p \nmid a$ for some prime element p of A. If x is integral over A then

$$(a/b)^n + a_1(a/b)^{n-1} + \ldots + a_n(a/b)^0 = 0$$

for some $a_1, \ldots, a_n \in A$. On multiplying by b^n, we see that:

$$a^n = -b\big(a_1 a^{n-1} b^0 - \ldots - a_n a^0 b^{n-1}\big)\ .$$

Thus $p \mid a^n$ and so $p \mid a$, a contradiction. □

Lemma 6.12. *For rings $A \subset B$, the integral closure $\overline{A}$ of A in B is integrally closed in B.*

Proof. If $x \in B$ is integral over $\overline{A}$ then $A \subset \overline{A} \subset \overline{A}[x]$ are both integral extensions (for the second inclusion, use Proposition 6.6[(ii)⇒(i)]). Thus $A \subset \overline{A}[x]$ is an integral extension by Proposition 6.8. So x is A-integral, and thus $x \in \overline{A}$ by the definition of $\overline{A}$. □

Proposition 6.13. *Let $A \subset B$ be rings. Then:*

i) *If B is integral over A:*
  (a) *$B/\mathfrak{b}$ is integral*[25] *over $A/\underbrace{\mathfrak{b}^c}_{=\mathfrak{b}\cap A}$ for every ideal $\mathfrak{b}$ of B.*
  (b) *$S^{-1}B$ is integral*[26] *over $S^{-1}A$ for every multiplicative subset $S \subset A$.*

ii) *If $\overline{A}$ is the integral closure of A in B and $\overline{S^{-1}A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$, then $\overline{S^{-1}A} = S^{-1}\overline{A}$.*
(from this (i-b) follows immediately, but the proof will use (i-b))

[24] Recall that A is a UFD if A is an integral domain such that every $0 \neq x \in A$ can be written as a product of irreducible elements, and this representation of x is unique up to reordering and multiplying the factors by units. Recall: In a UFD an element is irreducible if and only if it is prime.

[25] The composite ring homomorphism $A \hookrightarrow B \twoheadrightarrow B/\mathfrak{b}$ has kernel $\mathfrak{b}^c = \mathfrak{b} \cap A$, and thus gives rise to an injective map $A/\mathfrak{b}^c \to B/\mathfrak{b}$.

[26] Here S is a multiplicative subset of A, and so also of B. In general, the image of a multiplicative subset under a ring homomorphism is multiplicative.

Let's be extremely pedantic regarding why we can view $S^{-1}A$ as a subring of $S^{-1}B$ given what we've proved previously (we've only discussed a similar thing in relation to modules, not rings): View A and B as A-modules. Then we've seen that $S^{-1}A \to S^{-1}B$, $\frac{a}{s} \mapsto \frac{a}{s}$ is an injective $S^{-1}A$-linear map, and clearly this injective function is a ring homomorphism.

Proof. (i-a) Write $\iota\colon A/\mathfrak{b}^c \to B/\mathfrak{b}$ for the natural inclusion $\iota(a+\mathfrak{b}^c) = a+\mathfrak{b}$. Take $b+\mathfrak{b} \in B/\mathfrak{b}$. Then $b^n + a_1 b^{n-1} + \cdots + a_n b^0 = 0$ for some $n \geq 1$, $a_i \in A$. Reduce modulo $\mathfrak{b}$:

$$(b+\mathfrak{b})^n + \underbrace{(a_1+\mathfrak{b})}_{=\iota(a_1+\mathfrak{b}^c)}(b+\mathfrak{b})^{n-1} + \cdots + \underbrace{(a_n+\mathfrak{b})}_{=\iota(a_n+\mathfrak{b}^c)}(b+\mathfrak{b})^0 = 0$$

and so $b+\mathfrak{b}$ is integral over $A/\mathfrak{b}^c$.

(i-b) Take $\frac{b}{s} \in S^{-1}B$. Then $b^n + a_1 b^{n-1} + \cdots + a_n b^0 = 0$ for some $n \geq 1$, $a_i \in A$. Apply the localization map $B \to S^{-1}B$, $b \mapsto \frac{b}{1}$, and then multiply by $\frac{1}{s^n}$:

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \frac{a_1}{s^2}\left(\frac{b}{s}\right)^{n-2} + \cdots + \frac{a_n}{s^n}\left(\frac{b}{s}\right)^0 = 0 \ ,$$

that is, $\frac{b}{s}$ is integral over $S^{-1}A$.

(ii) By (i-b), $S^{-1}\overline{A}$ is integral over $S^{-1}A$. Now, take $\frac{b}{s} \in S^{-1}B$, integral over $S^{-1}A$. Then

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_1}{s_1}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_n}{s_n}\right)\left(\frac{b}{s}\right)^0 = \frac{0}{1}$$

for some $n \geq 1$, $a_i \in A$, $s_i \in S$. Let $t = s_1 \cdots s_n$, and multiply both sides by $(st)^n$:

$$\frac{\overbrace{(tb)^n + \left(\frac{t^1}{s_1}s^1 a_1\right)(tb)^{n-1} + \cdots + \left(\frac{t^n}{s_n}s^n a_n\right)(tb)^0}^{=:a}}{1} = \frac{0}{1}$$

and so there is $u \in S$ such that $ua = 0$. Thus $u^n a = 0$ and so

$$(utb)^n + \left(u^1\frac{t^1}{s_1}s^1 a_1\right)(utb)^{n-1} + \cdots + \left(u^n\frac{t^n}{s_n}s^n a_n\right)(utb)^0 = 0 \ .$$

So $utb \in \overline{A}$, and so $\frac{b}{s} = \frac{utb}{uts} \in S^{-1}\overline{A}$. □

Lemma 6.14. *Let $A \subset B$ be an integral extension of rings. Then:*

i) $A \cap B^\times = A^\times$ *(where $R^\times$ is the group of units of a ring R).*

ii) *If A and B are integral domains:*
B is a field if and only if A is a field.

Proof. (i) The $\supset$ inclusion is clear. To prove $\subset$, take $a \in A \cap B^\times$. Then there is $b \in B$ such that $ba = 1$, and we want to show that $b \in A$. Since b is integral over A, there are $a_1, \ldots, a_n \in A$ such that $b^n + a_1 b^{n-1} + \ldots + a_n b^0 = 0$. Multiply both sides by a^{n-1} to see that $b + \underbrace{a_1 + a_2 a + a_3 a^2 + \cdots + a_n a^{n-1}}_{\in A} = 0$, and thus $b \in A$.

(ii) If B is a field then, using (i), $A^\times = A \cap B^\times = A \cap (B \setminus \{0\}) = A \setminus \{0\}$, and thus A is a field.

Assume that A is a field. Take $0 \neq b \in B$. We need to show that b has an inverse in B. Since b is integral over A, there are $a_1, \ldots, a_n \in A$, with $n \geq 1$ minimal, such that

$$b^n + a_1 b^{n-1} + \ldots + a_n b^0 = 0 \ .$$

That is,

$$b \left(\underbrace{b^{n-1} + a_1 b^{n-2} + \ldots + a_{n-1}}_{=:\Delta} \right) = -a_n \ .$$

Now, $\Delta \neq 0$ by the minimality of n, and $b \neq 0$ by assumption. Thus $a_n \neq 0$ because B is an integral domain, and so a_n has an inverse $a_n^{-1} \in A$ because A is a field. Thus $b\big(-a_n^{-1}\Delta\big) = 1$. □

Corollary 6.15. *For an integral extension of rings $A \subset B$ and a prime ideal $\mathfrak{q}$ of B, $\mathfrak{q} \cap A$ is a maximal ideal of A if and only if $\mathfrak{q}$ is a maximal ideal of B.*

Proof. The kernel of the composition $A \hookrightarrow B \to B/\mathfrak{q}$ is $\mathfrak{q} \cap A$ and hence induces an embedding $A/(\mathfrak{q} \cap A) \hookrightarrow B/\mathfrak{q}$. Now, $\mathfrak{q} \cap A$ is a prime ideal of A, and so $A/(\mathfrak{q} \cap A)$ and $B/\mathfrak{q}$ are integral domains. Also, $B/\mathfrak{q}$ is integral over $A/(\mathfrak{q} \cap A)$ by Proposition 6.13 since B is integral over A. By Proposition 6.14, $A/(\mathfrak{q} \cap A)$ is a field $\Leftrightarrow$ $B/\mathfrak{q}$ is a field. Hence $\mathfrak{q} \cap A$ is maximal $\Leftrightarrow$ $\mathfrak{q}$ is maximal. □

7. Noether's Normalization Theorem and Hilbert's Nullstellensatz

7.1. **Noether's normalization theorem.**

Definition 7.1. Let A be an algebra over a field k. Then $x_1, \ldots, x_n \in A$ are *k-algebraically independent* if $p(x_1, \cdots, x_n) \neq 0$ for every nonzero polynomial $p \in k[T_1, \ldots, T_n]$.

Equivalently, $x_1, \cdots, x_n$ are k-algebraically independent if the k-algebra homomorphism $k[T_1, \ldots, T_n] \to A$, $T_i \mapsto x_i$, is injective (and is thus an isomorphism $k[T_1, \ldots, T_n] \xrightarrow{\sim} k[x_1, \ldots, x_n]$, where $k[x_1, \ldots, x_n]$ is the k-subalgebra of A generated by $x_1, \cdots, x_n$).

Theorem 7.2 (Noether's normalization theorem)**.** *Let $A \neq 0$ be a finitely generated algebra over a field k. Then there are k-algebraically independent $x_1, \ldots, x_n \in A$, $n \geq 0$, such that A is finite over $A' := k[x_1, \ldots, x_n]$.*

Example 7.3 (Example of the proof method)**.** Consider[27] $A = k\big[T, T^{-1}\big]$, k a field. Then $k[T] \subset k\big[T, T^{-1}\big]$ is not a finite extension. Indeed, T^{-1} is not integral over $k[T]$: If T^{-1} were integral over $k[T]$ then $\big(T^{-1}\big)^n \in$

[27] $k\big[T, T^{-1}\big] \cong k[X, Y]/(XY - 1)$ as k-algebras.

$\mathrm{span}_{k[T]}\Big\{\big(T^{-1}\big)^0, \dots, \big(T^{-1}\big)^{n-1}\Big\}$ for some $n \geq 1$, and so, multiplying by T^n, we have $1 \in \mathrm{span}_{k[T]}\big\{T^n, T^{n-1}, \dots, T^1\big\}$, a contradiciton.

However, choose a scalar $c \in k$. Then the set $\big\{T, T^{-1} - cT\big\}$ generates A as a k-algebra since $T^{-1} = cT + \big(T^{-1} - cT\big)$. We will show that $k\big[T^{-1} - cT\big] \subset \underbrace{k\big[T, T^{-1}\big]}_{= k[T^{-1} - cT][T]}$ is a finite extension (unless we are very unlucky in the choice of c). We just need to show that T is integral over $k\big[T^{-1} - cT\big]$ (by Proposition 6.6). Our method is:

(1) Consider the equation $T^{-1}T - 1 = 0$, holding in the algebra $k\big[T, T^{-1}\big]$.

(2) Express the equation in the variables $\big\{T, T^{-1} - cT\big\}$ rather than $\big\{T, T^{-1}\big\}$ by subtracting and adding cT to T^{-1}:
$$\big(\big(T^{-1} - cT\big) + cT\big)T - 1 = 0 \ .$$

(3) Expand the parentheses:
$$\underbrace{c}_{\in k} T^2 + \underbrace{\big(T^{-1} - cT\big)}_{\in k[T^{-1} - cT]} T - \underbrace{1}_{\in k[T^{-1} - cT]} = 0 \ .$$

(4) As long as we choose $c \neq 0$, we can divide by c and see that T is integral over $k\big[T^{-1} - cT\big]$.

The proof of Noether's normalization theorem relies on the idea above, together with an induction on the number of generators of A.

Proof of Noether's normalization theorem. We give a proof that assumes that the field k is infinite[28].

Proof strategy: Induction on the minimal number of generators of A as a k-algebra.

Base case (0 generators): $A = k$. Set $n = 0$, $A' = A$.

Induction step: Assume that $\{x_1, \dots, x_m\} \subset A$ generates A as a k-algebra, and that the theorem holds when A is generated as a k-algebra by a set with less than m elements.

If $x_1, \dots, x_m$ are algebraically independent over k, we are done. Otherwise, we shall see that $\exists c_1, \dots, c_{m-1} \in k$ such that x_m is integral over the k-subalgebra $B = k[x_1 - c_1 x_m, \dots, x_{m-1} - c_{m-1} x_m]$ of A. Then A is finite over B because $A = B[x_m]$. By the induction hypothesis, B is finite over some $A' = k[z_1, \dots, z_n]$, where $z_1, \dots, z_n \in B$ are algebraically independent over k. Thus A is finite over A' by the transitivity of finiteness.

Remains to show **Claim:** $\exists c_1, \dots, c_{m-1} \in k$ such that x_m is integral over B. **Proof of claim:** Take a polynomial $0 \neq f \in k[T_1, \dots, T_m]$, $r \coloneqq \deg f$, such that $f(x_1, \dots, x_m) = 0$ (f exists since $x_1, \dots, x_m$ are not algebraically

[28] See Mumford's Red Book or Wikipedia for Nagata's proof that works for every field.

independent over k). Write f as the sum of its homogeneous parts (e.g., $f = \left(T_1^2T_2 + 3T_2^3\right) + (2T_1T_3 + T_2T_3) + (T_2 + T_3) + 1$). Let F be the part degree r (the highest degree).

For $c_1, \dots, c_{m-1} \in k$ (to be chosen later), we have

$$\underbrace{f(T_1 + c_1T_m, \dots, T_{m-1} + c_{m-1}T_m, T_m)}_{=:g(T_1,\dots,T_m)} = F(c_1, \dots, c_{m-1}, 1)T_m^r$$
$$+ \{\text{terms of degree} < r \text{ in } T_m\}$$

Above, the coefficient $F(c_1, \dots, c_{m-1}, 1)$ of T_m^r is in k, while those of the lower powers of T_m are in $k[T_1, \dots, T_{m-1}]$.

We have defined a polynomial $g \in k[T_1, \dots, T_m]$ such that

$$g(x_1 - c_1x_m, \dots, x_{m-1} - c_{m-1}x_m, x_m) = f(x_1, \dots, x_m) = 0 \ .$$

Treating g as a polynomial in T_m over $k[T_1, \dots, T_{m-1}]$, the coefficient of T_m^r in g is the scalar $F(c_1, \dots, c_{m-1}, 1) \in k$, and the degree of g is at most r. Thus x_m is integral over B if $F(c_1, \dots, c_{m-1}, 1) \neq 0$.

Luckily, $F(T_1, \dots, T_{m-1}, 1)$ is not the zero polynomial because $F(T_1, \dots, T_m)$ is a nonzero homomogeneous polynomial[29]. Thus $\exists c_1, \dots, c_{m-1} \in k$ such that $F(c_1, \dots, c_{m-1}, 1) \neq 0$ (since k is an infinite field[30]). □

Remark 7.4. The proof above of Theorem 7.2 shows that for a finitely generated k-algebra $A = k[t_1, \cdots, t_\ell]$ (k an infinite field), there is a matrix $P = \begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix} \in M_{\ell\times\ell}(k)$ such that, for the elements $x_1, \dots, x_\ell \in A$ given by $\begin{pmatrix} x_1 \\ \vdots \\ x_\ell \end{pmatrix} = P \begin{pmatrix} t_1 \\ \vdots \\ t_\ell \end{pmatrix}$, we have $A = k[x_1, \dots, x_\ell]$ (since P is invertible), $x_1, \dots, x_n$ are k-algebraically independent for some $0 \le n \le \ell$, and A is finite over $k[x_1, \dots, x_n]$. **[non-examinable from here to the end of this remark]** The proof gives the feeling that "almost" every P works (at each step of the induction, we only needed to take scalars that are not a root of a certain nonzero polynomial - almost every choice of scalars works by Schwartz–Zippel). Arguing more carefully (but still according to the general strategy of the proof given above), one can show that there is a polynomial h in the $\binom{\ell}{2}$ variables corresponding the entries above the diagonal in P, such that if P is upper triangular with 1-s on the diagonal and $h(P) \neq 0$ then $x_1, \dots, x_n$ are k-algebraically independent for some $n \geq 0$, and A is finite over $k[x_1, \dots, x_n]$. In this situation, we say that a *general* P works

[29] You've seen this in Example Sheet 1, and showed that homogeneousity is needed.

[30] You've seen this too in Example Sheet 1: The Schwartz–Zippel Lemma.

(people often say *generic* instead of general) to mean that all P work except for the zeros of some nonzero polynomial. This kind of genarality can often be related to the notion of a generic point of a scheme. This polynomial h exists for any field k (even a finite field), but if k is finite and too small, it is possible that there is no P with $h(P) \neq 0$. It is not much harder to give a proof of Noether's normalization theorem that works over any field: the linear change of variables is replaced by a polynomial change of variables. See Nagata's proof in Mumford's Red Book or on Wikipedia.

Remark 7.5. **[non-examinable]** For algebras over, say, $\mathbb{C}$, the geometric meaning of Noether's normalization theorem is as follows: Let X be an algebraic subset of $\mathbb{A}^n_{\mathbb{C}}$. Consider the map $X \hookrightarrow \mathbb{A}^n_{\mathbb{C}} \xrightarrow{T} \mathbb{A}^n_{\mathbb{C}} \xrightarrow{\pi} \mathbb{A}^d_{\mathbb{C}}$, where T is a $\mathbb{C}$-linear isomorphism and π is the projection map $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_d)$, $d = \dim X$. The theorem says that for most T (in particular, for at least one T), the resulting map $X \to \mathbb{A}^d_{\mathbb{C}}$ is a finite map with Zariski-dense image. This means exactly that the corresponding map $\mathbb{C}[T_1, \ldots, T_d] \to \mathbb{C}[T_1, \ldots, T_n]/I(X)$ in the category of $\mathbb{C}$-algebras is an injective finite $\mathbb{C}$-algebra homomorphism. Being finite, the map $f \colon X \to \mathbb{A}^d_{\mathbb{C}}$ has some wonderful properties: It maps closed sets to closed sets (a closed map). So it must be surjective. Finiteness also implies quasi-finiteness: Every fiber $f^{-1}(y)$, $y \in \mathbb{A}^d_{\mathbb{C}}$ is finite (and non-empty since f is surjective). Finite maps are also dimension-preserving, and so f maps each irreducible component C of X to an irreducible algebraic set of the same dimension (the image of C is closed since f is a closed map; irreducibility is preserved anyway by any polynomial map). If we take one more variable and consider the map $\mathbb{C}[T_1, \ldots, T_{d+1}] \to \mathbb{C}[T_1, \ldots, T_n]/I(X)$, it is clearly still finite, but not longer injective. Geometrically it means that the corresponding map $g \colon X \to \mathbb{A}^{d+1}_{\mathbb{C}}$ is finite, but no longer surjective. Still, g is closed and preserves the dimension of each irreducible component, and so if X is an irreducible algebraic set of dimension d, then $g(X)$ is an irreducible algebraic subset of $\mathbb{A}^{d+1}_{\mathbb{C}}$ of dimension d, i.e. an irreducible hypersurface. This is useful because every hypersurface is the zero locus of a single polynomial.

7.2. Hilbert's nullstellensatz.

Proposition 7.6 (Zariski's lemma). *Let $k \subset K$ be fields, where K is finitely generated as a k-algebra. Then K is a finite k-algebra (i.e., $\dim_k K < \infty$).*

Proof. By Noether's normalization theorem, K is finite over a k-subalgebra $A = k[x_1, \ldots, x_d]$, $d \geq 0$, where $x_1, \ldots, x_d \in K$ are algebraically independent over k. Since A and K are integral domains and K is a field, Lemma 6.14 says that A is a field as well. Thus $d = 0$ (because a polynomial algebra in more than 0 variables is never a field because the variables are not units). □

From now on, let $k \subset \Omega$ be fields, where Ω is algebraically closed.

Definition 7.7.

(1) Let S be a subset of $k[T_1, \ldots, T_n]$. Then $V(S) = \{\mathbf{x} \in \Omega^n \mid f(\mathbf{x}) = 0 \ \forall f \in S\}$. A set of the form $V(S)$ is called a *k-algebraic subset* of Ω^n (or an *algebraic subset of Ω^n defined over k*).

(2) Let X be a subset of Ω^n. Then

$$I(X) = \{f \in k[T_1, \ldots, T_n] \mid f(\mathbf{x}) = 0 \ \forall \mathbf{x} \in X\} \ .$$

Clearly, if $\mathfrak{a}$ is the ideal of $k[T_1, \ldots, T_n]$ generated by S then $V(\mathfrak{a}) = V(S)$.

Remark 7.8. An *algebraic subset* X of Ω^n (without the k- prefix) is defined to be an Ω-algebraic subset of Ω^n (i.e., setting $k = \Omega$). Every k-algebraic subset of Ω^n is an algebraic subset of Ω^n. But $\{i\}$ is an algebraic subset of $\mathbb{C}^1$ which is not an $\mathbb{R}$-algebraic subset: A polynomial $f \in \mathbb{R}[T]$ such that $f(i) = 0$ must satisfy $f(-i) = 0$, so every $\mathbb{R}$-algebraic subset of $\mathbb{C}^1$ that contains i must also contain $-i$. Thus the k- prefix adds information. Note that for $iT \in \mathbb{C}[T]$, $\underbrace{V(\{iT\})}_{\subset \mathbb{C}^1} = V(\{T\}) = \{0\}$. So, $\{iT\}$ gives rise to an $\mathbb{R}$-algebraic subset of $\mathbb{C}^1$ even though the coefficients of iT are not in $\mathbb{R}$. **[non-examinable from here to the end of the remark]** Assume that $\operatorname{char} k = 0$. Given $f_1, \ldots, f_s \in \Omega[T_1, \ldots, T_n]$, generating an ideal $\mathfrak{a}$ of $\Omega[T_1, \ldots, T_n]$, there are algorithmic ways to start from $f_1, \ldots, f_s$ and generate a certain generating set for $\mathfrak{a}$ called a *reduced Groebner basis* $g_1, \ldots, g_t \in \mathfrak{a}$. Let k be the smallest subfield of Ω that contains all of the coefficients $g_1, \ldots, g_t$. Then $\mathfrak{a}$ is generated by polynomials over k (clearly), and the coefficients of any generating set of $\mathfrak{a}$ generate a subfield of Ω that contains k (this requires a proof). So, k is the smallest subfield of Ω such that the algebraic subset $V(\mathfrak{a})$ of Ω^n is a k-algebraic subset of Ω^n. The proof of this algorithmic observation relies on *Galois descent*. Here's an example: For $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n$, let $\sigma\mathbf{x} = (\sigma(x_1), \ldots, \sigma(x_n))$. For a subset X of $\mathbb{C}^n$ let $\sigma X = \{\sigma(\mathbf{x}) \mid \mathbf{x} \in X\}$. So $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on the collection of subsets of $\mathbb{C}^n$. It clearly sends a $\mathbb{C}$-algebraic subset to a $\mathbb{C}$-algebraic subset. Now, set $n = 1$ and consider the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \tau\}$ on $\mathbb{C}^1$. Then $\tau\{i\} = \{-i\} \neq \{i\}$. Thus, the subgroup of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ of elements that fix $\{i\}$ is exactly $H = \{\mathrm{id}\}$ (the important notion here is fixing setwise, not pointwise, but here we have a singleton anyway). Under the correspondence between fields between $\mathbb{R}$ and $\mathbb{C}$ and subgroups of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, $H = \{\mathrm{id}\}$ corresponds to $\mathbb{C}$. So the smallest field k between $\mathbb{R}$ and $\mathbb{C}$ such that $\{i\}$ is k-algebraic is $k = \mathbb{C}$ (I did not prove this observation regarding Galois groups). This works in general, and is often employed in classic algebraic geometry with $\mathrm{Gal}\big(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q}\big)$ to find the smallest extension of $\mathbb{Q}$ that enables to define a given $\mathbb{Q}^{\text{alg}}$-algebraic set ($\mathbb{Q}^{\text{alg}}$ is the subfield of $\mathbb{C}$ of algebraic numbers over $\mathbb{Q}$). These Galois considerations can be used to show that for a given ideal $\mathfrak{a}$ of $\Omega[T_1, \ldots, T_n]$, the intersection of all subfields k of Ω such that $\mathfrak{a}$ can be defined over k is itself a field over which $\mathfrak{a}$ can be defined (an observation of Weil). This is the *field of definition* of $\mathfrak{a}$. As mentioned earlier, these Galois considerations are used to prove the algorithmic observations above regarding reduced Groebner bases and fields of definition.

Recall, from field theory, that if $k \subset L$ is a finite field extension (i.e. $\dim_k L < \infty$) then there is an injective k-algebra homomorphism $\varphi_L \colon L \to \Omega$. That is, Ω contains contains a copy of each finite extension L of k, such that the inclusions of k in L and in Ω are compatible (i.e. restricting φ_L to k results in the inclusion map $k \subset \Omega$).

Theorem 7.9. *Let $\mathfrak{a}$ be an ideal of $k[T_1, \ldots, T_n]$. Then*

i) ***Weak Nullstellensatz:*** *$V(\mathfrak{a}) = \emptyset$ if and only if $1 \in \mathfrak{a}$.*

ii) ***Strong Nullstellensatz:*** *$\sqrt{\mathfrak{a}} = I(V(\mathfrak{a}))$.*

Proof. (i) Clearly $V(\mathfrak{a}) = \emptyset$ if $1 \in \mathfrak{a}$. Conversely, assume that $1 \notin \mathfrak{a}$. Take $\mathfrak{m} \in \operatorname{mspec} k[T_1, \ldots, T_n]$ such that $\mathfrak{a} \subset \mathfrak{m}$. Then $k[T_1, \ldots, T_n]/\mathfrak{m}$ is a field, finitely generated as a k-algebra. Thus $\dim_k k[T_1, \ldots, T_n]/\mathfrak{m} < \infty$ by Proposition 7.6. Hence, we have an injective k-algebra homomorphism $k[T_1, \ldots, T_n]/\mathfrak{m} \to \Omega$. Composing with the quotient map $k[T_1, \ldots, T_n] \to k[T_1, \ldots, T_n]/\mathfrak{m}$, we obtain a k-algebra homomorphism

$$\varphi \colon k[T_1, \ldots, T_n] \to \Omega$$

such that $\ker \varphi = \mathfrak{m}$. Recall that a k-algebra homomorphism φ from $k[T_1, \ldots, T_n]$ is determined uniquely by the images of $T_1, \ldots, T_n$. More explicitly, we have $\varphi(f) = f(\mathbf{x})$ for $\mathbf{x} := (\varphi(T_1), \ldots, \varphi(T_n))$. Thus, for all $f \in \underbrace{\mathfrak{a}}_{\subset \mathfrak{m}}$, we have

$$f(\mathbf{x}) = \varphi(f) = 0 \ ,$$

and so $\mathbf{x} \in V(\mathfrak{a})$, and thus $V(\mathfrak{a}) \neq \emptyset$.

(ii) Let $f \in \sqrt{\mathfrak{a}}$. Then $f^\ell \in \mathfrak{a}$, $\ell \geq 1$, and thus $f^\ell(\mathbf{x}) = 0$ for every $\mathbf{x} \in V(\mathfrak{a})$. So $f(\mathbf{x}) = 0$ since Ω is an integral domain. That is $f \in I(V(\mathfrak{a}))$.

Conversely, take $f \in \underbrace{I(V(\mathfrak{a}))}_{\subset k[T_1, \ldots, T_n]}$. We wish to show that some power of f lies in $\mathfrak{a}$. Consider $A = k[T_1, \ldots, T_n]/\mathfrak{a}$, and let $\overline{f}$ be the image of f in A. Then, our goal is to show that $\overline{f}$ is nilpotent. Equivalently, we need to show that $\underbrace{A_{\overline{f}}}_{=\{\overline{f}^m | m \geq 0\}^{-1} A} = \{0\}$. But $A_{\overline{f}} \cong k[T_1, \ldots, T_n, T_{n+1}] \Big/ \left(\underbrace{\mathfrak{a}^e + (T_{n+1} f - 1)}_{=:\mathfrak{b}} \right)$

(here $\mathfrak{a}^e$ is the extension $\mathfrak{a}$ from $k[T_1,\dots,T_n]$ to $k[T_1,\dots,T_{n+1}]$), and so we need to show that $1 \in \mathfrak{b}$. By the Weak Nullstellensatz, it suffices to show that $\underbrace{V(\mathfrak{b})}_{\subset\Omega^{n+1}} = \emptyset$, as we do now: If $\underbrace{(x_1,\dots,x_{n+1})}_{=:\mathbf{x}} \in V(\mathfrak{b})$ then $\underbrace{(x_1,\dots,x_n)}_{=:\mathbf{x}_0} \in \underbrace{V(\mathfrak{a})}_{\subset\Omega^n}$, and so $f(\mathbf{x}_0) = 0$, and hence $f(\mathbf{x}) = 0$. So $\left(\underbrace{T_{n+1}f - 1}_{\in\mathfrak{b}}\right)(\mathbf{x}) = -1 \neq 0$, a contradiction. □

Remark 7.10. Let $\mathfrak{a} = (f_1,\dots,f_t)$ be an ideal of $k[T_1,\dots,T_n]$. The weak NSZ says that if $V(\mathfrak{a}) = \emptyset$ then there are $p_1,\dots,p_t \in k[T_1,\dots,T_n]$ such that

$$\sum_{i=1}^{t} p_i f_i = 1 \tag{7.1}$$

(and clearly the existence of such $p_1,\dots,p_t$ implies that $V(\mathfrak{a}) = \emptyset$). **[non-examinable from here until the end of the remark]**. The *effective NSZ* gives us a bound on the degrees of $p_1,\dots,p_t$. For example, it is known that if $V(\mathfrak{a}) = \emptyset$ then we can find $p_1,\dots,p_t$ satisfying (7.1) such that

$$\deg p_i \le \underbrace{(\max\{3, \deg f_1,\dots,\deg f_t\})^n}_{=:D} \qquad \forall 1 \le i \le t\ . \tag{7.2}$$

Now, for fixed $f_1,\dots,f_t$, (7.1) becomes system of linear equations in the coefficients of $p_1,\dots,p_t$. By (7.2), if there's a solution to this system, then there's a solution where all coefficients of each p_i of degree higher than D are 0, giving a finite system of linear equations in finitely many variables. Thus we may determine whether or not there is a solution via Gauss elimination. This gives us an algorithm to check whether $V(\mathfrak{a}) = \emptyset$, which takes as input a set of generators for $\mathfrak{a}$.

Remark 7.11. **[non-examinable]** The non-explicit part of the proof of the weak Nullstellensatz was the existence of the maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$. For this we invoked (without saying so) Zorn's Lemma. In fact, finding such $\mathfrak{m}$ is equivalent to finding a simulatenous solution for the polynomials in $\mathfrak{a}$. Insted of invoking Zorn's lemma, it is possible to find such a solution explicitly using one of several algorithms, using resultants or Groebner bases.

Recall that an ideal I of a ring R is *radical* if $I = \sqrt{I}$. The formula $\sqrt{\sqrt{I}} = \sqrt{I}$ implies that the radical of an ideal is a radical ideal.

Fact 7.12.

i) *For subsets $X \subset Y$ of Ω^n, we have $I(X) \supset I(Y)$. For subsets $S \subset T$ of $k[T_1,\dots,T_n]$, we have $V(S) \supset V(T)$. That is, both $I(\cdot)$ and $V(\cdot)$ are inclusion reversing (and thus $I(V(\cdot))$ and $V(I(\cdot))$ respect inclusions).*

ii) *For $S \subset k[T_1, \dots, T_n]$, we have $S \subset I(V(S))$.*
Proof: *If $f \in S$ and $\mathbf{x} \in V(S)$ then $f(\mathbf{x}) = 0$ by the definition of $V(S)$, and so f vanishes on all of $V(S)$, i.e. $f \in I(V(S))$.*

iii) *For a subset $X \subset \Omega^n$, we have $X \subset V(I(X))$.*
Proof: *If $\mathbf{x} \in X$ and $f \in I(X)$ then $f(\mathbf{x}) = 0$ by the definition of $I(X)$, and so $\mathbf{x}$ is a root of all $I(X)$, i.e. $\mathbf{x} \in V(I(X))$. So $X \subset V(I(X))$.*

iv) *In fact, $V(I(X))$ is the smallest k-algebraic subset of Ω^n that contains X.*
Proof:
(a) *Clearly $V(I(X))$ is k-algebraic, and we've just seen that it contains X.*
(b) *If $X \subset Y$ for some k-algebraic set $Y \subset \Omega^n$, then $Y = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $k[T_1, \dots, T_n]$, and so*

$$V(I(X)) \subset V(I(Y)) = V\left(\underbrace{I(V(\mathfrak{a}))}_{\supset \mathfrak{a}}\right) \subset V(\mathfrak{a}) = Y \ .$$

v) *In particular, $V(I(X)) = X$ if $X \subset \Omega^n$ is k-algebraic.*

vi) *For every set $X \subset \Omega^n$, the ideal $I(X)$ of $k[T_1, \dots, T_n]$ is radical.*
Proof: *If $f^\ell \in I(X)$ then $f^\ell(\mathbf{x})$ for all $\mathbf{x} \in X$, and so $f(\mathbf{x}) = 0$ since Ω is an integral domain, i.e. $f \in I(X)$.*

The folllowing corollary of the strong NSZ relates geometry and algebra.

Proposition 7.13. *Let $n \geq 0$. Then we have a bijection:*

$$\{\ k\text{-algebraic subsets of } \Omega^n\ \} \leftrightarrow \{\ \text{radical ideals of } k[T_1, \dots, T_n]\ \} \tag{7.3}$$

given by $X \mapsto I(X)$ and $V(\mathfrak{a}) \leftarrow\!\shortmid \mathfrak{a}$.

Proof. We've just seen that $I(X)$ is a radical ideal for every k-algebraic subset $X \subset \Omega^n$, and that $X = V(I(X))$. Now, let $\mathfrak{a}$ be a radical ideal of $k[T_1, \dots, T_n]$. Then $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$ by the strong NSZ and since $\mathfrak{a}$ is radical. □

The set of radical ideals of $k[T_1, \dots, T_n]$ contains $\operatorname{spec} k[T_1, \dots, T_n]$, which contains $\operatorname{mspec} k[T_1, \dots, T_n]$. What a k-algebraic subsets of Ω^n correspond to prime and to maximal ideals? We study this a bit now.

Remark 7.14. Some observations regarding the bijection from Proposition 7.13.

(1) Since the bijection of Proposition 7.13 reverses inclusion, the set $\mathcal{A}$ of minimal nonempty k-algebraic subsets of Ω^n corresponds bijectively with the set $\operatorname{mspec} k[T_1, \dots, T_n]$ of maximal ideals of $k[T_1, \dots, T_n]$.

(2) Let $\mathcal{C} = \{\{\mathbf{x}\} \mid \mathbf{x} \in k^n\}$. Then $\mathcal{C} \subset \mathcal{A}$ because for every $\mathbf{x} \in k^n$, we have $\{\mathbf{x}\} = V(\mathfrak{m}_{\mathbf{x}})$ for $\mathfrak{m}_{\mathbf{x}} \coloneqq (T_1 - x_1, \dots, T_n - x_n)$, showing that $\{\mathbf{x}\}$ is k-algebraic (while minimality is clear for a singleton). Note that $\mathfrak{m}_{\mathbf{x}}$ is a maximal ideal since $k[T_1, \dots, T_n]/\mathfrak{m}_{\mathbf{x}} \cong k$ is a field. Applying $I(\cdot)$, we see that[31] $I(\{\mathbf{x}\}) = I(V(\mathfrak{m}_{\mathbf{x}})) = \mathfrak{m}_{\mathbf{x}}$.

(3) So, we have an injective map $\mathbf{x} \mapsto \mathfrak{m}_{\mathbf{x}} \colon k^n \to \operatorname{mspec} k[T_1, \dots, T_n]$, but in general it is not a bijection. It will be a bijection if and only if $\mathcal{C} = \mathcal{A}$ but this is not always the case. One reason for this is that $\mathcal{A}$ may contain sets that are not singletons. For example, for $k = \mathbb{R}$ and $\Omega = \mathbb{C}$, the set $X = \{i, -i\}$ is a minimal $\mathbb{R}$-algebraic subset of $\mathbb{C}^1$, corresponding to the maximal ideal $I(\{i, -i\}) = \big(T^2 + 1\big)$. This already proves that $\big(T^2 + 1\big)$ is not of the form $\mathfrak{m}_{\mathbf{x}}$ for any $\mathbf{x} \in \mathbb{R}^1$, but you can also observe that $\mathbb{R}[T]/\mathfrak{m}_{\mathbf{x}} \cong \mathbb{R}$ for such $\mathbf{x}$, while $\mathbb{R}[T]/\big(T^2 + 1\big) \cong \mathbb{C} \ncong \mathbb{R}$.

(4) In the special case $k = \Omega$, we have $\mathcal{C} = \{\{\mathbf{x}\} \mid \mathbf{x} \in \Omega^n\}$, forcing $\mathcal{C} = \mathcal{A}$ (if every singleton is k-algebraic, then every minimal nonempty k-algebraic set is a singleton). So the map $\mathbf{x} \mapsto \mathfrak{m}_{\mathbf{x}} \colon \Omega^n \to \operatorname{mspec} \Omega[T_1, \dots, T_n]$ is a bijection.

(5) **Claim:** Every maximal ideal of $k[T_1, \dots, T_n]$ is a contraction of a maximal ideal of $\Omega[T_1, \dots, T_n]$.
Proof: Take $\mathfrak{m} \in \operatorname{mspec} k[T_1, \dots, T_n]$. Then $\mathfrak{m} = I(X)$ for some minimal nonempty k-algebraic subset of Ω^n. Take $\mathbf{x} \in X$. Then $V(I(\{\mathbf{x}\}))$ is the smallest k-algebraic subset of Ω^n containing $\mathbf{x}$,and thus $V(I(\{\mathbf{x}\})) = X$ by the minimality of X. Thus

$$\mathfrak{m} = I(X) = I(V(I(\{\mathbf{x}\}))) = I(\{\mathbf{x}\})$$

where in the last step we applied $I(V(\cdot))$ to the radical ideal $I(\{\mathbf{x}\})$. But $I(\{\mathbf{x}\})$ is equal to the intersection of $I^{\Omega}(\{\mathbf{x}\}) \coloneqq \{f \in \Omega[T_1, \dots, T_n] \mid f(\mathbf{x}) = 0\}$ with $k[T_1, \dots, T_n]$, while $I^{\Omega}(\{\mathbf{x}\})$ is the maximal ideal $(T_1 - x_1, \dots, T_n - x_n)$ of $\Omega[T_1, \dots, T_n]$ by our previous discussion.

(6) A possibly surprising minimal k-algebraic set: We saw in the case $k = \mathbb{R}$ and $\Omega = \mathbb{C}$ (and $n = 1$) that $\mathcal{C} \neq \mathcal{A}$ because $\mathcal{A}$ contains subsets with more than one element. Now consider the case $k = \mathbb{F}_p(X)$, i.e. the field of rational functions in X over $\mathbb{F}_p$, and $\Omega = k^{\mathrm{alg}}$ (the algebraic closure of k). Again take $n = 1$. The subset $\big\{X^{1/p}\big\}$ of Ω^1 is

[31] This argument shows that $I(\{\mathbf{x}\}) = \mathfrak{m}_{\mathbf{x}}$ by eventually relying on the strong NSZ, but you can also just note that clearly $\mathfrak{m}_{\mathbf{x}} \subset I(\{\mathbf{x}\})$ and $1 \notin (\{\mathbf{x}\})$, and an inclusion of maximal ideal in a proper ideal must be an equality. Yet another argument for the inclusion $I(\{\mathbf{x}\}) \subset \mathfrak{m}_{\mathbf{x}}$ is to note that $I(\{\mathbf{x}\}) = \ker \varphi_{\mathbf{x}}$ for the k-algebra homomorphism $\varphi_{\mathbf{x}} \colon k[T_1, \dots, T_n] \to k$ mapping $T_i \mapsto x_i$. If $f \in \ker \varphi_{\mathbf{x}}$ then $g(0, \dots, 0) = 0$ for $g(T_1, \dots, T_n) \coloneqq f(T_1 + x_1, \dots, T_n + x_n)$, and so the constant coefficient of g is 0, and hence $g \in (T_1, \dots, T_n)$. Thus $f = g(T_1 - x_1, \dots, T_n - x_n) \in (T_1 - x_1, \dots, T_n - x_n) \in \mathfrak{m}_{\mathbf{x}}$.

$\mathbb{F}_p(X)$-algebraic since $\left\{X^{1/p}\right\} = V\left(\underbrace{T^p - X}_{=\left(T-X^{1/p}\right)^p}\right)$. In this example, not only that $\mathcal{C}$ does not exhaust $\mathcal{A}$, but $\mathcal{C}$ does not even exhaust the set of k-algebraic singletons. If you want, prove that this cannot happen for separable extensions, i.e. that if $k \subset \Omega$ is separable (e.g. when $\operatorname{char} k = 0$ or when $k = \mathbb{F}_p$ and $\Omega = \mathbb{F}_p^{\mathrm{alg}}$) then all sets in $\mathcal{C} \setminus \mathcal{A}$ have at least 2 elements.

Definition 7.15. An algebraic (i.e. Ω-algebraic) set $X \subset \Omega^n$ is *irreducible* if $X \neq \emptyset$ and X is not equal to the union of two proper algebraic subsets of X.

Proposition 7.16. *An algebraic set $X \subset \Omega^n$ is irreducible if and only if the radical ideal $I(X)$ of $\Omega[T_1, \dots, T_n]$ is prime.*

Proof. Write $X = V(\mathfrak{a})$, $\mathfrak{a} \subset \Omega[T_1, \dots, T_n]$ an ideal. Assume that X is irreducible. Take $f, g \in \Omega[T_1, \dots, T_n]$ such that $fg \in I(X)$. Then for every $\mathbf{x} \in X$, $f(\mathbf{x}) = 0$ or $g(\mathbf{x}) = 0$. That is[32], $X \subset V(f) \cup V(g)$, and so $X = \left(\underbrace{X \cap V(f)}_{=V(\mathfrak{a}+(f))}\right) \cup \left(\underbrace{X \cap V(g)}_{=V(\mathfrak{a}+(g))}\right)$ (a union of algebraic sets). Since X is irreducible, this implies that $X \subset V(f)$ or $X \subset V(g)$. WLOG $X \subset V(f)$. Taking $I(\cdot)$, we have[33] $I(X) \supset \underbrace{I(V(f))}_{\supset\sqrt{(f)}}$. Thus $f \in I(X)$, and so $I(X)$ is prime.

Conversely, assume that $I(X)$ is prime. Take $X = X_1 \cup X_2$, a union of algebraic subsets of Ω^n. Then $I(X) = I(X_1) \cap I(X_2)$. By ES2.Q2(a)[34], this means that $I(X) = I(X_1)$ or $I(X) = I(X_2)$. WLOG $I(X) = I(X_1)$. Then $\underbrace{V(I(X))}_{=X} = \underbrace{V(I(X_1))}_{=X_1}$. Finally, note that $1 \notin I(X)$ (prime ideals are proper ideals by definition), and so $X \neq \emptyset$ by the weak NSZ. □

Remark 7.17. **[non-examinable]** For an algebraically closed field Ω, we have seen a bijection $\Omega^n \to \operatorname{mspec} \Omega[T_1, \dots, T_n]$ given by $\mathbf{x} \mapsto \mathfrak{m}_{\mathbf{x}} = (T_1 - x_1, \dots, T_n - x_n)$, and a bijection $\{$ irreducible algebraic subset of Ω^n $\} \to \operatorname{spec} \Omega[T_1, \dots, T_n]$. The second bijection extends the first if we think of each point $\mathbf{x} \in \Omega^n$ as the algebraic set $\{\mathbf{x}\}$ (which is clearly irreducible).

[32] We write $V(f)$ for $V(\{f\})$.

[33] By the strong NSZ, we have $I(V(f)) = \sqrt{(f)}$, but here we only needed the easy-to-prove inclusion.

[34] This exercise says that in an arbitrary ring R, if a prime ideal $\mathfrak{p}$ is equal to the intersection of finitely many ideals, $\mathfrak{p} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_\ell$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Now to morphisms: A map $\Omega^n \to \Omega^\ell$ is *regular* if it maps $\mathbf{t} \mapsto (f_1(\mathbf{t}), \dots, f_\ell(\mathbf{t}))$ for polynomials $f_1, \dots, f_\ell \in \Omega[T_1, \dots, T_n]$. On the other hand, an Ω-algebra homomorphism $\Omega[X_1, \dots, X_\ell] \to \Omega[T_1, \dots, T_n]$ is given by the images $g_1, \dots, g_\ell \in \Omega[T_1, \dots, T_n]$ of $X_1, \dots, X_\ell$. Thus, in both cases the data defining the map is an ℓ-tuple of elements of $\Omega[T_1, \dots, T_n]$. By the bijections mentioned above, we may think of the regular map $\Omega^n \to \Omega^\ell$ as a map $\operatorname{mspec} \Omega[T_1, \dots, T_n] \to \operatorname{mspec} \Omega[X_1, \dots, X_\ell]$ sending $(T_1 - t_1, \dots, T_n - t_n) \mapsto (X_1 - f_1(\mathbf{t}), \dots, X_\ell - f_\ell(\mathbf{t}))$ for $\mathbf{t} = (t_1, \dots, t_n) \in \Omega^n$ (call maps of this form regular too). So, forget about the viewpoint of Ω^n and Ω^ℓ: We have regular maps $\operatorname{mspec} \Omega[T_1, \dots, T_n] \to \operatorname{mspec} \Omega[X_1, \dots, X_\ell]$ and Ω-algebra homomorphisms $\Omega[X_1, \dots, X_\ell] \to \Omega[T_1, \dots, T_n]$, and each type of map is given by any chosen ℓ-tuple of polynomials in $\Omega[T_1, \dots, T_n]$. Now, given an Ω-algebra homomorphism $\varphi \colon \Omega[X_1, \dots, X_\ell] \to \Omega[T_1, \dots, T_n]$, $\varphi(X_i) = f_i$, we have a contraction map $\varphi^* \colon \operatorname{spec} \Omega[T_1, \dots, T_n] \to \operatorname{spec} \Omega[X_1, \dots, X_\ell]$. For a maximal ideal $\mathfrak{m} = (T_1 - t_1, \dots, T_n - t_n)$ of $\Omega[T_1, \dots, T_n]$, we have $\varphi^*(\mathfrak{m}) = \varphi^{-1}(\mathfrak{m}) = (X_1 - f_1(\mathbf{t}), \dots, X_\ell - f_\ell(\mathbf{t}))$ for $\mathbf{t} = (t_1, \dots, t_n)$. Indeed, for $g \in \Omega[X_1, \dots, X_\ell]$, we have $\varphi(g) \in \mathfrak{m}$ if and only if $g(f_1(\mathbf{t}), \dots, f_\ell(\mathbf{t})) = 0$ if and only if $g \in (X_1 - f_1(\mathbf{t}), \dots, X_\ell - f_\ell(\mathbf{t}))$. In particular, in this case, the contraction map φ^* restricts to a map $\operatorname{mspec}[T_1, \dots, T_n] \to \operatorname{mspec} \Omega[X_1, \dots, X_\ell]$ (in general, contraction maps do not necessarily send maximal ideals to maximal ideals). We have thus obtained a bijection

$$\{ \text{ regular maps } \operatorname{mspec} \Omega[T_1, \dots, T_n] \to \operatorname{mspec} \Omega[X_1, \dots, X_\ell] \ \} \leftrightarrow \{ \ \Omega\text{-algebra homomorphisms } \Omega[X_1, ..$$

given by $\varphi^* \leftarrow\!\shortmid \varphi$.

The fact that maximal ideals contract to maximal ideals remains true for algebra homomorphisms between finitely generated k-algebras, where k is any field, not necessarily algebraically closed. But, as we saw earlier, the injective map $k^n \to \operatorname{mspec} k[T_1, \dots, T_n]$, $\mathbf{x} \mapsto \mathfrak{m}_{\mathbf{x}}$, is not necessarily surjective. For more general ring homomorphisms, such as the inclusion $\mathbb{Z} \to \mathbb{Q}$, maximal ideals do not necessarily contract to maximal ideals ($(0) \subset \mathbb{Q}$ contracts to $(0) \subset \mathbb{Z}$). For this reason, among others, modern algebraic geometry considers all of $\operatorname{spec} R$ as a geometric space for any ring R. In the classical setting, where we consider $R = \Omega[T_1, \dots, T_n]$, this is the same as considering the space of all irreducible algebraic subsets of Ω^n instead of Ω^n itself (noting that each point $\mathbf{x}$ of Ω^n gives rise to the irreducible algebraic set $\{\mathbf{x}\}$, but there are many additional irreducible algebraic subsets of Ω^n). Taking spec instead of mspec is not necessary in the classical setting, but it is crucial for the study of general rings. The clear geometric interpretation of the classical setting can give intuition for what ought to be true and what constructions ought to be helpful in modren algebraic geometry.

8. Integral and finite extensions (Part II)

The following definition generalizes the notion of an integral element over a ring.

Definition 8.1 (Integrality over an ideal)**.** Let $A \subset B$ be rings, $\mathfrak{a}$ be an ideal of A.

i) For $x \in B$, x is *integral over* $\mathfrak{a}$ (or $\mathfrak{a}$-integral) if there is a monic polynomial $f = T^n + a_1 T^{n-1} + \cdots + a_n T^0 \in A[T]$, $a_i \in \mathfrak{a}$, such that $f(x) = 0$.

ii) The *integral closure* of $\mathfrak{a}$ in B is $\{x \in B \mid x \text{ is } \mathfrak{a}\text{-integral}\}$.

It turns out that the integral closure of $\mathfrak{a}$ in B is an ideal of a subring of B (in particular, closed under addition and multiplication[35]). The following proposition shows more than that.

Proposition 8.2. *Let $A \subset B$ be rings, and let $\overline{A}$ be the integral closure of A in B. Let $\mathfrak{a}$ be an ideal of A. Then the integral closure of $\mathfrak{a}$ in B is $\sqrt{\mathfrak{a}\overline{A}}$ (i.e. the radical in $\overline{A}$ of the extension of $\mathfrak{a}$ to $\overline{A}$).*

Proof. If $b \in B$ is integral over $\mathfrak{a}$ then $b^n + a_1 b^{n-1} + \cdots + a_n b^0 = 0$, $n \geq 1$, $a_1, \ldots, a_n \in \mathfrak{a}$. Thus $b \in \overline{A}$, and so $b^0, \ldots, b^{n-1} \in \overline{A}$, and thus $b^n = -\big(a_1 b^{n-1} + \cdots + a_n b^0\big) \in \mathfrak{a}\overline{A}$. Thus $b \in \sqrt{\mathfrak{a}\overline{A}}$.

Conversely, let $b \in \sqrt{\mathfrak{a}\overline{A}}$. Then, $b^n \in \mathfrak{a}\overline{A}$ for some $n \geq 1$, that is,

$$b^n = \sum_{i=1}^{m} a_i x_i \qquad a_i \in \mathfrak{a} \qquad x_i \in \overline{A},\ m \geq 0\ . \tag{8.1}$$

Each x_i is integral over A and so $M := \underbrace{A[x_1, \ldots, x_m]}_{\ni b^n}$ is a finite A-algebra by Proposition 6.6 (i.e. finitely generated as an A-module). Also, we have an inclusion of A-modules: $b^n M \subset \mathfrak{a}M$ by (8.1). Thus, we may apply Proposition 5.1 to the A-linear map $f\colon M \to M$, $f(m) = b^n m$, $f(M) \subset \mathfrak{a}M$, and see that

$$f^\ell + \alpha_1 f^{\ell-1} + \cdots + \alpha_\ell f^0 = 0 \qquad (\text{ in } \operatorname{End}_R M\ ),$$

$\alpha_i \in \mathfrak{a}$, $\ell \geq 1$. Evaluating at $m = \underbrace{1_A}_{\in M}$, we deduce that

$$\underbrace{(b^n)^\ell}_{=b^{n\ell}} + \alpha_1 \underbrace{(b^n)^{\ell-1}}_{=b^{n(\ell-1)}} + \cdots + \alpha_\ell \underbrace{(b^n)^0}_{b^0} = 0 \qquad (\text{ in } M \subset B\ ),$$

[35] But unlike the integral closure of A in B, the integral closure of $\mathfrak{a}$ in B does not have to include 1_A, and so is not always a subring of B.

and so b is $\mathfrak{a}$-integral[36]. □

Corollary 8.3. *Let $A \subset B$ be rings, and let $\mathfrak{a}$ be an ideal of A. Then the integral closure of $\mathfrak{a}$ in B is closed under addition and multiplication.*

Proof. Immeidate from Proposition 8.2. □

Corollary 8.4. *Let $A \subset B$ be rings, and let $\mathfrak{a}$ be an ideal of A. Let $b \in B$. Then b is $\mathfrak{a}$-integral $\Leftrightarrow$ b is $\underbrace{\sqrt{\mathfrak{a}}}_{\subset A}$-integral.*

Proof. Let $\overline{A}$ be the integral closure of A in B. We need to show that the integral closure of $\sqrt{\mathfrak{a}}$ in B is contained in the integral closure of $\mathfrak{a}$ in B (and thus they are equal). By Proposition 8.2, our goal is to show $\sqrt{(\sqrt{\mathfrak{a}})\overline{A}} \subset \sqrt{\mathfrak{a}\overline{A}}$. In general, for any ring homomorphism $f\colon R \to S$ and ideal I of R[37], $\sqrt{I}^e \subset \sqrt{I^e}$. So $(\sqrt{\mathfrak{a}})\overline{A} \subset \sqrt{\mathfrak{a}\overline{A}}$. Taking $\sqrt{\cdot}$ on both sides, we have $\sqrt{(\sqrt{\mathfrak{a}})\overline{A}} \subset \sqrt{\sqrt{\mathfrak{a}\overline{A}}} = \sqrt{\mathfrak{a}\overline{A}}$. □

Proposition 8.5. *Let $A \subset B$ be integral domains, where A is integrally closed. Let $\mathfrak{a} \subset A$ be an ideal, and take $b \in B$. Consider the field extension* $\operatorname{Frac} A \subset \operatorname{Frac} B$. *Then the following are equivalent:*

i) *b is integral over $\mathfrak{a}$.*

ii) $\underbrace{\frac{b}{1}}_{\in \operatorname{Frac} B}$ *is algebraic over* $\operatorname{Frac} A$ *with minimal polynomial over* $\operatorname{Frac} A$ *of the form $T^n + \frac{a_1}{1}T^{n-1} + \cdots + \frac{a_n}{1}T^0$, $n \geq 1$, $a_i \in \sqrt{\mathfrak{a}}$.*

Proof. Assume (2). Then,

$$\frac{b^n + a_1 b^{n-1} + \cdots + a_n b^0}{1} = \frac{0}{1} \qquad (\text{ in } \operatorname{Frac} B\ ),$$

$a_i \in \sqrt{\mathfrak{a}}$, and so

$$b^n + a_1 b^{n-1} + \cdots + a_n b^0 = 0 \qquad (\text{ in } B\ )$$

and thus b is $\sqrt{\mathfrak{a}}$-integral, and so b is $\mathfrak{a}$-integral by Corollary 8.4.

Assume (1). Let $f \in (\operatorname{Frac} A)[T]$ be the minimal polynomial of $\frac{b}{1}$ over $\operatorname{Frac} A$. We wish to show that each coefficient of f belongs to $\frac{\sqrt{\mathfrak{a}}}{1} := \left\{\frac{a}{1} \mid a \in \sqrt{\mathfrak{a}}\right\}$. By Proposition 8.2, $\frac{\sqrt{\mathfrak{a}}}{1}$ is the integral closure of $\mathfrak{a}$ in $\operatorname{Frac} A$

[36] Note how the expression showing that b^n is $\mathfrak{a}$-integral show in fact that b is $\mathfrak{a}$-integral simply because $(b^n)^{\ell-i} = b^{n(\ell-i)}$ for all $0 \leq i \leq \ell$. For the same reason, in general, if x^n is integral then so is x.

[37] You have seen this in an example sheet. Let's show this again: If $b \in \sqrt{I}^e$ then $b = b_1 f(x_1) + \cdots + b_\ell f(x_\ell)$, $b_i \in B$, $x_i \in A$, $x_i^{n_i} \in I$, $n_i \geq 1$. Set $n = n_1 + \cdots + n_\ell$. Then $b^n \in I^e$, and so $b \in \sqrt{I^e}$.

since A is integrally closed. Thus, it suffices to show that the coefficients of f are in $\operatorname{Frac} A$ and are $\mathfrak{a}$-integral (they are in $\operatorname{Frac} A$ by definition). Fix an algebraically closed field Ω containing $\operatorname{Frac} A$, and let

$$f = \prod_{i=1}^{\ell}(T - \alpha_i) \qquad \alpha_i \in \Omega \qquad \alpha_1 = \frac{b}{1} \ . \tag{8.2}$$

By expanding the brackets in (8.2), one sees that each coefficient of f is a sum of products of $\alpha_1, \dots, \alpha_\ell$. Thus, by Corollary 8.3, it suffices to prove that each α_i is $\mathfrak{a}$-integral.

By our assumption (1), we have

$$b^n + a_1 b^{n-1} + \cdots + a_n b^0 = 0 \qquad (\text{ in } B\ )$$

for some $n \geq 1$ and $a_1, \dots, a_n \in \mathfrak{a}$, and so $h\big(\frac{b}{1}\big) = 0$ for

$$h = T^n + \frac{a_1}{1} T^{n-1} + \cdots + \frac{a_n}{1} T^0 \in (\operatorname{Frac} A)[T] \ .$$

For each $1 \leq i \leq \ell$, we have a $(\operatorname{Frac} A)$-algebra isomorphism $\varphi_i \colon (\operatorname{Frac} A)\big[\frac{b}{1}\big] \to (\operatorname{Frac} A)[\alpha_i]$, $\varphi_i\big(\frac{b}{1}\big) = \alpha_i$, because[38] $\frac{b}{1}$ and α_i have the same minimal polynomial f over $\operatorname{Frac} A$. Thus $h(\alpha_i) = h\big(\varphi_i\big(\frac{b}{1}\big)\big) = \varphi_i\left(\underbrace{h\left(\frac{b}{1}\right)}_{=0}\right) = 0$, where the second equality follows since h is a $(\operatorname{Frac} A)$-algebra homomorphism and since the coefficients of h are in $\operatorname{Frac} A$. So α_i is integral over $\mathfrak{a}$. □

9. Cohen–Seidenberg Theorems (Going Up/Down)

Given an integral extension $A \subset B$, $\iota \colon A \hookrightarrow B$ the inclusion map, we have a contraction map $\iota^* \colon \operatorname{spec} B \to \operatorname{spec} A$, $\iota^*(\mathfrak{q}) = \mathfrak{q} \cap A$. In this section we study ι^*, and in particular, the fibers of ι^*. Similar results are true for any ring homomorphism $f \colon A \to B$ that makes B into an integral A-algebra. The case of a general f follows from the case of the inclusion map ι.

For rings $A \subset B$ and $\mathfrak{p} \in \operatorname{spec} A$, we let $A_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1} A$ (as usual) and also $B_\mathfrak{p} \coloneqq (A \setminus \mathfrak{p})^{-1} B$. Indeed, $A \setminus \mathfrak{p}$ is a multiplicative subset of B. But note that $B_\mathfrak{p}$ is not a "localization of B at a prime ideal of B". Importantly, $B_\mathfrak{p}$ is usually not a local ring - it can have more than one maximal ideal. The following proposition gives a bijective correspondence between $\operatorname{mspec} B_\mathfrak{p}$ and the fiber of $\mathfrak{p}$ under the contraction map $\iota^* \colon \operatorname{spec} B \to \operatorname{spec} A$.

[38] Indeed, we have $(\operatorname{Frac} A)$-algebra isomorphisms $(\operatorname{Frac} A)[T]/(f) \to (\operatorname{Frac} A)\big[\frac{b}{1}\big]$ and $(\operatorname{Frac} A)[T]/(f) \to (\operatorname{Frac} A)[\alpha_i]$, sending $T + (f) \mapsto \frac{b}{1}$ and $T + (f) \mapsto \alpha_i$, respectively.

Proposition 9.1. *Let $A \subset B$ be an integral extension of rings, and let $\mathfrak{p} \in \operatorname{spec} A$. Then there is bijection*

$$\{\mathfrak{q} \in \operatorname{spec} B \mid \mathfrak{q} \cap A = \mathfrak{p}\} \leftrightarrow \operatorname{mspec} B_{\mathfrak{p}} \tag{9.1}$$

given by extension and contraction of ideals along the localization map $B \to B_{\mathfrak{p}}$, i.e. $\mathfrak{q} \mapsto \mathfrak{q}B_{\mathfrak{p}}$ and $\mathfrak{m}^c \leftarrow\!\shortmid \mathfrak{m}$.

Proof. By Proposition 4.16, applied to the localization map $B \to B_{\mathfrak{p}}$, extension and contraction of ideals gives a bijection $\{\mathfrak{q} \in \operatorname{spec} B \mid \mathfrak{q} \cap A \subset \mathfrak{p}\} \leftrightarrow \operatorname{spec} B_{\mathfrak{p}}$, restricting to an injective map $\{\mathfrak{q} \in \operatorname{spec} B \mid \mathfrak{q} \cap A = \mathfrak{p}\} \to \operatorname{spec} B_{\mathfrak{p}}$. It remains to show that the image of the latter map is precisely $\operatorname{mspec} B_{\mathfrak{p}}$.

Let $S = A \backslash \mathfrak{p}$, and take $\mathfrak{q} \in \operatorname{spec} B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then $\mathfrak{q}B_{\mathfrak{p}} \in \operatorname{spec} B_{\mathfrak{p}}$ by Proposition 4.16. By Proposition 6.13, the extension $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ is integral. Thus $\mathfrak{q}B_{\mathfrak{p}} \in \operatorname{mspec} B_{\mathfrak{p}}$ if $(\mathfrak{q}B_{\mathfrak{p}}) \cap A_{\mathfrak{p}} \in \operatorname{mspec} A_{\mathfrak{p}}$ by Corollary 6.15. This is indeed the case: By Proposition 4.14,

$$(\mathfrak{q}B_{\mathfrak{p}}) \cap A_{\mathfrak{p}} = S^{-1}\mathfrak{q} \cap S^{-1}A = S^{-1}(\mathfrak{q} \cap A) = S^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}} \ ,$$

while $\mathfrak{p}A_{\mathfrak{p}}$ is the unique element of $\operatorname{mspec} A_{\mathfrak{p}}$.

Conversely, take $\mathfrak{m} \in \operatorname{mspec} B_{\mathfrak{p}}$. By Proposition 4.16, every ideal of $B_{\mathfrak{p}}$ is extended from B, and in particular $(\mathfrak{m}^c)B_{\mathfrak{p}} = \mathfrak{m}$ (and $\mathfrak{m}^c \in \operatorname{spec} B$). It remains to show that $\mathfrak{m}^c \cap A = \mathfrak{p}$. Consider the following commutative diagram:

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d] \\
A_{\mathfrak{p}} \arrow[r] & B_{\mathfrak{p}}
\end{tikzcd}$$

Contracting $\mathfrak{m}$ to $A_{\mathfrak{p}}$ and then to A results in the same prime ideal of A obtained by contracting $\mathfrak{m}$ to B and then to A. Since $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ is an integral extension, the contraction of $\mathfrak{m}$ to $A_{\mathfrak{p}}$ is a maximal ideal. But $\mathfrak{p}A_{\mathfrak{p}}$ is the unique maximal ideal of $A_{\mathfrak{p}}$, and it contracts to $\mathfrak{p}$ in A. Thus, $\mathfrak{m}^c \cap A = \mathfrak{p}$. □

The following proposition says that all fibers of $\iota^* \colon \operatorname{spec} B \to \operatorname{spec} A$ are not empty for an integral extension of rings $A \subset B$.

Proposition 9.2 (Lying over)**.** *Let $A \subset B$ be an integral extension of rings. Let $\mathfrak{p} \in \operatorname{spec} A$. Then there is $\mathfrak{q} \in \operatorname{spec} B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. Let $S = A \setminus \mathfrak{p}$. By Proposition 9.1, it suffices to show that $\operatorname{mspec} B_{\mathfrak{p}} \neq \emptyset$, i.e. that $B_{\mathfrak{p}}$ is not the zero ring. Indeed, $0 \notin S$, and so $B_{\mathfrak{p}} \neq 0$. □

Proposition 9.3 (Going up)**.** *Let $A \subset B$ be an integral extension of rings, let $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{spec} A$, $\mathfrak{p}_1 \subset \mathfrak{p}_2$, and $\mathfrak{q}_1 \in \operatorname{spec} B$, $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there is $\mathfrak{q}_2 \in \operatorname{spec} B$ such that $\mathfrak{q}_1 \subset \mathfrak{q}_2$ and $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.*

Proof. Since $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A$, we have an injective map $A/\mathfrak{p}_1 \hookrightarrow B/\mathfrak{q}_1$, $a + \mathfrak{p}_1 \mapsto a + \mathfrak{q}_1$, and $B/\mathfrak{q}_1$ is integral over $A/\mathfrak{p}_1$ by Proposition 6.13. By Proposition 9.2, there is $\mathfrak{q}_2/\mathfrak{q}_1 \in \operatorname{spec} B/\mathfrak{q}_1$, $\mathfrak{q}_2 \in \operatorname{spec} B$, that contracts to $\mathfrak{p}_2/\mathfrak{p}_1$ in $A/\mathfrak{p}_1$. Thus $\mathfrak{q}_2$ contains $\mathfrak{q}_1$, and $\mathfrak{q}_2$ contracts to $\mathfrak{p}_2$ in A by the following commutative diagram:

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d] \\
A/\mathfrak{p}_1 \arrow[r] & B/\mathfrak{q}_1
\end{tikzcd}$$

Indeed, $\mathfrak{q}_2/\mathfrak{q}_1$ contracts to $\mathfrak{p}_2/\mathfrak{p}_1$ in $A/\mathfrak{p}_1$, which contracts to $\mathfrak{p}_2$ in A. On the other hand, $\mathfrak{q}_2/\mathfrak{q}_1$ contracts to $\mathfrak{q}_2$ in B. The commutativity of the diagram implies that $\mathfrak{q}_2$ contracts to $\mathfrak{p}_2$ in A. □

Proposition 9.4 (Incomparability)**.** *Let $A \subset B$ be an integral extension of rings, and let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of B such that $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ and $\mathfrak{q} \subset \mathfrak{q}'$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Let $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. By Proposition 9.1, $\mathfrak{q}B_{\mathfrak{p}}$ and $\mathfrak{q}'B_{\mathfrak{p}}$ belong to $\operatorname{mspec} B_{\mathfrak{p}}$. Since $\mathfrak{q}B_{\mathfrak{p}} \subset \mathfrak{q}'B_{\mathfrak{p}}$, it follows that $\mathfrak{q}B_{\mathfrak{p}} = \mathfrak{q}'B_{\mathfrak{p}}$. By Proposition 9.1 again, we have $\mathfrak{q} = \mathfrak{q}'$. □

Proposition 9.5 (Going down)**.** *Let $A \subset B$ be an integral extension of integral domains, A integrally closed (in $\operatorname{Frac} A$). Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{spec} A$, $\mathfrak{p}_1 \supset \mathfrak{p}_2$, and $\mathfrak{q}_1 \in \operatorname{spec} B$, $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there is $\mathfrak{q}_2 \in \operatorname{spec} B$ such that $\mathfrak{q}_1 \supset \mathfrak{q}_2$ and $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.*

Proof. Consider the composite map $A \to B \to B_{\mathfrak{q}_1}$. The localization map is injective since B is an integral domain. We want to show that $\mathfrak{p}_2$ is contracted from a prime ideal $\mathfrak{n}$ of $B_{\mathfrak{q}_1}$ because then $\mathfrak{q}_2 := \mathfrak{n} \cap B$ is contained in $\mathfrak{q}_1$ and contracts to $\mathfrak{p}_2$ i n A. To show that $\mathfrak{p}_2$ is a contracted ideal w.r.t. $A \to B \to B_{\mathfrak{q}_1}$, we need to show that $(\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A \subset \mathfrak{p}_2$ (the reverse inclusion always holds when extending and then contracting). Think of the extension $\mathfrak{p}_2 B_{\mathfrak{q}_1}$ in two steps: $\mathfrak{p}_2 \mapsto \mathfrak{p}_2 B \mapsto \mathfrak{p}_2 B_{\mathfrak{q}_1}$.

Take $\frac{y}{s} \in (\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A$, $y \in \mathfrak{p}_2 B$, $s \in B \setminus \mathfrak{q}_1$ (every element of $\mathfrak{p}_2 B_{\mathfrak{q}_1}$ is of this form). Since B is integral over A, the integral closure of $\mathfrak{p}_2$ in B is $\sqrt{\mathfrak{p}_2 B}$. Thus y is integral over $\mathfrak{p}_2$. Thus, by Proposition 8.5, the minimal equation[39] of y over $\operatorname{Frac} A$ is of the form

$$y^r + \underbrace{u_1}_{\in \mathfrak{p}_2} y^{r-1} + \cdots + \underbrace{u_r}_{\in \mathfrak{p}_2} = 0 \ .$$

[39] The minimal equation is just the equation $f(y) = 0$, where f is the minimal polynomial of y over $\operatorname{Frac} A$.

Now, $\underbrace{y}_{\in B} = \underbrace{\frac{y}{s}}_{\in A}\underbrace{s}_{\in B}$, and so $y, s \in \operatorname{Frac} B$ and $\frac{y}{s} \in \operatorname{Frac} A$. Thus, the minimal equation of s over $\operatorname{Frac} A$ is obtained[40] by writing

$$\left(\frac{y}{s}s\right)^r + \underbrace{u_1}_{\in \mathfrak{p}_2}\left(\frac{y}{s}s\right)^{r-1} + \cdots + \underbrace{u_r}_{\in \mathfrak{p}_2} = 0$$

and dividing by $\left(\frac{y}{s}\right)^r$:

$$s^r + \underbrace{\left(\frac{s}{y}\right)^1}_{\in \operatorname{Frac} A}\underbrace{u_1}_{\in \mathfrak{p}_2} s^{r-1} + \cdots + \underbrace{\left(\frac{s}{y}\right)^r}_{\in \operatorname{Frac} A}\underbrace{u_r}_{\in \mathfrak{p}_2} = 0 \ . \tag{9.2}$$

But $s \in B$, and so s is integral over A, and thus Proposition 8.5 says that all of the coefficients $\left(\frac{s}{y}\right)^1 \underbrace{u_1}_{\in \mathfrak{p}_2}, \ldots, \left(\frac{s}{y}\right)^r \underbrace{u_r}_{\in \mathfrak{p}_2}$ are in A.

Suppose that $\frac{y}{s} \notin \mathfrak{p}_2$. Then $\underbrace{u_i}_{\in \mathfrak{p}_2} = \underbrace{\left(\frac{y}{s}\right)^i}_{\notin \mathfrak{p}_2}\underbrace{\left(\frac{s}{y}\right)^i u_i}_{\in A}$, and so $\left(\frac{s}{y}\right)^i u_i \in \mathfrak{p}_2$. Thus $s^r \in \underbrace{\mathfrak{p}_2 B}_{\subset \mathfrak{p}_1 B = (\mathfrak{q}_1 \cap A)B \subset \mathfrak{q}_1}$ by (9.2), and so $s \in \mathfrak{q}_1$, a contradiction. □

Definition 9.6. Let $f\colon A \to B$ be a ring homomorphism. Then,

(1) f is *finite* (resp. *integral*) if it makes B into a finite (resp. integral) A-algebra.
(2) f is *flat* if it makes B into a flat A-module.

Definition 9.7. Let $f\colon A \to B$ be a ring homomorphism. Consider the contraction map $f^*\colon \operatorname{spec} B \to \operatorname{spec} A$. Then,

(1) f *satisfies lying over* if f^* is surjective.
(2) f *satisfies going up* if for all $\mathfrak{p}_1 \subset \mathfrak{p}_2$ in $\operatorname{spec} A$ and $\mathfrak{q}_1 \in \operatorname{spec} B$ such that $f^*(\mathfrak{q}_1) = \mathfrak{p}_1$, there is $\mathfrak{q}_1 \subset \mathfrak{q}_2 \in \operatorname{spec} B$ such that $f^*(\mathfrak{q}_2) = \mathfrak{p}_2$.
(3) f *satisfies going down* if for all $\mathfrak{p}_1 \supset \mathfrak{p}_2$ in $\operatorname{spec} A$ and $\mathfrak{q}_1 \in \operatorname{spec} B$ such that $f^*(\mathfrak{q}_1) = \mathfrak{p}_1$ there is $\mathfrak{q}_1 \supset \mathfrak{q}_2 \in \operatorname{spec} B$ such that $f^*(\mathfrak{q}_2) = \mathfrak{p}_2$.

[40] In general, if we have a field extension $K \subset L$ and elements $x \in L$ and $0 \neq k \in K$, then the minimal equation of kx can be obtained from the minimal equation of x by multiplying by k^r, where r is the degree of the minimal polynomial of x over K. Indeed, this gives an equation showing that kx is algebraic over K, and if there was such an equation of lower degree, then we could divide by k^r to obtain a K-algebraicity equation for x of degree $< r$, a contradiction. Alternatively, one notes that the subfields $K(x)$ and $K(kx)$ of L are equal, and their dimensions over K are equal to the degrees of the minimal polynomails of x and kx over K, respectively, and thus these degrees are equal.

Remark 9.8. A ring extension $A \subset B$ that satisfies going up (i.e. the inclusion map $\iota\colon A \to B$ satisfies going up), must also satisfy lying over. **Proof:** Take $\mathfrak{p} \in \operatorname{spec} A$. Then $B_{\mathfrak{p}} \neq 0$ since $0 \notin A \setminus \mathfrak{p}$, and thus $B_{\mathfrak{p}}$ has a maximal ideal $\mathfrak{m}$. So the contraction $\mathfrak{q}$ of $\mathfrak{m}$ along the localization map $B \to B_{\mathfrak{p}}$ is a prime ideal of B such that $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$, i.e. $\mathfrak{q} \cap A \subset \mathfrak{p}$. By the going up property of $A \subset B$, applied to $\mathfrak{q} \cap A \subset \mathfrak{p}$, there is $\mathfrak{q}_2 \in \operatorname{spec} B$ such that $\mathfrak{q}_2 \cap A = \mathfrak{p}$.

Remark 9.9. We've seen that the inclusion map $\iota\colon A \to B$ of an integral extension of rings satisfies going up (and hence also lying over). But every ring homomorphism $f\colon A \to B$ can be decomposed as $A \to f(A) \to B$, where the first map is a quotient map, and the second map is the inclusion map of the extension $f(A) \subset B$. This extension is integral if and only if f is integral. A quotient map clearly satisfies lying over, going up and going down. We conclude that every integral ring homomorphism $f\colon A \to B$ satisfies going up (and hence also lying over).

Remark 9.10. **[non-examinable]** Every flat ring homomorphism $f\colon A \to B$ satisfies going down (with no further conditions on the rings A and B).

Remark 9.11. **[non-examinable]** The Cohen–Seidenberg theorems have geometric significance. For example, a ring homomorphism $f\colon A \to B$ satisfies going up if and only if $f^*\colon \operatorname{spec} B \to \operatorname{spec} A$ is a closed map under the Zariski topology (i.e. maps closed sets to closed set). This is in contrast to regular maps in general, say $\varphi\colon X \to \mathbb{C}$, where $X = \{(a,b) \in \mathbb{C}^2 \mid ab = 1\}$ and $\varphi(a,b) = x$. Then $\operatorname{im}\varphi = \mathbb{C} \setminus \{0\}$ is not closed in the Zariski topology (since every polynomial vanishing on $\mathbb{C} \setminus \{0\}$ must vanish on the larger set $\mathbb{C}$). This implies that the natural $\mathbb{C}$-algebra map $\mathbb{C}[T_1] \to \mathbb{C}[T_1, T_2]/(T_1T_2 - 1)$ is not integral, as we've shown directly in the discussion preceding Noether's normalization lemma.

10. Primary Decomposition

Let p be a prime number and $n \geq 2$. Then $\mathbb{Z}/(p^n)$ is not an integral domain, but for every zero divisor $a + \mathbb{Z} \in \mathbb{Z}/(p^n)$ we have $p \mid a$ and so $(a + \mathbb{Z})^n = 0$, and thus $a + \mathbb{Z}$ is nilpotent. Thus, for every $n \geq 1$, every zero divisor in $\mathbb{Z}/(p)^n$ is nilpotent.

On the other, in $\mathbb{Z}/(6)$, the elements $2 + \mathbb{Z}$ and $3 + \mathbb{Z}$ are zero divisors, but not nilpotent.

Definition 10.1. Let I be an ideal of R. Then[41]:

i) I is *prime* if $R/I \neq 0$ and the only zero divisor in R/I is 0.

[41] We recall the notions of prime and radical ideals in order to compare them to the notion of primary ideals.

ii) I is *radical* if the only nilpotent element in R/I is 0.
iii) I is *primary* if $R/I \neq 0$ and all zero divisors in R/I are nilpotent.

Thus, an ideal is prime if and only if it is radical and primary. Note that R itself is a radical ideal, but R is neither prime nor primary. Since every nilpotent element is a zero divisor, we have the following implications:

Example 10.2. Let $R = \mathbb{Z}$. Then (0) is a prime ideal (hence also radical and primary). Let $0 \neq x \in \mathbb{Z}$. Then,

i) (x) is prime if and only if $|x|$ is a prime number.
ii) (x) is radical if and only if x is square-free.
iii) (x) is primary if and only if $x = p^n$, $n \geq 1$, for some prime number p.

Example 10.3. Thus (6) is radical, but not primary, while (9) is primary but not radical. In $\mathbb{Z}$, an ideal is primary if and only if it is a power $\mathfrak{p}^n$ of a prime ideal $\mathfrak{p}$. But in general rings, the powers of prime ideals are not the same as the primary ideals (we will give examples).

Proposition 10.4. *Let I be an ideal of R.*

i) *If I is primary then $\sqrt{I} \in \operatorname{spec} R$.*
__Definition:__ For $\mathfrak{p} \in \operatorname{spec} R$, a $\mathfrak{p}$-primary ideal is a primary ideal such that $\sqrt{I} = \mathfrak{p}$.
ii) *If $\underbrace{\sqrt{I}}_{=:\mathfrak{m}} \in \operatorname{mspec} R$ then I is primary $\mathfrak{m}$-primary.*
(but if $\sqrt{I} \in \operatorname{spec} R$, I does not have to be primary).
iii) *$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is $\mathfrak{p}$-primary if $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary.*
iv) *If I has a primary decomposition (i.e. an expression $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, $\mathfrak{q}_i$ primary), then it has a minimal primary decomposition (i.e. an expression as above, where the prime ideals $\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}$ are distinct and $I \subsetneq \bigcap_{j \neq i} \mathfrak{q}_i$ for all $1 \leq j \leq n$).*
[This follows immediately from (iii)]
v) *If R is noetherian, then every ideal I of R has a primary decomposition.*

Proof. See Example Sheet 3. □

Example 10.5. In $\mathbb{Z}$, $(90) = (2) \cap \left(3^2\right) \cap (5)$ is a primary decomposition. Primary decomposition in general rings generalizes the notion of factorization into prime powers in $\mathbb{Z}$, but the general concept only has partial uniquenss properties (see below). In the computation below, we will make use of ES3.6(a): for ideals I and J of a ring R, we have $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$,$\sqrt{I^n} = \sqrt{I}$ for all $n \geq 1$, and [$1 \in I$ if and only if $1 \in \sqrt{I}$].

Let $\mathfrak{p} \in \operatorname{spec} R$, $n \geq 1$. If $\mathfrak{p}^n$ is primary then $\mathfrak{p}^n$ is $\mathfrak{p}$-primary since $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.

i) **Not every primary ideal is a power of a prime ideal:** Let $R = k[X,Y]$ and $\mathfrak{q} = \big(X, Y^2\big)$. Then $R/\mathfrak{q} \cong k[Y]/\big(Y^2\big)$, where every zero divisor is a multiple of Y and hence is nilpotent, and so $\mathfrak{q}$ is primary. Moreover,

$$\begin{aligned}\sqrt{\mathfrak{q}} &= \sqrt{(X) + (Y)^2}\\ &= \sqrt{\underbrace{\sqrt{(X)}}_{=(X)} + \underbrace{\sqrt{(Y)^2}}_{=(Y)}}\\ &= \sqrt{\underbrace{(X) + (Y)}_{=(X,Y)}}\\ &= (X,Y)\end{aligned}$$

where the last equality follows since $\mathfrak{m} \coloneqq (X,Y)$ is a maximal ideal. Thus, if $\mathfrak{q} = \mathfrak{p}^n$ for some $\mathfrak{p} \in \operatorname{spec} R$ and $n \geq 1$ then necessarily $\mathfrak{p} = \mathfrak{m}$. However $\mathfrak{m}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{m}$, and so $\mathfrak{q}$ is not a power of a prime ideal.

ii) **A power $\mathfrak{p}^n$ of a prime ideal $\mathfrak{p}$ is not necessarily primary (although $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ must be prime):** Let $R = k[X,Y,Z]/\big(XY - Z^2\big)$, k a field, and let $\overline{X}, \overline{Y}, \overline{Z}$ be the images of X, Y, Z in R, respectively. Then $\mathfrak{p} = \big(\overline{X}, \overline{Z}\big)$ is prime since $R/\mathfrak{p} \cong k[Y]$ is an integral domain. But $\mathfrak{p}^2 = \Big(\overline{X}^2, \overline{Z}^2, \overline{XZ}\Big)$ is not primary: $\overline{XY} = \overline{Z}^2 \in \mathfrak{p}^2$ and $\overline{X} \notin \mathfrak{p}^2$, and so the image of $\overline{Y}$ in $R/\mathfrak{p}^2$ is a zero divisor, but the image of $\overline{Y}$ in $R/\mathfrak{p}^2$ is not nilpotent: Indeed, $\overline{Y}$ does not belong to the radical $\sqrt{\mathfrak{p}^2} = \mathfrak{p} = \big(\overline{X}, \overline{Z}\big)$ of $\mathfrak{p}^2$ since $R/\mathfrak{p} \cong k[Y]$ in the natural way (i.e. $\overline{Y}$ does not vanish in the quotient $R/\mathfrak{p}$).

Theorem 10.6. *Let I be an ideal of R that has*[42] *a minimal primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, and write $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.*

i) ***The associated prime ideals of I:*** *$\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ depend only on I (and not on the chosen minimal primary decomposition). In fact,*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \Big\{\sqrt{(I : x)} \mid x \in R\Big\} \cap \operatorname{spec} R$$

(the RHS clearly depends only on I).

ii) ***The isolated prime ideals of I:*** *The set of minimal elements among $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ consists exactly of the prime ideals of R corresponding to the minimal prime ideals of R/I.*

[42] Equivalently, we can just assume that I has any primary decomposition, by the previous proposition. Note that not every ideal in every ring has a primary decomposition - having a primary decomposition is an assumption about I.

The embedded prime ideals of I***:*** *An associated prime ideal of* I *is* embedded *if it is not isolated.*

iii) ***The isolated primary components of*** I***:*** *If* $\mathfrak{p}_1, \dots, \mathfrak{p}_t$*,* $t \le n$*, are the isolated prime ideals of* I*, then* $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ *depend only on* I *(in fact,* $\mathfrak{q}_i = I^{ec}$ *w.r.t. the localization map* $R \to R_{\mathfrak{p}_i}$*).*

Proof. (1) and (2) are exercises in Example Sheet 3. We skip the proof of (3), but you can find it in Atiyah–Macdonald. □

Example 10.7. Let $R = k[X,Y]$, k a field, and $I = \big(X^2, XY\big)$. Then:

$$I = (X) \cap \underbrace{(X,Y)^2}_{=(X^2,XY,Y^2)}$$

$$I = (X) \cap \big(X^2, Y\big)$$

are both primary decompositions of I:

i) (X) is prime and hence (X)-primary.

ii) $\sqrt{(X,Y)^2} = (X,Y)$ and $\sqrt{(X^2,Y)} = (X,Y)$, and (X,Y) is a maximal ideal, and so $(X,Y)^2$ and $\big(X^2,Y\big)$ are (X,Y)-primary.

iii) $\underbrace{(X,Y)^2}_{=(X^2,XY,Y^2)} \neq \big(X^2, Y\big)$ since, e.g. $Y \notin (X,Y)^2$.

iv) $I = (X) \cap (X,Y)^2$: $\subset$ is clear. Take $f \in (X) \cap (X,Y)^2$. Then $f = aX = bX^2 + cXY + dY^2$, $a,b,c,d \in k[X,Y]$. Then $d = eX$, $e \in k[X,Y]$. Thus $X\big(a - bX - cY - eY^2\big) = 0$, and so $a \in (X,Y)$, and thus $f \in X(X,Y) = I$.

v) $I = (X) \cap \big(X^2,Y\big)$: $\subset$ is clear. Take $f \in (X) \cap \big(X^2, Y\big)$. Then $f = aX = bX^2 + cY$, $a,b,c \in k[X,Y]$. Then $c = dX$, $d \in k[X,Y]$, and thus $X(a - bX - dY) = 0$, and so $a \in (X,Y)$, and hence $f \in X(X,Y) = I$.

vi) So, the associated primes of I are $(X) \subset (X,Y)$, and thus (X) is the only isolated prime of I, and (X) is also the only isolated primary component of I.

Remark 10.8. Let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a minimal primary decomposition of I, $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ are the isolated prime ideals of I. Then $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$ (check!), and this is a minimal primary decomposition of $\sqrt{I}$ because $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ are distinct, and there are no inclusions between them, and if $\bigcap_{i \neq j} \mathfrak{p}_i \subset \mathfrak{p}_j$ then $\mathfrak{p}_i \subset \mathfrak{p}_i$ for some $i \neq j$ (ES2.2a), a contradiction.

Thus, if I is radical (i.e. $I = \sqrt{I}$) then I has a unique primary decomposition (the intersection of the associated prime ideals of I, which are all isolated). That is, for radical ideals the situation is simple in the following senses: (i) There are no embedded primes, (ii) The isolated primary components are the isolated primes. So, in a noetherian ring (where all ideals have a primary decomposition), to give a radical ideal is the same as to give a finite collection $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ of prime ideals such that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all i, j.

So, in a noetherian ring R, the process of passing from I to $\sqrt{I}$ amounts to remembering only the isolated prime ideals of I and forgetting all other information about I. In $R = k[T_1, \dots, T_n]$ (fixing some algegbraically closed field $\Omega \supset k$), we have $V(I) = V\left(\sqrt{I}\right)$ and $I(V(I)) = \sqrt{I}$. Thus, the information recorded by the algebraic set $V(I)$ is exactly $\sqrt{I}$, or, equivalently, the set of isolated primes of I.

Remark 10.9. The notions of isolated and embedded primes of an ideal, and of the isolated primary components, are central. The notion of the primary decomposition is less useful in modern algebraic geometry, mostly because of the non-uniqueness. Still, primary decompositions can be useful when making explicit computations and coming up with counter-examples.

Remark 10.10. **[non-examinable]** For some rings R, not every ideal I has a primary decomposition. If I has a primary decomposition, we've seen that the set of isolated primes of I is, on one hand, finite, and on the other hand, equal to the set of minimal prime ideals among those containing I. So, if we construct a ring R that has infinitely many minimal primes ideals, then the ideal (0) of R does not have a prime decomposition. The ring $C[0, 1]$ of continuous functions $[0, 1] \to \mathbb{R}$ is an example of this.

11. Direct and inverse limits, completions

Definition 11.1. Let[43] $\mathcal{C}$ be one of the following categories: Sets, Groups, Rings, R-modules, R-algebras (R a fixed ring).

i) A *directed set* $(I, \leq)$ is a partially ordered set such that $\forall a, b \in I$ there is $c \in I$ such that $a \leq c$ and $b \leq c$.
ii) A *direct system* over I is a pair $\left((X_i)_{\in I}, (f_{ij})_{\substack{i,j \in I \\ i \leq j}}\right)$, where each X_i is an object and each $f_{ij} \colon M_i \to M_j$ is a morphism, such that:
   (a) $f_{ii} = \mathrm{id}_{X_i}$ for all i.
   (b) $f_{jk} \circ f_{ij} = f_{ik}$ for $i \leq j \leq k$.
iii) An *inverse system* over I is a pair $\left((Y_i)_{\in I}, (h_{ij})_{\substack{i,j \in I \\ i \leq j}}\right)$, where each Y_i is an object and each $f_{ij} \colon Y_j \to Y_i$ is a morphism, such that:
   (a) $h_{ii} = \mathrm{id}_{Y_i}$ for all i.
   (b) $h_{ij} \circ h_{jk} = h_{ki}$ for all $i \leq j \leq k$.

[43] Direct and inverse limits are more general, but I prefer we limit ourselves to these categories.

Example 11.2. Let $I = \mathbb{N}$ with the usual order $\leq$. Let p be a prime number.

i) Recall that for $a, b \in \mathbb{N}$, if $a \mid b$ then there is a ring[44] embedding $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$.
Let $X_i = \mathbb{F}_{p^{i!}}$, let $f_{i,(i+1)} \colon \mathbb{F}_{p^{i!}} \to \mathbb{F}_{p^{(i+1)!}}$ be a fixed ring embedding for all $i \geq 1$, and let $f_{ij} = f_{(j-1),j} \circ \cdots \circ f_{i,(i+1)}$ for $i \leq j$.
Then $\Big((X_i), (f_{ij})_{i \leq j}\Big)$ is a direct system.

ii) Let $Y_i = \mathbb{Z}/p^i\mathbb{Z}$, and for $i \leq j$, let $h_{ij} \colon \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ be the natural projection.
Then $\Big((Y_i), (h_{ij})_{i \leq j}\Big)$ is an inverse system.

Definition 11.3. Let $(I, \leq)$ be a directed set.

i) Let $D = \Big((X_i)_{i \in I}, (f_{ij})_{i \leq j}\Big)$ be a direct system on I. The *direct limit*

$$\varinjlim X_i$$

of D is $\left(\coprod_{i \in I} X_i\right)/\sim$, where $\sim$ is the smallest equivalence relation such that $x_i \sim f_{ij}(x_i)$ for all $i \leq j$ and $x_i \in X_i$.
Equivalently, $x_i \sim x_j$ for $x_i \in X_i$ and $x_j \in X_j$ if and only if there is $k \in I$, $k \geq i$, $k \geq j$, such that $f_{ik}(x_i) = f_{jk}(x_j)$.

ii) *Let $E = \Big((Y_i)_{i \in I}, (h_{ij})_{i \leq j}\Big)$ be an inverse system on I. The* inverse limit

$$\varprojlim Y_i$$

of E is

$$\left\{ \mathbf{y} \in \prod_{i \in I} Y_i \mid y_i = h_{ij}(y_j) \qquad \forall i \leq j \right\} .$$

The notations $\varinjlim$ and $\varprojlim$ for the direct and inverse limits, respectively, supress the morphisms f_{ij}, but the morphisms are crucial to the constructions and must be understood from the context.

The direct limit is equipped with natural homomorphisms $X_j \to \varinjlim X_i$ for all $j \in I$. The inverse limit is equipped with natural homomorphisms $\varprojlim Y_i \to Y_j$ for all $j \in I$.

Example 11.4.

i) $\varinjlim \mathbb{F}_{p^i}$ is a field, with a ring homomorphism $\mathbb{F}_p \to \varinjlim \mathbb{F}_{p^i}$ (necessarily injective).

[44] In general, a ring homomorphism between fields is a field homomorphism. The two notions are the same (when the domain and range rings are fields).

(a) $\varinjlim \mathbb{F}_{p^i}$ is algebraic over $\mathbb{F}_p$. Indeed, take $[x] \in \big(\coprod_{i\in I} \mathbb{F}_{p^{i!}}\big)/\sim$, $x \in \coprod_{i\geq 1} \mathbb{F}_{p^i}$ ($[\cdot]$ standing for the $\sim$-equivalence class). Then $x \in \mathbb{F}_{p^{i!}}$ for some $i \geq 1$, and so $x^{p^{i!}} - x = 0$. Thus $[x]^{p^{i!}} - [x] = 0$, and so $[x]$ is algebraic over $\mathbb{F}_p$.

(b) The field $\varinjlim \mathbb{F}_{p^i}$ is algebraically closed: Every polynomial in $\big(\varinjlim \mathbb{F}_{p^i}\big)[T]$ is of the form $[h]$, $h \in \mathbb{F}_{p^{j!}}[T]$ for some $j \geq 1$ ($[h]$ here denotes the result of applying $[\cdot]$ to each coefficient of h). The splitting field of h over $\mathbb{F}_{p^{j!}}$ is isomorphic to a finite field $\mathbb{F}_{p^\ell}$, $j! \mid \ell$, and $\mathbb{F}_{p^\ell}$ embeds in $\mathbb{F}_{p^{\ell!}}$. So, h splits over $\mathbb{F}_{p^{\ell!}}$ under some embedding $\mathbb{F}_{p^{j!}} \to \mathbb{F}_{p^{\ell!}}$. Thus h splits over $\mathbb{F}_{p^{\ell!}}$ under every[45] embedding $\mathbb{F}_{p^{j!}} \to \mathbb{F}_{p^{\ell!}}$, and in particular under the embedding $f_{j\ell}\colon \mathbb{F}_{p^{j!}} \to \mathbb{F}_{p^{\ell!}}$. Thus $[h] = [f_{j\ell}(h)]$ splits in $\varinjlim \mathbb{F}_{p^i}$ (here $f_{j\ell}(h)$ refers to applying $f_{j\ell}$ to each coefficient of h).

ii) $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ the *ring of p-adic integers.*
For example $p = 5$. Each sequence $(d_i)_{i=0}^\infty$ of integers, $0 \leq d_i < 5$, gives rise to an element of $\mathbb{Z}_5$: $x = \Big(\sum_{k=0}^{i-1} d_k \cdot 5^k + 5^i\mathbb{Z}\Big)_{i=1}^\infty$. You can think of x as a number written in base 5, where the digits extend to the left. The natural map $\mathbb{Z}_5 \to \mathbb{Z}/5^i\mathbb{Z}$ reveals the rightmost i digits. The number 1 in $\mathbb{Z}_5$ is simply $\big(1 + 5^i\mathbb{Z}\big)_{i=1}^\infty$. The number -1 in $\mathbb{Z}_5$ is

$$\big(4 + 5\mathbb{Z}, 24 + 5^2\mathbb{Z}, 124 + 5^3\mathbb{Z}, 624 + 5^4\mathbb{Z}, \dots\big)$$

or, in base 5:

$$\big(4_5 + 5\mathbb{Z}, 44_5 + 5^2\mathbb{Z}, 444_5 + 5^3\mathbb{Z}, 4444_5 + 5^4\mathbb{Z}, \dots\big)\ .$$

Remark 11.5. Our example of a direct limit was to form the "union" of a collection of sets which are not subsets of one large sets, but have some identifications between them. Another type of example is given by *stalks* in algebraic geometry. There X_i is the set of certain functions on a certain neighbourhood U_i of a fixed point x in some fixed space, and each morphsim $f_{ij}\colon X_i \to X_j$ of the directed set is the restriction map, from U_i to U_j, of functions (where $i \leq j$ if $U_j \subset U_i$).

[45] Let $a \mid b$ be positive integers, and take two field embeddings $\sigma, \tau\colon \mathbb{F}_{p^a} \to \mathbb{F}_{p^b}$. Then $\sigma(\mathbb{F}_{p^a}) = \tau(\mathbb{F}_{p^a})$ because $\mathbb{F}_{p^b}$ contains a unique copy of $\mathbb{F}_{p^a}$ (namely, the set of roots of $T^{p^a} - T$). Thus, we have a field automorphism $\mathbb{F}_{p^a} \to \mathbb{F}_{p^a}$ given by $x \mapsto \sigma^{-1}(\tau(x))$. A field automorphism of $\mathbb{F}_{p^a}$ must be of the form $x \mapsto x^{p^s}$, $s \geq 0$, and so $\sigma^{-1}(\tau(x)) = x^{p^s}$ for all $x \in \mathbb{F}_{p^a}$, i.e. $\tau(x) = \sigma\Big(x^{p^s}\Big) = (\sigma(x))^{p^s}$. Note that $y \mapsto y^{p^s}$ defines an automorphism of $\mathbb{F}_{p^b}$ (not only of $\mathbb{F}_{p^a}$ and of its copy inside $\mathbb{F}_{p^b}$). Now take a polynomial $h \in \mathbb{F}_{p^a}[T]$ such that $\sigma(h) \in \mathbb{F}_{p^b}[T]$ splits into linear factors $\sigma(h) = \prod_{i=1}^\ell \Bigg(T - \underbrace{\alpha_i}_{\in \mathbb{F}_{p^b}}\Bigg)$. Then $\tau(h) = \prod_{i=1}^\ell \Big(T - \alpha_i^{p^s}\Big)$, and so $\tau(h)$ also splits into linear factors over $\mathbb{F}_{p^b}$.

Example 11.6. Let $(I, \leq)$ be a directed set. Let $D = (X_i, f_{ij})$ be a direct system on I, and let $E = (Y_i, h_{ij})$ be an inverse system on I. Then $\varinjlim X_i$ (resp. $\varprojlim Y_i$) enjoys a universal property w.r.t. D (resp. E) that characterizes it uniquely:

(1) **The universal property of the direct limit:**
For an object A and a system of morphisms $(g_i \colon X_i \to A)_{i\in I}$ such that $g_i = g_j \circ f_{ij}$ for all $i \leq j$, there is a unique morphism $g\colon \varinjlim X_i \to A$ such that each g_i factors as $X_j \longrightarrow \varinjlim X_i \xrightarrow{g_i} A$, where the left map is the canonical map from X_j to the direct limit.
Example: In the category of sets, a function from the disjoint $\coprod_i X_i$ union of sets into a set A is the same as a a collection of functions $(X_i \to A)_{i\in I}$ (this example is quite degenrate: the partial order $\leq$ is reflextive $x \leq x$, but has no other relations, so the direct system has no morphisms).

(2) **The univesal property of the inverse limit:**
For an object B and a system of morphisms $(g_i \colon B \to Y_i)_{i\in I}$ such that $g_i = h_{ij} \circ g_j$ for all $i \leq j$, there is a unique morphism $g\colon B \to \varprojlim Y_i$ such that each g_j factors as $B \xrightarrow{g} \varprojlim Y_i \longrightarrow Y_j$, where the right morphism is the canonical map from the inverse limit to Y_j.
Example: Take the quotient maps $g_i \colon \mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$. Then, for $i \leq j$, g_i factors as $\mathbb{Z} \xrightarrow{g_j} \mathbb{Z}/p^j\mathbb{Z} \xrightarrow{h_{ij}} \mathbb{Z}/p^i\mathbb{Z}$. This gives rise to a map $g\colon \mathbb{Z} \to \underbrace{\varprojlim \mathbb{Z}/p^i\mathbb{Z}}_{=:\mathbb{Z}_p}$ given by $g(x) = \big(x + p^i\mathbb{Z}\big)_{i=1}^{\infty}$.

We now generalize the construction of $\mathbb{Z}_p$.

Definition 11.7. Given a ring R and an ideal $\mathfrak{a}$ of R, the $\mathfrak{a}$-dic completion of R is $\hat{R} = \varprojlim R/\mathfrak{a}^i$.

More precisely, we have a directed set $(\mathbb{N}, \leq)$, $\leq$ being the usual order on $\mathbb{N}$, and an inverse system $\Big(\big(R/\mathfrak{a}^i\big)_{i=1}^{\infty}, (f_{ij})_{i\leq j}\Big)$, where $f_{ij}\colon R/\mathfrak{a}^j \to R/\mathfrak{a}^i$ is the usual projection.

Example 11.8.

i) For $R = \mathbb{Z}$ and $\mathfrak{a} = (p)$, p a prime number, we have $\hat{R} = \mathbb{Z}_p$.
ii) For $R = k[T]$, k a field, and $\mathfrak{a} = (T)$, we have $\hat{R} = k[[T]]$, the ring of formal power series in T over k.
iii) For $R = k[T]$ and $\mathfrak{a} = (T_1, \ldots, T_n)$, we have $\mathfrak{a}^i = \mathrm{span}_k\{T_1^{e_1} \cdots T_n^{e_n} \mid e_1 + \cdots + e_n \geq i\}$, and so $\hat{R} = k[[T_1, \ldots, T_n]]$, the ring of formal power series in $T_1, \ldots, T_n$ over k.

There is a similar construction for modules:

Definition 11.9. For an R-module M and an ideal $\mathfrak{a}$ of R, the $\mathfrak{a}$-adic completion of M is $\hat{M} = \varprojlim M/\mathfrak{a}^i M$.

The $\mathfrak{a}$-adic completion is a special case of the following:

Definition 11.10. Let M be an R-module.

i) A *filtration* of M is a sequence of submodules $(M_n)_{n\geq 0}$ such that $M_n \supset M_{n+1}$ and $M_0 = M$.
ii) The completion of M w.r.t. to the filtration $(M_n)_{n\geq 0}$ is $\varprojlim M/M_n$ (this refers to the direct system on $\mathbb{N}$ with M/M_n as the objects, and with the projections as the morphisms).

So the $\mathfrak{a}$-adic completion of an R-module M is the completion of M w.r.t. the filtration $\left(\mathfrak{a}^i M\right)_{i=0}^{\infty}$.

Relative to the $\mathfrak{a}$-adic completions, $\hat{M}$ becomes an $\hat{R}$-module:

$$\left(r_i + \mathfrak{a}^i\right)_{i\geq 0} \cdot \left(m_i + \mathfrak{a}^i M\right)_{i\geq 0} := \left(r_i m_i + \mathfrak{a}^i M\right)_{i\geq 0} .$$

Recall that for a multiplicative subset S of R: (i) If R is noetherian then $S^{-1}R$ is noetherian, (ii) $S^{-1}R \otimes_R (\cdot)$ is a flat R-module (equivalently, $M \mapsto S^{-1}M$, $f \mapsto S^{-1}f$, is an exact functor). The analogous results for $\mathfrak{a}$-adic completions are:

Theorem 11.11. *Let R be a noetherian ring, and let $\hat{R}$ be the $\mathfrak{a}$-adic completion of R, $\mathfrak{a}$ an ideal of R. Then:*

i) *$\hat{R}$ is noetherian.*
ii) *$\hat{R} \otimes_R (\cdot)$ is an exact functor.*
iii) *If M is a finitely generated R-module then the map $\hat{R} \otimes_R M \to \hat{M}$, sending $x \otimes m \mapsto xm$, is an $\hat{R}$-linear isomorphism.*

Notably, all parts of Theorem 11.11 assume that the ring R is noetherian. For a noetherian R, restricting attention to finitely generated R-modules, (ii) and (iii) together imply that $M \mapsto \hat{M}$ is an exact functor.

As a consequence of Theorem 11.11(i) and Hilbert's basis theorem, we have:

Corollary 11.12. *If R is a noetherian ring then $R[[T_1, \ldots, T_n]]$ is noetherian.*

Proof. $R[[T_1, \ldots, T_n]]$ is isomorphic to the $\mathfrak{m}$-adic completion of $R[T_1, \ldots, T_n]$ for $\mathfrak{m} = (T_1, \ldots, T_n)$. □

We will not prove Theorem 11.11. The proof could be found in the excellent Chapter 10 of Atiyah–Macdonald. We will, however, study some of the technical tools of that chapter: exactly those tools that will also be needed in the chapter on dimension theory.

12. Filtrations, Graded rings

12.1. **Graded rings and modules.**

Definition 12.1. A graded ring is a ring A together with a family $(A_n)_{n\geq 0}$ of additive subgroups of A such that $A = \bigoplus_{n=0}^{\infty} A_n$ (internal direct sum) and $A_m A_n \subset A_{m+n}$ for all $m, n \geq 0$.

Note that A_0 is a subring of A:

(1) A_0 is clearly an abelian subgroup of A, and is closed under multiplication since $A_0 A_0 \subset A_{0+0}$.

(2) We show that $1_A \in A_0$: Write $1_A = \sum_{i=0}^{m} y_i$, $y_i \in A_i$. Let $z_n \in A_n$, $n \geq 0$. Then $\underbrace{z_n}_{\in A_n} = 1_A z_n = \sum_{i=0}^{m} \underbrace{y_i z_n}_{\in A_{n+i}}$. The LHS is in A_n and so the RHS is equal to $\underbrace{y_0}_{\in A_0} z_n$. Thus $y_0 z = z$ for all $z \in A$, and so $1_A = y_0 \in A_0$.

Thus, each A_m is an A_0-module.

Example 12.2. $k[T_1, \ldots, T_r] = \bigoplus_{n\geq 0}^{\infty} A_n$, where A_n is the set of consisting of 0 and all homogeneous polynomials of degree n.

Definition 12.3. Let $A = \bigoplus_{n\geq 0}^{\infty} A_n$ be a graded ring.

(1) A *graded A-module* is an A-module M, $M = \oplus_{n\geq 0}^{\infty} M_n$, M_n an additive subgroup of M, such that $A_m M_n \subset M_{m+n}$ for all $m, n \geq 0$ (thus each M_n is an A_0-module).

(2) A *homomorphism of graded A-modules* is an A-module homomorphism $f\colon \bigoplus_{n\geq 0} M_n \to \bigoplus_{n\geq 0} N_n$ such that $f(M_n) \subset N_n$ for all $n \geq 0$.

(3) An element $x \in M$ is *homogeneous* of *degree n* if $x \in M_n$. Any $y \in M$ can be written as $y = \sum_n y_n$, $y_n \in M_n$, where all but finitely many y_n's are 0. The nonzero y_n are the *homogeneous components* of y.

(4) Write $A_+ = \oplus_{n\geq 1}^{\infty} A_n$ (then A_+ is an ideal of A: $\ker(A \to A_0) = A_+$ for the natural projection $A \to A_0$).

Proposition 12.4. *The following are equivalent for a graded ring $A = \bigoplus_{n=0}^{\infty} A_n$:*

i) *A is noetherian.*

ii) *A_0 is noetherian and A is finitely generated as an A_0-algebra.*

Proof. (ii) $\Rightarrow$ (i) by Hilbert's basis theorem.

Assume (i). Then the ring A_0 is noetherian since $A_0 \cong A/A_+$. Now, the ideal A_+ is generated by the set of all homogeneous elements of A of nonzero degree, and so, since A is noetherian, the ideal A_+ is also generated by a finite set $x_1, \ldots, x_s$ of homogeneous elements, $x_i \in A_{k_i}$ (respectively), $k_i > 0$.

Let A' be the A_0-subalgebra of A generated by $x_1, \dots, x_s$. It suffices to show that $A_n \subset A'$ for all $n \geq 0$. We argue by induction on n. Clearly $A_0 \subset A'$. Now take $y \in A_n$, $n > 0$. Since $y \in A_+$, we have $\underbrace{y}_{\in A_n} = \sum_{i=1}^s r_i x_i$, $r_i \in A$. Applying the projection $A \to A_n$, y stays y, and $r_i x_i$ is mapped to $a_i x_i$ for some $a_i \in A_{n-k_i}$. So $y = \sum_{i=1}^s a_i x_i$. By the induction hypothesis (note that $k_i > 0$), each a_i is a polynomial in $x_1, \dots, x_s$ with coefficients in A_0. Hence $y \in A'$. □

12.1.1. *The associated graded ring.*

Definition 12.5. Let $\mathfrak{a}$ be an ideal of R.

i) A filtration of an R-module M is a sequence $(M_n)_{n=0}^\infty$ of submodules of M such that $M_0 = M$ and $M_n \supset M_{n+1}$ for all $n \geq 0$.
ii) The filtration $(M_n)_{n=0}^\infty$ is an $\mathfrak{a}$-filtration if $\mathfrak{a}M_n \subset M_{n+1}$ for all $n \geq 0$.
iii) An $\mathfrak{a}$-filtration $(M_n)_{n=0}^\infty$ is $\mathfrak{a}$-stable if $\mathfrak{a}M_n = M_{n+1}$ for all large enough n.

Example 12.6. $(\mathfrak{a}^n M)_{n \geq 0}$ is a stable $\mathfrak{a}$-filtration.

Definition 12.7. Let $\mathfrak{a}$ be an ideal of R. The associated graded ring of R (w.r.t. $\mathfrak{a}$) is

$$G_{\mathfrak{a}}(R) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n / \mathfrak{a}^{n+1} \qquad (\mathfrak{a}^0 = A)$$

This a graded ring, where multiplication is defined as follows: For $x \in \mathfrak{a}^n$ and $y \in \mathfrak{a}^m$, if $\overline{x}, \overline{y}$ are the images of x, y in the summands $\mathfrak{a}^n/\mathfrak{a}^{n+1}$, $\mathfrak{a}^m/\mathfrak{a}^{m+1}$ (respectively), then $\overline{x} \cdot \overline{y}$ is the image of xy in $\mathfrak{a}^{n+m}/\mathfrak{a}^{n+m+1}$ (check that this is well defined!).

For an R-module M and an $\mathfrak{a}$-filtration $(M_n)_{n \geq 0}$, define

$$G(M) = \bigoplus_{n=0}^{\infty} M_n / M_{n+1} \ ,$$

which is a graded $G_{\mathfrak{a}}(R)$-module in a natural way: For $x \in \mathfrak{a}^n$ and $m \in M_k$, if $\overline{x}, \overline{m}$ are the images of x and m in $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ and M_k/M_{k+1} (respectively), then $\overline{x} \cdot \overline{m}$ is the image of xm in M_{k+n}/M_{k+n+1}. We write $G_n(M)$ for M_n/M_{n+1}.

Proposition 12.8. *Assume that the ring R is noetherian. Let $\mathfrak{a}$ be an ideal of R. Then:*

i) *$G_{\mathfrak{a}}(R)$ is a noetherian ring.*
ii) *If M is a finitely generated R-module and $(M_n)_{n \geq 0}$ is a stable $\mathfrak{a}$-filtration of M, then $G(M)$ is a finitely generated graded $G_{\mathfrak{a}}(R)$-module.*

Proof. (i) Since R is noetherian, $\mathfrak{a}$ is finitely generated by some $x_1, \ldots, x_s$ Let $\overline{x}_i$ be the image of x_i if $\mathfrak{a}/\mathfrak{a}^2$. Then $G_{\mathfrak{a}}(R) = (R/\mathfrak{a}) \oplus \bigoplus_{n=1}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}$ is generated as an $R/\mathfrak{a}$-algebra by $\overline{x}_1, \ldots, \overline{x}_n$ (check!). But $R/\mathfrak{a}$ is a noetherian ring, so $G_{\mathfrak{a}}(R)$ is noetherian by Hilbert's basis theorem.

(ii) Take n_0 such that $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ for all $r \geq 0$. Then $G(M)$ is generated by $\bigoplus_{n \leq n_0} M_n/M_{n+1}$ as a $G_{\mathfrak{a}}(R)$-module. Each M_n/M_{n+1} is a noetherian R-module (M is noetherian since it is finitely generated over the noetherian ring R, and so M_n also is), and is annihilated by $\mathfrak{a}$. So it is a finitely generated $R/\mathfrak{a}$-module, and thus $\bigoplus_{n \leq n_0} M_n/M_{n+1}$ is a finitely generated $R/\mathfrak{a}$-module. Thus $G(M)$ is finitely generated as a $G_{\mathfrak{a}}(R)$-module. □

12.2. **Filtrations.**

Definition 12.9. Let $(M_n)_{n\geq 0}$ and $(M'_n)_{n \geq 0}$ be filtrations of an R-module M. Then $(M_n)_{n\geq 0}$ and $(M'_n)_{n \geq 0}$ are *equivalent* if there is $n_0 \geq 0$ such that $M_{n+n_0} \subset M'_n$ and $M'_{n+n_0} \subset M_n$ for all $n \geq 0$ (check that this defines an equivalence relation on the class of filtrations of M).

Lemma 12.10. *Let $\mathfrak{a}$ be an ideal of R. Then every stable $\mathfrak{a}$-filtration $(M_n)_{n\geq 0}$ of an R is equivalent to $(\mathfrak{a}^n M)_{n\geq 0}$ (and so all stable $\mathfrak{a}$-filtrations of M are equivalent to each other).*

Proof. Since $(M_n)_{n\geq 1}$ is an $\mathfrak{a}$-filtration, for all n we have $M_n \supset \mathfrak{a}M_{n-1} \supset \mathfrak{a}^2 M_{n-2} \supset \cdots \supset \mathfrak{a}^n M \supset \mathfrak{a}^{n+n_0} M$ for any $n_0 \geq 0$. On the other hand, there is $n_0 \geq 0$ such that $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$ since the $\mathfrak{a}$-filtration $(M_n)_{\geq 0}$ is stable. Hence $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subset \mathfrak{a}^n M$. □

12.2.1. *The Artin–Rees Lemma.* Let $\mathfrak{a}$ be an ideal of R. Let M be an R-module and $(M_n)_{n\geq 0}$ an $\mathfrak{a}$-filtration of M. We now define a graded ring R^* and a graded R^*-module M^*. We will use these constructions in order to prove the Artin–Rees Lemma, but not later (unlike the associated graded ring construction, which we will use in the chapter on dimension theory).

Let

$$R^* \coloneqq \bigoplus_{n=0}^{\infty} \mathfrak{a}^n \qquad (\ \mathfrak{a}^0 = R\ )$$

and

$$M^* \coloneqq \bigoplus_{n=0}^{\infty} M_n\ .$$

For $x \in \mathfrak{a}^n$ and $y \in \mathfrak{a}^\ell$ (thought of as element of the n-th and ℓ-th summands in the definition of R^*), the product of x and y in R^* is $xy \in \mathfrak{a}^{n+\ell}$, as an element of the $(n+\ell)$-th summand of R^*. This makes R^* into a graded ring.

The $x \in \mathfrak{a}^n$ (in the n-th summand of R^*) and $m \in M_\ell$ (in the ℓ-th summand of M^*), the R^*-module structure on M^* is given by thinking of $xm \in \mathfrak{a}^n M_\ell$ as an element of the $(n+\ell)$-th summand of M^* (indeed $\mathfrak{a}^n M_\ell \subset M_{n+\ell}$ since $(M_n)_{\geq 0}$ is an $\mathfrak{a}$-filtration). This makes M^* into a graded R^*-module.

If the ring R is noetherian then $\mathfrak{a}$ is generated by some $x_1, \dots, x_r$ and R^* is generated as an R-algebra by $x_1, \dots, x_r \in \mathfrak{a}$ (thought of as elements of the second summand in $R^* = R \oplus \underbrace{\mathfrak{a}}_{\text{here}} \oplus \mathfrak{a}^2 \oplus \cdots$). So R^* is noetherian by Hilbert's basis theorem.

Lemma 12.11. *Let R be a noetherian ring, M a finitely generated R-module, $(M_n)_{n\geq 0}$ an $\mathfrak{a}$-filtration of M. Then the following are equivalent:*

i) *M^* is a finitely generated R^*-module.*

ii) *The $\mathfrak{a}$-filtration $(M_n)_{n\geq 0}$ is stable.*

Proof. **Observation 1:** Each M_n is a finitely generated R-module since M is a noetherian R-module since M is finitely generated and R is noetherian.

Observation 2: Consider the following R^*-submodule of M^*:

$$M_n^* = M_0 \oplus \cdots \oplus M_n \oplus \bigoplus_{i=1}^{\infty} \mathfrak{a}^i M_n \ .$$

Then the ascending chain $(M_n^*)_{n\geq 0}$ stabilizes $\Leftrightarrow$ the $\mathfrak{a}$-filtration $(M_n)_{n\geq 0}$ is stable.

Assume (i). We have seen that R^* is noetherian whenever R is, and so M^* is a noetherian R^*-module by (i). Thus $(M_n^*)_{n\geq 0}$ stabilizes, and so $(M_n)_{n\geq 0}$ is stable.

Assume (ii). Then $(M_n^*)_{n\geq 0}$ stabilizes at some $n_0 \geq 0$. But $M^* = \bigcup_{n\geq 0} M_n^*$ (ascending union), and thus $M^* = M_{n_0}^*$, and we wish to show that $M_{n_0}^*$ is finitely generated as an R^*-module. Now, $M_{n_0}^*$ is generated as an R^*-module by $Q \coloneqq \bigoplus_{r=0}^{n_0} M_r$. Each M_r is a finitely generated R-module and thus Q is generated by some finite set S as an R-module. The same set S generates M^* as an R^*-module. □

The Artin–Rees[46] Lemma (see below) says that over a noetherian ring, a stable $\mathfrak{a}$-filtration of a finitely generated module induces a stable $\mathfrak{a}$-filtration on each submodule.

Proposition 12.12 (Artin–Rees Lemma)**.** *Assume that the ring R is noetherian. Let $\mathfrak{a}$ be an ideal of R, M a finitely generated R-module, $(M_n)_{n\geq 0}$ a stable $\mathfrak{a}$-filtration of M, N a submodule of M. Then $(N \cap M_n)_{n\geq 0}$ is a stable $\mathfrak{a}$-filtration of N.*

[46] There are several closely related results known as the Artin–Rees Lemma. They are a direct consequence of our version.

Proof. We have $\mathfrak{a}(N \cap M_\ell) \subset N \cap \underbrace{\mathfrak{a}M_\ell}_{\subset M_{\ell+1}}$, and so $\Big(\underbrace{N \cap M_\ell}_{=:N_\ell}\Big)_{\ell \geq 0}$ is an $\mathfrak{a}$-filtration of N. Thus $N^* = \bigoplus_{\ell \geq 0} N_\ell$ is a graded R^*-module and a submodule of $M^* = \bigoplus_{\ell \geq 0} M_\ell$. As discussed, R^* is noetherian since R is. The $\mathfrak{a}$-filtration $(M_\ell)_{\ell \geq 0}$ is stable and so M^* is a finitely generated R^*-module by Lemma 12.11. So M^* is a noetherian R^*-module. Thus N^* is a finitely generated R^*-module. So $(N_\ell)_{\ell \geq 0}$ is stable by Lemma 12.11. □

We will apply the Artin–Rees Lemma to study dimension, and see additional applications of the lemma in Example Sheet 4.

13. Dimension Theory

Definition 13.1.

i) The *length* of a chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d$ of distinct prime ideals of R is d (there are $d+1$ ideals in a chain of length d).
ii) The *height* $\operatorname{ht}\mathfrak{p}$ of $\mathfrak{p} \in \operatorname{spec} R$ is the supremum of the set of lengths of chains of distinct prime ideals of R contained in $\mathfrak{p}$.
iii) The *Krull dimension* (or just, *dimension*) of R is
$$\dim R = \sup\{\operatorname{ht}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{spec} R\}\ ,$$
and so
$$\dim R = \sup\{\operatorname{ht}\mathfrak{m} \mid \mathfrak{m} \in \operatorname{mspec} R\}$$
(since a chain of prime ideals that does not end with a maximal ideal can be extended).

Also, $\operatorname{ht}\mathfrak{p} = \dim R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{spec} R$, and so
$$\dim R = \sup\{\dim R_{\mathfrak{m}} \mid \mathfrak{m} \in \operatorname{mspec} R\}\ .$$
Hence, the computation of the dimension of a general ring reduces to the computations of the dimension of local rings.

Definition 13.2. For an ideal I of R,
$$\operatorname{ht} I = \inf\{\operatorname{ht}\mathfrak{p} \mid I \subset \mathfrak{p} \in \operatorname{spec} R\}\ .$$

Remark 13.3. **[non-examinable]** You can view the definition of $\dim R$ as analogous to the fact that for a k-vector space V, $\dim_k V$ is the supremum over the set of lengths of chains of distinct k-linear subspaces of V, e.g. $\{0\} \times \{0\} \subsetneq \{0\} \times \mathbb{R} \subsetneq \mathbb{R} \times \mathbb{R}$ shows that $\dim_{\mathbb{R}} \mathbb{R}^2 \geq 2$, and there is no longer chain of distinct $\mathbb{R}$-linear subspaces of $\mathbb{R}^2$ and so $\dim_{\mathbb{R}} \mathbb{R}^2 = 2$. More on this connection in any course in algebraic geometry. This particular example corresponds to the chain $(0) \subset (X) \subset (X, Y)$ of prime ideals of $\mathbb{R}[X, Y]$.

Proposition 13.4. *Let $A \subset B$ be an integral extension of rings. Then*

i) $\dim A = \dim B$.
ii) *If A and B are integral domains and k-algebras, k a field, then* $\operatorname{trdeg}_k A = \operatorname{trdeg}_k B$.

Proof. (i) First, we show that $\dim A \leq \dim B$. Take a chain

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d \qquad \mathfrak{p}_i \in \operatorname{spec} A \qquad d \geq 0 \ .$$

By Lying-over and Going-up (Propositions 9.2 and 9.3), there are $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_d$, $\mathfrak{q}_i \in \operatorname{spec} B$, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$. We must have $\mathfrak{q}_i \neq \mathfrak{q}_{i+1}$ because $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$. Thus $\dim B \geq d$, and so $\dim B \geq \dim A$.

Now, we show that $\dim A \geq \dim B$. Take a chain

$$\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_d \qquad \mathfrak{q}_i \in \operatorname{spec} B \qquad d \geq 0 \ .$$

Contracting to A, we obtain a chain

$$\mathfrak{q}_0 \cap A \subset \cdots \subset \mathfrak{q}_d \cap A \ ,$$

$\mathfrak{q}_i \cap A \in \operatorname{spec} A$. We must have $\mathfrak{q}_i \cap A \neq \mathfrak{q}_{i+1} \cap A$ because $\mathfrak{q}_i \subsetneq \mathfrak{q}$ and by Incomparability (Proposition 9.4). Thus, $\dim A \geq d$, and so $\dim A \geq \dim B$.

(ii) Exercise. □

Let A be a finitely generated k-algebra, k a field. By Noether's normalization theorem, we have an integral injective ring homomorphism $k[T_1, \ldots, T_n] \to A$, $d \geq 0$. By ES3.Q10, $\dim k[T_1, \ldots, T_n] = n$ (you will prove a more general fact in ES4). Thus $\dim A = n$ by Proposition 13.4(i). In particular, the number n in Noether's normalization theorem is determined uniquely by A.

Proposition 13.5. *Let A be a finitely generated k-algebra, k a field, and an integral domain. Then*

$$\dim A = \operatorname{trdeg}_k A \ .$$

Proof. By Noether's normalization theorem we have an embedding $k[T_1, \ldots, T_d] \to A$. By Proposition 13.4,

$$\dim A = \underbrace{\dim k[T_1, \ldots, T_d]}_{=d}$$

and

$$\operatorname{trdeg}_k A = \underbrace{\operatorname{trdeg}_k k[T_1, \ldots, T_d]}_{=d} \ .$$

□

13.1. **Hilbert functions and polynomials.** Let $A = \oplus_{n\geq 0} A_n$ be a noetherian graded ring. By Proposition 12.4, A_0 is a noetherian ring, and A is generated as an A_0-algebra by some $x_1, \dots, x_s$, $x_i \in A_{k_i}$, $k_i > 0$.

Let $0 \neq M = \oplus_{n\geq 0} M_n$ be a finitely generated graded A-module. Then each M_n is an A_0-module. **Claim:** M_n is a finitely generated A_0-module. **Proof:** We have $M = \operatorname{span}_A\{m_1, \dots, m_t\}$, $m_i \in M_{r_i}$, $r_i \geq 0$. Thus $M_n = \left\{\sum_{i=1}^t a_i m_i \mid a_i \in A_{n-r_i}\right\}$. Thus

$$M_n = \operatorname{span}_{A_0}\left\{ x_1^{e_1} \cdots x_s^{e_s} \cdot m_i \mid 1 \leq i \leq t,\, \sum_{j=1}^{s} k_j e_j = n - r_i \right\}.$$

From now on, we make another assumption:

$$\text{The ring } A_0 \text{ is artinian .}$$

Thus, each M_n is a finitely generated module over the artinian ring A_0. So M_n is both noetherian and artinian, and so it has finite length, i.e. $\ell(M_n) < \infty$ (see ES2.1b). Recall that the length of an A_0-module P is supremum of the set of lengths of all composition series for P. If $A_0 = k$ is a field then $\ell(P) = \dim_k P$.

Definition 13.6. Let $A = \bigoplus_{n\geq 0} A_n$ be a noetherian graded ring, generated by $x_1, \dots, x_s$, $x_i \in A_{k_i}$, $k_i > 0$, where A_0 is artinian. Let $M = \bigoplus_{n\geq 0} M_n$ be a finitely generated graded A-module. The *Poincaré series* of M is the power series:

$$P(M,T) = \sum_{n=0}^{\infty} \ell(M_n) T^n \qquad \in \mathbb{Z}[[T]]$$

(where $R[[T]]$ stands for the ring of formal power series over the ring R).

Theorem 13.7 (Hilbert–Serre)**.** *$P(M,T)$ is a rational function in T of the form $\frac{f(T)}{\prod_{i=1}^s (1-T^{k_i})}$, $f(T) \in \mathbb{Z}[T]$.*

Proof. Recall that A is generated as an A_0-algebra by $x_1, \dots, x_s$, $x_i \in A_{k_i}$, $k_i > 0$. The proof is by induction on s.

In the base case $s = 0$, $P(M,T)$ is in $\mathbb{Z}[T]$ (i.e. a polynomial): Indeed, in this case $A = A_0$. Thus M is generated as an A_0-module by some finite subset $S \subset M$. Take $n_0 \geq 0$ such that $S \subset M_0 \oplus \cdots \oplus M_{n_0}$. Then $M_n = 0$ for all $n > n_0$, and so $P(M,T)$ is a polynomial.

Assume that $s > 0$ and that the theorem holds for $s - 1$. Write[47] $M = \bigoplus_{n\in\mathbb{Z}} M_n$, where $M_n = 0$ for all $n < 0$. Let $n \in \mathbb{Z}$. Then $m \mapsto x_s m \colon M_n \to$

[47] Previously, we defined graded module where the summands are indexed by $\mathbb{Z}_{\geq 0}$. But we can do the same thing where the indices are in $\mathbb{Z}$.

M_{n+k_s} is a homomorphism of A_0-modules. Thus it gives rise to an exact sequence of A_0-modules

$$0 \to K_n \to M_n \xrightarrow{x_s} M_{n+k_s} \to L_{n+k_s} \to 0 \tag{13.1}$$

($K_n = \ker(m \mapsto x_s m)$ and $L_{n+k_s} = M_{n+k_s}/\operatorname{im}(m \mapsto x_s m)$).

Let $K = \oplus_{n\in\mathbb{Z}} K_n$ and $L = \oplus_{n\in\mathbb{Z}} L_{n+k_s}$. Both K and L are graded A-modules (For K, note that if $m \in K_n$ and $a_i \in A_i$, $i \geq 0$, then $a_i m \in M_{n+i}$ and $x_s a_i m = a_i x_s m = 0$, and so $a_i m \in K_{n+i}$. For L, we have $L = (\oplus_{n\in\mathbb{Z}} M_{n+k_s})/(\oplus_{n\in\mathbb{Z}} \operatorname{im}(m \mapsto x_s m \colon M_n \to M_{n+k_s})))$. So the graded A-modules K and L are finitely generated (since K and L are, respectively, a submodule and a quotient of M, and A is noetherian). Both K and L are annihilated by x_s (check!). So both are finitely generated $A_0[x_1, \ldots, x_{s-1}]$-modules.

Applying $\ell(\cdot)$ to (13.1) (see ES1.Q12), we have

$$\ell(K_n) - \ell(M_n) + \ell(M_{n+k_s}) - \ell(L_{n+k_s}) = 0 \ .$$

Hence

$$\ell(M_{n+k_s}) \cdot T^{n+k_s} - T^{k_s}\ell(M_n) \cdot T^n = \ell(L_{n+k_s}) \cdot T^{n+k_s} - T^{k_s}\ell(K_n) \cdot T^n \ .$$

Summing over all $n \in \mathbb{Z}$, we have

$$\left(1 - T^{k_s}\right) P(M,T) = P(L,T) - T^{k_s} P(K,T) \ . \tag{13.2}$$

The claim now follows from the induction hypothesis applied to L and K. □

The rational function $R(T) = \frac{f(T)}{\prod_{i=1}^{s}(1-T^{k_i})}$ is holomorphic on $\{z \in \mathbb{C} \mid |z| < 1\}$, and $P(M,T) = \sum_{n=0}^{\infty} \ell(M_n) T^n$ is the Taylor expansion of $R(T)$ at $T = 0$. Thus the radius of convergence of $P(M,T)$ to $R(T)$ is at least 1.

At $T = 1$, R may have a pole (unless f vanishes at $T = 1$ to a high enough order). Write $d(M)$ for the order of the pole at $T = 1$ of of $R(T)$.

Claim: $d(M) \geq 0$. **Proof:** If $d(M) < 0$ then $R(T)$ vanishes at $T = 1$. Thus, for all $k \geq 0$,

$$\begin{aligned} 0 &= \lim_{T\to 1^-} \underbrace{\left(\frac{f(T)}{\prod_{i=1}^{s}(1-T^{k_i})}\right)}_{=P(M,T)} \\ &= \lim_{T\to 1^-} \underbrace{P(M,T)}_{=\sum_{n\geq 0}\ell(M_n)T^n} \\ &\geq \lim_{T\to 1^-} \ell(M_k) T^k \\ &= \ell(M_k) \ , \end{aligned}$$

and so $\ell(M_k) = 0$ for all $k \geq 0$. Hence $M = 0$, a contradiction.

Example 13.8. Consider the polynomial ring $A = k[T_1, \ldots, T_s] = \bigoplus_{n\geq 0} A_n$, where A_n is the additive subgroup consisting of 0 and all homogeneous polynomials of degree n.

i) A is generated as an $\underbrace{A_0}_{=k}$-algebra by $T_1, \ldots, T_s \in A_1$. Thus $k_1 = \ldots = k_s = 1$ for this choice of generators.

ii) By Stars and Bars, there are exactly $\binom{s+n-1}{s-1}$ monomials of degree n in $k[T_1, \ldots, T_s]$, and they form a k-linear basis for A_n. So $\ell(A_n) = \dim_k A_n = \binom{n+s-1}{n} = p(n)$ for a polynomial $p \in \mathbb{Q}[T]$ of degree $s-1$.

iii) Thinking of A as a graded A-module[48],

$$\begin{aligned} P(A,T) &= \sum_{n\geq 0} \binom{n+s-1}{n} T^n \\ &= \left(\sum_{\ell\geq 0} T^\ell\right)^s \\ &= \frac{1}{(1-T)^s} \,, \end{aligned}$$

which has the form predicted by Theorem 13.7.

The existence of the polynomial $p \in \mathbb{Q}[T]$ as in (ii) of the example above, in the situation of (i) in the same example, is a special case of the following result.

Proposition 13.9 (Hilbert Polynomial)**.** *If $k_1 = \ldots = k_s = 1$ then there is a polynomial $\mathrm{HP}_M \in \mathbb{Q}[T]$ of degree*[49] *$d(M) - 1$ such that $\ell(M_n) = \mathrm{HP}_M(n)$ for all large enough n (check that there is at most one such polynomial - and hence there is exactly one!).*

Proof. Write $d = d(M)$. By the Theorem 13.7, and since $d \geq 0$, there is $f \in \mathbb{Z}[T]$ such that $\ell(M_n)$ is the coefficient of T^n in $\frac{f(T)}{(1-T)^d}$, and $f(1) \neq 0$.

Write $f(T) = \sum_{k=0}^{\deg f} a_k T^k$, $a_k \in \mathbb{Z}$. Now[50]

$$(1-T)^{-d} = \sum_{j=0}^{\infty} \underbrace{\binom{j+d-1}{j}}_{=:b_j} \cdot T^j \ ,$$

[48] Arguing more directly, both the number of monomials of degree n in s variables, and the coefficient of T^n in $\left(\sum_{\ell\geq 0} T^\ell\right)^s$, are equal to the number of elements of $(\mathbb{Z}_{\geq 0})^s$ whose sum is n. So, we can make the computation even if we don't remember the Stars and Bars formula $\binom{n+s-1}{n}$.

[49] Convention: The degree of the zero polynomial is -1.

[50] Our convention: $\binom{n}{-1} = 0$ if $n \geq 0$ and $\binom{-1}{-1} = 1$.

and so

$$\ell(M_n) = \sum_{i=0}^{\deg f} a_i b_{n-i} \qquad \forall n \geq \deg f \ ,$$

where $b_{n-i} = \binom{n-i+d-1}{n-i}$.

Now $\binom{n-i+d-1}{n-i}$ is a polynomial in n of degree $d-1$, and the coefficient of n^{d-1} is $1/(d-1)!$. Thus, for all $n \geq \deg f$, $\ell(M_n) = p(n)$ for a polynomial $\mathrm{HP}_M \in \mathbb{Q}[T]$ of degree most $d-1$, and the coefficient of n^{d-1} in HP_M is $\left(\underbrace{\sum_{k=0}^{\deg f} a_k}_{=f(1)\neq 0}\right)/(d-1)! \neq 0$, and so $\deg \mathrm{HP}_M = d-1$. □

The function $n \mapsto \ell(M_n)$ is the *Hilbert function* of the graded A-module M. The polynomial HP_M is the *Hilbert polynomial* of M. Note that $\mathrm{HP}_M \in \mathbb{Q}[T]$ sends $\mathbb{Z}_{\geq 0}$ to $\mathbb{Z}_{\geq 0}$, but usually HP_M is not in $\mathbb{Z}[T]$ (recall, for example, that $\frac{1}{2}T(T+1)$ sends integers to integers).

Remark 13.10. **[non-examinable]** This remark motivates the need to have a purely algebraic definition of dimension (i.e. the Krull dimension). There are many other reasons to want this, not listed below, but I think the following points, together, are particularly nice.

(1) **Number of independent directions:** Assume that $\dim \mathbb{C}[T_1, \ldots, T_n]/I = d$, $V(I) \subset \mathbb{C}^n$ is irreducible, and $\mathbf{x}$ is a non-singular point of $V(I) \subset \mathbb{C}^n$ (almost all points are non-singular) then the dimension (over $\mathbb{R}$) of the tangent space to $V(I)$ at $\mathbf{x}$ is $2d$ (the factor of 2 comes from $[\mathbb{C} : \mathbb{R}] = 2$).

(2) $p^{\dim}$ **points with all entries in $\mathbb{F}_p$:** Let p be a prime number. If $f_1, \ldots, f_r \in \mathbb{F}_p[T]$, $\dim \mathbb{F}_p^{\mathrm{alg}}[T_1, \ldots, T_n]/\underbrace{(f_1, \ldots, f_r)}_{=J} = d$, and $V(J) \subset \mathbb{F}_p^{\mathrm{alg}}$ is irreducible then

$$\left|V(J) \cap \mathbb{F}_p^n\right| = (1+\varepsilon)p^d \qquad |\varepsilon| \leq Cp^{-1/2} \ ,$$

where C depends only on J. That is, $V(J)$ has approximately p^d points with all entries in $\mathbb{F}_p$. This is the **Lang–Weil bound**. If $V(J)$ is not irreducible then we have a similar estimate $\left|V(J) \cap \mathbb{F}_p^n\right| \approx cp^d$, where c is the number of irreducible components of $V(J)$ that can be defined over $\mathbb{F}_p$ among the irreducible components of $V(J)$ of dimension d (this number can be 0 even if $V(J) \neq \emptyset$).

(3) **Computation of the dimension:** Given an ideal $I = (f_1, \ldots, f_s)$ of $\mathbb{C}[T_1, \ldots, T_n]$, we can compute a Groebner basis $\{g_1, \ldots, g_t\}$ (a special

kind of generating set), and then read the dimension of $\mathbb{C}[T_1,\dots,T_n]/I$ easily. For example, in $\mathbb{C}[X,Y,Z]$, the polynomials $Y^3-Z^2, X^2-Y, XY-Z, XZ-Y^2$ form a Groebner basis for the ideal I of $\mathbb{C}[X,Y,Z]$ that they generate (w.r.t. to grlex order, to be precise). The leading monomials (w.r.t. grlex) are Y^3, X^2, XY, XZ. The set $S=\{X,Y\}$ of variables is of minimal cardinality among sets satisfying the following property: each of the leading monomials above involves a variable in S. Thus (this is a theorem) $\dim\mathbb{C}[X,Y,Z]/I = |\{X,Y,Z\}\setminus S| = 1$. This works in general with any number of variables and any ideal I. This theorem can be proved using Hilbert polynomials. The theorem works over every algebraically closed field, not just over $\mathbb{C}$.

(4) **$\mathbb{C}$ vs. $\mathbb{F}_p^{\mathrm{alg}}$:** Let $f_1,\dots,f_s\in\mathbb{Z}[T_1,\dots,T_n]$ generate an ideal I of $\mathbb{C}[T_1,\dots,T_n]$. For a prime number p, let I_p be the ideal of $\mathbb{F}_p^{\mathrm{alg}}[T_1,\dots,T_n]$ generated by the images of $f_1,\dots,f_s$ mod p. If $\dim\mathbb{C}[T_1,\dots,T_n]/I = d$ and $V(I)\subset\mathbb{C}^n$ is irreducible, then for all but finitely many prime numbers p we have $\dim\mathbb{C}[T_1,\dots,T_n]/I = d$ and $V(I_p)\subset\left(\mathbb{F}_p^{\mathrm{alg}}\right)^n$ is irreducible. To prove the claim about the dimensions elementarily, note that a Groebner basis generated from $f_1,\dots,f_s$ will still be over $\mathbb{Q}$. Multiplying by the denominators, the Groebner basis will be over $\mathbb{Z}$. Reducing mod p, a Groebner basis stays a Groebner basis as long as none of the leading coefficients vanish mod p. Now use (3). So $\log_p\left|V(I_p)\cap\mathbb{F}_p^n\right|\approx d$ by Lang–Weil, as described above (for all but finitely many prime numbers p).

(5) **Putting it all together:** Let I be an ideal of $\mathbb{Z}[T_1,\dots,T_n]$ such that $V(I)\subset\mathbb{C}^n$ is irreducible. Combining all of the above, we see that we can compute the dimension over $\mathbb{R}$ of the tangent space to $V(I)\subset\mathbb{C}^n$ at any non-singular point by computing the cardinality of $V(I_p)\cap\mathbb{F}_p^n$. The latter can sometimes be done with tools of combinatorics or analysis. I find this connection between varieties over $\mathbb{C}$ and over $\mathbb{F}_p$ very beautiful.

Note that if I is a specific ideal given by an explicit set of generators, we have described in (3) an algorithm to compute the dimension. But sometimes we do not completely understand I, but we can still approximate $\left|V(I_p)\cap\mathbb{F}_p^n\right|$. Remember, though, that there is a finite number of bad primes for which this does not work, and we do not necessarily know what these primes are.

(6) More generally, if $V(I)\subset\mathbb{C}^n$ is not known to be irreducible, we can still study it by approximating $\left|V(I_p)\cap\mathbb{F}_p^n\right|$ for various prime numbers (e.g. in order to prove that $V(I)$ is irreducible). There is a technique to do that, based on Chebotarev's density theorem from

number theory. Chebotarev's theorem becomes more efficient if one assumes information about the Dedekind zeta functions of number fields (e.g. assumes the Generalized Riemann Hypothesis). This efficiency is useful because it allows us to study $V(I)$ by approximating $\left|V(I_p) \cap \mathbb{F}_p^n\right|$ only for a relatively small number of relatively small primes, and this may be easier. J.P. Serre has a beautiful book about this, titled simply "$N_X(p)$" (in Serre's notation, $X = V(I)$, and $N_X(p) = \left|V(I_p) \cap \mathbb{F}_p^n\right|$).

13.2. **Dimension theory of noetherian local rings.**

Lemma 13.11. *Let $(A, \mathfrak{m})$ be a noetherian local ring. Then*

1. *An ideal $\mathfrak{q}$ of A is $\mathfrak{m}$-primary $\Leftrightarrow$ $\mathfrak{m}^t \subset \mathfrak{q} \subset \mathfrak{m}$ for some $t \geq 1$.*
2. *For a $\mathfrak{m}$-primary ideal $\mathfrak{q}$ of A, $A/\mathfrak{q}$ is artinian.*

Proof. (i) If $\mathfrak{m}^t \subset \mathfrak{q} \subset \mathfrak{m}$ then $\underbrace{\sqrt{\mathfrak{m}^t}}_{=\mathfrak{m}} \subset \sqrt{\mathfrak{q}} \subset \sqrt{\mathfrak{m}}$ and so $\sqrt{\mathfrak{q}} = \mathfrak{m}$ and thus $\mathfrak{q}$ is $\mathfrak{m}$-primary. Conversely, if $\mathfrak{q}$ is $\mathfrak{m}$-primary then $\sqrt{\mathfrak{q}} = \mathfrak{m}$ and so $\mathfrak{m}^t \subset \mathfrak{q}$ for some $t \geq 1$ (in a noetherian ring, every ideal contains a power of its radical, see ES2.Q2e), and clearly $\mathfrak{q} \subset \mathfrak{m}$.

(ii) First, $(A/\mathfrak{q}, \mathfrak{m}/\mathfrak{q})$ is a noetherian local ring. If $\mathfrak{q} \subset \mathfrak{p} \subset \mathfrak{m}$ and $\mathfrak{p} \in \operatorname{spec} A$ then $\underbrace{\sqrt{\mathfrak{q}}}_{=\mathfrak{m}} \subset \mathfrak{p}$ and so $\mathfrak{p} = \mathfrak{m}$. Thus $\mathfrak{m}/\mathfrak{q}$ is the only prime ideal of $A/\mathfrak{q}$, and so $\dim A/\mathfrak{q} = 0$. Thus $A/\mathfrak{q}$ is artinian. □

Fix a noetherian local ring $(A, \mathfrak{m})$. Here are three numbers we can extract from A:

1. $\dim A$ (the Krull dimension of A).
2. $\delta(A) = \min\{\delta(\mathfrak{q}) \mid \mathfrak{q} \text{ is an } \mathfrak{m}\text{-primary ideal of } A\}$,
   where $\delta(\mathfrak{q})$ is the cardinality of the smallest generating set for the ideal $\mathfrak{q}$.
3. $d(G_\mathfrak{m}(A))$ (the order of the pole at $T = 1$ of the rational function $P(G_\mathfrak{m}(A), T) = \sum_{n=0}^{\infty} \ell\big(\mathfrak{m}^n/\mathfrak{m}^{n+1}\big) \cdot T^n$).

Our goal here is to prove that all three are equal:

Theorem 13.12 (Dimension theorem)**.** *For a noetherian local ring $(A, \mathfrak{m})$, $\delta(A) = d(G_\mathfrak{m}(A)) = \dim A$.*

Proof. Combining Propositions 13.18, 13.20, 13.22 below, we have $\delta(A) \geq d(G_\mathfrak{m}(A)) \geq \dim A \geq \delta(A)$. □

Before proving the three propositions that imply Theorem 13.12, we show an application. Recall that a *minimal prime ideal* of an ideal $\mathfrak{a}$ of a ring R is a minimal element of $\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subset \mathfrak{p}\}$.

Corollary 13.13 (Krull's Height Theorem). *Let $\mathfrak{a} = (x_1, \dots, x_r)$ be an ideal of a noetherian ring A. Then $\operatorname{ht}\mathfrak{p} \leq r$ for every minimal prime ideal $\mathfrak{p}$ of $\mathfrak{a}$.*

Remark 13.14. Consider the localization map $A \to A_\mathfrak{p}$. If $\mathfrak{n} \in \operatorname{spec} A_\mathfrak{p}$ contains $\mathfrak{a}A_\mathfrak{p}$ then $\mathfrak{a} \subset (\mathfrak{a}A_\mathfrak{p})^c \subset \mathfrak{n}^c \subset \mathfrak{p}$, and so $\mathfrak{n}^c = \mathfrak{p}$, and thus $\mathfrak{n} = \mathfrak{n}^{ce} = \mathfrak{p}A_\mathfrak{p}$. Thus $\sqrt{\mathfrak{a}A_\mathfrak{p}} = \mathfrak{p}A_\mathfrak{p}$ (the radical of an ideal I is equal to the intersection of the prime ideals containing I). Thus $\mathfrak{a}A_\mathfrak{p}$ is $\mathfrak{p}A_\mathfrak{p}$-primary since $\mathfrak{p}A_\mathfrak{p} \in \operatorname{mspec} A_\mathfrak{p}$. But $\mathfrak{a}A_\mathfrak{p}$ is generated by $\frac{x_1}{1}, \dots, \frac{x_r}{1}$, and thus $\operatorname{ht}\mathfrak{p} = \dim A_\mathfrak{p} = \delta(A_\mathfrak{p}) \leq \delta(\mathfrak{a}A_\mathfrak{p}) \leq r$.

Remark 13.15. **[non-examinable]** In Example Sheet 4, you will show that if A is an integral domain and a finitely generated algebra over a field, then $\dim A/\mathfrak{p} = \dim A - \operatorname{ht}\mathfrak{p}$ (you will also show that this is false in more general noetherian rings). Thus, in this case we can think of $\operatorname{ht}\mathfrak{p}$ as codimension. Geometrically, this implies that for an algebraic set X defined by r polynomials on the affine space $\mathbb{A}^n_\mathbb{C}$, every irreducible component of X is of dimension at least $n - r$. This generalizes what you know from linear algebra: A linear subspace defined by r linear equations on k^n has dimension at least $n - r$.

Lemma 13.16. *Let $p \in \mathbb{Q}[T]$. Then $\sum_{k=0}^{n-1} p(k) = q(n)$ for all $n \geq 0$ for some $q \in \mathbb{Q}[T]$, where the leading term of q depends only on the leading term of p, and $\deg q = 1 + \deg p$ (unless $p = 0$, and then $q = 0$).*

Proof. This follows since $\sum_{k=0}^{n-1} k^\ell$ is a polynomial in n of degree $\ell+1$ (exercise). □

Definition 13.17. Consider a function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$.

(1) If there are $g \in \mathbb{Q}[T]$ and $n_0 \in \mathbb{Z}$ such that $f(n) = g(n)$ for all $n \geq n_0$, we shall say that f is *eventually a polynomial*.
(2) If f is eventually a polynomial then $g \in \mathbb{Q}[T]$ above is determined uniquely by f, and so we may define (i) $\deg f$, (ii) the leading coefficient of f, and (iii) the leading term of f, as those of g (recall, e.g. that the leading coefficient of $\frac{1}{2}T^3 + 4T$ is $\frac{1}{2}$, while its leading term is $\frac{1}{2}T^3$).

Let $(A, \mathfrak{m})$ be a noetherian local ring.

Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal of A. Consider the associated graded rings $G_\mathfrak{q}(A) = A/\mathfrak{q} \oplus \bigoplus_{n\geq 1} \mathfrak{q}^n/\mathfrak{q}^{n+1}$ and $G_\mathfrak{m}(A) = A/\mathfrak{m} \oplus \bigoplus_{n\geq 1} \mathfrak{m}^n/\mathfrak{m}^{n+1}$. By Lemma 13.11, the rings $A/\mathfrak{q}$ and $A/\mathfrak{m}$ are artininian. Furthermore, $\mathfrak{q}$ is generated by $\delta(\mathfrak{q}) < \infty$ elements (since A is noetherian), and so $G_\mathfrak{q}(A)$ is generated as an $A/\mathfrak{q}$-algebra by $\delta(\mathfrak{q}) < \infty$ homogeneous elements of degree 1 (which are the images in $\mathfrak{q}/\mathfrak{q}^2$ of the $\delta(\mathfrak{q})$ generators of $\mathfrak{q}$). Similarly, $G_\mathfrak{m}(A)$ is generated as an $A/\mathfrak{m}$-algebra by $\delta(\mathfrak{m}) < \infty$ homogeneous elements of degree 1.

By Proposition 13.9, $\ell\big(\mathfrak{q}^n/\mathfrak{q}^{n+1}\big)$ and $\ell\big(\mathfrak{m}^n/\mathfrak{m}^{n+1}\big)$ are eventually polynomials of degrees $d(G_{\mathfrak{q}}(A))-1$ and $d(G_{\mathfrak{m}}(A))-1$, respectively. Hence, by Lemma 13.16, $\underbrace{\ell(A/\mathfrak{q}^n)}_{=\sum_{k=0}^{n-1}\ell\left(\mathfrak{q}^{k+1}/\mathfrak{q}^k\right)}$ and $\underbrace{\ell(A/\mathfrak{m}^n)}_{=\sum_{k=0}^{n-1}\ell(\mathfrak{m}^{n+1}/\mathfrak{m}^n)}$ are eventually polynomials of degrees $d(G_{\mathfrak{q}}(A))$ and $d(G_{\mathfrak{m}}(A))$, respectively. In fact, $d(G_{\mathfrak{q}}(A))=d(G_{\mathfrak{m}}(A))$ (see the proof of Proposition 13.18 below).

Proposition 13.18. $\delta(A)\geq d(G_{\mathfrak{m}}(A))$.

Proof. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal of A. By Lemma 13.11, $\mathfrak{m}^t\subset\mathfrak{q}\subset\mathfrak{m}$ for some $t\geq 1$, and thus $\ell(A/\mathfrak{m}^n)\leq\ell(A/\mathfrak{q}^n)\leq\ell\big(A/\mathfrak{m}^{tn}\big)$ for all $n\geq 0$. So[51] $\deg\ell(A/\mathfrak{q}^n)=\deg\ell(A/\mathfrak{m}^n)$, and so $d(G_{\mathfrak{q}}(A))=d(G_{\mathfrak{m}}(A))$.

By Theorem 13.7, the Poincare series $P(G_{\mathfrak{q}}(A),T)$ is a rational function of the form $\frac{f(T)}{(1-T)^{\delta(\mathfrak{q})}}$, and thus $d(G_{\mathfrak{q}}(A))\leq\delta(\mathfrak{q})$. Hence $d(G_{\mathfrak{m}}(A))\leq\delta(\mathfrak{q})$. Taking $\mathfrak{q}$ to be an $\mathfrak{m}$-primary ideal of A such that $\delta(A)=\delta(\mathfrak{q})$ completes the proof. □

Lemma 13.19. *If $x\in\mathfrak{m}$ is not a zero divisor then $d\big(G_{\mathfrak{m}/(x)}(A/(x))\big)\leq d(G_{\mathfrak{m}}(A))-1$.*

Proof. Consider the noetherian local ring $(A/(x),\mathfrak{m}/(x))$. Then

$$d\big(G_{\mathfrak{m}/(x)}(A/(x))\big)=\deg\ell\left((A/(x))/\underbrace{(\mathfrak{m}/(x))^n}_{=(\mathfrak{m}^n+(x))/(x)}\right)=\deg\ell(A/(\mathfrak{m}^n+(x)))\ .$$

On the other hand,

$$d(G_{\mathfrak{m}}(A))=\deg\ell(A/\mathfrak{m}^n)\ .$$

Thus, we need to prove that $\deg\ell(A/(\mathfrak{m}^n+(x)))\leq\deg\ell(A/\mathfrak{m}^n)-1$.

The short exact sequence

$$0\longrightarrow\underbrace{(\mathfrak{m}^n+(x))/\mathfrak{m}^n}_{\cong(x)/(\mathfrak{m}^n\cap(x))}\longrightarrow A/\mathfrak{m}^n\longrightarrow A/(\mathfrak{m}^n+(x))\longrightarrow 0$$

shows that $\ell(A/(\mathfrak{m}^n+(x)))=\ell(A/\mathfrak{m}^n)-\ell((x)/(\mathfrak{m}^n\cap(x)))$, and also that $\ell((x)/(\mathfrak{m}^n\cap(x)))$ is eventually a polynomial (since the other two terms are). Thus it suffices to show that the leading terms of $\ell(A/\mathfrak{m}^n)$ and $\ell((x)/(\mathfrak{m}^n\cap(x)))$ are the same.

Since x is not a zero divisor, we have an A-linear isomorphism $A\to(x)$ given by $a\mapsto ax$. This map induces an A-linear isomorphism $A/\mathfrak{m}^n\to(x)/\mathfrak{m}^n(x)$ for all n, and thus $\ell(A/\mathfrak{m}^n)=\ell((x)/\mathfrak{m}^n(x))$. Thus, it remains to show that $\ell((x)/\mathfrak{m}^n(x))$ and $\ell((x)/(\mathfrak{m}^n\cap(x)))$ have the same leading term.

[51] If $|f(n)|\leq|g(n)|\leq|f(tn)|$ for all $n\geq 1$ for polynomials $f,g\in\mathbb{Q}[T]$, then $\deg f(x)\leq\deg g(x)\leq\underbrace{\deg f(tx)}_{=\deg f(x)}$.

Clearly $(\mathfrak{m}^n)_{n\geq 0}$ is a stable $\mathfrak{m}$-filtration of the noetherian ring A, and so, by Artin–Rees (Proposition 12.12), $(\mathfrak{m}^n \cap (x))_{n\geq 0}$ is a stable $\mathfrak{m}$-filtration of the submodule (x) of A. Thus, the filtrations $(\mathfrak{m}^n \cap (x))_{n\geq 0}$ and $(\mathfrak{m}^n(x))_{n\geq 0}$ of (x) are equivalent by Lemma 12.10. That is, $\mathfrak{m}^{n+n_0} \cap (x) \subset \mathfrak{m}^n(x)$ and $\mathfrak{m}^{n+n_0}(x) \subset \mathfrak{m}^n \cap (x)$ for all $n \geq 0$ for some $n_0 \geq 0$. Hence

$$\ell\big((x)/\mathfrak{m}^{n-n_0} \cap (x)\big) \leq \ell((x)/\mathfrak{m}^n(x)) \leq \ell\big((x)/\mathfrak{m}^{n+n_0} \cap (x)\big)$$

and thus[52] $\ell((x)/\mathfrak{m}^n(x))$ and $\ell((x)/\mathfrak{m}^n \cap (x))$ have the same leading term. □

Proposition 13.20. *$d(G_{\mathfrak{m}}(A)) \geq \dim A$.*

Proof. We prove the claim by induction on $d(G_{\mathfrak{m}}(A))$. If $d(G_{\mathfrak{m}}(A)) = 0$ then $\deg \ell\big(\mathfrak{m}^n/\mathfrak{m}^{n+1}\big) = -1$, and so, for all large enough n, $\ell\big(\mathfrak{m}^n/\mathfrak{m}^{n+1}\big) = 0$, i.e., $\underbrace{\mathfrak{m}^{n+1}}_{=\mathfrak{m}\cdot\mathfrak{m}^n} = \mathfrak{m}^n$, and so $\mathfrak{m}^n = 0$ by Nakayama's Lemma. Thus A is an artinian ring (since A is a noetherian ring where some finite product of maximal ideals is 0, see Example Sheet), and so $\dim A = 0$.

Assume that $d(G_{\mathfrak{m}}(A)) > 0$. If $\dim A = 0$ we are done. Assume that $\dim A \geq 1$. Take a chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$, $r \geq 1$, of prime ideals of A. It suffices to show that $d(G_{\mathfrak{m}}(A)) \geq r$.

Consider the noetherian local integral domain $(A/\mathfrak{p}_0, \mathfrak{m}/\mathfrak{p}_0)$, and let $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Then $\underbrace{d\big(G_{\mathfrak{m}/\mathfrak{p}_0}(A/\mathfrak{p}_0)\big)}_{=\deg \ell((A/\mathfrak{p}_0)/(\mathfrak{m}/\mathfrak{p}_0)^n)} \leq \underbrace{d\big(G_{\mathfrak{m}}(A)\big)}_{=\deg \ell(A/\mathfrak{m}^n)}$: Indeed, $(A/\mathfrak{p}_0)/(\mathfrak{m}/\mathfrak{p}_0)^n = (A/\mathfrak{p}_0)/((\mathfrak{m}^n + \mathfrak{p}_0)/\mathfrak{p}_0) \cong A/(\mathfrak{m}^n + \mathfrak{p}_0)$ is isomorphic to a quotient of $A/\mathfrak{m}^n$, and thus $\ell((A/\mathfrak{p}_0)/(\mathfrak{m}/\mathfrak{p}_0)^n) \leq \ell(A/\mathfrak{m}^n)$ for all $n \geq 1$.

By Lemma 13.19 and since $x \notin \mathfrak{p}_0$, we have

$$d\big(G_{\mathfrak{m}/(\mathfrak{p}_0+(x))}(A/(\mathfrak{p}_0 + (x)))\big) \leq \underbrace{d\big(G_{\mathfrak{m}/\mathfrak{p}_0}(A/\mathfrak{p}_0)\big)}_{\leq d(G_{\mathfrak{m}}(A))} - 1$$

and thus the induction hypothesis implies that

$$d\big(G_{\mathfrak{m}/(\mathfrak{p}_0+(x))}(A/(\mathfrak{p}_0 + (x)))\big) \geq \dim A/(\mathfrak{p}_0 + (x)) \ ,$$

and so together we have

$$d(G_{\mathfrak{m}}(A)) \geq \dim A/(\mathfrak{p}_0 + (x)) + 1$$

and thus it suffices to show that

$$\dim A/(\mathfrak{p}_0 + (x)) \geq r - 1 \ .$$

This indeed the case because the images of $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ in $A/\left(\underbrace{\mathfrak{p}_0 + (x)}_{\subset \mathfrak{p}_1}\right)$ form a strictly ascending chain of prime ideals. □

[52] If $f(n - n_0) \leq g(n) \leq f(n + n_0)$ for all large enough n for polynomials $f, g \in \mathbb{Q}[T]$ and some $n_0 \geq 0$, then f and g have the same leading term.

Remark 13.21. **[non-examinable]** The proof considered the ring $A/(\mathfrak{p}_0 + (x))$. The geometric intuition (I am only assuming familiarity with algebraic sets) is that if $A = \mathbb{C}[T_1, \dots, T_n]/I$ corresponds to an algebraic set $X = V(I)$, then $A/\mathfrak{p}_0$ corresponds to an irreducible component Y of X (if $\mathfrak{p}_0$ is minimal), and $A/(\mathfrak{p}_0 + (x))$ corresponds to the intersection of the irreducible component with the hypersurface defined by the equation $p(T_1, \dots, T_n) = 0$, where $x = p + I$. We expect the dimension of an irreducible algebraic set Y to decrease after intersecting Y with a hypersurface that does not contain Y. Using Lemma 13.19, we see that this property indeed holds if we think of $d(G_{\mathfrak{m}}(\cdot))$ as a measure of dimension. This enables us to reason by induction, and eventually to conclude that $d(G_{\mathfrak{m}}(A))$ really is the Krull dimension of a noetherian local ring $(A, \mathfrak{m})$, once the proof of the Dimension Theorem is complete.

Proposition 13.22. $\dim A \geq \delta(A)$ *(i.e., there is a an* $\mathfrak{m}$*-primary ideal* $\mathfrak{q}$ *generated by* $\dim A$ *elements).*

Proof. Write $d = \dim A$. Then $\operatorname{ht} \mathfrak{m} = d$, and every $\mathfrak{m} \neq \mathfrak{p} \in \operatorname{spec} A$ satisfies $\operatorname{ht} \mathfrak{p} < d$. Thus, it is enough to construct an ideal $\mathfrak{q} = (x_1, \dots, x_d) \subset \mathfrak{m}$ of A such that $\operatorname{ht} \mathfrak{q} \geq d$ because then $\operatorname{ht} \mathfrak{p} \geq d$ for every $\mathfrak{q} \subset \mathfrak{p} \in \operatorname{spec} A$, and so $\mathfrak{p} = \mathfrak{m}$, and thus $\sqrt{\mathfrak{q}} = \bigcap_{\mathfrak{q} \subset \mathfrak{p} \in \operatorname{spec} A} = \mathfrak{m}$, and hence $\mathfrak{q}$ is $\mathfrak{m}$-primary.

We construct $x_1, \dots, x_d \in \mathfrak{m}$ inductively such that $\operatorname{ht} \underbrace{(x_1, \dots, x_i)}_{=:\mathfrak{q}_i} \geq i$ for all i. The base case $\mathfrak{q}_0 = (0)$ satisfies $\operatorname{ht} \mathfrak{q}_0 \geq 0$ (since $\mathfrak{q}_0$ is contained in a minimal prime ideal of A, which must have height 0).

Take $\mathfrak{q}_{i-1} = (x_1, \dots, x_{i-1})$, $i - 1 < d$, such that $\operatorname{ht} \mathfrak{q}_{i-1} \geq i - 1$. There are only finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ of A of height $i - 1$ that contain $\mathfrak{q}_{i-1}$ because:

(1) each $\mathfrak{p}_i$ is a minimal prime ideal of $\mathfrak{q}_{i-1}$ since $\operatorname{ht} \mathfrak{q}_{i-1} \geq i - 1$, and
(2) $\mathfrak{q}_{i-1}$ has only finitely many minimal prime ideals since A is noetherian (see ES2.Q2c).

Now, $i - 1 < d = \operatorname{ht} \mathfrak{m}$, and so $\mathfrak{m} \not\subseteq \mathfrak{p}_j$ for all j, and so $\mathfrak{m} \not\subseteq \bigcup_{j=1}^{t} \mathfrak{p}_j$ by Prime Avoidance (ES1.Q5a). Take x_i to be any element of $\mathfrak{m} \setminus \bigcup_{j=1}^{t} \mathfrak{p}_j$, and let $\mathfrak{q}_i = (x_1, \dots, x_i)$. Then every $\mathfrak{p} \in \operatorname{spec} A$ such that $\mathfrak{q}_i \subset \mathfrak{p}$ satisfies $\mathfrak{q}_{i-1} \subset \mathfrak{p}$ and $\mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ (since $x_i \in \mathfrak{p}$). Thus $\operatorname{ht} \mathfrak{p} \geq i$. Hence $\operatorname{ht} \mathfrak{q}_i \geq i$. □

Remark 13.23. The proof of the Dimension Theorem 13.12 is now complete. Thus, so is the proof of Krull's Height Theorem (Corollary 13.13). Therefore, each of the ideals $\mathfrak{q}_i$ in the proof of Proposition 13.22 satisfies $\operatorname{ht} \mathfrak{q}_i \leq i$ since $\mathfrak{q}_i$ is generated by i elements, and thus, in fact, $\operatorname{ht} \mathfrak{q}_i = i$.

14. Dedekind domains and discrete valuation rings

Definition 14.1.

(1) A *discrete valuation* v on a field K is a surjective group homomorphism[53] $v\colon K^\times \to \mathbb{Z}$ such that $v(x+y) \geq \min\{v(x), v(y)\}$. Write $v(0) = \infty$.

(2) The *valuation ring* of v is the ring $\{x \in K \mid v(x) \geq 0\}$.

(3) An integral domain A is a *discrete valuation ring* (DVR) if A is the valuation ring of some discrete valuation v on $\operatorname{Frac} A$.

If $v\colon K^\times \to \mathbb{Z}$ is a discrete valuation on a field K then $v(1) = v(1 \cdot 1) = 2v(1)$ and so $v(1) = 0$. Thus $0 = v(1) = v((-1)(-1)) = 2v(-1)$ and so $v(-1) = 0$. Hence, for all $x \in K^\times$, we have $v(-x) = v((-1)x) = v(-1) + v(x) = v(x)$.

Example 14.2.

(1) Take $K = \mathbb{Q}$ and a prime number p. Every $x \in \mathbb{Q}$ can be written as $x = p^n \frac{a}{b}$ for integers n, a, b, where a and b are not divisible by p. Let $v_p(x) = n$. Then v_p is a discrete valuation on $\mathbb{Q}$. The valuation ring of v_p is

$$\{x \in \mathbb{Q} \mid v_p(x) \geq 0\} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\right\} = \mathbb{Z}_{(p)} \ ,$$

i.e. the localization of $\mathbb{Z}$ at the prime ideal (p).

(2) Let $K = k(T)$, the field of rational function over k, and an irreducible polynomial $f \in k[T]$. Then, similarly to the previous example, we have a discrete valuation v_f with valuation ring $k[T]_{(f)}$.

Fact 14.3. *Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation, and $A = \{x \in K \mid v(x) \geq 0\}$ the valuation ring of v (necessarily A is a DVR). Then:*

(1) *An element $x \in A$ belongs to $A^\times$ if and only if $v(x) = 0$.*
Proof: *If $x = 0$ then $v(x) = \infty \neq 0$. Now, take $x \neq 0$. Then $x \in A^\times$ $\Leftrightarrow x^{-1} \in A \Leftrightarrow \underbrace{v(x^{-1})}_{=-v(x)} \geq 0 \Leftrightarrow v(x) \leq 0 \Leftrightarrow v(x) = 0$.*

(2) *A is a domain.*
Proof: *A is a subring of the field K.*

(3) *Take any $\pi \in A$ with $v(\pi) = 1$. Then the nonzero ideals of A are precisely $\underbrace{(\pi^0)}_{=A} \supsetneq (\pi^1) \supsetneq (\pi^2) \supsetneq \cdots$, and so $(A, (\pi))$ is a noetherian local domain.*
Proof: *Let $\mathfrak{a} \neq 0$ be an ideal of A. Let $k = \min\{v(x) \mid x \in \mathfrak{a}\}$. Then $k < \infty$ since $\mathfrak{a} \neq 0$. For $x \in \mathfrak{a}$, we have $v(x\pi^{-k}) = v(x) - k \geq 0$, and so $x\pi^{-k} \in A$, and thus $x = x\pi^{-k} \cdot \pi^k \in (\pi^k)$. So $\mathfrak{a} \subset (\pi^k)$. On*

[53] i.e. $v(ab) = v(a) + v(b)$ for all $a, b \in K^\times$.

the other hand, for $x_0 \in \mathfrak{a}$ such that $v(x_0) = k$, we have $v\big(\pi^k x_0^{-1}\big) = k - k = 0$, and so $\pi^k = \pi^k x_0^{-1} \cdot x_0 \in \mathfrak{a}$. Thus $\big(\pi^k\big) \subset \mathfrak{a}$. So $\mathfrak{a} = \big(\pi^k\big)$. Finally, the inclusions are strict since $(\pi^n) = \{x \in A \mid v(x) \geq n\}$ (check!). This also shows that v is determined uniquely by A (explain!).

(4) $\operatorname{spec} A = \{(0), (\pi)\}$, *and so* $\dim A = 1$.
Proof: *(0) is prime and (π) is maximal by the points above. For $k \geq 2$, the ideal $\big(\pi^k\big)$ of A is not prime because, e.g., $\pi^k \in \big(\pi^k\big)$, while $\pi \notin \big(\pi^k\big)$.*

We have shown, in particular, that:

Lemma 14.4. *Every DVR is a noetherian local domain of dimension* 1.

Note that a ring A is a local domain of dimension 1 if and only if $\operatorname{spec} A = \{(0), \mathfrak{m}\}$ for some $\mathfrak{m} \neq (0)$ (necessarily maximal). Indeed, "domain" means that (0) is prime, "local" means that there is exactly one maximal ideal $\mathfrak{m}$, and "dimension 1" means that $\mathfrak{m} \neq (0)$ and that there are no prime ideals between (0) and $\mathfrak{m}$. If we assume further that A is noetherian, then the chain $\mathfrak{m}^0 \supset \mathfrak{m}^1 \supset \mathfrak{m}^2 \supset \cdots$ is strictly desceding. Indeed, if $\mathfrak{m}^{n+1} = \mathfrak{m}^n$ for some n, then $\mathfrak{m}^n = 0$ by Nakayama's lemma, and thus the notherian ring A is artinian (as in the example sheet), and so $\dim A = 0$, a contradiction.

Among noetherian local domains of dimension 1, DVRs are characterized in several equivalent ways:

Proposition 14.5. ***[Only* (1) ⇒ (2) ⇒ (3) *fully covered in the lecture. For the rest, see ES4.]*** *Let $(A, \mathfrak{m})$ be a noetherian local domain of dimension* 1. *Then, the following conditions are equivalent:*

(1) *A is a DVR.*
(2) *A is integrally closed.*
(3) *$\mathfrak{m}$ is a principal*[54] *ideal.*
(4) *Every nonzero ideal of A is a power of $\mathfrak{m}$.*
(5) *There is*[55] *$\pi \in A$ such that every nonzero ideal of A is equal to (π^n) for some $n \geq 0$.*

Proof. (1) ⇒ (2): Assume that A is a DVR. Then A is the valuation ring for some discrete valuation $v\colon \operatorname{Frac} A \to \mathbb{Z}$. Take $x \in \operatorname{Frac} A$ integral over A.

[54] Any generator of $\mathfrak{m}$ is called a *uniformizer*, or *uniformizing parameter*.

[55] Thus π is a uniformizer.

Then $x^n + a_1x^{n-1} + \cdots + a_nx^0 = 0$, $n \geq 1$, $a_i \in A$. Thus

$$\begin{aligned}\underbrace{v(x^n)}_{nv(x)} &= v\big(a_1x^{n-1} + \cdots + a_nx^0\big) \\ &\geq \min_{1\leq i\leq n}\left[\underbrace{v(a_i)}_{\geq 0} + (n-i)v(x)\right].\end{aligned}$$

So $nv(x) \geq (n-i_0)v(x)$ for some $1 \leq i_0 \leq n$, and thus $i_0v(x) \geq 0$ and so $v(x) \geq 0$ and thus $x \in A$.

(2) ⇒ (3): Assume that A is integrally closed. We want to find $x \in A$ such that $\mathfrak{m} = Ax$. It suffices to find $x \in \operatorname{Frac} A$ such that $\mathfrak{m} = Ax$ because this implies that $\mathfrak{m} \ni 1 \cdot x$ and so $x \in A$. Equivalently, we are looking for $x \in \operatorname{Frac} A$ such that $x^{-1}\mathfrak{m} = A$. It suffices to require (I) $x^{-1}\mathfrak{m} \subset A$ and (II) $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$ because (I) ensures that $x^{-1}\mathfrak{m}$ is an ideal of A (check!), and (II) ensures $x^{-1}\mathfrak{m}$ is not contained in the unique maximal ideal of A.

Write $x = \frac{a}{b}$ for nonzero $a, b \in A$. To ensure (I), we need $\frac{b}{a}\mathfrak{m} \subset A$, i.e. (I') $b\mathfrak{m} \subset Aa$. To ensure (II), it suffices to ask for x^{-1} not to be integral over A (because then, if $x^{-1}\mathfrak{m} \subset \mathfrak{m}$, then $\mathfrak{m}$ would be a faithful $A\big[x^{-1}\big]$-module, finitely generated over A since A is noetherian, contradicting Lemma 6.4). Since A is integrally closed, this is the same as requiring $\underbrace{x^{-1}}_{=b/a} \notin A$, i.e. (II') $b \notin Aa$.

We are left with choosing a and b to ensure (I') and (II'). Take any $0 \neq a \in \mathfrak{m}$. Then $\sqrt{Aa} = \mathfrak{m}$ since $\operatorname{spec} A = \{(0), \mathfrak{m}\}$. Thus $\mathfrak{m}^t \subset Aa$ for some t (in a noetherian ring, every ideal contains a power of its radical). Take t to be minimal, i.e. $\mathfrak{m}^{t-1} \not\subset Aa$. Choose any $b \in \mathfrak{m}^{t-1} \setminus Aa$, clearly ensuring (II'). Then $b\mathfrak{m} \subset \mathfrak{m}^t \subset Aa$, and so (I') holds as well.

(3) ⇒ (4): Let $\mathfrak{a}$ be a nonzero proper ideal of A. Then $\sqrt{\mathfrak{a}} = \mathfrak{m}$ since $\operatorname{spec} A = \{(0), \mathfrak{m}\}$. Thus, $\mathfrak{m}^\ell \subset \mathfrak{a}$ for some $\ell \geq 1$, and so $\mathfrak{m}^{\ell+1} \subsetneq \mathfrak{a}$, and in particular $\mathfrak{a} \not\subset \mathfrak{m}^{\ell+1}$. Thus, since $\mathfrak{a} \subset \mathfrak{m}^1$, there is $t \geq 1$ such that $\mathfrak{a} \subset \mathfrak{m}^t$ but $\mathfrak{a} \not\subset \mathfrak{m}^{t+1}$. Assume that $\mathfrak{m}$ is principal, i.e. $\mathfrak{m} = (\pi)$, $\pi \in A$. Take $y \in \mathfrak{a} \setminus \mathfrak{m}^{t+1}$. Then $y = a\pi^t$ for some $a \in A$, but $y \notin \mathfrak{m}^{t+1}$, and so $a \notin \mathfrak{m}$, and thus $a \in A^\times$. Thus $\pi^t \in \mathfrak{a}$, and so $\big(\pi^t\big) \subset \mathfrak{a} \subset \big(\pi^t\big)$, i.e. $\mathfrak{a} = \mathfrak{m}^t$.

(4) ⇒ (5): We have $\mathfrak{m} \neq \mathfrak{m}^2$. Take $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then $(\pi) = \mathfrak{m}^r$ for some $r \geq 1$ by hypothesis, and so $r = 1$ since $\pi \notin \mathfrak{m}^2$, i.e. $(\pi) = \mathfrak{m}$. So, every nonzero ideal of A is of the form $\mathfrak{m}^r = (x^r)$, $r \geq 0$.

(5) ⇒ (1): Assume (5). The chain $((\pi^n))_{n\geq 0}$ is strictly decreasing: If $\underbrace{\big(\pi^{n+1}\big)}_{=\pi(\pi^n)} = (\pi^n)$, then $\big(\pi^{n+i}\big) = (\pi^n)$ for all $i \geq 0$ and so A has finitely many ideals, in contradiction with our previous discussion. Thus, for $0 \neq a \in A$,

$(a) = \left(\pi^{v(a)}\right)$ for exactly one integer $v(a) \geq 0$. For $\frac{a}{b} \in \operatorname{Frac}(A)^\times$, we let $v\left(\frac{a}{b}\right) = v(a) - v(b)$. It is left to the reader (see Example Sheet 4) to check that v is a discrete valuation, and that A is its valuation ring. □

Exercise 14.6. Let A be a noetherian local domain of dimension 1. Prove that A is a DVR if and only if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$, where $k = A/\mathfrak{m}$.

We have characterized DVRs among noetherian local domains of dimension 1. Their global counterpart to DVRs are Dedekind domains, which are a special kind of noetherian domains of dimension 1.

First, note that a ring A is an integral domain of dimension 1 if and only if $(0) \in \operatorname{spec} A$ and every nonzero prime ideal of A is maximal.

Definition 14.7 (Dedekind domain)**.** Let A be a noetherian domain of dimension 1. Then A is a *Dedekind domain* if it satisfies one (hence all) of the following equivalent conditions:

(1) A is integrally closed.
(2) $A_\mathfrak{p}$ is a DVR for each $0 \neq \mathfrak{p} \in \operatorname{spec} A$ (i.e. for each $\mathfrak{p} \in \operatorname{mspec} A$).

Proof of equivalence. First, note that for each $\mathfrak{m} \in \operatorname{mspec} A$, $A_\mathfrak{m}$ is a noetherian local domain of dimension $\dim A_\mathfrak{m} = \operatorname{ht} \mathfrak{m} = 1$. By Proposition 14.5, $A_\mathfrak{m}$ is a DVR if and only if $A_\mathfrak{m}$ is integrally closed. Hence, equivalence follows from ES3.Q7, which says that a domain A is integrally closed if and only if $A_\mathfrak{m}$ is integrally closed for all $\mathfrak{m} \in \operatorname{mspec} A$. □

Before we continue, we need the following fact:

Fact 14.8. ***[Not covered in the lecture, see ES4]*** *Consider the localization map $R \to S^{-1}R$ for a multiplicative subset S of R. Take $\mathfrak{p} \in \operatorname{spec} R$ such that $\mathfrak{p} \cap S = \emptyset$, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of R. Then $\mathfrak{q}$ is contracted from $S^{-1}R$.*

Proof. By Proposition, we need to show that the image $\overline{S}$ of S in $R/\mathfrak{q}$ does not contain zero divisors. Since $\mathfrak{q}$ is primary, this is the same as showing that $\overline{S}$ does not contain nilpotent elements. If it did contain a nilpotent element $s + \mathfrak{q}$, $s \in S$, i.e. $s^n + \mathfrak{q} = 0$ for some $n \geq 1$, then $s \in \sqrt{\mathfrak{q}} = \mathfrak{p}$, contradicting the assumption $\mathfrak{p} \cap S = \emptyset$. □

Proposition 14.9. ***[Not covered in the lecture, see ES4]*** *Let A be a Dedekind domain and $(0) \neq \mathfrak{p} \in \operatorname{spec} A$. Then the set of $\mathfrak{p}$-primary ideals of A is $\{\mathfrak{p}^n\}_{n\geq 1}$, and $(\mathfrak{p}^n)_{n\geq 1}$ is a strictly descending sequence.*

Proof. On one hand, $\sqrt{\mathfrak{p}^n} = \sqrt{\mathfrak{p}} = \mathfrak{p}$, a maximal ideal, and so $\mathfrak{p}^n$ is $\mathfrak{p}$-primary. Conversely, let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of A. Then $\mathfrak{q}A_\mathfrak{p}$ is a nonzero proper ideal of the DVR $A_\mathfrak{p}$, and thus $\mathfrak{q}A_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n = \mathfrak{p}^n A_\mathfrak{p}$ for some $n \geq 1$ by Proposition 14.5(4). By Fact 14.8, $\mathfrak{q} = (\mathfrak{q}A_\mathfrak{p})^c$ and $\mathfrak{p}^n = (\mathfrak{p}^n A_\mathfrak{p})^c$, and thus

$\mathfrak{q} = \mathfrak{p}^n$. As for the last assertion, if $\mathfrak{p}^{n+1} = \mathfrak{p}^n$, $n \geq 0$, then $\mathfrak{p}^{n+1}A_\mathfrak{p} = \mathfrak{p}^n A_\mathfrak{p}$, and thus $\underbrace{\mathfrak{p}^n A_\mathfrak{p}}_{=(\mathfrak{p}A_\mathfrak{p})^n} = (0)$ by Nakayama's Lemma, and so $\mathfrak{p}A_\mathfrak{p} = 0$ since $A_\mathfrak{p}$ is a domain, and thus $\mathfrak{p} = (0)$, a contradiction. □

Let $\mathfrak{a} \neq (0)$ be an ideal of a Dedekind domain A. Then $\mathfrak{a}$ has a minimal primary decomposition since A is noetherian. In light of Proposition 14.9, this can be written as $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \cdots \cap \mathfrak{p}_n^{e_n}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are all nonzero since $\mathfrak{a} \neq (0)$. The associated prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are in $\operatorname{mspec} A$, and thus there are no inclusions among them. So $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the isolated prime ideals of $\mathfrak{a}$, and $\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_n^{e_n}$ are the isolated primary components of $\mathfrak{a}$. So $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_n^{e_n}$ are uniquely determined by $\mathfrak{a}$. Hence, $e_1, \ldots, e_n$ are also uniquely determined by $\mathfrak{a}$ by the last assertion of Proposition 14.9.

Proposition 14.10. *Let A be a Dedekind domain, and $\mathfrak{a} \neq 0$ an ideal of A. Then $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in (\operatorname{spec} A) \setminus \{(0)\}$ are distinct and $e_i \geq 1$. Furthermore, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $e_1, \ldots, e_n$ are uniquely determined (up to reordering).*

Proof. Consider distinct $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in (\operatorname{spec} A) \setminus \{(0)\}$, and $e_1, \ldots, e_n$, $e_i \geq 1$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are pairwise co-prime since they are distinct and maximal. Thus $\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_n^{e_n}$ are pairwise co-prime by ES3.Q6b. Thus $\mathfrak{p}_1^{e_1} \cap \cdots \cap \mathfrak{p}_n^{e_n} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ by the Chinese Remainder Theorem[56] (ES1.Q4). Thus the existence and uniqueness follow from the discussion above. □

Remark 14.11. **[Not covered in the lecture, see ES4]** For a factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ as in Proposition 14.10, we have $\mathfrak{a}R_{\mathfrak{p}_i} = (\mathfrak{p}_1 R_{\mathfrak{p}_i})^{e_1} \cdots (\mathfrak{p}_n R_{\mathfrak{p}_i})^{e_n} = (\mathfrak{p}_i R_{\mathfrak{p}_i})^{e_i}$ (explain using Proposition 4.16(3) !). Now, $R_{\mathfrak{p}_i}$ is a DVR, with a uniformizer $\pi_i \in R_{\mathfrak{p}_i}$, $\mathfrak{p}_i R_{\mathfrak{p}_i} = (\pi_i)$, and a discrete valuation $v_i \colon \operatorname{Frac}(R_{\mathfrak{p}_i}) \to \mathbb{Z}$. So $v_i(\mathfrak{a}R_{\mathfrak{p}_i}) = e_i$.

Proposition 14.12. *Let K be a number field[57]. Let $\mathcal{O}_K$ be the ring of integers of K (i.e., the integral closure of $\mathbb{Z}$ in K). Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Clearly, $\mathcal{O}_K$ is a domain since it is a subring of the field $\mathcal{O}_K$. We have $\mathcal{O}_K \subset \operatorname{Frac} \mathcal{O}_K \subset K$ (in fact[58] $\operatorname{Frac} \mathcal{O}_K = K$). By Lemma 6.12, $\mathcal{O}_K$ is integrally closed in K, and thus also in $\operatorname{Frac} \mathcal{O}_K$. Now, $\mathbb{Z} \subset \mathcal{O}_K$ is an integral extension, and thus $\dim \mathcal{O}_K = \dim \mathbb{Z} = 1$.

[56] The Chinese Remainder Theorem, as stated in the example sheet, gives us that the kernel of the natural map $A \to A/\mathfrak{p}_1^{e_1} \times \cdots \times A/\mathfrak{p}_n^{e_n}$ is $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, but this kernel is evidently also equal to $\mathfrak{p}_1^{e_1} \cap \cdots \cap \mathfrak{p}_n^{e_n}$.

[57] A *number field* K is a finite extension of $\mathbb{Q}$, i.e. $[K : \mathbb{Q}] < \infty$.

[58] We only need the trivial inclusion $\operatorname{Frac} \mathcal{O}_K \subset K$, but it feels silly not to mention that this is an equality becuase this is such a basic fact. **Proof:** If $x \in K$ then x is algebraic over

We have shown that $\mathcal{O}_K$ is an integrally closed domain of dimension 1. It remains to show that $\mathcal{O}_K$ is a noetherian ring, i.e. a noetherian $\mathcal{O}_K$-module. In fact, $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$ as $\mathbb{Z}$-modules, and thus $\mathcal{O}_K$ is a noetherian $\mathbb{Z}$-module, a fortiori a noetherian $\mathcal{O}_K$-module (explain!). We record this fact in the next proposition. □

Proposition 14.13. *[**non-exmainble**] The ring of integers of a number field K is isomorphic is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

Proof. See any text on algebraic number theory (or Atiyah–Macdonald). □

Remark 14.14. **[non-examinable]** More generally, for an extension $A \subset \operatorname{Frac} A \subset K$, where A is a Dedekind domain and $K/\operatorname{Frac} A$ is a finite separable field extension, the integral closure $\overline{A}$ of A in L is a Dedekind domain. The proof is similar to the one above, except for the fact that $\overline{A}$ does not have to be a free A-module (but in general $\overline{A}$ an A-submodule of a free A-module of rank $[K : \operatorname{Frac} A]$, and hence $\overline{A}$ is a noethrian A-module, and hence $\overline{A}$ is a noetherian $\overline{A}$-module, i.e. a noetherian ring). If A is a PID then $\overline{A} \cong A^{[K:\operatorname{Frac} A]}$ as A-modules, like in the case $\underbrace{\mathbb{Z}}_{=A} \subset \underbrace{\mathbb{Q}}_{=\operatorname{Frac} A} \subset K$ discussed above.

$\mathbb{Q}$ since $[K : \mathbb{Q}] < \infty$, and so $a_0x^n + \cdots + a_nx^0 = 0$ for some $\underbrace{a_0}_{\neq 0}, \ldots, a_n \in \mathbb{Z}$ (explain!). Multiplying both sides by a_0^{n-1}, we see that a_0x is integral over $\mathbb{Z}$, i.e. $a_0x \in \mathcal{O}_K$. Thus $x = \frac{a_0x}{a_0} \in \operatorname{Frac} \mathcal{O}_K$ (as $a_0 \in \mathbb{Z} \subset \mathcal{O}_K$).

15. Example Sheets

Example Sheet 1. In all exercises, k is a field and R is a ring (commutative and unital).

(1)
- (a) Let I be a finitely generated ideal of R, and let S be a generating subset of I. Prove that there is a finite subset S_0 of S that generates I.
- (b) Let $f \in k[T_1, \dots, T_n]$ be a nonzero homogeneous polynomial. Prove that $f(T_1, \dots, T_{n-1}, 1)$ is a nonzero polynomial. Show that the assumption that f is homogeneous cannot be dropped.
- (c) Let $0 \neq f \in k[T_1, \dots, T_n]$, $d = \deg f$.
  - (i) For $S \subset k$, prove that $\{(s_1, \dots, s_n) \in S^n \mid f(s_1, \dots, s_n) = 0\}$ has at most $d|S|^{n-1}$ elements [**Hint:** Induct on n].
  - (ii) Deduce that if k is infinite then there is $(x_1, \dots, x_n) \in k^n$ such that $f(x_1, \dots, x_n) \neq 0$. Show that the assumption that k is infinite cannot be dropped.

(2) Let M, N be modules over a ring R. Prove[59]:
- (a) ***Commutativity:*** $M \otimes N \xrightarrow{\sim} N \otimes M$ as R-modules via a map sending $m \otimes n \mapsto n \otimes m$.
- (b) ***Associativity:*** $(M \otimes N) \otimes P \xrightarrow{\sim} M \otimes (N \otimes P) \xrightarrow{\sim} M \otimes N \otimes P$ as R-modules via maps sending $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p) \mapsto m \otimes n \otimes p$ (where the rightmost term is defined using R-trilinear maps in the natural way).
- (c) ***Distributivity:*** $(\bigoplus_i M_i) \otimes P \xrightarrow{\sim} \bigoplus_i (M_i \otimes P)$ as R-modules via a map sending $(m_i)_i \otimes p \mapsto (m_i \otimes p)_i$.
- (d) ***Identity element:*** $R \otimes M \xrightarrow{\sim} M$ as R-modules via a map sending $r \otimes m \mapsto rm$.
- (e) ***Quotients:*** For submodules $M' \subset M$, $N' \subset N$, let L be the R-submodule of $M \otimes N$ generated by

$$\{m' \otimes n \mid (m', n) \in M' \times N\} \cup \{m \otimes n' \mid (m, n') \in M \times N'\} .$$

[59] I like proving such claims by producing homomorphisms in both directions using universal properties, and then showing that they are two-sided inverses. Another, similar, approach is to use the uniqueness of the tensor product w.r.t. the universal property.

Prove that $(M/M') \otimes (N/N') \xrightarrow{\sim} (M \otimes N)/L$ via a map sending $(m + M') \otimes (n + N') \mapsto m \otimes n + L$.

(f) Deduce that $(R/I) \otimes M \xrightarrow{\sim} M/IM$ via a map sending $(r + I) \otimes m \mapsto rm + IM$.

(3) Let $\varphi\colon A \to B$ be a ring homomorphism. The *contraction* of an ideal $\mathfrak{b}$ of B is the ideal $\mathfrak{b}^c := \varphi^{-1}(\mathfrak{b})$ of A. The *extension* of an ideal $\mathfrak{a}$ of A is the ideal $\mathfrak{a}^e := (\varphi(\mathfrak{a}))$ of B (i.e., the ideal of B generated by the image of $\mathfrak{a}$ under φ).

(a) Show that $\mathfrak{b}^c$ is an ideal of A, but $\varphi(\mathfrak{a})$ is not necessarily an ideal of B (although $\mathfrak{a}^e$ clearly is).

(b) Let $\mathfrak{a}_1, \mathfrak{a}_2$ be ideals of A, and $\mathfrak{b}_1, \mathfrak{b}_2$ ideals of B. Prove:

$$(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e \qquad (\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$$

$$(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c \qquad \sqrt{\mathfrak{b}}^c = \sqrt{\mathfrak{b}^c}$$

(here $\sqrt{I}$ is the *radical* of an ideal I of a ring R, i.e. $\sqrt{I} = \{x \in R \mid \exists n \geq 1 \; x^n \in I\}$).

[Recall that the sum and intersection of two ideals as sets are ideals, but the product $\{xy \mid x \in I, y \in J\}$ of two ideals I and J as sets is usually not an ideal. When we write IJ, we are referring to the ideal generated by this product set.]

(c) Prove that $\mathfrak{a} \subset \mathfrak{a}^{ec}$ and $\mathfrak{b} \supset \mathfrak{b}^{ce}$. Then prove that $\mathfrak{b}^c = \mathfrak{b}^{cec}$ and $\mathfrak{a}^e = \mathfrak{a}^{ece}$.

(d) Ideals of A of the the form $\mathfrak{b}^c$ are called *contracted ideals*. Ideals of B of the form $\mathfrak{a}^e$ are called *extended ideals*. Prove that an ideal $\mathfrak{a}$ of A is contracted if and only if $\mathfrak{a}^{ec} = \mathfrak{a}$, and an ideal of $\mathfrak{b}$ is extended if and only if $\mathfrak{b}^{ce} = \mathfrak{b}$. Then prove that we have a bijection

$$\{ \text{ contracted ideals of } A \} \leftrightarrow \{ \text{ extended ideals of } B \}$$

given by $\mathfrak{a} \mapsto \mathfrak{a}^e$ and $\mathfrak{b}^c \leftarrow\!\shortmid \mathfrak{b}$.

(e) Give an example of a ring homomorphism $\varphi\colon A \to B$, an ideal of A that is not contracted, and an ideal of B that is not extended.

(4) **Chinese remainder theorem:** Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of a ring A such that $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime for all $i \neq j$ (i.e., $\mathfrak{a}_i + \mathfrak{a}_j = A$). Prove that the map $x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n) \colon A \to A/\mathfrak{a}_1 \times \ldots \times A/\mathfrak{a}_n$ is surjective with kernel $\mathfrak{a}_1 \ldots \mathfrak{a}_n$.

(5) Let $I_1, \ldots, I_r, \mathfrak{a}$, $r \geq 1$, be ideals of a ring A, such that $\mathfrak{a} \not\subseteq I_i$ for all $1 \leq i \leq r$. Prove:

(a) **Prime avoidance:** If $|\{1 \leq i \leq r \mid I_i \text{ is not prime}\}| \leq 2$ then $\mathfrak{a} \not\subseteq \bigcup_{i=1}^r I_i$.

(b) If A contains an infinite field then $\mathfrak{a} \not\subseteq \bigcup_{i=1}^r I_i$.

(c) It is possible that $\mathfrak{a} \subset \bigcup_{i=1}^r I_i$ (give an example).

(6) Let I be an ideal of a noetherian ring R. Prove that there is $n \geq 1$ such that $\left(\sqrt{I}\right)^n \subset I$.

(7) **Unboundedly many generators:** Consider the ideal $\mathfrak{a}_n = \left(X^n Y^0, X^{n-1} Y^1, \ldots, X^0 Y^n\right)$ of the polynomial ring $k[X, Y]$, k a field. Prove that any generating set for $\mathfrak{a}_n$ has at least $n+1$ elements (**Hint:** Consider the image of $\mathfrak{a}_n$ in $k[X, Y]/\mathfrak{a}_{n+1}$).

(8) Is every subalgebra of a noetherian k-algebra itself noetherian? Show that the subalgebra $k\left[\left\{T_1 T_2^i\right\}_{0=1}^{\infty}\right]$ of $k[T_1, T_2]$ is not noetherian.

(9) Let R be a nonzero ring. Prove that if there is a surjective R-module homomorphism $R^n \to R^\ell$ then $n \geq \ell$. Deduce that if $R^n \cong R^\ell$ as R-modules then $n = \ell$. **Aside:** It's also true that if there is an injective R-module homomorphism $R^n \to R^\ell$ then $n \leq \ell$.

(10) Let V and W be finite-dimensional vector spaces over a field k.

(a) Prove that there is a k-linear isomorphism $V^* \underset{k}{\otimes} W \xrightarrow{\sim} \mathrm{Hom}_k(V, W)$ sending $\varphi \otimes w \to (v \mapsto \varphi(v) w)$.

(b) Show that there is a k-linear map $V^* \otimes V \to k$ sending $\varphi \otimes v \mapsto \varphi(v)$, which corresponds, under the isomorphism in (c), to the usual trace[60] map $\operatorname{Hom}_k(V, V) \to k$.

(c) The *rank* $\operatorname{rank} t$ of a tensor $t \in M \otimes_R N$ (M, N some R-modules) is the least number pure tensors that sum up to t. Let $\alpha \in V^* \underset{F}{\otimes} W$. Describe[61] $\operatorname{rank} \alpha$ in terms on the linear transformation corresponding to α (under the isomorphism in (c)). Then, compute $\max\limits_{\beta \in V \underset{k}{\otimes} W} \operatorname{rank} \beta$.

(d) Use the basis-free definition of the trace to prove the formula[62] $\operatorname{tr} AB = \operatorname{tr} BA$ for matrices $A \in M_{a\times b}(k)$, $B \in M_{b\times a}(k)$.

(e) Let $f\colon M \otimes_R N \to L$ be an R-module homomorphism. Prove that f injective on pure tensors (i.e. maps different pure tensors to different elements of L) if and only if every nonzero element of $\ker f$ has tensor rank at least 3.

(f) Let V be a 2-dimensional vector space over a field k, and let $f\colon V \otimes_k V \to W$ be a k-linear map, injective on the pure tensors (W some k-vector space). Prove that f is injective.

(g) Give an example of k-vector spaces V, W and a k-linear map $f\colon V \otimes_k V \to W$ that is injective on pure tensors but not injective.

(11)

[60] This construction gives us a definition of the trace of an operator that does not require choosing a basis.

[61] Once you solve this problem you'll have an efficient algorithm to compute the tensor rank in a tensor product of two finite dimensional vector spaces. But note that computing the tensor rank in a tensor product $U \otimes V \otimes W$ of three vector spaces is NP-complete (so if P $\neq$ NP as widely conjectured, then there is no polynomial time algorithm to compute the tensor rank in $U \otimes V \otimes W$).

[62] In undergraduate courses this formula is often proved directly, and is then used to show that tr is invariant under a change of basis. But with the basis-free approach, we automatically deduce invariance. Also, there's a basis-free approach to defining the determinant through a construction called the *exterior power*, which is analogous to the tensor power $V^{\otimes n}$, but with a universal property for alternating multilinear maps rather than all multilinear maps.

(a) Let $B = A[T]/(f)$, A a ring, f a monic polynomial. Prove that the A-algebra B is a flat A-module.

(b) Prove that the A-algebra $B \coloneqq k[X,Y]/(XY)$ is not a flat $k[X]$-module. **Hint:** Consider the embedding $(X) \to k[X]$.

(12) Let $\mathcal{C}$ be a class of R-modules (e.g. all finitely generated R-modules) and let λ be a function on $\mathcal{C}$ with values in $\mathbb{Z}$, such that $\lambda(M) = \lambda(M')$ whenever $M \cong M'$ as R-modules. Assume that λ is *additive,* i.e. for every short exact sequence $0 \to M' \to M \to M'' \to 0$ we have $\lambda(M) = \lambda(M') + \lambda(M'')$. Consider an exact sequence of R-modules

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

(where the M_i and all kernels and images belongs to $\mathcal{C}$). Prove that

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0 \ .$$

(13) Let $f\colon R \to S$ be a ring homomorphism. Let M be an S-module and N an R-module. Prove that

$$M \otimes_R N \cong M \otimes_S (S \otimes_R N)$$

as S-modules by isomorphisms sending $m \otimes n \mapsto m \otimes (1 \otimes n)$ and $(sm) \otimes n \leftarrow\!\shortmid m \otimes (s \otimes n)$ [the proof appears in the notes]

(14) Let R be an integral domain, and V a $\operatorname{Frac} R$-module. Let $M \neq 0$ be an R-submodule of $\operatorname{Frac} R$. Prove that $M \otimes_R V \cong V$ as R-modules by an isomorphism sending $m \otimes v \mapsto mv$.

(15)

(a) Let k be a field, and take matrices $A \in M_m(k)$ and $B \in M_n(k)$, that have eigenvalues $\lambda \in k$ and $\mu \in k$, respectively. Prove that $A \otimes B$ has eigenvalue $\lambda\mu$ and $A \otimes I_n + I_m \otimes B$ has eigenvalue $\lambda + \mu$.

(b) Given algebraic integers $a, b \in \mathbb{C}$ (this means that each of a and b is a root of a monic polynomial with coefficients in $\mathbb{Z}$), deduce that $a + b$ and ab are algebraic integers, and describe an algorithm that take monic polynomials $f, g \in \mathbb{Z}[T]$ such that $f(a) = g(b) = 0$ and produces monic polynomials $p, q \in \mathbb{Z}[T]$

such that $p(a+b) = q(ab) = 0$. Deduce also that the set of algebraic integers in $\mathbb{C}$ forms a ring.

(16)

(a) Prove that $M \otimes_R M'$ is flat whenever M and M' are flat R-modules [**Note:** This implies, by induction, that $M_1 \otimes \cdots \otimes M_k$ is flat whenever $M_1, \ldots, M_k$ are all flat].

(b) For injective R-linear maps $f\colon M \to M'$ and $g\colon N \to N'$ prove that if either M, N' are both flat, or M', N are both flat, then $f \otimes g$ is injective.

(c) Prove that if $f_1\colon M_1 \to N_1, \ldots, f_k\colon M_k \to N_k$ are injective R-linear maps, where $M_1, \ldots, M_k, N_1, \ldots, N_k$ are all flat, then $f_1 \otimes \cdots \otimes f_k$ is injective. Deduce that if $f\colon M \to N$ is an injective R-linear map between flat modules then $f^{\otimes k}$ is injective for all $k \geq 1$.

(17) We say that a short exact sequence of R-module

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

splits if it isomorphic to the short exact sequence

$$0 \longrightarrow A \xrightarrow{\iota_A} A \oplus C \xrightarrow{\pi_C} C \longrightarrow 0$$

where ι_A is the canonical embedding and π_C is the canonical projection.

Prove the splitting lemma, which says that the following are equivalent:

(a) The sequence splits.
(b) There is an R-linear map $s\colon C \to B$ such that $g \circ s = \mathrm{id}_C$.
(c) There is an R-linear map $r\colon B \to A$ such that $r \circ f = \mathrm{id}_A$.

(18) Find a short exact sequence $0 \to A \to B \to C \to 0$ of R-module that does not split although $B \cong A \oplus C$ as R-modules.

(19) Let $M \neq 0$ be a finitely generated R-module. Prove that $M^{\otimes k} \neq 0$ for all $k \geq 1$. [**Hint 1:** Let x be an element of a minimal generating set for M. Prove that $x \otimes \cdots \otimes x \neq 0$ in $M^{\otimes k}$. **Hint 2:** To show that $x \otimes \cdots \otimes x \neq 0$, use the universal property of $M^{\otimes k}$ for k-multilinear

maps to produce an R-linear map φ from $M^{\otimes k}$ to some R-module such that $\varphi(x \otimes \cdots \otimes x) \neq 0$.]

Example Sheet 2. In all exercises, k is a field and R is a ring (commutative and unital).

(1) Let M be an R-module. A *chain* of submodules of M is a finite sequence $(M_i)_{i=1}^n$ of submodules of M such that

$$\underbrace{M_0}_{=M} \supsetneq M_1 \supsetneq \cdots \supsetneq \underbrace{M_n}_{=0} .$$

The *length* of the chain is n. A *composition series* of M is a maximal chain of submodules of M (i.e. there are no R-submodules strictly between M_{i+1} and M_i, i.e. M_i/M_{i+1} is a simple module by the bijective correspondence between R-submodules of M_i/M_{i+1} and the R-submodules of M_i that contain M_{i+1}).

(a) Assume that M has a composition series of length n. Prove that every composition series of M has length n, and that every chain of submodules of M can be extended to a composition series. [**Hint 1:** Write $\ell(K)$ for the length of the shortest composition series of K. Prove that $\ell(N) < \ell(M)$ for every proper submodule N of M. **Hint 2:** Deduce that $\ell(M)$ is the common length of all composition series of M, and $\ell(M)$ is also an upper bound on the length of all chains of submodules of M. **Hint 3:** Now, finish the proof.]

(b) For an R-module M, write $\ell(M)$ for the common length of all composition series of M ($\ell(M) = \infty$ if M has no composition series). Prove that $\ell(M) < \infty$ if and only if M is both noetherian and artinian.

(c) Prove that $\ell(\cdot)$ is additive (in the sense of Question 12 in Example Sheet 1) on the class of R-modules of finite length.

(d) Let V be a k-vector space. Prove that the following are equivalent:

(i) $\dim_k V < \infty$.
(ii) $\ell(V) < \infty$.
(iii) V is noetherian.
(iv) V is artinian.

(e) Assume that there are maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ of R (not necessarily distinct) such that $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Prove that R is noetherian if and only if R is artinian. [**Hint:** Construct a finite chain of ideals of R, descending from R to 0, such that for consecutive ideal $I \supset J$ in the chain, the natural R module structure $R \to \mathrm{End}(I/J)$ on I/J factors as the composition of ring homomorphisms $R \to k \to \mathrm{End}(I/J)$, where k is a certain field, and $R \to k$ is surjective.]

(2)

(a) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{p}$ be ideals of R, where $\mathfrak{p}$ is prime. Prove that if $\bigcap_i \mathfrak{a}_i \subset \mathfrak{p}$ then $\mathfrak{a}_i \subset \mathfrak{p}$ for some i, and that if $\bigcap_i \mathfrak{a}_i = \mathfrak{p}$ then $\mathfrak{a}_i = \mathfrak{p}$ for some i.

(b) Let I be a radical ideal of R (i.e. $\sqrt{I} = I$). Prove that if $x, y \in R$ and $xy \in I$ then $I = \sqrt{I + (x)} \cap \sqrt{I + (y)}$.

(c) For an ideal I of R, a *minimal prime ideal* over I is a prime ideal $\mathfrak{p}$ of R such that $I \subset \mathfrak{p}$ and if $I \subset \mathfrak{q} \subset \mathfrak{p}$ for some prime ideal $\mathfrak{q}$ of R, then $\mathfrak{q} = \mathfrak{p}$ (a *minimal prime ideal* of R is a minimal prime ideal over (0), or, equivalently, a minimal prime ideal over $\sqrt{(0)}$ since every prime ideal of R contains $\sqrt{(0)}$).
Prove that a radical ideal in a noetherian ring has only finitely many minimal prime ideals [**Hint:** First prove that such an ideal is equal to the intersection of finitely many prime ideals. Prove this by contradiction, where noetherianity is used to take a maximal counter-example (explain!)]

(d) Let I be a radical ideal in a noetherian ring. If you solved (c) according to the hint, you already know that I is the intersection of finitely many prime ideals. If not (but preferrably, even if you did), deduce this from (c) using a claim from the lectures.

(e) Prove that every ideal in a noetherian ring contains a power of its radical, and deduce that $\mathrm{nil}\, R$ is a nilpotent ideal (i.e. $(\mathrm{nil}\, R)^\ell = 0$ for some $\ell \geq 1$, where in general I^ℓ is the ideal generated by products of the form $x_1 \cdots x_\ell$, $x_i \in I$) when R is noetherian.

(3)

(a) Let R be an artinian ring. Prove:

(i) Every prime ideal of R is maximal. [**Hint:** $R/\mathfrak{p}$ is an artinian integral domain. Is it a field?]

(ii) $\operatorname{nil} R = J(R)$ (deduce from (i)). Here $J(R)$ is the *Jacobson radical* of R, which defined as the intersection of all maximal ideals of R.

(iii) R has finitely many prime (equivalently, maximal) ideals. [**Hint:** Find a finite intersection of maximal ideals of R, contained in all other finite intersections of maximal ideals of R.]

(iv) $\operatorname{nil} R$ is a nilpotent ideal. [**Hint:** $\Big((\operatorname{nil} R)^\ell\Big)_{\ell \geq 1}$ stabilizes in some finite step at an ideal $\mathfrak{a}$ (why?) and you need to prove that $\mathfrak{a} = 0$. Assume not. Prove that there is an ideal $\mathfrak{c}$ of R, minimal with respect to the property $\mathfrak{ac} \neq 0$. Prove that $\mathfrak{c}$ is principal, i.e. $\mathfrak{c} = (x)$, $x \in R$. Prove that $x\mathfrak{a} = (x)$, and deduce that $x = xy$ for some $y \in \operatorname{nil} R$. Derive a contradiction.]

(b) Prove that a nonzero ring R is artinian if and only if R is noetherian and $\dim R = 0$ (Here $\dim R$ refers to the Krull dimension of the ring R. By definition, $\dim R$ is n for the longest chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n$. So $\dim R = 0$ if and only if $R \neq 0$ and every prime ideal of R is maximal. Note that the zero ring $\{0\}$ is the only ring with no prime ideals. By convention, $\dim\{0\} = -\infty$ or $\dim\{0\} = -1$).
[**Hint:** In both directions, use 1(e). Many of the other claims in Q1, Q2, Q3 above are useful.]

(4)

(a) **The prime ideal principle:** Let $\mathcal{F}$ be a set of proper ideals of a ring R such that for every ideal I of R and $x \in R$, if $I + (x) \notin \mathcal{F}$ and $(I : x) \notin \mathcal{F}$ then $I \notin \mathcal{F}$. Let J be a maximal element of $\mathcal{F}$ (i.e. $J \in \mathcal{F}$ is not contained in any other element of $\mathcal{F}$). Prove that J is a prime ideal.

(b) Let I be an ideal of R, and let $x \in R$. Prove that if $I + (x) = (a)$ and $(I : x) = (b)$, $a, b \in R$, then $I = (ab)$.

(c) Prove that if every prime ideal of an integral domain R is principal then R is a PID.

(5) Let $S \subset R$ be a multiplicative subset and take an R-module M. Verify that the law $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$ is well defined and makes $S^{-1}M$ into an abelian group, with $\frac{0}{1}$ as the zero element.
If you have time, verify the rest of the claims skipped in class regarding the basic construction of $S^{-1}M$ and $S^{-1}R$.

(6) The Hom functors are left exact: Let Q, P be R-modules.
 (a) Prove that if $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence of R-modules, then so is

$$0 \longrightarrow \operatorname{Hom}_R(Q, A) \xrightarrow{f_*} \operatorname{Hom}_R(Q, B) \xrightarrow{g_*} \operatorname{Hom}_R(Q, C) \ .$$

 (b) Prove that if $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is an exact sequence of R-modules, then so is

$$0 \longrightarrow \operatorname{Hom}_R(C, P) \xrightarrow{g^*} \operatorname{Hom}_R(B, P) \xrightarrow{f^*} \operatorname{Hom}_R(A, P) \ .$$

(7) Prove that a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ of R-modules is exact if for every R-module Q, the sequence $\operatorname{Hom}_R(Q, A) \xrightarrow{f_*} \operatorname{Hom}_R(Q, B) \xrightarrow{g_*} \operatorname{Hom}_R(Q, C)$ is exact (where $f_*\varphi = f \circ \varphi$ and $g_*\psi = g \circ \psi$).

(8) An R-module P is *projective* if for every R-module N and submodule $N' \subset N$, every R-linear map $M \to N/N'$ factors as $M \xrightarrow{g} N \xrightarrow{\pi} N/N'$ for some R-linear g, where π is the quotient map (g is not required to be unique; this is not a universal property).
 (a) Let M be an R-module. Prove that the following conditions are equivalent:
  (i) M is a projective R-module.
  (ii) The $\operatorname{Hom}_R(M, \cdot)$ functor is exact[63].
  (iii) Every short exact sequence of the form $0 \to A \to B \to M \to 0$ splits.
  (iv) There is an R-module N such that $M \oplus N$ is a free R-module (i.e. M is a direct summand of a free module).

[63] Recall that a functor is exact if it preserves the exactness of all exact sequences. It's best to recall or prove first that a functor that preserves the exactness of all short exact sequences is exact.

(b) Prove that every projective module is flat.

(c) Give an example of a projective module that is not free (over some ring R).

(d) Prove that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, but not a projective $\mathbb{Z}$-module.

(e) Consider the ideal $\mathfrak{m} = (X, Y)$ of $R = k[X, Y]$, k a field.
   (i) Find $n \geq 0$ and $f_1, \dots, f_\ell \in \mathfrak{m}^{\oplus n}$ such that $\mathfrak{m} \otimes_R \mathfrak{m} \cong \mathfrak{m}^{\oplus n}/(f_1, \dots, f_\ell)$ as R-modules.
   Hint: First find an exact sequence $R^t \to R^n \to \mathfrak{m} \to 0$ of R-modules, $t, n \geq 0$. It may be helpful to recall that R is a UFD.

   (ii) Prove that $\mathfrak{m}$ is a torsion-free R-module which is not flat.

(f) **Nothing to prove:** We have shown that free ⇒ projective ⇒ flat ⇒ torsion free, and that none of the reverse implications holds in general.

(9) Let $R_1, \dots, R_n$ be rings and $R = R_1 \times \cdots \times R_n$.
   (a) Prove that every ideal of R is of the form $I = I_1 \times \cdots \times I_n$, I_j an ideal of R_j. What are the tuples $(I_1, \dots, I_n)$ for which I is a prime ideal[64]?

   (b) Explain why the ideals $R_1 \times \{0\}$ and $\{0\} \times R_2$ of $R_1 \times R_2$ are not subrings of $R_1 \times R_2$ (in the category of commutative unital rings).

   (c) An element $e \in R$ is an *idempotent* if $e^2 = e$. An idempotent $e \in R$ is *nontrivial* if $e \notin \{0, 1\}$. Prove that:
      (i) If $e_1 \in R$ is an idempotent and $e_2 \coloneqq 1 - e_1$ then $e_1 e_2 = 0$. If e_1 is nontrivial then so is e_2.

      (ii) The ideal Re_1 of I, which is an abelian group closed under multiplication, becomes a ring if one declares the multiplicative identity to be e_1 (and similarly for Re_2).

      (iii) $R \to Re_1 \times Re_2$, $r \mapsto (re_1, re_2)$ is a ring isomorphism.

[64] Note that ideals in an infinite product of rings can be much more complicated, and the existence of some of them often depends on the axiom of choice.

(iv) A ring R is isomorphic to a product of nonzero rings if and only if R contains a nontrivial idempotent element.

(10) Localization:

(a) We have seen that if $S \subset R$ is a multiplicative subset, M an R-module and $N \subset M$ a submodule, then $S^{-1}N$ can be thought of as an $S^{-1}R$-submodule of $S^{-1}M$. Forget about N. Take $T \subset S$, another multiplicative subset of R. Prove that there is a $T^{-1}R$-linear map $f\colon T^{-1}M \to S^{-1}M$ sending $\frac{m}{t} \mapsto \frac{m}{t}$, show that f is not necessarily injective. Show that if all elements of S are not zero divisors and $M = R$ then $f\colon T^{-1}R \to S^{-1}R$ is injective.

(b) Let S be a multiplicative subset of R, and take an ideal I of A. Prove that $\sqrt{I}^e = \sqrt{I^e}$, where the ideal extension are taken with respect to the localization map $R \to S^{-1}R$ (the $\subset$ inclusion holds for every ring homomorphism). In particular, $(\operatorname{nil} A)^e = \operatorname{nil} S^{-1}A$, where $\operatorname{nil} R = \sqrt{(0)}$ is the ideal consisting of the nilpotent elements of R.

(c) Let $\mathfrak{p}$ be a minimal prime ideal of a ring A. Show that all of the elements of $\mathfrak{p}$ are zero divisors in A.

(d) Let A be an integral domain. Then all localizations of A are canonically embedded in $\operatorname{Frac}(A)$. Show that $A = \bigcap_{\mathfrak{m} \in \operatorname{mspec} A} A_{\mathfrak{m}}$.

(e) Prove that a ring A is reduced (i.e., 0 is the only nilpotent element in A) $\Leftrightarrow$ $A_{\mathfrak{p}}$ is reduced for every $\mathfrak{p} \in \operatorname{spec} A$.

(f) Does the previous question remain true if both occurrences of “reduced” are replaced by “an integral domain”?

(g) Give an example of an integral domain A, and a ring B, $A \subset B \subset \operatorname{Frac} A$, such that $B \neq S^{-1}A$ for all multiplicative subsets S of A.

(11) Take a polynomial $f \in R[T]$. Prove:

(a) If $x \in R$ is nilpotent then $1 + x$ is invertible. Deduce that if y is nilpotent and z is invertible then $y + z$ is invertible.

(b) f is invertible if and only if the constant term of f is invertible and all other coefficients of f are nilpotent.

(c) f is nilpotent if and only if all of its coefficients are nilpotent.

(d) f is a zero divisor if and only if $af = 0$ for some $0 \neq a \in R$.

(12) Prove that if R is reduced (i.e. $\sqrt{(0)} = (0)$ in R), then R can be embedded in a product of integral domains. Is such R necessarily isomorphic to a product of integral domains?

(13) Prove that every ring R is a quotient of an integral domain.

(14) Let S be a multiplicative subset of the ring R. Prove that if R is a noetherian (resp. artinian) ring then $S^{-1}R$ is noetherian (resp. artinian) ring.

(15) The *height* $\mathrm{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ of A is the maximal length d of a chain of prime ideals of the form:

$$\underbrace{\mathfrak{p}_d}_{=\mathfrak{p}} \supsetneq \mathfrak{p}_{d-1} \supsetneq \cdots \supsetneq \mathfrak{p}_0$$

(there are $d+1$ prime ideals in a chain of length d). The (*Krull*) *dimension* $\dim A$ of A is

$$\sup\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ a prime ideal of } A\} \ .$$

(by convension, the dimension of the zero ring is define to be -1 or $-\infty$).

(a) Let k be a field. Prove that $\dim k[T_1, \ldots, T_n] \geq n$ (this is, in fact, an equality - see later in the course).

(b) Let $x \in R$, R a ring. Prove that

$$S_{\{x\}} = \{x^n(1 - rx) \mid n \geq 0, r \in R\}$$

is a multiplicative subset of R.

(c) Define $R_{\{x\}} = S_{\{x\}}^{-1}R$. Let $n \geq 0$. Prove that

$$\dim R \leq n \qquad \Leftrightarrow \qquad \big(\dim R_{\{x\}} \leq n - 1 \ \forall x \in R\big)$$

according to the following steps:

(i) Prove that $\mathfrak{m} \cap S_{\{x\}} \neq \emptyset$ whenever $\mathfrak{m}$ is a maximal ideal of R and $x \in R$.

(ii) Prove that $\mathfrak{p} \cap S_{\{x\}} = \emptyset$ whenever $\mathfrak{p}$ is a non-maximal prime ideal of R and $x \in \mathfrak{m} \setminus \mathfrak{p}$ for some maximal ideal $\mathfrak{m}$ that contains $\mathfrak{p}$ properly.

(iii) Complete the proof [**Hint:** Use the relationship between the set of prime ideals of $S^{-1}R$ and a certain set of prime ideals of R.]

(d) **In the next example sheet:** Use the claim above to prove that $\dim A \leq \operatorname{trdeg} A$ for every finitely generated k-algebra such that A is an integral domain (here $\operatorname{trdeg} A$ is the *transcedence degree* of $\operatorname{Frac} A$, a concept that you will be asked to recall). Deduce that $\dim k[T_1, \ldots, T_n] = n$. You can solve this question now if you remember basic facts about trdeg.

Example Sheet 3. In all exercises, k is a field and R is a ring (commutative and unital).

(1) Nakayama:

(a) Let $(R, \mathfrak{m})$ be a local ring, M a finitely generated R-module, and take $x_1, \ldots, x_n \in M$ whose images in $M/\mathfrak{m}M$ span $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space. Prove that $x_1, \cdots, x_n$ generate M as an R-module.

(b) Let $(R, \mathfrak{m})$ be a noetherian local ring. Prove that $a_1, \ldots, a_n \in \mathfrak{m}$ generate the ideal $\mathfrak{m} \Leftrightarrow a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2$ span $\mathfrak{m}/\mathfrak{m}^2$ as an $R/\mathfrak{m}$-vector space. Prove that $\mathfrak{m}$ can be generated by $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ elements of R, but not by fewer elements of R.

(c) Let p be a prime number. Find a module M over $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b \right\}$ such that $\big((p)\mathbb{Z}_{(p)}\big)M = M$ but $M \neq 0$. Why does that not contradict Nakayama's lemma?

(d) For finitely generated modules M, N over a local ring $(A, \mathfrak{m})$, show that if $M \otimes_A N = 0$ then $M = 0$ or $N = 0$.
Hint: First solve the case where A is a field. Then tensor with $A/\mathfrak{m}$ and use Nakayama.

(e) Let $\varphi \colon M \to M$ an endomorphism of a finitely generated A-module M. Prove: φ is surjective $\Rightarrow$ φ is injective, but the reverse implication $\Leftarrow$ does not always hold. For the $\Rightarrow$ implication, show that the assumption that M is finitely generated is necessary.
Hint: To prove $(\Rightarrow)$, make M into an $A[T]$-module by letting T act as φ.

(f) Deduce that every generating set of cardinality n for the R-module R^n is a basis (R a nonzero ring).

(g) Prove that if R^n embeds in R^m as an R-module, R a nonzero ring, then $n \leq m$.
Hint: If $n > m$, consider the map $R^m \to R^n$ sending $(x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_m, 0, \ldots, 0)$, and find a way to use Cayley–Hamilton.

(2) **[remember the statement, but solve this problem only once done with everything else]** Let M be an R-module and consider

an exact sequence of R-modules $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ where C is flat. Prove that $0 \longrightarrow A \otimes M \overset{f\otimes \mathrm{id}_M}{\longrightarrow} B \otimes M \overset{g\otimes \mathrm{id}_M}{\longrightarrow} C \otimes M \longrightarrow 0$ is exact.

Hint: We have a short exact sequence $0 \to K \to F \to M \to 0$ where F is a free R-module (why?). We have a commutative diagram:

$$\begin{tikzcd}
A \otimes K \arrow[r] \arrow[d] & B \otimes K \arrow[r] \arrow[d] & C \otimes K \arrow[d] \\
A \otimes F \arrow[r] \arrow[d] & B \otimes F \arrow[r] \arrow[d] & C \otimes F \arrow[d] \\
A \otimes M \arrow[r] & B \otimes M \arrow[r] & C \otimes M
\end{tikzcd}$$

You can add some 0's to the diagram (on the left/right/top/bottom) such that all horizontal and all vertical sequences are exact (do that and explain). Now chase the diagram to show that $A \otimes M \to B \otimes M$ is injective (why is that enough?).

(3) Let $R = \prod_{i\in I} F_i$, where each F_i is a field (I not necessarily finite). Prove that $R_{\mathfrak{p}}$ is a field for every $\mathfrak{p} \in \operatorname{spec} R$. Deduce that "noetherian" is not a local property of rings (compare this to the result proved in Example Class 2).
Hint: Prove that $\operatorname{spec} R = \operatorname{mspec} R$ by showing that for every $r \in R$ there is $s \in R$ such that $r = r^2 s$. Note also that $\underbrace{\operatorname{nil} R}_{=\sqrt{(0)}} = (0)$.

(4) Let $A \subset B \subset C$ be rings such that (i) A is noetherian, (ii) C is finitely generated as an A-algebra, (iii) C is finite over B. Prove that B is finitely generated as an A-algebra.

(5) Let I be an ideal of a finitely generated k-algebra A. Prove that $\sqrt{I}$ is equal to the intersection of all maximal ideals containing I.
Hint: Use the strong Nullstellensatz.

(6) Radicals:
(a) Let I and J be ideals of R. Prove that $\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}$, that $\sqrt{I^n} = \sqrt{I}$ for all $n \geq 1$, and that $\sqrt{I}$ is a proper ideal of R whenerver I is a proper ideal of R.

(b) Let I and J be ideals of R. Prove that that the following conditions are equivalent.
   (i) I and J are coprime (i.e. $I + J = R$).
   (ii) I^n and J^n are coprime for all $n \geq 1$.
   (iii) I^n and J^n are coprime for at least one $n \geq 1$.
   (iv) $\sqrt{I}$ and $\sqrt{J}$ are coprime.

(c) Let k be an algebraically closed field, and let X, Y be algebraic subsets of k^n. Consider the equalities:
   (i) $I(X \cup Y) \overset{?}{=} I(X) \cap I(Y)$
   (ii) $I(X \cap Y) \overset{?}{=} I(X) + I(Y)$

   One of them is always true. For the other to be true you need to add $\sqrt{\cdot}$ over one of its sides. Do that, then prove both, then show that taking $\sqrt{\cdot}$ is necessary.

(7) Let A be an integral domain. Prove that the following conditions are equivalent:
   (a) A is integrally closed.
   (b) $A_\mathfrak{p}$ is integrally closed for all $\mathfrak{p} \in \operatorname{spec} A$.
   (c) $A_\mathfrak{m}$ is integrally closed for all $\mathfrak{m} \in \operatorname{mspec} A$.

   Hint: Use a local property from the lectures. Use a claim about localizations and integral closures from the lectures.

(8) Let $n \geq 1$. Write $V_\mathbb{C}(\cdot)$ for $V(\cdot)$, as in the lectures, with $k = \mathbb{Q}$ and $\Omega = \mathbb{C}$. Let I and J be ideals of $\mathbb{Z}[T_1, \ldots, T_n]$ such that $\underbrace{V(I)}_{\subset \mathbb{C}^n} \subset \underbrace{V(J)}_{\subset \mathbb{C}^n}$.
   For a prime number p, write I_p and J_p for the images of I and J (respectively) in $\mathbb{F}_p[T_1, \ldots, T_n]$ (i.e. reduce each coefficient of each polynomial mod p). Prove that $V_{\overline{\mathbb{F}}_p}(I_p) \subset V_{\overline{\mathbb{F}}_p}(J_p)$ for all but finitely many prime numbers p (here $V_{\overline{\mathbb{F}}_p}(\cdot)$ is $V(\cdot)$ as in the lectures with $k = \mathbb{F}_p$ and $\Omega = \overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$).

(9) Primary decomposition: An ideal $\mathfrak{q}$ of a ring A is *primary* if $\mathfrak{q} \neq A$ and all zero divisors in $A/\mathfrak{q}$ are nilpotent.
   Short in time? That's fine. Solve (a), (b), (c), (f). Read the statements of all of the parts of this question. Remember the statements of (g), (j), (k). Better also prove the first assertion in (k) about a finite intersection of irreducible ideals.

(a) Prove that if $\mathfrak{q}$ is primary then $\sqrt{\mathfrak{q}}$ is the smallest prime ideal containing $\mathfrak{q}$ (in this case we say that $\mathfrak{q}$ is $\mathfrak{p}$-primary, $\mathfrak{p} = \sqrt{\mathfrak{q}}$).

(b) Prove that if $\sqrt{\mathfrak{q}}$ is maximal for an ideal $\mathfrak{q}$ of A then $\mathfrak{q}$ is primary (and thus $\mathfrak{m}$-primary for $\mathfrak{m} = \sqrt{\mathfrak{q}}$). Deduce that every power of a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary.

(c) Let $\varphi\colon A \to B$ be a ring homomorphism, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of B, $\mathfrak{p} \in \operatorname{spec} B$. Prove that $\mathfrak{q}$ contracts to a $\mathfrak{p}^c$-primary ideal of A.

(d) Let $\mathfrak{q}$ and $\mathfrak{p}$ be ideals of A such that $\mathfrak{q} \subset \mathfrak{p} \subset \sqrt{\mathfrak{q}}$ and ($ab \in \mathfrak{q} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{q}$). Prove that $\mathfrak{p}$ is prime and $\mathfrak{q}$ is $\mathfrak{p}$-primary.

(e) Prove that a finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary ($\mathfrak{p} \in \operatorname{spec} A$).
Hint: Use (d).

(f) A *minimal prime ideal* of an ideal $\mathfrak{a}$ of A is an ideal $\mathfrak{p}$ of A corresponding to a minimal prime ideal of $A/\mathfrak{a}$.
A *primary decomposition* of an ideal $\mathfrak{a}$ of A is a finite set S of primary ideals whose intersection is $\mathfrak{a}$.
Such a decomposition is *minimal* if the ideals $\sqrt{\mathfrak{q}}$, $\mathfrak{q} \in S$ are distinct, and no element of S contains the the intersections of the others.
Prove that if $\mathfrak{a}$ admits a primary decomposition then it admits a minimal prime decomposition.

(g) Prove that if $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary, then the minimal prime ideals of $\mathfrak{a}$ are the minimal elements of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

(h) For an ideal $\mathfrak{a}$ of A and $x \in A$, let

$$(\mathfrak{a} : x) = \{a \in A \mid ax \in \mathfrak{a}\} .$$

Check that $(\mathfrak{a} : x)$ is an ideal of A, containing $\mathfrak{a}$, and equal to A if $x \in \mathfrak{a}$.

(i) Prove that if $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal and $x \in A \setminus \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary (while by (h), if $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = A$).

(j) Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Prove that

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \left\{\sqrt{(\mathfrak{a} : x)} \mid x \in A,\ \sqrt{(\mathfrak{a} : x)} \in \operatorname{spec} A\right\}$$

(in particular, the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ does not depend on the choice of minimal primary decomposition).

(k) An ideal $\mathfrak{a}$ is *irreducible* if it is not the intersection of two larger ideals.
Prove that in a noetherian ring, every ideal is a finite intersection of irreducible ideals, and every irreducible ideal is primary (and thus every ideal in a noetherian ring has a primary decomposition).

(10) Recall the notion of *trascendence degree* (the review below suffices). For a k-algebra A such that A is an integral domain, define $\operatorname{trdeg}_k A := \operatorname{trdeg}_k \operatorname{Frac} A$.

(a) Prove that $\dim A \leq \operatorname{trdeg}_k A$.
Hint: Argue by induction on $\operatorname{trdeg}_k A$. Use ES2.Q15(c): to compute $A_{\{x\}}$ (as in ES2.Q15), $x \in A$, separate to cases: (i) x algebraic over k, (ii) x transcendental over k.

(b) Deduce that $k[T_1, \ldots, T_n] = n$.

(11) Let R be a nonzero ring. Use Zorn's lemma to prove that R has a minimal prime ideal (i.e. a prime ideal not containing any other prime ideal). Deduce that every prime ideal of R contains a minimal prime ideal.

A review of transcendence bases. Let $k \subset L$ be fields. A subset A of L is a *transcedence basis* for L over k if it satisfies one (hence all) of the equivalent conditions in the following proposition:

Proposition 15.1. *The following conditions are equivalent:*

(1) *A is algebraically independent over k, and L is algebraic over $k(A)$.*
(2) *A is algebraically independent over k, but $A \cup \{\beta\}$ is not algebraically independent over k for any $\beta \in L$.*
(3) *L is algebraic over $k(A)$, but not over $k(A \setminus \{\alpha\})$ for any $\alpha \in A$.*

Proof. See any book on field theory. □

The following proposition implies that L has a transcendence basis over k (plug $A = \emptyset$ into (i)).

Proposition 15.2.

i) *If $A \subset L$ is algebraically independent over k, then there is a transcedence basis B for L over k such that $A \subset B$.*

ii) *All transcedence bases for L over k have the same cardinality.*

iii) *For fields $k \subset L \subset E$, if B and C are transcedence bases for L/k and E/L, respectively, then $B \cup C$ is a transcedence basis for E/k.*

The common cardinality of all trascendence bases for L over k (see Proposition 15.2(ii)) is called the *transcedence degree* of L over k, and is denoted $\operatorname{trdeg}_k L$. By Proposition 15.2(iii), $\operatorname{trdeg}_k E = \operatorname{trdeg}_k L + \operatorname{trdeg}_L E$.

Example Sheet 4. In all exercises, k is a field and R is a ring (commutative and unital).

(1)

(a) Prove that every minimal nonzero prime ideal $\mathfrak{p}$ of a UFD A is principal.

(b) Let A be a PID. Prove that $\dim A = 0$ (and then A is a field) or $\dim A = 1$ (and then A is not a field).

(2) Prove that $\operatorname{trdeg}_k k[T_1, \dots, T_n]/(f) = n - 1$ for every irreducible polynomial $f \in k[T_1, \dots, T_n]$.

(3) Let A be a finitely generated k-algebra and an integral domain.

(a) Let $\mathfrak{p}_r \supsetneq \cdots \supsetneq \mathfrak{p}_0$ be a non-refinable chain of prime ideals of A (i.e. $\mathfrak{p}_r$ is a maximal ideal, $\mathfrak{p}_0$ is a minimal prime ideal, and there is no prime ideal strictly between $\mathfrak{p}_i$ and $\mathfrak{p}_{i+1}$ for all $0 \leq i < r$). Prove that $r = \dim A$.
Hint: Use induction on $\dim A$, Noether normalization, Q1, Q2, the Incomparability and Going-down Theorems, Proposition 13.5 from the lecture notes, and maybe more.

(b) Prove that $\dim A/\mathfrak{p} + \operatorname{ht} \mathfrak{p} = \dim A$ for every $\mathfrak{p} \in \operatorname{spec} A$.

(4) Let $R = \mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, 2 \nmid b \right\}$ and $A = R[T]$. Prove: (i) the ideals $\mathfrak{m}_1 = (2T - 1)$ and $\mathfrak{m}_2 = (T, 2)$ of A are maximal, (ii) A is a noetherian integral domain, (iii) $\dim A/\mathfrak{m}_1 + \operatorname{ht} \mathfrak{m}_1 = 1$ and $\dim A/\mathfrak{m}_2 + \operatorname{ht} \mathfrak{m}_2 = 2$.

(5) Let A be a ring, $\dim A < \infty$. Prove that

$$\dim A + 1 \leq \dim A[T] \leq 1 + 2 \dim A$$

as follows:

(a) For $\mathfrak{p} \in \operatorname{spec} A$, show that $\mathfrak{p}[T]$ (the subset of $A[T]$ of polynomials with coefficient in $\mathfrak{p}$) and $(\mathfrak{p}, T)$ are prime ideals of $A[T]$, and deduce that $\dim A + 1 \leq \dim A[T]$.

(b) For $\mathfrak{p} \in \operatorname{spec} A$, show that the longest chain of prime ideals of $A[T]$ that contract to $\mathfrak{p}$ is of length 1, and deduce that $\dim A[T] \leq 1 + 2\dim A$.
Hint: Take such a chain of prime ideals, extend each of them to $S^{-1}(A[T]) \cong A_{\mathfrak{p}}[T]$, $S = A \setminus \mathfrak{p}$, and then to $A_{\mathfrak{p}}[T]/((\mathfrak{p}A_{\mathfrak{p}})[T])$.

(6) Let A be a noetherian ring, $\dim A < \infty$. Prove that $\dim A[T] = 1 + \dim A$, and deduce that $\dim k[T_1, \dots, T_n] = n$ for a field k.
Hint: One inequality was proved in Q5. For the other inequality, use Hilbert's basis theorem, Krull's height theorem and its converse (see below), and also Q5, Q5a, Q5b.

(7) **Converse to Krull's height theorem:** Let $\mathfrak{a}$ be a proper ideal of a noetherian ring A, $\operatorname{ht}\mathfrak{a} = r$. Prove that there are $a_1, \dots, a_r \in \mathfrak{a}$ such that $\operatorname{ht}(a_1, \dots, a_i) = i$ for each $0 \leq i \leq r$ (recall: $\operatorname{ht}\mathfrak{b} = \min_{\mathfrak{b}\subset\mathfrak{p}\in\operatorname{spec} A} \operatorname{ht}\mathfrak{p}$).

(8) **Dimension:**

(a) Let $\mathfrak{a}$ be an ideal of $k[T_1, \dots, T_n]$, k an algebraically closed field. We have seen that $\mathfrak{a}$ has finitely many minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$, and that $\sqrt{\mathfrak{a}} = \bigcap_i \mathfrak{p}_i$. Thus $V(\mathfrak{a}) = \bigcup_i V(\mathfrak{p}_i)$. We've seen that each $V(\mathfrak{p}_i)$ is an irreducible algebraic subset of $\mathbb{A}^n_k$. The $V(\mathfrak{p}_1), \dots, V(\mathfrak{p}_n)$ are the *irreducible components* of $V(\mathfrak{a})$. Prove that if $\mathfrak{a} = (f_1, \dots, f_r)$ then each irreducible component of $V(\mathfrak{a})$ is of dimension at least $n - r$ (where the dimension of an irreducible algebraic set X is the maximal length d of a chain $X = X_d \supsetneq \cdots \supsetneq X_0$ of irreducible algebraic sets).
Hint: This is a direct consequence of Krull's height theorem and Q3b.

(b) **Krull's principal ideal theorem:** Let $x \in A$, A a noetherian ring, x not a zero divisor. Prove that $\operatorname{ht}\mathfrak{p} = 1$ for every minimal prime ideal of (x) **Hint:** Use Krull's height theorem and ES2.Q10c.

(c) Prove that $\dim A \leq \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ for a noetherian local ring $(A, \mathfrak{m})$.

(9) Let R be a noetherian ring. Is it necessarily true that every descending chain of prime ideals of R stabilizes?

(10) Hilbert function of a polynomial algebra with a nonstandard grading:

(a) Consider $A = k[T_1, T_2]$, and let $\deg'(T_1^{e_1}T^{e_2}) = e_1 + 2e_2$. Let A_n, $n \geq 0$, be the subset of A consisting of all polynomials that are $\deg'$-homogeneous of degree n (i.e., k-linear combinations of monomials m with $\deg'(m) = n$). Prove that $A = \bigoplus_{n\geq 0} A_n$ is a graded ring.

(b) Prove that there is no polynomial f such that $f(n) = \dim_k A_n$ for all large enough n (compare this to our definition of the Hilbert polynomial, and check why it does not apply here).

(c) Write down the Poincare series $\sum_{n\geq 0}(\dim A_n) \cdot T^N$ of A (with our nonstandard grading) as a rational function.

(11) Let $A \neq 0$ be a finitely generated k-algebra (not necessarily an integral domain). Let t be the maximal cardinality of a k-algebraically independent subset of A. Prove that $t = \dim A$.

(12)

(a) Let $(A, \mathfrak{m})$ be an artinian local ring. Prove that $\operatorname{spec} A = \{\mathfrak{m}\}$ and $\operatorname{nil} A = \mathfrak{m}$.

(b) Let $(A, \mathfrak{m})$ be a noetherian local ring. Prove that exactly one of the following statements holds:

(i) A is not artinian and $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all $n \geq 0$.

(ii) A is artinian and $\mathfrak{m}^n = 0$ for some $n \geq 0$.

(c) Give an example of an artinian local ring that is not a field.

(d) **Every artinian ring is a finite product of artinian local rings:** Let A be an artinian ring. Recall (ES2), that $\operatorname{spec} A = \operatorname{mspec} A$ is a finite set $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$, and that $\mathfrak{m}_1^\ell \cdots \mathfrak{m}_n^\ell = 0$ for some $\ell \geq 1$. Prove that the natural map $\varphi\colon A \to A/\mathfrak{m}_1^\ell \times \cdots \times A/\mathfrak{m}_n^\ell$ is a ring homomorphism and that each $\left(A/\mathfrak{m}_i^\ell, \mathfrak{m}_i/\mathfrak{m}_i^\ell\right)$ is an artinian local ring.

(e) **[non-examinable]** Let A be a ring such that $A \cong \prod_{i=1}^{n} A_i$, where A_i is an artinian local ring. Prove that A is artinian. Write $\pi_i \colon A \to A_i$ for the natural projection. Prove that the ideal (0) of A has a unique primary decomposition $(0) = \bigcap_{i=1}^{n} \ker \pi_i$, and thus n and the rings $A_1, \dots, A_n$ are determined uniquely up to their order (and up to isomorphism).

(13) In the lectures we proved that if R is a noetherian ring then $\operatorname{ht} \mathfrak{p} < \infty$ for every $\mathfrak{p} \in \operatorname{spec} R$. Here we construct a noetherian ring R such that $\dim R = \infty$.
Let $A = k[T_1, T_2, \dots]$, k a field. Let $\mathfrak{p}_i = \left(T_{i^2}, \dots, T_{(i+1)^2-1}\right)$ for all $i \geq 1$, and let $S = R \setminus \bigcup_{i=1}^{\infty} \mathfrak{p}_i$.

(a) Prove that S is a multiplicative set.

(b) Prove that $S^{-1}\mathfrak{p}_i = 2i + 1$ for $i \geq 1$ ($S^{-1}\mathfrak{p}_i$ is the extenstion $\mathfrak{p}_i^e$ of the ideal $\mathfrak{p}_i$ with respect to the localization map $A \to S^{-1}A$). Conclude that $\dim S^{-1}A = \infty$.

(c) **[non-examinable]** Prove that the ring $S^{-1}A$ is noetherian. **Hint:** Use a claim from the lecture notes, proved in an example class, that gives a local condition for noetherianity of a ring (noetherianity is not a local property).

(14) A filtration $(M_n)_{n \geq 0}$ of an R-module M defines a topology on M given by the topological basis $\{x + M_n \mid x \in M, n \geq 0\}$. In particular, for an ideal $\mathfrak{a}$ of R, the $\mathfrak{a}$-*adic* topology on M is the topology corresponding to the filtration $(\mathfrak{a}^n M)_{n \geq 0}$.
Let R be a noetherian ring, $\mathfrak{a}$ an ideal of R, M a finitely generated R-module, and N a submodule of M. Prove that the topology on N induced from the $\mathfrak{a}$-adic topology on M is the same as the $\mathfrak{a}$-adic topology on N. **Hint:** This follows rather easily from two claims from the lectures.

(15)

(a) Let M be an R-module, and $\mathfrak{a}$ an ideal of R. Consider the $\mathfrak{a}$-adic completion map $\phi \colon M \to \varprojlim M/\mathfrak{a}^n M$. Note that $\ker \phi = \bigcap_{n \geq 0} \mathfrak{a}^n M$.

(b) Assume that R is noetherian and local, M is finitely generated over R, and $\mathfrak{a}$ is a proper ideal of R. Prove that ϕ is injective. **Note:** This is true also if R is a noetherian integral domain (not necessarily local).

(16) Let $A = \bigoplus_{n\geq 0} A_n$ be a noetherian graded ring with A_0 artinian. Let $0 \neq M = \bigoplus_{n\geq 0} M_n$ be a finitely generated graded A-module. Take $k \geq 0$ and $x \in A_k$ such that $\{m \in M \mid xm = 0\} = \{0\}$. Prove that $d(M/xM) = d(M) - 1$ (here we think of M/xM as a graded A-module in the natural way).
Hint: Review the proof of the Hilbert–Serre Theorem.

(17) Dedekind domains:
  (a) Complete the proofs skipped in the last lecture (see the notes if needed):
    (i) Let $(A, \mathfrak{m})$ be a noetherian local domain of dimension 1. Prove the following implications: $\mathfrak{m}$ is a principal ideal $\Rightarrow$ Every nonzero ideal of A is a power of $\mathfrak{m}$ $\Rightarrow$ There is $\pi \in A$ such that every nonzero ideal of A is equal to (π^n) for some $n \geq 0$ $\Rightarrow$ A is a DVR.
    (ii) Consider the localization map $R \to S^{-1}R$ for some multiplicative subset S of a ring R. Take $\mathfrak{p} \in \operatorname{spec} R$ such that $\mathfrak{p} \cap S = \emptyset$, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of R. Prove that $\mathfrak{q}$ is contracted from $S^{-1}R$.
    (iii) Let A be a Dedekind domain and $(0) \neq \mathfrak{p} \in \operatorname{spec} A$. Prove that the set of $\mathfrak{p}$-primary ideals of A is $\{\mathfrak{p}^n\}_{n\geq 1}$, and that $(\mathfrak{p}^n)_{n\geq 1}$ is a strictly descending sequence.
  (b) Prove or disprove each of the following statements:
    (i) If v_1 and v_2 are discrete valuations on fields K_1 and K_2 (respectively) such that the valuation rings of v_1 and v_2 are isomorphic rings, then the fields K_1 and K_2 are isomorphic.
    (ii) If v_1 and v_2 are discrete valuations on a field K such that the valuation rings of v_1 and v_2 are equal then $v_1 = v_2$.
  (c) Let $\mathfrak{a}$ be a nonzero ideal of a Dedekind domain A, and let $0 \neq \mathfrak{p} \in \operatorname{spec} A$. What information about the decomposition of $\mathfrak{a}$ as a product of powers of prime ideals of A can be extracted from the ideal $\mathfrak{a}A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$?