B2.2: COMMUTATIVE ALGEBRA

KONSTANTIN ARDAKOV

All rings in this course will be assumed commutative and containing an identity element. For a ring R we denote by $R[t_1, \dots, t_n]$ the polynomial ring in indeterminates t_i with coefficients in R.

1. Introduction

Examples 1.1. *We begin by listing a number of examples of commutative rings, arising from disparate parts of pure mathematics.*

(0) Every field F is a ring.

(1) Let X be a set and F a field.

- *(a) Fun$(X, F) := \{f : X \to F\}$ is a ring under pointwise addition and multiplication of functions.*
- *(b) If X is a topological space and we endow F with the discrete topology, Cont$(X, F) := \{f : X \to F, f$ is continuous$\}$ is a subring of Fun(X, F).*
- *(c) If $F = \mathbb{R}$ or $\mathbb{C}$ and X is a manifold over F, then Sm$(X, F) := \{f : X \to F : f$ is smooth$\}$ is a subring of Fun(X, F).*

(2) (a) $\mathbb{Z} \subset \mathbb{Q}$, (b) $\mathbb{Z}[i] \subset \mathbb{Q}[i]$, (c) $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\omega] \subset \mathbb{Q}(\sqrt{-3})$ where $\omega := \frac{-1+\sqrt{-3}}{2}$, and more generally, (d) $\mathcal{O}_K \subset K$ for a finite field extension K of $\mathbb{Q}$, where

$$\mathcal{O}_K := \{\alpha \in K : \quad \exists \quad \textit{monic} \quad f(X) \in \mathbb{Z}[X] \quad \textit{such that} \quad f(\alpha) = 0\}$$

is the ring of integers *of K.*

(3) Let F be a field.

- *(a) The rings of polynomials*

$$F \subset F[t_1] \subset F[t_1, t_2] \subset \cdots \subset F[t_1, \dots, t_n].$$

- *(b) finitely generated F-algebras; these are the same things as quotients of polynomial rings $F[t_1, \dots, t_n]$ by an ideal.*

Date: Hilary term, 2020. These notes are an edited version of lecture notes by Nik Nikolov and Dan Segal.

Examples (1) come from *Topology and Analysis*; examples (2) come from *Algebraic Number Theory*, and examples (3) come from *Algebraic Geometry.*

The main object of study of *(Affine) Algebraic geometry* are the *affine algebraic varieties* (which we will call *algebraic sets* in this course).

Let F be a field, $n \in \mathbb{N}$ and let $R := F[t_1, \ldots, t_n]$ be the polynomial ring in n variables t_i, and let F^n denote the n-dimensional vector space of row vectors.

Definition 1.2.

(a) Let $S \subseteq R$ be a collection of polynomials from R. Define

$$\mathcal{V}(S) := \{\mathbf{x} = (x_i) \in F^n \mid f(\mathbf{x}) = 0 \ \forall f \in S\}.$$

(b) A set $U \subseteq F^n$ is an algebraic set *if $U = \mathcal{V}(S)$ for some $S \subseteq R$ (equivalently $U = \mathcal{V}(I)$ for some ideal I of R).*

Thus $\mathcal{V}(S)$ is just the subset in F^n of common zeroes for all polynomials in S (it may happen of course that this is the empty set). It is easy to see that $\mathcal{V}(S) = \mathcal{V}(I)$ where $I = \langle S \rangle$ is the ideal generated by S in R. Here are some examples:

- Every singleton point $\{\mathbf{a}\} \subset F^n$ is algebraic, because

$$\{\mathbf{a}\} = \{\mathbf{x} \in F^n : x_1 = a_1, \ldots, x_n = a_n\} = \mathcal{V}(\{t_1 - a_1, \ldots, t_n - a_n\}).$$

- If $f(x, y) = y^2 - x^3 + x$ then $\mathcal{V}(\{f\}) = \{(a, b) \in F^2 : b^2 = a^3 - a\}$ is an example of an *algebraic curve.*

We may consider an opposite operation associating an ideal to each subset of F^n.

Definition 1.3. *Let $Z \subseteq F^n$ be any subset. Define*

$$\mathcal{I}(Z) := \{f(t_1, \ldots, t_n) \in R \mid f(\mathbf{x}) = 0 \ \forall \mathbf{x} \in Z\}.$$

Thus $\mathcal{I}(Z)$ is the set of polynomials which vanish on all of Z. It is clear that $\mathcal{I}(Z)$ is an ideal of R.

Proposition 1.4. *Let $I \subseteq I' \subseteq R$ be ideals and $Z \subseteq Z' \subseteq F^n$ subsets.*

(1) $\mathcal{V}(I') \subseteq \mathcal{V}(I)$,
(2) $\mathcal{I}(Z') \subseteq \mathcal{I}(Z)$.
(3) $I \subseteq \mathcal{I}(\mathcal{V}(I))$,
(4) $Z \subseteq \mathcal{V}(\mathcal{I}(Z))$, moreover there is equality if Z is an algebraic set.

Proof. Exercise. □

Proposition 1.4 shows that $\mathcal{I}$ and $\mathcal{V}$ are *order reversing* maps between the set of ideals of R and the algebraic subsets of F^n:

$$\left\{\begin{array}{c} \textit{algebraic subsets} \\ Z \subset F^n \end{array}\right\} \begin{array}{c} \xrightarrow{\mathcal{I}} \\ \xleftarrow{\mathcal{V}} \end{array} \left\{\begin{array}{c} \textit{ideals} \\ I \subset F[t_1, \ldots, t_n] \end{array}\right\}.$$

Moreover, $\mathcal{V}$ is surjective because $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$, whereas Proposition 1.4(4) shows $\mathcal{I}$ is injective. Understanding the relationship between an algebraic set Z and the ideal $\mathcal{I}(Z)$ is the beginning of algebraic geometry which we will address in Section 4.

In *C2.6 Scheme Theory* you will see how appropriate generalisations of the constructions in Example 1.1(1) gives meaning to the slogan

every commutative ring is a ring of functions on some topological space.

The Theory of Schemes, underpinned by the solid foundation of Commutative Algebra, allows geometric intuition and techniques to be applied to Algebraic Number Theory, leading to deep results such as Wiles' proof of Fermat's Last Theorem.

The aim of this course is to study basic structural properties of the class of *Noetherian rings* which are commonly found in Algebraic Geometry and Algebraic Number Theory: the rings appearing in Examples 1.1(2) and (3) all satisfy the *Noetherian condition*.

2. Noetherian rings and modules

Let R be a ring and let M be an R-module. Recall that M is said to be *finitely generated* if there exist elements $m_1, \ldots, m_k \in M$ such that $M = \sum_{i=1}^{k} Rm_i$.

Lemma 2.1. *The following three conditions on M are equivalent.*

(a) Any submodule of M is finitely generated.

(b) Any nonempty set of submodules of M has a maximal element under inclusion.

(c) Any ascending chain of submodules $N_1 \leq N_2 \leq N_3 \leq \cdots$ eventually becomes stationary.

Proof. (c) implies (b) is easy.

(b) implies (a): Let N be a submodule of M and let X be the collection of finitely generated submodules of N. X contains $\{0\}$ and so by (b) there is a maximal element $N_0 \in X$. We claim that $N_0 = N$. Otheriwise there is some $x \in N \backslash N_0$ and then $N_0 + Rx$ is a finitely generated submodule of N which is larger than N, contradiction. So $N_0 = N$ is finitely generated.

(a) implies (c): Let $N_1 \leq N_2 \leq \cdots$ be an ascending chain of submodules and let $N := \cup_{i=1}^{\infty} N_i$. Then N is a submodule of M which is finitely generated by (a). Suppose N is generated by elements $x_1, \ldots, x_n$. For each x_i there is some N_{k_i} such that $x_i \in N_{k_i}$. Take $k = \max_i\{k_i\}$. We see that all $x_i \in N_k$ and so $N = N_k$. Therefore the chain becomes stationary at N_k. □

Definition 2.2. *An R-module M is said to be* Noetherian *if it satisfies any of the three equivalent conditions of Lemma 2.1.*

Proposition 2.3. *Let $N \leq M$ be two R-modules. Then M is Noetherian if and only if both N and M/N are Noetherian.*

Proof. Problem sheet 1, Q4. □

As a consequence we see that $M^n := M \oplus M \oplus \cdots \oplus M$ is Noetherian for any Noetherian module M.

Definition 2.4. *A ring R is* Noetherian *if R is a Noetherian R-module.*

Examples of Noetherian rings are fields, $\mathbb{Z}$, PIDs and (as we shall see momentarily) polynomial rings over fields. An example of a ring which is not Noetherian is the polynomial ring of infinitely many indeterminates $\mathbb{Z}[t_1, t_2, \ldots]$.

Proposition 2.5. *A homomorphic image of a Noetherian ring is Noetherian.*

Proof. Let $f : A \to B$ be a surjective ring homomorphism with A Noetherian. Then $B \simeq A/\ker f$ and the ideals of B are in $1-1$ correspondence with the ideals of A containing $\ker f$. Now A satisfies the ascending chain condition on its ideals and therefore so does $A/\ker f \simeq B$.

Proposition 2.6. *Let R be a Noetherian ring. Then an R-module M is Noetherian if and only if M is finitely generated as an R-module.*

Proof. If M is Noetherian then M is finitely generated as a module. Conversely, suppose that $M = \sum_{i=1}^{k} Rm_i$ for some $m_i \in M$. Then M is a homomorphic image of the free R-module R^k with basis: Define the module homomorphism $f : R^k \to M$ by $f(r_1, \ldots, r_k) := \sum_i r_i m_i$. Since R and R^k are Noetherian modules so is $M \simeq R^k/\ker f$. □

The main result of this section is

Theorem 2.7 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then the polynomial ring $R[t]$ is Noetherian.*

Proof of Theorem 2.7. It is enough to show that any ideal I of $R[t]$ is finitely generated. If $I = \{0\}$ this is clear. Suppose I is not zero. Let M be the set of all leading coefficients of all non-zero [1] polynomials in I, union $\{0\}$; one can check directly that M is an ideal of R. Because R is Noetherian, M must be finitely generated, so there are some polynomials $p_1, \dots, p_k \in I$ such that p_i has leading coefficient c_i and $M = Rc_1 + Rc_2 + \cdots + Rc_k$. Let $N = \max\{\deg p_i \mid 1 \leq i \leq k\}$ and let $K = I \cap \left(R \oplus Rt \oplus \cdots \oplus Rt^N\right)$. Note that K is an R-submodule of an R-module isomorphic to R^{N+1}, so by Proposition 2.3, K is finitely generated as an R-module, say by elements $a_1, \dots, a_s \in K \subset I$. Let J be the ideal of $R[t]$ generated by $a_1, \dots, a_s, p_1, \dots, p_k$. We claim that $J = I$. Clearly $J \leq I$ and it remains to prove $I \leq J$. Let $f \in I$ and argue by induction on $\deg f$ that $f \in J$. If $\deg f \leq N$ then $f \in K = \sum_i Ra_i$ and so $f \in J$. Suppose that $\deg f > N$. Let $a \in M$ be the leading coefficient of f. We have $a = \sum_j r_j c_j$ for some $r_j \in R$. Consider the polynomial $g := f - \sum_j r_j t^{\deg f - \deg p_j} p_j$ and note that $\deg g < \deg f$. Since $g \in I$ we can assume from the induction hypothesis that $g \in J$. Therefore $f \in J$. Hence $I = J$ is a finitely generated ideal of $R[t]$. Therefore $R[t]$ is a Noetherian ring. □

Corollary 2.8. *Let F be a field. Then every ideal of $F[t_1, \dots, t_n]$ has a finite generating set.*

Definition 2.9. *Let $A \leq B$ be two rings.*

(1) Given elements $b_1, \dots, b_k \in B$, $A[b_1, \dots, b_k]$ denotes the smallest subring of B containing A and all b_i.

(2) We say that B is finitely generated as an A-algebra*, or that B is* finitely generated as a ring over A *if there exist elements $b_1, \dots, b_k \in B$ such that $B = A[b_1, \dots, b_k]$.*

This is equivalent to the existence of a surjective ring homomorphism

$$f : A[t_1, \dots, t_k] \to B$$

which is the identity on A and $f(t_i) = b_i$ for each i.

[1] What should be the leading coefficient of the zero polynomial? What, indeed, is the degree of the zero polynomial?

Corollary 2.10. *Let R be a Noetherian ring and suppose $S \geq R$ is a ring which is finitely generated as R-algebra. Then S is a Noetherian ring.*

Proof. The above discussion shows that S is a homomorphic image of the polynomial ring $R[t_1, \ldots, t_k]$ and with Theorem 2.7 and induction on k we deduce that $R[t_1, \ldots, t_k]$ is a Noetherian ring. Therefore S is a Noetherian ring. □

This has the following central application to algebraic geometry.

Corollary 2.11. *Let $X \subseteq F[t_1, \ldots, t_k]$ be any subset. Then there is a finite subset $Y \subseteq X$ such that $\mathcal{V}(X) = \mathcal{V}(Y)$.*

Proof. Since $F[t_1, \ldots, t_k]$ is a Noetherian ring by Corollary 2.8, the set of ideals of R satisfies the ascending chain condition by Lemma 2.1. So $\langle X \rangle = \langle Y \rangle$ for some finite subset Y of X. We conclude that

$$\mathcal{V}(X) = \mathcal{V}(\langle X \rangle) = \mathcal{V}(\langle Y \rangle) = \mathcal{V}(Y). \qquad \square$$

So: every algebraic subset of F^n is a finite intersection of hypersurfaces.

3. The Nilradical

Definition 3.1. *A prime ideal P of a ring is said to be* minimal *if P does not contain another prime ideal $Q \subset P$.*

Theorem 3.2. *Let R be a Noetherian ring. Then R has finitely many minimal prime ideals and every prime ideal contains a minimal prime ideal.*

Proof. Let's say that an ideal I of R is *good* if $I \supseteq P_1 \cdots P_k$ for some prime ideals P_i, not necessarily distinct. We claim that all ideals of R are good. Otherwise let $\mathcal{S}$ be the set of bad ideals and since R is Noetherian, by Lemma 2.1 there is a maximal element of $\mathcal{S}$, call it J. Clearly J is not prime. So there exist elements x, y outside J such that $xy \in J$. Let $S = J + Rx, T = J + Ry$, we have $ST \subseteq J$ and both S and T are strictly larger than J and hence must be good ideals. Therefore $P_1 \cdots P_k \subseteq S, P'_1 \cdots P'_l \subseteq T$ for some prime ideals P_i, P'_i of R. But then $P_1 \cdots P_k P'_1 \cdots P'_l \subseteq TS \subseteq J$ and so J is good, contradiction. So all ideals of R are good and in particular $\{0\}$ is good and so $P_1 \cdots P_k = 0$ for some prime ideals P_i. Let Y be the set of minimal ideals from the set $\{P_1, \ldots, P_k\}$. We claim that Y is the set of all minimal prime ideals of R. Indeed if I is any prime ideal, then $P_1 \cdots P_k \subseteq I$ and so $P_i \subseteq I$ for some i, justifying our claim. This also proves the second statement of the theorem. □

Definition 3.3. *Let R be a ring.*

(a) Let I be an ideal of R. An ideal P of R is said to be a minimal prime over I *if P is prime, $I \subseteq P$, and whenever $I \subseteq Q \subseteq P$ with Q prime, we must have $Q = P$.*
(b) $\min(I)$ *denotes the set of all minimal primes over I.*
(c) $x \in R$ is nilpotent *if $x^n = 0$ for some $n \geq 1$.*
(d) The nilradical *of a ring R, denoted by* $\operatorname{nilrad}(R)$*, is the set of all nilpotent elements of R.*

It follows from Theorem 3.2 that if R is Noetherian then $\min(I)$ is finite for every ideal I of R. An easy exercise shows that $\operatorname{nilrad}(R)$ is always an ideal of R.

Proposition 3.4. *The nilradical of a Noetherian ring is nilpotent.*

Proof. Choose generators $x_1, \ldots, x_k$ for $I := nilrad(R)$. Let $x_i^{n_i} = 0$ for some integers $n_i \in \mathbb{N}$ and take $n = n_1 + \cdots + n_k$. Then

$$I^n = (Rx_1 + Rx_2 + \cdots + Rx_k)^n \subseteq \sum_{s_1+\cdots+s_k=n} Rx_1^{s_1} \cdots x_k^{s_k}$$

where the sum is over all tuples s_i subject to $\sum_{i=1}^k s_i = n$. We must have at least one j such that $s_j \geq n_j$ and then $x_j^{s_j} = 0$. Therefore the right hand side above is the zero ideal and so $I^n = 0$. □

In the absence of the Noetherian hypothesis on the ring, the nilradical might not be nilpotent: take any field F and consider the ideal generated by $t_1, t_2, \ldots$ in the ring $\bigcup_{k=1}^{\infty} F[t_1, \ldots, t_k]/\langle t_1, t_2^2, \ldots, t_k^k\rangle$.

There is another very useful characterization of the nilradical.

Theorem 3.5 (Krull's Theorem)**.** *For any ring R,* $\operatorname{nilrad}(R)$ *is the intersection of all prime ideals of R.*

The proof of this fact uses *Zorn's Lemma*. Recall that a *partial order* on a set X is a reflexive and transitive relation $\leq$ on X such that $a \leq b$ and $b \leq a$ implies $a = b$. If $\leq$ is a partial order on X, we call the pair $(X, \leq)$ a *partially ordered set*, or a *poset* for short. A *chain C* in a poset X is a subset $C \subseteq X$ which is *totally ordered*: for any $a, b \in C$ we have $a \leq b$ or $b \leq a$. If S is any subset of the poset X then an element $b \in X$ is an *upper bound* for S if $s \leq b$ holds for all $s \in S$. The following result is known as Zorn's Lemma. It is equivalent to the Axiom of Choice and also to the Well-ordering principle.

Lemma 3.6 (Zorn's Lemma)**.** *Let $(X, \leq)$ be a non-empty partially ordered set such that every chain of elements of X has an upper bound in X. Then X has a maximal element.*

A typical application of Zorn's lemma is the existence of maximal ideals in any non-zero unital ring R: recall that an ideal I of R is said to be *maximal* if I is proper ($I \neq R$) and if J is another ideal of R with $I \subseteq J \subseteq R$ then either $J = I$ or $J = R$. Let X be the set of all proper ideals of R, ordered by inclusion. Note that X is not empty since $\{0\} \in X$. If C is a chain in X we easily check that $\cup C \in X$ and so the condition of Lemma 3.6 is satisfied. Therefore X has maximal elements, i.e. maximal ideals.

Proof of Krull's Theorem. If x is nilpotent and P is a prime ideal then $x^n = 0 \in P$ for some n and so $x \in P$. So $\text{nilrad}(R) \subseteq J := \cap\{P \mid P \text{ prime ideal of } R\}$. For the converse suppose that x is not nilpotent. Let $S = \{x^n \mid n \geq 0\}$, then S is a multiplicatively closed subset of R avoiding 0. By Lemma 3.6, we can find an ideal P of R which is maximal subject to having $P \cap S = \emptyset$. By problem sheet 1 Q1, this ideal P is prime. So $x \notin J$. Thus $J \subseteq \text{nilrad}(R)$ and so $\text{nilrad}(R) = J$. □

Definition 3.7. *Let I be an ideal of R. The* radical of I *is*

$$\sqrt{I} := \text{rad}(I) := \{x \in R \mid x^n \in I, \textit{ for some } n \in \mathbb{N}\}.$$

So by definition $\text{rad}(I)/I = \text{nilrad}(R/I)$. Using Theorem 3.5 and Theorem 3.2, we obtain the following

Corollary 3.8. *Let I be an ideal of a ring R. Then*

(a) $\text{rad}(I) = \cap\{P \mid P$ *prime ideal of* R *with* $I \subseteq P\}$.
(b) If R is Noetherian and $\min(I) = \{P_1, \ldots, P_k\}$ *then*

$$\text{rad}(I) = P_1 \cap \cdots \cap P_k.$$

Connection with algebraic sets. Recall the definitions of the maps $\mathcal{V}$ and $\mathcal{I}$ from the Introduction. The following Proposition is an easy exercise.

Proposition 3.9. *Let I_j, $j = 1, 2, \ldots$ be ideals of the polynomial ring $R = F[t_1, \ldots, t_k]$. Then*

(1) $\mathcal{V}(\sum_j I_j) = \cap_j \mathcal{V}(I_j)$.
(2) $\mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1 I_2) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$.
(3) $\text{rad}(\mathcal{I}(Z)) = \mathcal{I}(Z)$ *for any subset* $Z \subseteq F^k$.

When studying algebraic sets it is natural first to express them as union of 'simpler' algebraic sets. For example the algebraic set $W = \mathcal{V}(t_1t_2)$ can be written as $W = L_1 \cup L_2$, a union of the two lines $L_i = \mathcal{V}(t_i), i = 1, 2$. This leads us to consider algebraic sets which cannot be decomposed further and we make the following definition.

Definition 3.10. *A non-empty algebraic set W is said to be* irreducible *if whenever $W = W_1 \cup W_2$ for some algebraic sets W_1, W_2 then $W_1 = W$ or $W_2 = W$.*

Proposition 3.11. *An algebraic set W is irreducible if and only if $\mathcal{I}(W)$ is a prime ideal.*

Proof. Suppose $\mathcal{I}(W)$ is a prime ideal and $W = W_1 \cup W_2$ with each $W_i \neq W$. Then by Proposition 1.4, $\mathcal{I}(W_i)$ is strictly larger than $\mathcal{I}(W)$ and we can find some $f_i \in \mathcal{I}(W_i) \backslash \mathcal{I}(W)$ for $i = 1, 2$. Then the polynomial f_1f_2 vanishes on both W_1 and W_2 hence it vanishes on W and so $f_1f_2 \in \mathcal{I}(W)$. Thus $\mathcal{I}(W)$ is not a prime ideal, contradiction. Therefore W must be irreducible.

We leave the converse as an exercise in Problem sheet 2. □

Theorem 3.12. *Every algebraic set is a union of finitely many irreducible algebraic sets.*

Proof. See Problem sheet 2. □

Lemma 3.13. *Let W be a non-empty algebraic set and suppose that $W = V_1 \cup \cdots \cup V_n$ where V_i are irreducible algebraic sets and n is minimal possible. Let $P_i := \mathcal{I}(V_i)$ for each $i = 1, \ldots, n$. Then*

$$\min(\mathcal{I}(W)) = \{P_1, \ldots, P_n\}.$$

Proof. Note that $V_i \not\subseteq V_j$ for any $i \neq j$ otherwise we may omit V_i from the union, and hence $P_i \not\subseteq P_j$ for any $i \neq j$. Now $\mathcal{I}(W) = \cap_{i=1}^n \mathcal{I}(V_i)$. If P is a prime ideal containing $\mathcal{I}(W)$ then P must contain at least one of the ideals $P_j := \mathcal{I}(V_i)$. It follows that $P_1, \ldots, P_n$ are precisely the minimal primes of the ideal $\mathcal{I}(W)$. □

In the setting of Lemma 3.13, it follows from Proposition 1.4 that the irreducible sets V_i in the minimal decomposition $W = V_1 \cup \cdots \cup V_n$ are determined *uniquely* by W, as one can recover the V_i from the ideal $\mathcal{I}(W)$ as the vanishing sets of the minimal primes above $\mathcal{I}(W)$.

Definition 3.14. *The V_i are called the* irreducible components *of the algebraic set W.*

It remains to determine the relationship between the algebraic set $W = \mathcal{V}(I)$ and the ideal $\mathcal{I}(W)$. This is the topic of the next section.

4. The Nullstellensatz

Theorem 4.1 (The Nullstellensatz)**.** *Let F be an algebraically closed field and let I be an ideal of the polynomial ring $R = F[t_1, \ldots, t_n]$. Then*

$$\mathcal{I}(\mathcal{V}(I)) = \mathrm{rad}(I).$$

Proof. Let $W = \mathcal{V}(I)$. Let $f \in \mathrm{rad}(I)$; then $f^n \in I$ for some $n \in \mathbb{N}$ and so f^n is zero on W. Hence f vanishes on W and so $f \in \mathcal{I}(\mathcal{V}(I))$. Conversely suppose $f \in \mathcal{I}(\mathcal{V}(I))$. We want to prove that $f \in \mathrm{rad}(I)$. If $f = 0$ this is clear, so assume $f \neq 0$. Consider the polynomial ring $S := R[z] = F[t_1, \ldots, t_k, z]$ where we have added an extra indeterminate variable z. Let J be the ideal of S generated by I together with the polynomial $zf - 1$. Observe that $\mathcal{V}(J) = \emptyset$: if the tuple $(\mathbf{a}, y) \in F^{k+1}$ (with $\mathbf{a} \in F^k$) belongs to $\mathcal{V}(J)$ then $\mathbf{a} \in W$ but then $f(\mathbf{a}) = 0$ so $(zf-1)(\mathbf{a}, y) = -1$ is not zero. Hence by Theorem 4.2 below, we must have $J = S$. Therefore there are polynomials $g, g_1, \ldots, g_m \in S$ and $f_1, \ldots f_m \in I$ such that

$$g(zf-1) + g_1 f_1 + \cdots + g_m f_m = 1$$

This is an identity of polynomials in variables $t_1, \ldots, t_k, z$. In particular it remains true when we substitute $z = 1/f$. Then g_i become polynomials in $t_1, \ldots, t_k$ and $1/f$. Bringing everything under a common denominator f^n we reach

$$\frac{g_1' f_1 + \cdots + g_m' f_m}{f^n} = 1$$

for some $g_i' \in R$. This implies $f^n = \sum_{i=1}^m g_i' f_i \in I$ since all $f_i \in I$. Thus $f \in \mathrm{rad}(I)$ and the Theorem is proved. □

Let I be an ideal of $R = F[t_1, \ldots, t_n]$ and let $\mathbf{a} \in F^n$. Then $\mathbf{a} \in V(I)$ if and only if $I \subseteq \mathcal{I}(\{a\})$, and $\mathcal{I}(\{a\})$ is a maximal ideal of R being the kernel of the F-algebra homomorphism $\mathrm{ev}_{\mathbf{a}} : R \to F$ given by $\mathrm{ev}_{\mathbf{a}}(f) = f(\mathbf{a})$. So, the points of the algebraic set $\mathcal{V}(I)$ correspond to certain maximal ideals of R which contain I, via $\mathbf{a} \mapsto \ker \mathrm{ev}_{\mathbf{a}}$. It would help if we had a better understanding of the set $\mathrm{Max}\, R$ of maximal ideals of R.

Theorem 4.2. *Let I be a proper ideal of R. Then $\mathcal{V}(I)$ is non-empty.*

Proof. By Corollary 2.10 and Lemma 2.1, there is a maximal ideal $M \in \operatorname{Max} R$ such that $I \subseteq M$. Because F is algebraically closed, Theorem 4.3 below implies that $M = \langle t_1 - a_1, \dots, t_n - a_n \rangle$ for some $\mathbf{a} \in F^k$. Hence $\mathbf{a} \in \mathcal{V}(I)$. □

Define a function $\mu : F^n \to \operatorname{Max}(R)$ by

$$\mu(a_1, \dots, a_n) := \sum_{i=1}^{n} R(t_i - a_i) = \langle t_1 - a_1, \dots, t_n - a_n \rangle.$$

It is easy to check the following:

- $\mu(\mathbf{a}) = \mathcal{I}(\{\mathbf{a}\}) = \ker \mathrm{ev}_{\mathbf{a}}$,
- $\mu(\mathbf{a}) \in \operatorname{Max}(R)$,
- the map μ is injective.

Theorem 4.3. *Assume that the field F is algebraically closed. Then $\mu : F^n \to \operatorname{Max} R$ is bijective.*

Proof. It remains to show that μ is surjective. Let M be a maximal ideal of R. By Theorem 4.4 below, R/M is a finite field extension of F, and since F is algebraically closed, it follows that $R/M \simeq F$ and so $\dim_F R/M = 1$. This implies $M + F = R$. In particular for each t_i there exists $a_i \in F$ such that $t_i - a_i \in M$. Then $\mu(a_1, \dots, a_n) \subseteq M$ and hence $M = \mu(a_1, \dots, a_n)$. □

Let $F \subseteq E$ be two fields. By $[E : F]$ we denote $\dim_F E$, the dimension of E as a vector space over F and we say that that the extension E/F is *finite* if $[E : F]$ is finite.

Theorem 4.4 (weak Nullstellensatz)**.** *Let $F \subseteq E$ be two fields such that E is finitely generated as an algebra over F. Then E/F is a finite extension.*

Proof. Suppose $E = F[x_1, \dots, x_n]$ and argue by induction on n. The case $n = 0$ is vacuous. Assuming the result is true for $n - 1$ consider the sequence of fields $F \subseteq F' \subseteq E$ where $F' := F(x_1)$ is the smallest subfield of E containing F and x. We have that E is finitely generated as F'-algebra by $n-1$ elements and hence by the induction hypothesis E/F' is finite. So E is finitely generated as F'-module and by Theorem 4.5 below, F' is finitely generated as F-algebra. Now Proposition 4.6 below gives that F'/F is finite and therefore we can apply the Tower Law to deduce $[E : F] = [E : F'][F' : F]$ is finite. □

We have now proved the Nullstellensatz, Theorem 4.1, modulo the following two statements.

Theorem 4.5 (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be three rings with A Noetherian. Suppose that C is finitely generated as an A-algebra and also that C is finitely generated as a B-module. Then B is finitely generated as A-algebra.*

The following is mostly part A material.

Proposition 4.6. *Let E/F be a field extension such that $E = F(x)$ for some element $x \in E$. The following are equivalent:*

(a) x is algebraic over F.
(b) E is generated by x as an F-algebra.
(c) E/F is a finite extension.
(d) E is finitely generated as an F-algebra.

Proof of Theorem 4.5. Suppose that $C = \sum_{i=1}^n By_i$ for some $y_i \in C$. Let $x_1, \ldots, x_m$ generate C as A-algebra. We have

$$x_i = \sum_{j=1}^{n} b_{ij} y_j \quad (1 \leq i \leq m)$$

$$y_j y_k = \sum_{l=1}^{n} b_{jkl} y_l \quad (1 \leq j, k \leq n)$$

for some $b_{ij}, b_{jkl} \in B$. Let B_0 be the subring of B generated by A and all the elements b_{ij}, b_{jkl}. Then B_0 is finitely generated as A-algebra and hence by Corollary 2.10, B_0 is a Noetherian ring. We have $A \subseteq B_0 \subseteq B \subseteq C$. Let $M = B_0 + \sum_{i=1}^n B_0 y_i$. By the definition of B_0 it follows that $A \subseteq M$ and $x_i M \subseteq M$ for all $i = 1, \ldots, m$. Therefore $cM \subseteq M$ for all $c \in C$ and since $1 \in M$ we have $C = M$. So C is finitely generated as B_0-module and in particular C is a Noetherian B_0-module. Its B_0-submodule B is therefore finitely generated. In particular there are elements $z_1, \ldots, z_r \in B$ such that $B = \sum_{s=1}^r B_0 z_i$. Then the set of all b_{ij}, b_{jkl}, z_s for all possible i, j, k, l, s generates B as an A-algebra. □

Proof of Lemma 4.6. (a) ⇒ (b) ⇒ (c) is Part A material.

(d) ⇒ (a). Suppose for a contradiction that x is not algebraic but transcendental over F. Then $E = F(x)$ is the field of rational functions in the variable x. Suppose E is generated as F-algebra by the elements $g_i = p_i/q_i$, $i = 1, \ldots, k$ where $p_i, q_i \in F[x]$ are polynomials in x. Let $r = \prod_{i=1}^k q_i$ and consider the element $a = 1/(xr + 1) \in E$. Then

$$a = f(g_1, \ldots, g_k)$$

for some polynomial $f \in F[t_1, \ldots, t_k]$. By multiplying by an appropriate power of r to clear the denominators on the right hand side, we reach the equation $a = s/r^n$ for some $n \in \mathbb{N}$ and polynomial $s \in F[x]$. Thus $r^n = s(xr+1)$. Since $xr+1$ is coprime to r^n, by Bezout's Lemma we can find $\alpha, \beta \in F[x]$ such that $\alpha(xr+1) + \beta r^n = 1$. Therefore $(\alpha + \beta s)(xr+1) = 1$, and $xr+1 \in F[x]$ is a unit. But no polynomial of degree ≥ 1 in $F[x]$ is a unit, so we have reached a contradiction. □

Corollary 4.7. *Let F and R be as in Theorem 4.1 and let I be an ideal of R. Then* $\operatorname{rad}(I)$ *is an intersection of maximal ideals of R.*

Proof. Let U be the intersection of all maximal ideals of R which contain I. Clearly $\operatorname{rad}(I) \subseteq U$, since $\operatorname{rad}(I)$ is the intersection of all prime ideals of R which contain I by Corollary 3.8(a).

Suppose now $f \notin \operatorname{rad}(I)$. By Theorem 4.1 we have $f \notin \mathcal{I}(\mathcal{V}(I))$ and so there is some $\mathbf{a} \in \mathcal{V}(I)$ such that $f(\mathbf{a}) \neq 0$ and in particular $f \notin \mu(\mathbf{a})$. On the other hand $I \subseteq \mu(\mathbf{a})$ and so $\mu(\mathbf{a})$ is a maximal ideal of R which contains I. So $f \notin U$. Thus $U \subseteq \operatorname{rad}(I)$ and so we have equality $U = \operatorname{rad}(I)$. □

Corollary 4.7 tells us that the polynomial algebras $F[t_1, \ldots, t_n]$ are special in the sense that they have lots of maximal ideals; enough for every prime ideal to arise as an intersection of maximal ideals above it.

Definition 4.8. *The ring R is said to be* local *if it has a unique maximal ideal.*

We will see many examples of local rings shortly, in §6. Corollary 4.7 also leads us to the following definitions.

Definition 4.9. *The* Jacobson radical *$J(R)$ of a ring R is defined to be the intersection of all maximal ideals of R.*

Clearly $\operatorname{nilrad}(R) \subseteq J(R)$.

Definition 4.10. *A ring R is said to be a* Jacobson ring *if* $J(R/I) = \operatorname{rad}(I)/I = \operatorname{nilrad}(R/I)$ *for each ideal I of R. Equivalently R is a Jacobson ring if each prime ideal of R is an intersection of maximal ideals.*

So in Corollary 4.7 we have proved that $F[t_1, \ldots, t_k]$ is a Jacobson ring whenever F is an algebraically closed field. In fact more is true: any finitely generated algebra over a field is a Jacobson ring. We will prove this later once we have developed a new tool: the notion of integral ring extensions. On the other hand, a local domain is *never* Jacobson, provided it is not a field.

5. Nakayama's lemma

Theorem 5.1. *[Cayley-Hamilton] Let R be a ring and let $A = (a_{ij}) \in M_n(R)$ be a square $n \times n$ matrix. Let $\chi_A(t) := \det(t\mathbf{I}_n - A)$ be the characteristic polynomial of A. Then $\chi_A(A) = 0$ inside $M_n(R)$.*

Proof. We begin by re-examining the case studied in Part A Linear Algebra where R is a field, F say, with the property that $\chi_A(t)$ splits completely over F. Write $\chi_A(t) = (t - \lambda_1) \cdots (t - \lambda_n)$ for some $\lambda_i \in F$. Let $V := F^n$ and let $T : V \to V$ be the F-linear map given by $T(\mathbf{v}) = A\mathbf{v}$. Since $\chi_A(t)$ splits completely over F, the matrix of T is upper triangular with respect to some basis $\{v_1, \ldots, v_n\}$ of V. Then

$$(T - \lambda_j 1)(v_j) \in Fv_1 + \cdots + Fv_{j-1} \quad \text{for all} \quad j = 1, \ldots, n$$

where $v_0 := 0$. An induction on $m \geq 1$ shows that

$$(T - \lambda_1 1) \cdots (T - \lambda_m 1)(v_j) = 0 \quad \text{for all} \quad j = 1, \ldots, m.$$

Taking $m = n$ shows that $\chi_A(T) = 0$ inside $\operatorname{End}_F(V)$. Since $\chi_A(A)$ is the matrix of $\chi_A(T)$ with respect to $\{v_1, \ldots, v_n\}$ we see that $\chi_A(A) = 0$ in this case.

Let $\varphi : R \to S$ be a ring homomorphism. It extends uniquely to ring homomorphisms $\varphi_1 : M_n(R) \to M_n(S)$, $\varphi_2 : R[t] \to S[t]$, and $\varphi_3 : M_n(R[t]) \to M_n(S[t])$. Then

$$\begin{aligned} \chi_{\varphi_1(A)}(t) &= \det(t\mathbf{I}_n - \varphi_1(A)) = \det(\varphi_3(t\mathbf{I}_n - A)) = \\ &= \varphi_2(\det(t\mathbf{I}_n - A)) = \varphi_2(\chi_A)(t) \end{aligned}$$

as elements in $S[t]$. Evaluate this at $\varphi_1(A) \in M_n(S)$ to obtain

$$\chi_{\varphi_1(A)}(\varphi_1(A)) = \varphi_2(\chi_A)(\varphi_1(A)) = \varphi_1(\chi_A(A)). \tag{1}$$

Now consider the case where R is an arbitrary integral domain, with field of fractions Q. Choose a splitting field F for $\chi_A(t) \in Q[t]$, and consider the *embedding* $j : R \hookrightarrow F$. Then applying (1), we have

$$j_1(\chi_A(A)) = \chi_{j_1(A)}(j_1(A)) = 0$$

by the first case. Since $j_1 : M_n(R) \to M_n(F)$ is still injective, we conclude that $\chi_A(A) = 0$ in $M_n(R)$.

Finally, consider the most general case. Let $U := \mathbb{Z}[x_{ij} : 1 \leq i, j \leq n]$ be the polynomial ring in n^2 variables, and let $X := (x_{ij}) \in M_n(U)$ be the *generic matrix.* There is a unique ring homomorphism $\varphi : U \to R$ such that $\varphi(x_{ij}) = a_{ij}$ for all i, j. Hence $\varphi_1(X) = A$. Now U is an integral domain, so $\chi_X(X) = 0$ by the above. Applying equation (1) again, we conclude that

$$\chi_A(A) = \chi_{\varphi_1(X)}(\varphi_1(X)) = \varphi_1(\chi_X(X)) = \varphi_1(0) = 0. \qquad \square$$

Theorem 5.2. *Let R be a ring and let M be a finitely generated R-module. Let I be an ideal of R and $\phi : M \to M$ be an endomorphism of M such that $\phi(M) \subseteq IM$. There exist $a_1, \dots, a_n \in I$ such that the module homomorphism*

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

as a map on M.

Proof of Theorem 5.2. Let $x_1, \dots, x_n \in M$ be generators of M. Let $V := R^n$ be the *free* R-module with basis $\{v_1, \dots, v_n\}$. There is a unique surjective R-module homomorphism $\pi : V \twoheadrightarrow M$ such that $\pi(v_i) = x_i$ for all $i = 1, \dots, n$. Since $\phi(M) \subseteq IM$ by assumption, we can find $c_{i,j} \in I$ such that $\phi(x_j) = \sum_{i=1}^n c_{ij}x_i$. Define an R-linear map $\psi : V \to V$ by $\psi(v_j) = \sum_{i=1}^n c_{ij}v_i$. Then ψ *lifts* ϕ in the sense that the diagram

$$\begin{tikzcd} V \arrow[r, "\pi"] \arrow[d, "\psi"'] & M \arrow[d, "\phi"] \\ V \arrow[r, "\pi"'] & M \end{tikzcd}$$

is commutative: $\phi \circ \pi = \pi \circ \psi$. It follows quickly that $p(\phi) \circ \pi = \pi \circ p(\psi)$ for all $p(t) \in R[t]$. Let $C = (c_{i,j}) \in M_n(R)$. By the Cayley-Hamilton Theorem 5.1, we have $\chi_C(C) = 0$, so $\chi_C(\psi) = 0$ in $\mathrm{End}_R(V)$. Hence $\chi_C(\phi) \circ \pi = 0$. Since $\pi : V \to V$ is surjective, we conclude that $\chi_C(\phi) = 0$ in $\mathrm{End}_R(M)$. Finally, note that $\chi_C(t) = t^n + a_1t^{n-1} + \cdots + a_n$ where $a_i \in I$, since a_i is a polynomial in the coefficients $c_{i,j}$ of C. . □

The gist of the formal argument above is that ϕ acts on M as ψ acts on V, and the same holds true for arbitrary polynomials in ϕ and ψ. Corollary 5.3 has an important special case (which is sometimes also stated as Nakayama's lemma).

Corollary 5.3. *[Nakayama's Lemma] Let M be a finitely generated R-module and let I be an ideal of M such that $M = IM$. Then there exists $x \in I$ such that $(1 + x)M = 0$.*

Proof. Take $\phi = \mathrm{Id}_M$ in Theorem 5.2. Then there exist $a_i \in I$ such that $(1 + a_1 + \cdots + a_n)M = 0$ and we can take $x = \sum_{i=1}^n a_i$. □

Corollary 5.4. *Let R be a ring and M be a finitely generated R-module such that $M = JM$, where $J = J(R)$ is the Jacobson radical of R. Then $M = \{0\}$.*

Proof. See Problem sheet 3. □

Corollary 5.5. *Let M be a finitely generated R-module and let $J = J(R)$. Let N be a submodule of M such that $M = N + JM$. Then $M = N$.*

Proof. Apply Corollary 5.4 to the module M/N. □

These results is particularly useful for local rings: the last corollary then implies that in order to generate a Noetherian module M over a local ring R with maximal ideal J, it is sufficient to generate the quotient M/JM. In turn M/JM is a vector space over the field R/J and the problem of generating M reduces to linear algebra in M/JM.

6. LOCALISATION

Now we describe a technique which often helps to simplify arguments and reduce them to the case of local rings.

Definition 6.1. *Let R be a ring.*

(1) Let $S \subseteq R$ be a subset. For each $s \in S$, let t_s be an indeterminate. Define the localisation of R at S *to be the ring*
$$R_S := \frac{R[t_s : s \in S]}{\langle s\, t_s - 1 : s \in S\rangle}.$$
(2) Let $\iota : R \to R_S$ be the canonical ring homomorphism.
(3) For each $r \in R, s \in S$, let r/s denote the image of rt_s in R_S.
(4) If $S = \{f\}$ for some $f \in R$ then we write $R_f := R_S$.

Thus, $1/s \in R_S$ is an inverse to $\iota(s)$ for all $s \in S$: we have formally adjoined the inverses of all elements of S. For this reason, we will sometimes write $S^{-1}R := R_S$.

Proposition 6.2 (Universal Property)**.** *Let $\varphi : R \to A$ be a ring homomorphism such that $\varphi(s) \in A^\times$ for all $s \in S$. Then there is a unique homomorphism $\psi : R_S \to A$ such that $\varphi = \psi \circ \iota$.*

We say that $S \subseteq R$ is *multiplicatively closed* if $st \in S$ whenever $s, t \in S$ and $1 \in S$.

Corollary 6.3. *Let $S \subseteq R$ and let T be the smallest multiplicatively closed subset of R containing S. Then $R_S \cong R_T$.*

Proof. Because R_S inverts T, by Proposition 6.2, there are ring homomorphisms $\psi : R_S \to R_T$ and $\theta : R_T \to R_S$ such that $\psi \circ \iota = \iota$ and $\theta \circ \iota = \iota$. Then $\theta \circ \psi \circ \iota = \theta \circ \iota = \iota$, so by the uniqueness, $\theta \circ \psi = 1_{R_S}$. Similarly $\psi \circ \theta = 1_{R_T}$. □

What do elements of R_S look like? In general, the map $\iota : R \to R_S$ is *not* injective.

Proposition 6.4. *Let $S \subset R$ be multiplicatively closed. Then*

(1) $R_S = \{r/s : r \in R, s \in S\}$, and
(2) $\ker \iota = \{r \in R :$ there is $t \in S$ such that $rt = 0\}$.

Proof. (1) By definition, R_S is generated as a ring by $\{1/s : s \in S\}$ and $\iota(R)$. But $a/s + b/t = (at + bs)/(st)$ and $a/s \cdot b/t = ab/st$, so as S is multiplicatively closed, every element of R_S is a fraction.

(2) Suppose $S = \{s^n : n \geq 0\}$, so that $R_S \cong R[t]/R[t](st - 1)$ by Corollary 6.3. If $\iota(r) = 0$ then $r = (a_0 + a_1 t + \cdots + a_n t^n)(st - 1)$ for some $a_i \in R$. Equating coefficients shows that $a_n s = 0, a_{n-1}s = a_n, \cdots, r = -a_0$. Hence $rs^{n+1} = 0$ where $s^{n+1} \in S$.

Now suppose that S is generated by $s_1, \ldots, s_m$ as a multiplicatively closed set, let $t = s_1 \cdot \cdots \cdot s_m$ and let $T = \{t^n : n \geq 0\} \subseteq S$. Then R_T inverts S so by Proposition 6.2 there's a ring map $\psi : R_S \to R_T$ such that $\psi \circ \iota = \iota$. But then if $\iota(r) = 0$ in R_S then also $\iota(r) = \psi(\iota(r)) = 0$ in R_T, so $t^n r = 0$ for some $n \geq 0$ by the first case.

In general, suppose $\iota(r) = 0$. Then there are finitely many $s_i \in S$ such that $r = \sum_{i=1}^m f_i(st_i - 1)$ where $t_i := t_{s_i}$. Setting any other variables appearing in f_i to be zero, we may assume without loss of generality that $f_i \in R[t_1, \ldots, t_m]$. Now apply the second case. □

Example 6.5. *Suppose R is a domain with field of fractions F and $S \subseteq R$ is multiplicatively closed. Then*

$$R_S \cong \{r/s \in Q : s \in S\}.$$

Proof. By Proposition 6.2, there is a map $\varphi : R_S \to Q$ such that $\varphi \circ \iota = \iota$. The image is $\{r/s \in Q : s \in S\}$ because S is multiplicatively closed. If $\varphi(r/s) = 0$ then $r = 0$ in Q but R injects into Q so $r = 0$ in R and hence $r/s = 0$ in R_S. □

What does localisation do to ideals?

Definition 6.6. *Let $\mathrm{Id}(A)$ denote the set of ideals of the ring A, and let $f : A \to B$ be a ring homomorphism.*

(1) Let $e : \mathrm{Id}(A) \to \mathrm{Id}(B)$ be defined by $e(I) := B \cdot I$. We call $e(I)$ the extended ideal.
(2) Let $c : \mathrm{Id}(B) \to \mathrm{Id}(A)$ be defined by $c(J) := f^{-1}(J)$. We call $c(J)$ the contracted ideal.

Note that if f is the inclusion of a subring A of B into B, then $c(J)$ is simply the ideal $J \cap A$ of A.

Lemma 6.7. *c sends $\operatorname{Spec}(B)$ to $\operatorname{Spec}(A)$.*

Proposition 6.8. *Let S be a multiplicatively closed subset of R.*

(1) The map $c : \operatorname{Id}(R_S) \to \operatorname{Id}(R)$ is injective.
(2) $I \in \operatorname{Id}(R)$ lies in the image of c if and only if it is S-closed: $rs \in I$ with $r \in R$ and $s \in S$ implies $r \in I$.
(3) c restricts to a bijection

$$c : \operatorname{Spec}(R_S) \quad \xrightarrow{\cong} \quad \{P \in \operatorname{Spec}(R) : P \cap S = \emptyset\}.$$

(4) c and e respect inclusions and intersections.
(5) e respects sums of ideals.

Proof. (1) If J is an ideal of R_S then $J = e(c(J))$: if $a/s \in J$ then $a \in c(J)$ and $a/s = (a/1) \cdot (1/s) \in e(c(J))$.

(2) Suppose $I = c(J)$ with $J \in \operatorname{Id}(R_S)$. If $rs \in I$ then $\iota(r)\iota(s) \in J$ so $\iota(r) \in J$ because $\iota(s) \in (R_S)^\times$. So $r \in I = \iota^{-1}(J)$ and I is S-closed. We will show that $I = c(e(I))$ whenever I is S-closed: if $r \in c(e(I))$ then $r/1 = a/s$ for some $s \in S$ and $a \in I$ so that $rs - a \in \ker \iota$. Hence $rst = at \in I$ for some $t \in S$ by Proposition 6.4, but $st \in S$ and I is S-closed so $r \in I$.

(3) The restriction of c to $\operatorname{Spec}(R_S)$ is injective by (1). If $Q \in \operatorname{Spec}(R_S)$ then $c(Q) \in \operatorname{Spec}(R)$ by Lemma 6.7 and $c(Q) \cap S = \emptyset$ because otherwise, $s \in c(Q)$ implies $\iota(s) = s/1 \in Q$ would force $Q = R_S$ because $s/1 \in (R_S)^\times$. So indeed $c(Q) \in \{P \in \operatorname{Spec}(R) : P \cap S = \emptyset\}$ for all $Q \in \operatorname{Spec}(R_S)$.

We must now show c is surjective. So, let $P \in \operatorname{Spec}(R)$ be such that $P \cap S = \emptyset$; we will first prove $c(e(P)) = P$. By the proof of (2) above, it is enough to show P is S-closed. But if $rs \in P$ with $s \in S$ then $s \notin P$ because $P \cap S = \emptyset$, so $r \in P$ because P is prime.

It remains to see that $e(P) \in \operatorname{Spec}(R_S)$. Suppose that $a/s, b/t \in R_S$ and $(a/s)(b/t) \in e(P)$. Then $ab \in c(e(P))$ which equals P by the above. Hence either $a \in P$ or $b \in P$, so $a/s \in e(P)$ or $b/t \in e(P)$.

(4,5) See Sheet 3, Question 2. □

Using Proposition 6.8(3), we obtain the following

Example 6.9. *Suppose R is a domain and $f \in R$. Then*

$$c : \operatorname{Spec}(R_f) \quad \xrightarrow{\cong} \quad \{P \in \operatorname{Spec}(R) : f \notin P\}.$$

Thus the process of "localising at f", i.e. inverting the element f of R corresponds to *removing* all prime ideals in R that contain f from $\operatorname{Spec}(R)$. Hence the name *localisation.*

Corollary 6.10. *If R is Noetherian then R_S is also Noetherian.*

Proof. A strictly ascending chain in $\operatorname{Id}(R_S)$ contracts to a strictly ascending chain of ideals in $\operatorname{Id}(R)$ by Proposition 6.8(1,4). □

Definition 6.11. *Let $P \in \operatorname{Spec}(R)$. The* localisation of R at P *is*

$$R_P := R_{R\backslash P}.$$

Note that $R\backslash P$ is multiplicatively closed precisely because P is prime. The clash of terminology is unfortunate, but completely standard.

Proposition 6.12. *Let $P \in \operatorname{Spec}(R)$.*

(1) R_P is a local ring with unique maximal ideal $e(P) = PR_P$.
(2) $\operatorname{Spec}(R_P) \cong \{Q \in \operatorname{Spec}(R) : Q \subseteq P\}$.

Proof. (1) Suppose that $r/s \in R_P$ is not in $e(P)$. This means that $r \notin P$. But then r becomes a unit in R_P, so $r/s \in (R_P)^\times$, too. So, every element of R_P away from $P \cdot R_P$ is a unit, and thus every proper ideal of R_P must be contained in $P \cdot R_P$. It remains to see that $P \cdot R_P$ is itself proper. But if not, then $1 \in P \cdot R_P$ forces $1 = p/s$ for some $p \in P$ and $s \in R\backslash P$ and then $(s - p)t = 0$ for some $t \in R\backslash P$ by Proposition 6.4(2). Hence $st = pt \in P$ with $s, t \notin P$ which is a contradiction.

(2) By Proposition 6.8 (3), c maps $\operatorname{Spec}(R_S)$ bijectively onto $\{Q \in \operatorname{Spec}(R) : Q \cap (R\backslash P) = \emptyset\}$. But $Q \cap (R\backslash P) = \emptyset$ if and only if $Q \subseteq P$. □

Proposition 6.13. *Let I and J be ideals in a ring R. Suppose that $IR_M \subseteq JR_M$ for each maximal ideal M of R. Then $I \subseteq J$.*

Proof. By replacing J by $I + J$ if necessary, we may assume that $I \subseteq J$. Suppose for the sake of contradiction that there is some $a \in I\backslash J$ and let $L := \{x \in R \mid xa \subseteq J\}$. Then L is a proper ideal of R since $1 \notin L$ and so by Zorn's Lemma 3.6 there is some maximal ideal M of R with $L \subseteq M$. Now $a \in IR_M \subseteq JR_M$ and so $a = x/y$ with $x \in J$ and $y \notin M$. But then $ays = xs \in J$ for some $s \notin M$ by Proposition 6.4(2). Hence $ys \in L \subseteq M$ with $y \notin M, s \notin M$; but M is maximal hence prime so we have reached a contradiction. Hence $I \subseteq J$. □

The above proposition is useful when we want to prove equality of two ideals I and J of a ring R: it is sufficient to show $IR_M = JR_M$ for each maximal ideal M and the problem reduces to working in the local ring R_M which is usually much easier to understand.

7. Integrality

Let $R \subseteq S$ be two rings.

Definition 7.1. *An element $x \in S$ is said to be* integral over R *if x is the root of a monic polynomial with coefficients in R, that is*

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \tag{2}$$

for some $a_i \in R$.

The ring S is said to be integral over R *if every element of S is integral over R. We also say that $R \subseteq S$ is an* integral extension.

Definition 7.2.

(a) The integral closure *of R in S is the set of all elements of S which are integral over R.*
(b) An integral domain R is said to be integrally closed *if it is equal to its integral closure in its field of fractions.*

Theorem 7.3. *Let C be the integral closure of R in S. Then C is a subring of S.*

Proposition 7.4. *Let $x \in S$. Then x is integral over R if and only if there is a finitely generated R-module $M \subseteq S$ such that $1 \in M$ and $xM \subseteq M$.*

Proof. Suppose x is integral over R and satisfies (2). We can take $M = \sum_{j=0}^{n-1} x^j R$. Conversely, if M is a finitely generated module with $xM \subseteq M$ by Theorem 5.2 there is a monic polynomial $f(t) \in R[t]$ such that $f(x)M = \{0\}$. Since $1 \in M$ we see that $f(x) = 0$ and x is integral over R. □

Proof of Theorem 7.3. Let $x, y \in C$ and let n and m be the degrees of the monic polynomials with roots x and y respectively. We set $M := \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x^i y^j R$. Then $1 \in M$, $xM \subseteq M$, $yM \subseteq M$ and so $(x+y)M \subseteq M$ and $xyM \subseteq M$. Proposition 7.4 now gives that $x+y$ and $xy \in C$. □

Proposition 7.5. *Let $R \subseteq S \subseteq T$ be three rings such that S is integral over R and T is integral over S. Then T is integral over R.*

Proof. Let $x \in T$ and let $a_i \in S$ such that $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Let $S' := R[a_1, \ldots, a_n] \subseteq S$. Since each a_i is integral over R the argument of Proposition 7.4 gives that S' is a finitely generated R-module. Let B be a finite set of generators of S', so $S' = \sum_{b \in B} Ra$.

Now consider

$$M := S'[x] = \sum_{i=0}^{n-1} S'x^i = \sum_{i=0}^{n-1} \sum_{b \in B} Rbx^i.$$

We have $1 \in M$, $xM \subseteq M$ and M is generated by the finite set $\cup_{i=0}^{n-1} x^i B$ as an R-module. So by Proposition 7.4 x is integral over R. Therefore T is integral over R. □

When $R \subseteq S$ is an integral extension there is a close relationship between the prime ideals of S and the prime ideals of R.

Proposition 7.6. *Let $R \subseteq S$ be an integral extension and suppose that S is a domain. Let I be a non-zero ideal of S. Then $I \cap R \neq \{0\}$.*

Proof. Let $x \in I \backslash \{0\}$ and let x satisfy (2) with n minimal possible. We can write this as $xh(x) = -a_n$ where $h(x) = x^{n-1} + \cdots + a_{n-1}$. Then $a_n \neq 0$ because S is a domain and both x and $h(x)$ are not zero. Since $x \in I$ we have $a_n \in I \cap R$. □

Proposition 7.7. *Let $R \subseteq S$ be an integral extension.*

(a) If S is a field then R is a field.

(b) If R is a field and S is a domain then S is a field.

(c) Let P be a prime ideal of S and let $Q := R \cap P$. Then P is a maximal ideal of S if and only if Q is a maximal ideal of R.

Proof. (a) Let $x \in R \backslash \{0\}$ and let $x^{-1} \in S$ satisfy the equation

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

with $a_i \in R$. This gives $x^{-1} = -(a_1 + a_2 x + \cdots + a_n x^{n-1})$ and so $x^{-1} \in R$.

(b) Let $0 \neq x \in S$. Then $xS \cap R \neq \{0\}$ by Proposition 7.6. Since R is a field, $xS \cap R = R$ so $1 \in xS$. Hence x is a unit and S is a field.

(c) We have $R/Q = R/(P \cap R) \simeq (R + P)/P \subseteq S/P$. Since S is integral over R by reducing the equation (2) modulo P we deduce that S/P is integral extension of R/Q. Note that S/P is a domain since P is a prime ideal of S. Now by parts (a) and (b) S/P is a field if and only if R/Q is a field. □

Theorem 7.8 (Going Up)**.** *Let $R \subseteq S$ be an integral extension. Let Q be a prime ideal of R.*

(a) There exists a prime ideal P of S such that $P \cap R = Q$.

(b) Suppose $P_1 \subseteq P_2$ are two prime ideals of S such that $P_1 \cap R = P_2 \cap R$. Then $P_1 = P_2$.

Proof. (a) Let $Y = R\backslash Q$ and note that Y is multiplicatively closed subset of R; hence also of S. Choose an ideal P of S maximal subject to the condition $P \cap Y = \emptyset$, such an ideal P exists by Lemma 3.6. Then P is a prime ideal of S by Problem sheet 1. From the choice of P we have $R \cap P \subseteq Q$. Suppose there exists $x \in Q$ with $x \notin P$. Then $P + Sx$ is an ideal strictly bigger than P and therefore there exists $z \in (P + Sx) \cap Y$. We can write $z = p + sx$ where $p \in P, s \in S$. The element s is integral over R and therefore $s^n + a_1 s^{n-1} + \cdots + a_n = 0$ for some $a_i \in R$. This gives

$$(xs)^n + a_1 x(xs)^{n-1} + \cdots + a_n x^n = 0$$

We have $xs \equiv z \bmod P$ and and therefore

$$z^n + a_1 x z^{n-1} + \cdots + a_n x^n \in P \cap R \subseteq Q.$$

Since $x \in Q$ this implies $z^n \in Q$ but $z \notin Q$ and Q is a prime ideal of R, contradiction. Therefore $P \cap R = Q$.

(b) Let $Q := P_1 \cap R = P_2 \cap R$ and consider the integral extension $R/Q \subseteq S/P_1$. The ring S/P_1 is a domain with ideal P_2/P_1 such that $(P_2/P_1) \cap (R/Q) = Q/Q = \{0\}_{R/Q}$. By Proposition 7.6 we must have that P_2/P_1 is the zero ideal, hence $P_1 = P_2$. □

The Going Up Theorem (Theorem 7.8) can also be proved using localisation. We can also "go up in chains":

Theorem 7.9. *Let $R \subseteq S$ be an integral extension and let*

$$Q_1 < Q_2 < \cdots < Q_k$$

be a chain of prime ideals of R. There exists a chain

$$P_1 < P_2 < \cdots < P_k$$

of prime ideals of S such that $P_i \cap R = Q_i$ for $i = 1, \ldots, k$.

Proof. We use induction on k, the case of $k = 1$ being Theorem 7.8(a). For the inductive step it is sufficient to prove the following:

Given prime ideals $Q_1 \subseteq Q_2$ of R and a prime ideal P_1 of S with $P_1 \cap R = Q_1$, there exists a prime ideal $P_2 \supseteq P_1$ such that $P_2 \cap R = Q_2$.

Let $\bar{R} = R/Q_1$, $\bar{S} = S/P_1$. Now $\bar{Q}_2 := Q_2/Q_1$ is a prime ideal of $\bar{R}$ and $\bar{S}$ is integral over $\bar{R}$. By Theorem 7.8(a) there is a prime ideal $\bar{P}_2$ of $\bar{S}$ such that $\bar{P}_2 \cap \bar{R} = \bar{Q}_2$.

There is a prime ideal P_2 of S with $P_2 \supseteq P_1$ such that $\bar{P}_2 = P_2/P_1$ and we claim that $P_2 \cap R = Q_2$. From the choice of $\bar{P}_2$ we have

$(P_2 \cap R) + P_1 = P_2 \cap (R + P_1) = Q_2 + P_1$. Taking intersection with R we obtain

$$P_2 \cap R = ((P_2 \cap R) + P_1) \cap R = (Q_2 + P_1) \cap R = Q_2.$$

This completes the induction step. □

Theorem 7.9 and Theorem 7.8 (b) together give the following.

Corollary 7.10. *Let $R \subseteq S$ be an integral extension.*

(a) A strictly increasing chain of prime ideals of S intersects R in a strictly increasing chain of prime ideals of R.
(b) Conversely, any strictly increasing chain of prime ideals of R is the intersection of R with some strictly increasing chain of prime ideals of S.

8. Krull dimension

Let F be an algebraically closed field. We want to define a notion of dimension to every algebraic set, which generalizes the dimension of the vector space F^k.

Definition 8.1. *Let $V \subseteq F^k$ be an irreducible algebraic set. The* dimension $\dim V$ *of V is the largest integer n such that there is a strictly increasing chain*

$$\emptyset \neq V_n \subset V_{n-1} \subset \cdots \subset V_0 = V \tag{3}$$

of irreducible algebraic sets V_i. More generally when V is not necessarily irreducible, we set $\dim V$ *to be the largest dimension of an irreducible component of V.*

For example if $V = \{\mathbf{a}\}$ is a single point in F^k then $\dim V = 0$. We will prove later that that $\dim V$ is always finite and in fact $\dim V \leq k$ with equality if and only if $V = F^k$.

Let $P_i = \mathcal{I}(V_i)$ where V_i are the irreducible sets of (3). Then $P_0 \subset P_1 \subset \cdots \subset P_n$ is a strictly increasing chain of prime ideals of the polynomial ring $R = F[t_1, \ldots, t_k]$. This leads to the following definition.

Definition 8.2. *Let R be a ring. The* Krull dimension *of R denoted by* $\dim R$ *is the largest n such that there is a chain*

$$P_0 \subset P_1 \subset \cdots \subset P_n \tag{4}$$

of prime ideals P_i of R. We set $\dim R = \infty$ *if no such integer n exists.*

Using Proposition 1.4(4) and Proposition 3.11 we see that for an irreducible algebraic set $V \subseteq F^k$ we have

$$\dim V = \dim F[t_1, \ldots, t_k]/\mathcal{I}(V).$$

A word of warning: the dimension of a Noetherian ring does not have to be finite (see the 2015 Exam paper C2.3, Q3 for an example).

Proposition 8.3. *If $R \subseteq S$ is an integral extension, then*

$$\dim R = \dim S.$$

Proof. This follows immediately from Corollary 7.10. □

Our next goal will be to prove that

$$\dim F[t_1, \ldots t_k] = k.$$

We will prove a more general result about the dimension of F- algebras. First we need more definitions.

Definition 8.4. *Let $F \subseteq E$ be a field extension. Elements $x_1, \ldots x_k \in E$ are said to be* algebraically dependent *over F if there is a non-zero polynomial $f \in F[t_1, \ldots, t_k]$ such that $f(x_1, \ldots, x_k) = 0$.*

We say that $x_1, \ldots, x_k$ are algebraically independent *(also said to be* transcendental*) over F if they are not algebraically dependent.*

Definition 8.5. *With $F \subseteq E$ as above the set $X := \{x_1, \ldots, x_n\}$ is a* transcendence basis *for E over F if X is a maximal algebraically independent subset of E.*

The notion of transcendence basis is defined even for infinite sets but we won't need this here. It is clear that if $E = F(c_1, \ldots, c_m)$ is finitely generated as a field over F then there is a finite subset $X \subseteq \{c_1, \ldots, c_m\}$ which is a transcendence basis for E/F. What needs proving is the analogue of fundamental property of bases of a vector space:

Proposition 8.6. *Any two transcendence bases for E over F have the same size.*

Proof. Let $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$ be two transcendence bases for E over F, with $m \geq n$; thus X and Y are algebraically independent over F, and E is algebraic over $F(X)$ and $F(Y)$. We will prove, by induction on $n = \min\{|X|, |Y|\}$, that in fact $m = n$. When $n = 0$, E is algebraic over $F(X) = F$. So no element of E can be transcendental over F, and thus $Y = \emptyset$. So $m = 0$ in this case.

Suppose that $m \geq n \geq 1$. Now E is algebraic over $F(X)$, so y_1 is algebraic over $F(X)$. Let $Z \subseteq X$ be minimal such that y_1

is algebraic over $F(Z)$; then Z is non-empty otherwise y_1 would be algebraic over F. Without loss of generality, we may assume that $Z = \{x_1, \ldots, x_k\}$ for some $1 \leq k \leq n$. Then we can find a non-zero $g(t) \in F(Z)[t]$ such that $g(y_1) = 0$. Clearing the denominators in g, we may assume that $g(t) \in F[x_1, \ldots, x_k][t]$. Since y_1 is not algebraic over F, without loss of generality at least one coefficient of $g(t)$ in $F[x_1, \ldots, x_k]$ involves x_1. Now write $g(t)$ as a polynomial in x_1 with coefficients in $F[x_2, \cdots, x_k][t]$ and let $a(x_2, \ldots, x_k, t)$ be its leading coefficient. Then $a(x_2, \ldots, x_k, y_1) \neq 0$ by the minimality of k, so $g(y_1) = 0$ is a non-zero polynomial equation satisfied by x_1 with coefficients in $F[x_2, \cdots, x_k, y_1]$. We conclude that x_1 is algebraic over $F(x_2, \ldots, x_k, y_1)$, and therefore x_1 *is algebraic over* $L := F(x_2, \ldots, x_n, y_1)$.

Note that $L(x_1)$ contains $F(X)$ and E is algebraic over $F(X)$, so E is algebraic over $L(x_1)$. Since x_1 is algebraic over L, we see that E is algebraic over L.

If $f(y_1, x_2, \ldots, x_n) = 0$ is a non-trivial polynomial relation with coefficients in F, then y_1 is algebraic over $F(x_2, \ldots, x_n)$; but then L would be algebraic over $F(x_2, \ldots, x_n)$ and then E would be algebraic over $F(x_2, \ldots, x_n)$ which is not the case since X is algebraically independent over F. So, $\{y_1, x_2, \ldots, x_n\}$ is algebraically independent over F.

Hence $\{x_2, \ldots, x_n\}$ and $\{y_2, \ldots, y_m\}$ are both algebraically independent over $F(y_1)$, and E is algebraic over both $F(y_1)(x_2, \ldots, x_n)$ and $F(y_1)(y_2, \ldots, y_m)$. By the inductive hypothesis applied to the subsets $\{x_2, \ldots, x_n\}$ and $\{y_2, \ldots, y_m\}$ of the field extension $E/F(y_1)$, we conclude that $m = n$. □

Definition 8.7. *Let $F \leq E$ be a field extension. The* transcendence degree $\text{tr.deg}_F E$ *of E over F is the cardinality of a transcendence basis for E over F.*

More generally for a domain R which is a finitely generated algebra over a field F we set $\text{tr.deg}_F R = \text{tr.deg}_F E$*, where E is the field of fractions of R.*

The following result is very useful in simplifying many proofs by reducing them to polynomial ring.

Theorem 8.8. *[Noether Normalisation Lemma] Let $R = F[y_1, \ldots, y_n]$ be a finitely generated as an algebra over a subfield F. There exists a subset $\{x_1, \ldots, x_k\}$ of R which is algebraically independent over F, and such that R is a finitely generated $F[x_1, \ldots, x_k]$-module.*

Proof. Proceed by induction on n. If $n = 0$ there is nothing to prove. It will be enough to show that there is a subring A of R, generated by $n - 1$ elements, such that R is a finitely generated A-module: then, by induction, we can find $\{x_1, \ldots, x_k\} \subset A$ algebraic over F such that A is finitely generated as an $F[x_1, \ldots, x_k]$-module and then R is also finitely generated as an $F[x_1, \ldots, x_k]$-module.

If $\{y_1, \ldots, y_n\}$ is already algebraically independent over F, there is nothing to prove. So, suppose that $f(y_1, \ldots, y_n) = 0$ for some non-zero $f(Y_1, \ldots, Y_n) \in F[Y_1, \ldots, Y_n]$. Write $f = \sum\limits_{\alpha \in S} \lambda_\alpha Y^\alpha$ where S is a finite subset of $\mathbb{N}^d$, $Y^\alpha := Y_1^{\alpha_1} \cdots Y_n^{\alpha_n}$ for each $\alpha \in \mathbb{N}^d$, and $\lambda_\alpha \in F$ is non-zero for each $\alpha \in S$. Thus $\{Y^\alpha : \alpha \in S\}$ is the set of monomials appearing in the polynomial f.

Choose an integer r strictly greater than $\max_{\alpha \in S} \max_{1 \leq i \leq n} \alpha_i$. Then it follows that the map $S \longrightarrow \mathbb{N}$ given by $\alpha \mapsto \alpha_1 + r\alpha_2 + \cdots + r^{n-1}\alpha_n$ is *injective.* For each $i = 2, \ldots, n$ define $z_i := y_i - y_1^{r^{i-1}}$ and substitute $y_i = z_i + y_1^{r^{i-1}}$ into the relation $f(y_1, \ldots, y_n) = 0$ to obtain

$$f(y_1, z_2 + y_1^r, z_3 + y_1^{r^2}, \ldots, z_n + y_1^{r^{n-1}}) = 0. \tag{5}$$

Expand this equation out, and note that the highest degree term in y_1 in the monomial

$$y_1^{\alpha_1}(z_2 + y_1^r)^{\alpha_2} \cdots (z_n + y_1^{r^{n-1}})^{\alpha_n}$$

is equal to y_1 to the power of $\alpha_1 + r\alpha_2 + \cdots + r^{n-1}\alpha_n$. By our choice of r, it follows that (5) gives a *monic* polynomial equation satisfied by y_1, with coefficients in $A := F[z_2, \ldots, z_n]$. For each $i = 2, \ldots, n$, $y_i = z_i + y_1^{r_{i-1}}$ is also integral over A by Theorem 7.3. It follows that $R = F[y_1, \ldots, y_n]$ is a finitely generated A-module as required. □

Theorem 8.9. *Let R be a domain which is finitely generated as an algebra over its subfield F. Then* $\dim R = \text{tr.deg}_F R$.

Proof. By Theorem 8.8 we can find $\{x_1, \ldots x_k\} \subset R$, algebraically independent over F, such that R is integral over the subring $A := F[x_1, \ldots, x_k]$. Note that A is a polynomial ring over F. We have $\dim R = \dim A$ by Proposition 8.3, and since the field of fractions of R is algebraic over $F(x_1, \ldots, x_k)$ we have $k = \text{tr.deg}_F R$. Now consider the chain of ideals of A

$$\{0\} = P_0 \subset P_1 \subset \cdots \subset P_k,$$

where $P_i = \langle x_1, \ldots, x_i \rangle$. Since A is a polynomial ring over F, each P_i is a prime ideal of A and so $\dim R = \dim A \geq k$.

Let $\{0\} = P_0 \subset P_1 \subset \cdots \subset P_m$ be a strict chain prime ideals of R of length m. Let $R_i := R/P_i$, this is a domain which is a finitely generated algebra over F and by Proposition 8.10 we have

$$k = \text{tr.deg}_F R > \text{tr.deg}_F R_1 > \cdots > \text{tr.deg}_F R_m \geq 0.$$

So $\text{tr.deg}_F R = k \geq m$. Hence $\dim R = k = \text{tr.deg}_F R$. □

Proposition 8.10. *Let R be a domain which is finitely generated as an algebra over a field F. Let P be a non-zero prime ideal of R. Then* $\text{tr.deg}_F R > \text{tr.deg}_F R/P$.

Proof. By Theorem 8.8, we can find $\{\bar{x}_1, \ldots, \bar{x}_k\} \subset R/P$ which is algebraically independent over F and such that R/P is a finitely generated $F[\bar{x}_1, \ldots, \bar{x}_k]$-module. So the field of fractions of R/P is integral over $F(\bar{x}_1, \ldots, \bar{x}_k)$ (see Problem Sheet 4, Question 4), which implies that $\text{tr.deg}_F R/P = k$ by Proposition 8.6. Choose elements $x_i \in R$ such that $\bar{x}_i = x_i + P$ and note that $\{x_1, \ldots, x_k\}$ are algebraically independent over F. Hence $\text{tr.deg}_F R \geq k$.

Let $A := F[x_1, \ldots, x_k]$, a polynomial ring over F; let $Y := A - \{0\}$ and let $E := Y^{-1}A = F(x_1, \ldots, x_k)$ be the field of fractions of A. Since R is finitely generated as an F-algebra, we can find elements $y_1, \ldots, y_n \in R$ such that $R = F[y_1, \ldots, y_n]$. Suppose for the sake of contradiction that $\text{tr.deg}_F R = k$. Then for each $i = 1, \ldots, n$ there exists a non-zero polynomial $g_i(t) \in A[t]$ such that $g_i(y_i) = 0$. Consider the localisation $S := Y^{-1}R$, which is an integral domain containing E. Then each y_i is algebraic over E, and since $R = F[y_1, \ldots, y_n]$ we conclude that *every* element of S is algebraic over E. So, S is a *finite field extension* of E. Since P is not the zero ideal in R, it follows that $Y^{-1}P = SP = S$, and therefore $P \cap Y \neq \emptyset$. But then $P \cap A$ contains a non-zero element $g \in F[x_1, \ldots, x_k]$ say, and then $g(\bar{x}_1, \ldots, \bar{x}_k) = 0$ gives a non-trivial algebraic relation between the $\{\bar{x}_1, \ldots, \bar{x}_k\}$ with coefficients in F — a contradiction.

Therefore $\text{tr.deg}_F(R/P) < \text{tr.deg}_F R$ as claimed. □

Corollary 8.11. *Let F be a field, and $R = F[t_1, \ldots, t_k]$ be a polynomial ring. Then* $\dim R = k$.

Corollary 8.12. *Let F be an algebraically closed field and let $V \subseteq F^k$ be an algebraic set. Then* $\dim V \leq k$, *and* $\dim V = k$ *if and only if* $V = F^k$.

Proof. We have $\mathcal{I}(F^k) = \{0\}$ and so $\dim F^k = \dim F[t_1, \ldots t_k] = k$ by Corollary 8.11.

Now suppose $V \subset F^k$ is a proper algebraic set of dimension l. We may replace V with an irreducible component and so without loss of generality may assume that V is irreducible. Then $\mathcal{I}(V)$ is a prime ideal by Proposition 3.11 which is non-zero since $V \neq F^k$. But then

$$l = \dim V = \dim F[t_1, \ldots, t_k]/P < k$$

by Proposition 8.10. □

9. Noetherian rings of small dimension. Dedekind domains

We can apply the theory developed so far to study the Noetherian rings of dimension 0 and 1. Recall that ideals $P_1, \ldots, P_n$ in a ring R are said to be *pairwise coprime* if $P_i + P_j = R$ whenever $i \neq j$.

Lemma 9.1 (Chinese Remainder Theorem)**.** *Let $P_1, \ldots, P_n$ be pairwise coprime ideals in the ring R. Then*

(a) the canonical ring homomorphism

$$\frac{R}{P_1 \cap \cdots \cap P_n} \longrightarrow \prod_{i=1}^{n} \frac{R}{P_i}$$

given by $(r+P_1 \cap \cdots \cap P_n) \mapsto (r+P_1, \ldots, r+P_n)$, is an isomorphism,
(b) $P_1 \cdots P_n = P_1 \cap \cdots \cap P_n$.

Proof. (a) The canonical map is injective. We prove that it is surjective by induction on n, the case $n = 1$ being trivial. Let $(r_1, \ldots, r_n) \in R^n$ be given. By the induction hypothesis, there exists $r \in R$ such that $r \equiv r_i \mod P_i$ for each $i = 1, \ldots, n-1$. For each $i = 1, \ldots, n-1$ choose $x_i \in P_i$ and $y_i \in P_n$ such that $x_i + y_i = 1$. Then

$$(x_1 + y_1)(x_2 + y_2) \cdots (x_{n-1} + y_{n-1}) = 1,$$

so $a := x_1 \cdots x_{n-1} \equiv 1 \mod P_n$ and $a \in P_1 \cap \cdots \cap P_{n-1}$. Finally, $(1-a)r + ar_n \equiv (1-0)r + 0r_n = r \equiv r_i \mod P_i$ for each $i < n$, whereas $(1-a)r + ar_n \equiv 0r + 1r_n = r_n \mod P_n$.

(b) We show by induction on n that $P_1 \cap \cdots \cap P_n \subseteq P_1 \cdot \cdots \cdot P_n$, the reverse inclusion being clear. Choose $a \in P_1 \cap \cdots \cap P_{n-1}$ such that $1 - a \in P_n$ as above and let $r \in P_1 \cap \cdots \cap P_n$. Then $r \in P_1 \cdot \cdots \cdot P_{n-1}$ by induction, so $r(1-a) \in P_1 \cdot \cdots \cdot P_n$, whereas $a \in P_1 \cdot \cdots \cdot P_{n-1}$ by induction and $r \in P_n$ so $ra \in P_1 \cdot \cdots \cdot P_n$. Hence $r = ra + r(1-a) \in P_1 \cdot \cdots \cdot P_n$ as claimed. □

Theorem 9.2. *Let R be a Noetherian ring of dimension zero. Then*

(a) $R/\operatorname{nilrad}(R)$ is isomorphic to a finite direct product of fields.

(b) R is isomorphic to a finite direct product of local rings of dimension zero.

Proof. (a) By Proposition 3.2 R has finitely many minimal prime ideals, say $P_1, \ldots, P_n$. By Theorem 3.5, $\mathrm{nilrad}(R) = \cap_{i=1}^n P_i$. Since $\dim R = 0$, each P_j is a maximal ideal of R so $P_i + P_j = R$ whenever $i \neq j$. Hence

$$\frac{R}{\mathrm{nilrad} R} = \frac{R}{\cap_i P_i} \simeq \prod_{i=1}^n \frac{R}{P_i}$$

by Lemma 9.1(a), and each R/P_i is a field by the maximality of P_i.

(b) Since $\mathrm{nilrad}(R)$ is nilpotent by Proposition 3.4, there is $m \in \mathbb{N}$ with such that $\prod_{i=1}^n P_i^m \subseteq (P_1 \cap \cdots \cap P_n)^m = \{0\}$. Now P_i^m and P_j^m are coprime for each $i \neq j$. Hence $\prod_{i=1}^n P_i^m = \cap_{i=1}^n P_i^m = \{0\}$ by Lemma 9.1(b), and now Lemma 9.1(a) implies that

$$R \simeq \frac{R}{\prod_{i=1}^n P_i^m} = \frac{R}{\cap_{i=1}^n P_i^m} \simeq \prod_{i=1}^n \frac{R}{P_i^m}.$$

Each R/P_i^m is a local ring of dimension zero. □

Conversely, a ring R such that $\mathrm{nilrad} R$ is a nilpotent finitely generated ideal and $R/\mathrm{nilrad}(R)$ is a finite direct product of fields, is a Noetherian ring of dimension 0. We leave the proof as an exercise.

We now move to Noetherian rings of dimension 1.

Recall from Definition 7.2(b) that a domain R is *integrally closed* if whenever a/b is an element of the field of fractions Q of R which is integral over R, we must have $a/b \in R$.

Definition 9.3. *A Noetherian domain R is said to be a* Dedekind domain *if $\dim R = 1$ and R is integrally closed.*

The ring of integers $\mathbb{Z}$, and more generally, any PID that is not a field, is a Dedekind domain. A rich source of Dedekind domains is provided by Algebraic Number Theory.

Let $E/\mathbb{Q}$ be a finite field extension of $\mathbb{Q}$ and let $\mathcal{O}_E$ be the integral closure of $\mathbb{Z}$ in E. Then $\mathcal{O}_E$ is a domain, and since $\mathcal{O}_E$ is integral over $\mathbb{Z}$ we have $\dim \mathcal{O}_E = \dim \mathbb{Z} = 1$ by Proposition 8.3.

Theorem 9.4. *Let $E/\mathbb{Q}$ be a finite field extension. Then $\mathcal{O}_E$ is finitely generated as a $\mathbb{Z}$-module, and hence is a Noetherian ring.*

Proof. Omitted. See B3.4 Algebraic Number Theory for a proof. □

Thus $\mathcal{O}_E$ is always a Dedekind domain.

An important characterisation of Dedekind domains is that their ideals have *unique factorization property.*

Theorem 9.5. *Let R be a Dedekind domain. Then any nonzero ideal I is a product of prime ideals. This factorization is unique up to reordering of the prime ideals.*

Proof. Note that in a Dedekind domain the set of maximal ideals coincides with the set of non-zero prime ideals. Now if P is a maximal ideal of R, then the localisation R_P is integrally closed by Problem Sheet 4, Question 4 and it is Noetherian by Corollary 6.10. Hence R_P is again a Dedekind domain, but now it is a *local* ring. By Problem Sheet 4, Question 6, R_P is a PID, and every non-zero ideal in R_P is a power of the unique maximal ideal P_P of R_P.

Let I be a non-zero ideal of R. Since R is Noetherian, the set $\min(I) = \{P_1, \ldots, P_m\}$ is finite by Theorem 3.2, so we can find $n_i \in \mathbb{N}$ such that $I_{P_i} = (P_{i,P_i})^{n_i}$. Each P_i is non-zero since I is non-zero, hence maximal. Let $J := P_1^{n_1} \cdots P_m^{n_m}$; by Proposition 6.13, to show that $I = J$ it is enough to check that $I_M = J_M$ for every maximal ideal M of R. If $M \in \min(I)$ then this holds by construction, since $(P_j^{n_j})_{P_i} = R_{P_i}$ whenever $j \neq i$. If M is a non-zero prime ideal different from any of the P_i then $I \nsubseteq M$ and so $IR_M = R_M = JR_M$.

Finally, an easy localisation argument using Problem Sheet 4, Question 6 shows that the integers n_i and the prime ideals P_i are uniquely determined by I. □

How far is a Dedekind domain from being a PID? Here is one answer:

Proposition 9.6. *Let R be a Dedekind domain. Then every ideal of R can be generated by at most 2 elements.*

Proof. By Problem Sheet 4 Question 6, the localisation R_P is a PID for every maximal ideal P of R. Hence every factor ring of R_P is a PIR (it might not be a domain, but at least every ideal is principal). Let n be a positive integer and consider the ideal $R \cap (P_P)^n$. It contains P^n and is contained in P. The only such ideals are powers of P by Theorem 9.5, and since its localisation at P equals that of P^n we conclude that it must be equal to P^n by Proposition 6.13. It follows that the natural map $R/P^n \to R_P/(P_P)^n$ is an isomorphism, so R/P^n is also a PIR. Now Theorem 9.5 together with Lemma 9.1 implies that R/J is a PIR for every non-zero ideal J of R.

Now let I be a non-zero ideal, choose a non-zero element $a \in I$ and let $J = Ra$. Then R/J is a PIR by the above, so $I/J = (R/J).(b+J) = (Rb + J)/J$ for some $b \in R$. Hence $I = Rb + J = Rb + Ra$ can be generated by a and b. □

Definition 9.7. *Let R be an integral domain with field of fractions K. A* fractional ideal *is a finitely generated non-zero R-submodule of K. Let $\mathcal{F}$ denote the set of all fractional ideals of R.*

Every fractional ideal is necessarily of the form αI for some finitely generated ideal I of R and some non-zero element α of K. The product of two fractional ideals is again a fractional ideal. In this way, $\mathcal{F}$ becomes a commutative monoid with identity element R.

Proposition 9.8. *If R is a Dedekind domain, then $\mathcal{F}$ is a* group.

Let I and J be two ideals of R. We say that I *divides* J if $J = IT$ for some ideal T of R.

Proposition 9.9. *Let R be a Dedekind domain and I and J two ideals of R. Then I divides J if and only if $J \subseteq I$.*

Proof. If I divides J then clearly $J \subseteq I$. Conversely suppose $J \subseteq I$. We can write $J = \prod_{i=1}^m P_i^{n_i}$ and $I = \prod_{i=1}^m P_i^{s_i}$ for some integers $n_i, s_i \geq 0$ and prime ideals P_i. Then $JR_{P_i} = P_i^{n_i} R_{P_i} \subseteq P_i^{s_i} R_{P_i} = IR_{P_i}$. Therefore $n_i \geq s_i$ for each i. Let $u_i = n_i - s_i$ and put $T := \prod_{i=1}^m P_i^{u_i}$. We have $IT = J$ and so I divides J. □

Proof of Proposition 9.8. Let $M \in \mathcal{F}$ be a fractional ideal. Then $M = \alpha I$ where I is a non-zero ideal of R and $0 \neq \alpha \in K$. Pick a non-zero element $x \in I$. Because R is a Dedekind domain, by Proposition 9.9, there is an ideal J of R such that $IJ = xR$. Hence $(\alpha I)(x^{-1}\alpha^{-1}J) = R$, so that $x^{-1}\alpha^{-1}J$ is the inverse of $M = \alpha I$ in $\mathcal{F}$. □

Definition 9.10. *Let R be a Dedekind domain with field of fractions K. The* Picard group *of R is* $\mathrm{Pic}(R) := \mathcal{F}/\{\alpha R : 0 \neq \alpha \in K\}$ *is the group of fractional ideals of R modulo the subgroup of principal fractional ideals.*

The Picard group is also known as the *ideal class group.* When $R = \mathcal{O}_E$ is the ring of integers of a finite field extension E of $\mathbb{Q}$, a deep theorem of algebraic number theory says that $\mathrm{Pic}(\mathcal{O}_E)$ is finite. The Picard group measures how far R is from being a PID, because $\mathrm{Pic}(R)$ is trivial if and only if every ideal of R is principal. The coordinate ring $\mathcal{O}(X)$ of any smooth affine curve X over a field is a Dedekind domain, with interesting Picard group. For example, when X is the (punctured) elliptic curve with coordinate ring

$$\mathcal{O}(X) = \mathbb{C}[x,y]/\langle y^2 - x(x-1)(x-\beta)\rangle, \qquad \beta \in \mathbb{C}\backslash\{0,1\},$$

the Picard group of $\mathcal{O}(X)$ is isomorphic to the torus $(\mathbb{R}/\mathbb{Z})^2$ as an abelian group. In general, Picard groups can be quite complicated: a theorem of Claborn (1966) tells us that given an abelian group A it is possible to find a Dedekind domain R with $\mathrm{Pic}(R)$ isomorphic to A.