Notes on Commutative Algebra

Dan Segal

February 2015

1 Preliminary definitions etc.

Rings: *commutative*, with *identity*, usually written 1 or 1_R. Ring homomorphisms are assumed to map 1 to 1. A *subring* is assumed to have the same identity element.

Usually R will denote an arbitrary ring (in this sense).

Polynomial rings

I will *always* use t, $t_1, \ldots, t_n$ to denote *independent indeterminates*. Thus $R[t]$ is the ring of polynomials in one variable over R, $R[t_1, \ldots, t_n]$ is the ring of polynomials in n variables over R, etc.

The most important property of these rings is the '**universal property**', which will frequently be used without special explanation:

- Given any ring homomorphism $f : R \to S$ and elements $s_1, \ldots, s_n \in S$, there exists a unique ring homomorphism $f^* : R[t_1, \ldots, t_n] \to S$ such that $f^*(r) = f(r)\ \forall r \in R$ and $f^*(t_i) = s_i$ for $i = 1, \ldots, n$.

Modules

An *R-module* is an abelian group M together with an action of R on M. This means: for each $r \in R$,

$$a \longmapsto ar \quad (a \in M)$$

is an *endomorphism of the abelian group* M (i.e. a homomorphism from M to itself), and moreover this assignment gives a *ring homomorphism* from R into $\mathrm{End}_{\mathbb{Z}}(M)$, the ring of all additive endomorphisms of M. In practical terms this means: for all $a,\ b \in M$ and all $r,\ s \in R$ we have

$$\begin{aligned} (a+b)r &= ar + br \\ a1 &= a \\ a(r+s) &= ar + as \\ a(rs) &= (ar)s. \end{aligned}$$

(Here M is a *right* R-module; similarly one has *left* R-modules, but over a commutative ring these are really the same thing.)

A *submodule* of M is an additive subgroup N such that $a \in N,\ r \in R \Longrightarrow ar \in N$. Then N is an R-module with the same (restricted) action of R. We write

$$N \leq M$$

to indicate that N is a submodule of M.

The quotient group M/N becomes an R-module via

$$(a+N)\,r = ar + N \quad (a \in M,\ r \in R).$$

(Check that this is well defined!)

We say that M is an *extension* of N by M/N. In general, M is said to be an extension of A by B if A is a submodule of M and $M/A \cong B$.

A module M is *simple* if $M \neq 0$ and M has no proper non-zero submodules, i.e. the only submodules of M are 0 and M. (Example: a vector space is simple iff it is 1-dimensional.)

If A and B are submodules of M then so are $A \cap B$ and

$$A + B = \{a + b \mid a \in A,\ b \in B\}.$$

This extends to any finite number of submodules in the obvious way, and to an arbitrary collection of submodules A_j $(j \in S)$ by

$$\sum_{j \in S} A_j = \{a_{i_1} + \cdots + a_{i_k} \mid a_j \in A_j,\ i_1, \ldots, i_k \in S,\ k \text{ finite}\}.$$

Examples

1. Any vector space over a field

2. R itself, or any ideal of R, with action given by ring multiplication (any ring R)

3. Any abelian group when $R = \mathbb{Z}$

4. V a vector space over a field F and θ a linear transformation of V. Take $R = F[t]$, the polynomial ring. Then V becomes an R-module if we let t 'act like θ', i.e. set

$$at = \theta(a) \quad (a \in V)$$

and extend the action using the rules. (See below for more details.)

If M and N are R-modules, a mapping $h : M \to N$ is a (module) homomorphism if h preserves both addition and the action of R, i.e.

$$h(ar + bs) = h(a)r + h(b)s \quad (a, b \in M,\ r, s \in R).$$

$\ker h$ is a submodule of M and $\operatorname{Im} h$ is a submodule of N. As usual we have the module isomorphism

$$\operatorname{Im} h \cong \frac{M}{\ker h}.$$

Note that an additive homomorphism $M \to M$ is an R-module homomorphism if and only if commutes with the action of R: formally, if $\gamma : R \to \operatorname{End}_{\mathbb{Z}}(M)$ is given by $\gamma(r) = (a \longmapsto ar)$, then

$$\operatorname{End}_R(M) = \{\theta \in \operatorname{End}_{\mathbb{Z}}(M) \mid \theta\gamma(r) = \gamma(r)\theta \ \forall r \in R\}.$$

It follows that if $\theta \in \operatorname{End}_R(M)$ then θ together with $\gamma(R)$ generates a *commutative* subring $\gamma(R)[\theta]$ of $\operatorname{End}_{\mathbb{Z}}(M)$, so we may define a ring homomorphism

$$\begin{gathered}\gamma^* : R[t] \to \operatorname{End}_{\mathbb{Z}}(M) \\ \gamma^*(r) = \gamma(r) \ \ \forall r \in R, \ \ \gamma^*(t) = \theta\end{gathered}$$

and in this way make M into an $R[t]$-module ('universal property of polynomial rings'). This is what we mean by saying 'make M into an $R[t]$-module by letting t act like θ'.

The modular law

This is one of the most useful (and simple) facts: *Let A, B, C be submodules of a module. If $A \leq B$ then*

$$(A + C) \cap B = A + (C \cap B).$$

The proof is virtually obvious (Exercise!). The way to remember this is to draw a lattice diagram.

Direct sums

Let M_i $(i = 1, \ldots, k)$ be modules (all over the same ring R). Their *direct sum*

$$M_1 \oplus \cdots \oplus M_k = \bigoplus_{i=1}^{k} M_i = \{(a_1, \ldots, a_k) \mid a_i \in M_i, \text{ each } i\}$$

is an R-module with componentwise action, i.e.

$$(a_1, \ldots, a_k)r = (a_1 r, \ldots, a_k r) \ \ (r \in R).$$

As usual, one says that a module M is the ('internal') direct sum of submodules $M_1, \ M_2 \ldots$ if the mapping

$$(a_1, \ldots, a_k) \longmapsto a_1 + \cdots + a_k$$

is an isomorphism from $\bigoplus_{i=1}^k M_i$ onto M. This is equivalent to the conditions:

$$M_1 + \cdots + M_k = M$$
$$M_i \cap \sum_{j \neq i} M_j = 0 \ (i = 1, \ldots, k).$$

Generating sets, free modules

The *free module of rank* n is $R^n = R \oplus \cdots \oplus R$ with n summands. Any R-module isomorphic to R^n for some n is called free.

A module M is *generated* by a subset Y of M if M *is the smallest submodule of* M *that contains* Y. This holds iff every element of M is a linear combination of elements of Y, i.e. is equal to one of the form

$$y_1 r_1 + \cdots + y_k r_k \tag{1}$$

for some $y_1, \ldots, y_k \in Y$ and $r_1, \ldots, r_k \in R$. We also say that Y is a *generating set* for M.

In general, we write YR to denote the submodule generated by Y, i.e. the set of all linear combinations (1).

M is *finitely generated* if a finite generating set exists. (Example: a finite-dimensional vector space is generated by a basis.)

In general, a module M is *free with basis* X if X is a generating set for M and every element of M is *uniquely* expressible as a linear combination of (finitely many) elements of X. When $X = \{x_1, \ldots, x_n\}$ is finite, this means that M can be identified with R^n by the isomorphism

$$x_1 r_1 + \cdots + x_k r_k \longmapsto (r_1, \ldots, r_k).$$

Proposition 1.1 *If* X *is a basis of* R^n *then* $|X| = n$.

Proof. Let I be a maximal ideal of R and $\pi : R \to R/I = k$ the quotient map. Then π induces an epimorphism from R^n onto k^n in the obvious way. Now $\pi(X)$ generates $\pi(R^n) = k^n$ as an R-module; this is the same as generating k^n as a k-module. It follows that $|X| \geq |\pi(X)| \geq \dim_k k^n = n$.

Say $|X| = m$. Then $R^n \cong R^m$, and the argument above applied to the image in R^m of the standard basis of R^n shows that $n \leq m$. This completes the proof. ■

Proposition 1.2 *Let* M *be an* R*-module. Then there is a free* R*-module* F *and an epimorphism (surjective homo.)* $\pi : F \to M$. *If* X *is a generating set for* M, *we can choose* F *to be free with basis* X_1 *so that* π *restricts to a bijection* $X_1 \to X$.

Theorem 1.3 *Let* $N \leq M$ *be* R*-modules, and suppose that* M/N *is free. Then* N *has a* complement *in* M, *i.e. there is a submodule* B *of* M *such that* $M = N \oplus B$ *(internal direct sum).*

Proofs: see Ex. Sheet 1.

Ideals

An *ideal* of R is an R-submodule of R. If I is an ideal of R, written

$$I \lhd R,$$

the quotient module R/I is not only a module but a *ring*, if we set

$$(r+I)(s+I) = rs + I.$$

This is called a quotient ring.

If $f : R \to S$ is a ring homomorphism then

$$\ker f = f^{-1}(0)$$

is an ideal of R, and

$$\operatorname{Im} f = \{f(r) \mid r \in R\}$$

is a subring of S. We have

$$\operatorname{Im} f \cong \frac{R}{\ker f},$$

an isomorphism of rings.

If I and J are ideals then so are $I + J$, $I \cap J$ and

$$IJ = \{x_1y_1 + \cdots + x_ky_k \mid x_i \in I,\ y_i \in J,\ k \text{ finite}\}. \tag{2}$$

Note that $IJ \subseteq I \cap J$.

As a matter of **notation**, we use the same definition (2) when J is an ideal of R and I is any R-module.

Prime ideals, maximal ideals

An ideal I of R is *prime* if R/I is an integral domain, i.e. $ab \in I \Longrightarrow [a \in I$ or $b \in I]$, and $1 \notin I$ (in an integral domain we *assume* that $1 \neq 0$).

An ideal I is *maximal* if it is maximal among *proper* ideals; this is equivalent to saying that the module R/I is simple. This is denoted

$$I \underset{\max}{\lhd} R.$$

Recall the basic facts: *I is maximal iff R/I is a field*, and *every maximal ideal is prime.*

Useful fact *Every proper ideal is contained in a maximal ideal.*

Proof. A maximal ideal is one maximal among those not containing 1. More generally, given any ideal I and an element $a \in R \smallsetminus I$, the set of ideals J with

$I \subseteq J$, $a \notin J$ is 'inductive', hence has a maximal member by **Zorn's Lemma** (see Appendix). In most cases we'll be dealing with Noetherian rings, where it's clear. ■

A set Y is *multiplicatively closed* if $x, y \in Y \Longrightarrow xy \in Y$, and Y is non-empty.

Lemma 1.4 *Let Y be a multiplicatively closed subset of R with $0 \notin Y$. Let P be an ideal maximal w.r.t. $P \cap Y = \varnothing$. Then P is prime.*

Proof. Ex. Sheet 1. ■

2 The Noetherian condition

Proposition 2.1 *Let M be a module. The following are equivalent:*
(a) *every strictly ascending chain of submodules in M is finite*
(b) *every submodule of M is finitely generated*
(c) *every nonempty collection of submodules of M has a maximal member.*

(A *maximal* member of a collection $\mathcal{S}$ of submodules means a submodule $A \in \mathcal{S}$ such that *no member of $\mathcal{S}$ properly contains A*. It does *not* mean that A necessarily contains all the other members of $\mathcal{S}$.)
Proof. (c)$\Longrightarrow$(a)$\Longleftrightarrow$(b) are easy. (a)$\Longrightarrow$(c): If (c) fails we can recursively construct an infinite strictly ascending chain. ■

A module satisfying (a) - (c) is called *Noetherian.*

Lemma 2.2 *Let M be an extension of A by B. Then M is Noetherian if and only if both A and B are Noetherian.*

The ring R is *Noetherian* if it is Noetherian as an R-module.

Corollary 2.3 *If R is Noetherian then every finitely generated R-module is Noetherian.*

Proofs: see Ex. Sheet 1.

Examples of Noetherian rings

1. Any field; 2. $\mathbb{Z}$; 3. More generally, any PID;

4. If R has a Noetherian subring S such that R is finitely generated as an S-module, then R is Noetherian (follows from Corollary 2.3);

5. If $R \cong A/I$ where A is a Noetherian ring and I is an ideal then R is Noetherian;

6. If R has a Noetherian subring S such that R is finitely generated as an S-algebra, then R is Noetherian (follows from *Hilbert's Basis Theorem*, as we'll see).

(R is *finitely generated as an S-algebra* means: there is a finite subset X of R such that R is generated as a *ring* by S and X, i.e. every element of R can be expressed as a polynomial 'variables' in X and coefficients in S.) Hilbert's Basis Theorem will be proved later.

Hilbert's Basis Theorem

Theorem 2.4 *Let R be a Noetherian ring. Then the polynomial ring $R[t]$ is Noetherian.*

Proof. Let

$$f = a_0 + \cdots + a_m t^m$$

be a non-zero polynomial of degree $\partial(f) = m \geq 0$, so $a_m \neq 0$. The *leading coefficient* of f is $\lambda(f) = a_m$. We set $\lambda(0) = 0$.

Let $I \neq 0$ be an ideal of $R[t]$. Put

$$\lambda(I) = \{\lambda(f) \mid f \in I\}.$$

Claim: $\lambda(I)$ is a non-zero ideal of R.

Proof: $\lambda(f)r = \lambda(fr)$ for $r \in R$. Let $f, g \in I$ with $f \neq 0$. I claim that $\lambda(f) + \lambda(g) = \lambda(h)$ for some $h \in I$. If $\partial(f) < \partial(g)$ then $\lambda(f) = \lambda(ft^e)$ where $e = \partial(g) - \partial(f)$, so we may suppose that in fact $\partial(f) = \partial(g)$. If $\lambda(f) + \lambda(g) \neq 0$ then $\lambda(f) + \lambda(g) = \lambda(f + g)$. If $\lambda(f) + \lambda(g) = 0$ then $\lambda(f) + \lambda(g) = \lambda(0)$.

Since R is Noetherian, we have $\lambda(I) = \sum_{i=1}^{k} s_i R$ for some $s_1, \ldots, s_k \in R$. For each i there exists $g_i \in I$ such that $\lambda(g_i) = s_i$; say $\partial(g_i) = m_i$. Put $m = \max\{m_i \mid 1 \leq i \leq k\}$, and let

$$J = I \cap (R + Rt + \cdots + Rt^m) = \{g \in I \mid \partial(g) \leq m\}.$$

Claim: J is finitely generated as an R-module.

Proof: $R + Rt + \cdots + Rt^m$ is a finitely generated R-module, hence Noetherian. Therefore J is finitely generated as an R-module.

Claim: $JR[t] = I$.

Proof: Suppose not. Let $f \in I$ be an element of least degree such that $f \notin JR[t]$. Then $\partial(f) = m + e > m$, say

$$f = a_0 + \cdots + a_{m+e} t^{m+e}$$

where $a_{m+e} = \lambda(f) \neq 0$. Now $\lambda(f) \in \lambda(I)$ so

$$a_{m+e} = \lambda(f) = \sum_{i=1}^{k} b_i s_i$$

for some $b_i \in R$. Let

$$g = \sum_{i=1}^{k} b_i g_i t^{m - m_i + e}.$$

We see that g has degree at most $m+e$ and the coefficient of t^{m+e} in g is $\sum_{i=1}^{k} b_i s_i = a_{m+e}$. So $f-g$ has degree at most $m+e-1 < \partial(f)$. Since $f-g \in I$, it follows by minimality of $\partial(f)$ that $f-g \in JR[t]$. But $g \in J$ and so $f \in JR[t]$, a contradiction.

Conclusion. Say $J = XR$ where X is a finite subset of $R[t]$. Then $I = JR[t] = XR[t]$. ■

Most important example: F a field. Then the polynomial ring $F[t_1, \ldots, t_k]$ is Noetherian, by induction on k.

This is fundamental to *algebraic geometry*, which studies *algebraic varieties*: the solution-sets of families of polynomial equations, and motivates a lot of the theory.

Algebras

A ring S is called an *R-algebra* if there is a ring homomorphism $i : R \to S$. When i is injective, in particular when R is a *field*, one usually forgets i and thinks of R as a subring of S (identifiying r with $i(r)$). In any case, S is then an R-module via

$$sr := s.i(r) \quad (s \in S,\ r \in R).$$

S is then *generated as an R-algebra* by a subset X if S is the smallest subring of S containing both $i(R)$ and X, equivalently: if every element of S is equal to a 'polynomial'

$$\sum_{j=1}^{n} w_j r_j$$

where each w_j is a product of elements of X. (*Example*: $F[t_1, \ldots, t_m]$ is an F-algebra generated by $\{t_1, \ldots, t_m\}$.)

Corollary 2.5 *If R is Noetherian and S is a finitely generated R-algebra then S is Noetherian.*

Proof. Say $S = R[x_1, \ldots, x_n]$. There is an epimorphism $\pi : R[t_1, \ldots, t_n] \to S$ sending t_i to x_i for each i, and $R[t_1, \ldots, t_n]$ is Noetherian by repeated applications of HBT. ■

3 The Radical

An element a of a ring is *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$.

An *ideal* I is nilpotent if $I^n = 0$ for some $n \in \mathbb{N}$; this is equivalent to saying that $x_1 x_2 \ldots x_n = 0$ whenever $x_1, x_2, \ldots, x_n \in I$.

Warning! If I is nilpotent then every element of I is nilpotent, but the *converse is not true in general.*

However:

Lemma 3.1 *If I is generated by finitely many nilpotent elements then I is nilpotent.*

Proof. Say $I = a_1R + \cdots + a_mR$. There exists n such that $a_i^n = 0$ for each i. I claim that $I^{mn} = 0$. Indeed, suppose $c_i = \sum_{j=1}^m a_j r_{ij} \in I$ for $i = 1, \ldots, t$. Then

$$\begin{aligned}\prod_{i=1}^t c_{ij} &= \prod_{i=1}^t \left(\sum_{j=1}^m a_j r_{ij} \right) \\ &= \sum_{j(1)=1}^m \cdots \sum_{j(t)=1}^m a_{j(1)} a_{j(2)} \ldots a_{j(t)} . r_{1j(1)} \ldots r_{tj(t)} .\end{aligned}$$

If $t \geq mn$ then for each tuple $(j(1), \ldots, j(t))$ with $1 \leq j(i) \leq m$ $\forall i$, at least one value of $j(i)$ must repeat at least n times. Then $a_{j(i)}$ occurs at least n times in the factor $a_{j(1)} a_{j(2)} \ldots a_{j(t)}$, which is then zero since $a_{j(i)}^n = 0$. ∎

Definition. The *nilradical* $\mathrm{nil}(R)$ of R is the set of all nilpotent elements of R.

Theorem 3.2

$$\mathrm{nil}(R) = \bigcap \{P \mid P \text{ a prime ideal of } R\}.$$

Proof. If $a^n = 0$ and P is a prime ideal then $a \in P$ since $0 \in P$.

Suppose that $a \in R$ is not nilpotent. Let $Y = \{a^n \mid n \in \mathbb{N}\}$. Obviously Y is multiplicatively closed, and $0 \notin Y$. Hence if Q is an ideal maximal w.r.t. $Q \cap Y = \varnothing$ then Q is prime.

Existence of Q: let $\mathcal{X}$ denote the set of all ideals J as above. $\mathcal{X}$ is non-empty since $0 \in \mathcal{X}$. If (J_α) is an ascending chain of ideals in $\mathcal{X}$ then $\bigcup_\alpha J_\alpha$ is in $\mathcal{X}$. So $\mathcal{X}$ is inductively ordered by inclusion, hence contains a maximal element by Zorn's Lemma. (If we assume that R is Noetherian, we don't need Zorn's Lemma.)

Conclusion. We've seen that if $a \in \mathrm{nil}(R)$ then $a \in P$ for every prime ideal P, and if $a \notin \mathrm{nil}(R)$ then $a \notin Q$ for some prime ideal Q. The result follows. ∎

Definition A *minimal prime* of R is a prime ideal P that is minimal w.r.t. inclusion, i.e. such that

$$Q \text{ prime}, Q \subseteq P \implies Q = P.$$

Warning: Note the asymmetry – *maximal* ideals are *proper* maximal ideals, but minimal primes are not assumed to be non-zero. In an integral domain (and only there), the unique minimal prime is the ideal 0.

Minimal primes don't always exist (as opposed to maximal ones!). However:

Theorem 3.3 *Let R be a Noetherian ring. Then R has only finitely many minimal primes, and every prime ideal contains a minimal prime.*

Proof. Let's call an ideal I of R 'decomposable' if there exist prime ideals $P_1, \ldots, P_k$ (not necessarily distinct) such that

$$\prod_{i=1}^{k} P_i \subseteq I.$$

I claim that *every proper ideal of R is decomposable.*

Proof: Suppose not. Then among the non-decomposable proper ideals there is a maximal one J, say. J is not prime, so there exist ideals A, B strictly containing J such that $AB \subseteq J$.

Now A and B are both decomposable. Say

$$\prod_{i=1}^{k} P_i \subseteq A, \quad \prod_{i=k+1}^{k+l} P_i \subseteq B.$$

Then

$$\prod_{i=1}^{k+l} P_i \subseteq AB \subseteq J,$$

thus J is decomposable, contradiction!

In particular, then, 0 is decomposable. Thus there exist distinct prime ideals $P_1, \ldots, P_m$ and natural numbers $e_1, \ldots, e_m$ such that

$$\prod_{i=1}^{m} P_i^{e_i} = 0. \tag{3}$$

If $P_i \subseteq P_j$ for some $j \neq i$ we can replace $P_i^{e_i} P_j^{e_j}$ by $P_i^{e_i+e_j}$; so we may assume that $P_i \nsubseteq P_j$ whenever $i \neq j$. (Formally, this includes the possibility $m = 1 = e_1$, when R is an integral domain.)

If Q is any prime ideal then $\prod_{i=1}^{m} P_i^{e_i} = 0 \subseteq Q$ implies $P_i \subseteq Q$ for some i. In particular, if $Q \subseteq P_j$ for some j this gives $P_i \subseteq Q \subseteq P_j$ whence $i = j$ and $Q = P_j$.

Thus $P_1, \ldots, P_m$ are minimal primes, and they are the only ones by the preceding observation. ■

The proof also gives another proof (what's the first proof?) of

Corollary 3.4 *If R is Noetherian with minimal primes $P_1, \ldots, P_m$ then $\prod_{i=1}^{m} P_i^{e_i} = 0$ for some $e_1, \ldots, e_m \in \mathbb{N}$.*

In particular, this shows that the non-zero elements of every minimal prime are *zero-divisors.*

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

$$\mathrm{rad}(I) = \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Thus $\mathrm{rad}(I)$ is the inverse image in R of $\mathrm{nil}(R/I)$ under the quotient mapping $R \to R/I$, so it is an ideal and

$$\frac{\mathrm{rad}(I)}{I} = \mathrm{nil}(R/I).$$

(In particular, $\mathrm{rad}(0) = \mathrm{nil}(R)$.)

The *minimal primes* of I are the prime ideals P of R that are minimal subject to $P \supseteq I$.

Corollary 3.5 *Let I be an ideal of R.*

(i)

$$\mathrm{rad}(I) = \bigcap \{P \mid I \subseteq P,\ P \text{ a prime ideal of } R\}.$$

(ii) If R is Noetherian then I has finitely many minimal primes $P_1, \ldots, P_m$ and

$$\mathrm{rad}(I) = P_1 \cap \cdots \cap P_m.$$

There exists $n \in \mathbb{N}$ such that

$$\mathrm{rad}(I)^{mn} \subseteq \prod_{i=1}^{m} P_i^n \subseteq I.$$

Proof. (i) follows from Theorem 3.2 applied to R/I.

(ii) follows since non-minimal primes can be removed from the intersection without changing it. The final claim follows from the last Corollary (all applied in the ring R/I). ■

4 Algebraic geometry

Definition. Let F be a field, $R = F[t_1, \ldots, t_k]$, $Y \subseteq R$, $W \subseteq F^k$. For $f \in R$ and $u = (u_1, \ldots, u_k) \in F^k$ we write $f(u) = f(u_1, \ldots, u_k)$.

$$\mathcal{V}(Y) = \left\{u \in F^k \mid f(u) = 0\ \forall f \in Y\right\}$$
$$\mathcal{I}(W) = \left\{f \in R \mid f(w) = 0\ \forall w \in W\right\}.$$

Thus $\mathcal{V}(Y)$ is the set of common zeros of all polynomials in Y, while $\mathcal{I}(W)$ is the set of all polynomials that vanish at every point of W.

A set of the form $\mathcal{V}(Y)$ is called an *algebraic set*. ($\mathcal{V}$ stands for 'variety', another name for algebraic set. But some authors use the word only for an *irreducible* algebraic set, so we'll avoid it.)

Lemma 4.1 *(i) $\mathcal{I}(W)$ is an ideal of R.*
(ii) If W is an algebraic set then $W = \mathcal{V}(\mathcal{I}(W))$.
(iii) If A_i $(i = 1, \ldots, m)$ are ideals then

$$\mathcal{V}(A_1 + A_2 + \cdots + A_m) = \bigcap_{i=1}^{m} \mathcal{V}(A_i),$$

$$\mathcal{V}(A_1 \cap A_2 \cap \ldots \cap A_m) = \mathcal{V}(A_1 A_2 \ldots A_m) = \bigcup_{i=1}^{m} \mathcal{V}(A_i).$$

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

The maps $\mathcal{I}$ from algebraic sets to ideals and $\mathcal{V}$ from ideals to algebraic sets are obviously *inclusion-reversing*. (ii) implies that $\mathcal{V}$ *is onto* and $\mathcal{I}$ *is one-to-one*. However, $\mathcal{I}$ is *not* onto, by (iv). The beginning of algebraic geometry is to discover which ideals correspond to algebraic sets.

Definition An algebraic set W is *irreducible* if it is not the union of two proper algebraic subsets.

Proposition 4.2 *An algebraic set W is irreducible if and only if $\mathcal{I}(W)$ is a prime ideal of R.*

Theorem 4.3 *Every algebraic set is the union of finitely many irreducible algebraic subsets.*

Proofs: See Ex. Sheet 2.

Suppose $W = \bigcup_{i=1}^{m} V_i$ where the V_i are irreducible algebraic subsets and m is as small as possible. Then $P_i = \mathcal{I}(V_i)$ is prime for each i and $P_i \nsubseteq P_j$ whenever $i \neq j$ (if $P_i \subseteq P_j$ then $V_i \supseteq V_j$ and V_j can be omitted from the union). Then

$$\mathcal{I}(W) = \bigcap_{i=1}^{m} P_i.$$

It follows that $P_1, \ldots, P_m$ are precisely the minimal primes of $\mathcal{I}(W)$. Thus *the irreducible components $V_1, \ldots, V_m$ are uniquely determined*, and we find them by finding the *minimal primes of $\mathcal{I}(W)$*.

Now W will be given as the solution-set of some equations, i.e. $W = \mathcal{V}(I)$ for some ideal I (the ideal generated by finitely many given polynomials). To find the irreducible components of W, it remains to identify the ideal $\mathcal{I}(W) = \mathcal{I}(\mathcal{V}(I))$. We know that $\mathcal{I}(W)$ contains at least $\mathrm{rad}(I)$.

5 The Nullstellensatz

Proposition 5.1 *Let $A \subseteq B \subseteq C$ be rings, where A is Noetherian. Suppose that*

- *C is finitely generated both as an A-algebra and as a B-module.*

Then B is finitely generated as an A-algebra.

Proof. Say

$$C = \sum_{i=1}^{n} y_i B.$$

Let $\{x_1, \ldots, x_m\}$ be a finite generating set for C as an A-algebra. We have

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

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

for suitable $b_{ij},\ b_{ijk} \in B$. Let B_0 be the A-subalgebra of B generated by $\{b_{ij},\ b_{jkl}\ |\text{all } i, j, k, l\}$. Then B_0 is Noetherian (Ex. sheet 3), and

$$A \subseteq B_0 \subseteq B \subseteq C.$$

Let

$$M = B_0 + \sum_{i=1}^{n} y_i B_0.$$

Then M is closed under multiplication by elements of A, and M is closed under addition and multiplication; so M is an A-algebra. Also $\{x_1, \ldots, x_m\} \subseteq M$, so $M \supseteq C$ and therefore $C = M$ is finitely generated as a B_0-module.

It follows that C is Noetherian as a B_0-module, and so its submodule B is finitely generated as a B_0-module. Say

$$B = \sum_{s=1}^{t} z_s B_0.$$

Then the set $\{b_{ij},\ b_{jkl},\ z_s\ |\text{all } i, j, k, l, s\}$ generates B as an A-algebra. ∎

Field extensions

Let $F \subseteq E$ be fields. The *degree* of the field extension E/F is

$$(E : F) = \dim_F(E),$$

the dimension of E as a vector space over F. We say E is a *finite over* F if $(E : F)$ is finite.

An element $x \in E$ is *algebraic* over F if $f(x) = 0$ for some non-zero polynomial $f \in F[t]$. We say that E is algebraic over F if every element of E is algebraic over F.

We write $E = F(x_1, \ldots, x_m)$ to mean that E is generated as a *field* over F by $x_1, \ldots, x_m$, i.e. E is the smallest subfield of E that contains both F and $\{x_1, \ldots, x_m\}$.

Lemma 5.2 *Suppose $E = F(x)$. The following are equivalent:*
(a) $(E : F)$ is finite
(b) x is algebraic over F
(c) E is generated by x as an F-algebra
(d) E is finitely generated as an F-algebra.

Proof. We may assume that $x \neq 0$. (a)$\Longrightarrow$(b) is easy. (b)$\Longrightarrow$(c): Let f be the minimal polynomial of x over F, and $F[x]$ the subalgebra of E generated by x. Then $F[x] \cong F[t]/fF[t]$, a field since f is irreducible, so $F[x] = F(x) = E$.

(c)$\Longrightarrow$(b): $x^{-1} = g(x)$ for some polynomial g, and then $f(x) := xg(x) - 1 = 0$.

(b)&(c)$\Longrightarrow$(a): If $f(x) = 0$ and f has degree n then $\{1, x, \ldots x^{n-1}\}$ spans $E = F[x]$ so $(E : F) \leq n$.

(d)$\Longrightarrow$(b) Suppose that x is not algebraic over F. Then $F[x]$ is the polynomial ring and E consists of rational functions $f(x)/g(x)$, $0 \neq g(x) \in F[x]$. Now suppose that $y_1, \ldots, y_k$ generate E as an F-algebra. Choosing a common denominator we write $y_i = f_i/g$, $i = 1, \ldots, k$.

If $\deg g = 0$ then $E \subseteq F[x]$, which is false since $x^{-1} \notin F[x]$. Hence $1 + g \neq 0$ so we can write

$$(1 + g) \cdot q(f_1/g, \ldots, f_k/g) = 1$$

for some polynomial q over F. Clearing denominators gives

$$(1 + g) \cdot q^* = g^n$$

for some $q^* \in F[x]$ and some n, a contradiction since $(1+g)$ and g are coprime in the UFD $F[x]$. (Note: the idea is to find a fraction whose denominator involves an irreducible factor not among the factors of g – this exists because there are infinitely many non-associate irreducible polynomials, and the idea of using $1+g$ is exacty the same as Euclid's proof that there are infinitely many primes.)

(a)$\Longrightarrow$(d) is obvious. ■

Theorem 5.3 ('Weak Nullstellensatz') *Let $F \subseteq E$ be fields. Suppose that E is finitely generated as an F-algebra. Then E is finite over F.*

Proof. Say E is generated as an F-algebra by $x_1, \ldots, x_m$, where, we may suppose, $m \geq 1$. Put $F_1 = F(x_1)$, the subfield of E generated by x_1 over F. Then $E = F_1[x_2, \ldots, x_m]$. Arguing by induction on m, we may suppose that $(E : F_1)$ is finite. (The induction starts with $m = 1$, when $E = F_1$.)

Now Proposition 5.1 shows that F_1 is finitely generated as an F-algebra, and it follows by Lemma 5.2 that $(F_1 : F)$ is finite. Therefore $(E : F) = (E : F_1)(F_1 : F)$ is finite. ■

Theorem 5.4 *Let F be a field and R a finitely generated F-algebra. Let P be a maximal ideal of R. Then $\dim_F(R/P)$ is finite.*

Proof. R/P is a finitely generated F-algebra and a field. ■

Corollary 5.5 *Let F be an algebraically closed field and $R = F[t_1, \ldots, t_k]$. The mapping*

$$\mu : (u_1, \ldots, u_k) \longmapsto \sum_{i=1}^{k} (t_i - u_i)R$$

is a bijection between F^k and the set $\mathcal{M}$ of all maximal ideals of R.

Proof. Given $\mathbf{u} = (u_1, \ldots, u_k) \in F^k$, there is a ring homomorphism $e_{\mathbf{u}} : R \to F$ such that $e_{\mathbf{u}}(t_i) = u_i$ for each i ('evaluation at $\mathbf{u}$'). Then $R/\ker e_{\mathbf{u}} \cong F$ so $\ker e_{\mathbf{u}}$ is a maximal ideal. To show that $\ker e_{\mathbf{u}} = \mu(\mathbf{u})$ is an Exercise. Thus $\mu(F^k) \subseteq \mathcal{M}$.

μ is $1-1$: Exercise.

μ is onto: Let P be a maximal ideal. Then $\dim_F(R/P)$ is finite, so R/P is a finite extension field of $(F+P)/P \cong F$. As F is algebraically closed this forces $(F+P)/P = R/P$ whence $F + P = R$. Thus $t_i = u_i + y_i$ with $u_i \in F$ and $y_i \in P$, whence

$$P \supseteq \ker e_{\mathbf{u}} = \mu(\mathbf{u}),$$

and equality follows since $\ker e_{\mathbf{u}}$ is maximal. ■

Note that $f \in \mu(\mathbf{u})$ implies $f(\mathbf{u}) = 0$, so we have $\mu(\mathbf{u}) \leq \mathcal{I}(\{\mathbf{u}\})$. As $\mu(\mathbf{u})$ is a maximal ideal, it follows that

$$\mu(\mathbf{u}) = \mathcal{I}(\{\mathbf{u}\}).$$

Corollary 5.6 *With F, R as above. Let $W = \mathcal{V}(I) \subseteq F^k$ be an algebraic set. If $M \underset{\max}{\lhd} R$ then $M \supseteq I$ if and only if $M \supseteq \mathcal{I}(W)$.*

Proof. We have $M = \mu(\mathbf{u}) = \mathcal{I}(\{\mathbf{u}\})$ for some $\mathbf{u} \in F^k$. Then

$$\begin{aligned} M = \mathcal{I}(\{\mathbf{u}\}) \supseteq I &\Longrightarrow \mathbf{u} \in \mathcal{V}(I) = W \\ &\Longrightarrow M = \mathcal{I}(\{\mathbf{u}\}) \supseteq \mathcal{I}(W). \end{aligned}$$

■

Moral Assuming that F is algebraically closed, we can identify points of F^k with elements of $\mathcal{M}$, i.e. maximal ideals in the ring $R = F[t_1, \ldots, t_k]$, and sets of points as subsets of $\mathcal{M}$.

6 Jacobson radical

The last Corollary suggests that we should investigate maximal ideals containing a given ideal. This motivates

Definition The *Jacobson radical* of a ring R is

$$J(R) = \bigcap \left\{ M \mid M \underset{\max}{\lhd} R \right\}.$$

Since maximal ideals are prime we always have $J(R) \geq \mathrm{nil}(R)$. R is a *Jacobson ring* if

$$J(R/I) = \mathrm{nil}(R/I) = \frac{\mathrm{rad}(I)}{I}$$

for every proper ideal I of R; equivalently, if *every prime ideal is an intersection of maximal ideals.*

Lemma 6.1 *Let F be a field and A a finite-dimensional F-algebra. If A is an integral domain then A is a field.*

Proof. If $0 \neq x \in A$ then $\dim_F(Ax) = \dim_F(A)$ so $1 \in Ax$. ■

Theorem 6.2 *Let F be a field and R a finitely generated F-algebra. Then R is a Jacobson ring.*

Proof. Let P be a prime ideal of R. We have to show that P is an intersection of maximal ideals. Replacing R by R/P we reduce to showing that $J(R) = 0$ if R is an integral domain. Let $0 \neq b \in R$; we will find a maximal ideal Q such that $b \notin Q$.

Let Q be maximal among all ideals I such that $b^n \notin I$ $\forall n \in \mathbb{N}$; this set of ideals is non-empty since $b^n \neq 0$ for all n (and so Q exists because R is Noetherian, or by ZL). Then Q is prime because the set $\{b^n \mid n \in \mathbb{N}\}$ is multiplicatively closed. Write $- : R \to R/Q$ for the quotient map.

Now set $S = \overline{R}[\overline{b}^{-1}]$, a subring of the field of fractions of $\overline{R}$. Since every non-zero ideal of $\overline{R}$ contains some power of $\overline{b}$ we see that every non-zero ideal of S contains a unit; so in fact S is a field.

Since S is finitely generated as an F-algebra, $\dim_F(S)$ is finite by Theorem 5.4. Therefore so is $\dim_F(\overline{R})$. It follows by the preceding Lemma that $\overline{R} = R/Q$ is a field, thus Q is maximal as required. ■

Remark The same result holds if F is *any Jacobson ring.* We won't prove this, but it can be done without much difficulty using the concept of an 'integral ring extension'.

Theorem 6.3 ('Hilbert's Nullstellensatz') *Assume that F is algebraically closed. Let I be an ideal of $R = F[t_1, \ldots, t_k]$. Then*

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

Proof. Put $W = \mathcal{V}(I)$. Let $I^*/I = J\left(R/I\right)$. Corollary 5.6 shows that

$$J\left(\frac{R}{\mathcal{I}(W)}\right) = \frac{I^*}{\mathcal{I}(W)}.$$

As R is a Jacobson ring, it follows that $\mathrm{rad}(\mathcal{I}(W)) = I^* = \mathrm{rad}(I)$, and we already know that $\mathcal{I}(W) = \mathrm{rad}(\mathcal{I}(W))$. ■

We can now answer the question from before, when F is *algebraically closed*: there are mutually inverse inclusion-reversing bijections between the collection of algebraic sets W in F^n and the collection of *radical ideals* I *in* $F[t_1, \ldots, t_k]$, given by

$$W \longmapsto \mathcal{I}(W)$$
$$I \longmapsto \mathcal{V}(I).$$

I is *radical* if $I = \mathrm{rad}(I)$: as we have seen, this holds precisely when I is the intersection of finitely many prime ideals; taking a minimal such expression, these are the ideals $\mathcal{I}(V_i)$ where $\mathcal{V}(I)$ is the union of irreducible algebraic sets V_i.

7 The Artin-Rees Lemma and the Cayley-Hamilton Theorem

Recall that if M is an R-module and I is an ideal of R then MI is the submodule of M generated by elements ax ($a \in M,\ x \in I$), so it consists of all finite linear combinations $\sum a_i x_i$ with $a_i \in M$ and $x_i \in I$; if I is generated by a subset X the it suffices to let the x_i range over X.

Theorem 7.1 ('Artin-Rees Lemma') *Let M be a Noetherian R-module, N a submodule of M, and I a finitely generated ideal of R. Then there exists $m \in \mathbb{N}$ such that $MI^m \cap N \subseteq NI$.*

Define

$$\mathrm{ann}_M(I) = \{a \in M \mid ax = 0 \ \ \forall x \in I\}.$$

Let's call an R-module M *good* if for each finitely generated ideal I of R there exists $m \in \mathbb{N}$ such that

$$MI^m \cap \mathrm{ann}_M(I) = 0.$$

To prove the theorem, it will suffice to show that every Noetherian module is good. Indeed, if M is Noetherian then so is $\overline{M} = M/NI$, and $N/NI \subseteq \mathrm{ann}_{\overline{M}}(I)$; thus

$$\frac{MI^m + NI}{NI} \cap \frac{N}{NI} \subseteq \overline{M}I^m \cap \mathrm{ann}_{\overline{M}}(I),$$

so if m is such that $\overline{M}I^m \cap \mathrm{ann}_{\overline{M}}(I) = 0$ then $MI^m \cap N \subseteq NI$.

Call M *only-just-bad* if M is not good, but M/A is good for every non-zero submodule A of M. Now let M be Noetherian, and suppose that M is not good. Let B be maximal among submodules of M such that M/B is not good (B exists since $M/0$ is not good). Clearly, then, M/B is only-just-bad. Thus it will suffice to show that only-just-bad modules don't exist.

Lemma 7.2 *If M is only-just-bad and $A,\ B$ are submodules of M with $A \cap B = 0$ then $A = 0$ or $B = 0$.*

Proof. Suppose that $A \neq 0$ and $B \neq 0$. Then $M_1 = M/A$ and $M_2 = M/B$ are both good. Define $\theta : M \to M_1 \oplus M_2$ by $\theta(u) = (u + A, u + B)$. Then $\ker \theta = A \cap B = 0$ so $M \cong \theta(M) \leq M_1 \oplus M_2$.

Now let I be a finitely generated ideal, and choose m large enough so that $M_i I^m \cap \operatorname{ann}_{M_i}(I) = 0$ for $i = 1, 2$. Then $\theta(M)I^m \leq M_1 I^m \oplus M_2 I^m$ and $\operatorname{ann}_{\theta(M)}(I) \leq \operatorname{ann}_{M_1}(I) \oplus \operatorname{ann}_{M_2}(I)$. It follows that

$$\theta(M)I^m \cap \operatorname{ann}_{\theta(M)}(I) = 0,$$

whence $MI^m \cap \operatorname{ann}_M(I) = 0$ since θ maps M isomorphically to $\theta(M)$. Thus M is good, contradiction. ■

Proposition 7.3 *Only-just-bad modules don't exist.*

Proof. Let M be only-just-bad. Then there exists a finitely generated ideal I such that $MI^n \cap \operatorname{ann}_M(I) \neq 0$ for every $n \in \mathbb{N}$. Choose I with the smallest possible number of generators. Then $I = J + xR$, where J can be generated by fewer elements as an ideal, so we have $MJ^m \cap \operatorname{ann}_M(J) = 0$ for some m (here, J could be the zero ideal, in which case we can take $m = 1$).

It follows by Lemma 7.2 that either $MJ^m = 0$ or $\operatorname{ann}_M(J) = 0$; but $\operatorname{ann}_M(J) \supseteq \operatorname{ann}_M(I) \neq 0$, so in fact $MJ^m = 0$. Then for any n we have

$$MI^{m+n} \subseteq MJ^m + Mx^n = Mx^n.$$

Now $\operatorname{ann}_M(x) \supseteq \operatorname{ann}_M(I) \neq 0$, so $Mx \cong M/\operatorname{ann}_M(x)$ is a good module. So there exists k such that

$$\begin{aligned} 0 &= (Mx)x^k \cap \operatorname{ann}_{Mx}(x) \\ &= Mx^{k+1} \cap (Mx \cap \operatorname{ann}_M(x)) = Mx^{k+1} \cap \operatorname{ann}_M(x). \end{aligned}$$

Putting it together we see that

$$MI^{m+k+1} \cap \operatorname{ann}_M(I) \subseteq Mx^{k+1} \cap \operatorname{ann}_M(x) = 0,$$

contradicting the choice of I. ■

This completes the proof of Theorem 7.1.

**********omitted: not examinable**********

Here is a super-slick **Alternative proof of ARL,** assuming that R is Noetherian.

Recall that if M is an R-module and I is an ideal of R then MI is the submodule of M generated by elements ax ($a \in M,\ x \in I$), so it consists of all finite linear combinations $\sum a_i x_i$ with $a_i \in M$ and $x_i \in I$; if I is generated by a subset X the it suffices to let the x_i range over X.

For a given R-module M we construct an $R[t]$-module $M[t]$ as follows. For each $n \geq 0$ let M_n be an R-module isomorphic to M. Then as an R-module,

$$M[t] = \bigoplus_{n=0}^{\infty} M_n.$$

For each $n \geq 0$ we fix an (R-module) isomorphism $\tau_n : M_n \to M_{n+1}$, and make t act on $M[t]$ by

$$\left(\sum_{n=0}^{k} a_n\right) t = \sum_{n=0}^{k} \tau_n(a_n) \qquad (a_n \in M_n).$$

Thus t maps M_n onto M_{n+1} for each n. Identifying M_0 with M, we then have $Mt^n = M_n$ for each n, and

$$M[t] = \bigoplus_{n=0}^{\infty} Mt^n.$$

Combining the actions of R and of t makes $M[t]$ into an $R[t]$-module. (Note that since each τ_n is an R-module isomorphism, the action of t on $M[t]$ commutes woith the action of R; so this is OK.)

Theorem 7.4 *Suppose that R is Noetherian. Let M be a finitely generated R-module, N a submodule of M, and I an ideal of R. Then there exists $m \in \mathbb{N}$ such that $MI^m \cap N \leq NI$.*

Proof. Let $N_n = MI^n \cap N$ for each n, put

$$N^* = \bigoplus_{n=0}^{\infty} N_n t^n \leq M[t],$$
$$M^* = \bigoplus_{n=0}^{\infty} MI^n t^n \leq M[t].$$

Say $I = x_1R + \cdots + x_lR$, and let S be the R-subalgebra of $R[t]$ generated by $\{x_1t, \ldots x_lt\}$. Thus

$$S = R + It + I^2t^2 + \cdots,$$

which makes it clear that $M^* = MS$. Similarly, $N_nt^n \cdot I^mt^m \subseteq N_{n+m}t^{n+m}$ for each n and m, and so N^* is an S-submodule of M^*.

As S is a finitely generated R-algebra, S is Noetherian. As M is finitely generated as an R-module, $M^* = MS$ is finitely generated as an S-module. Therefore M^* is a Noetherian S-module and so N^* is finitely generated as an

S-module. Hence for some k we have

$$\begin{aligned} N^* &= \left(\bigoplus_{n=0}^{k} N_n t^n\right) S \\ &= \left(\bigoplus_{n=0}^{k} N_n t^n\right)\left(R + \sum_{j=1}^{\infty} I^j t^j\right) \\ &= \bigoplus_{i=0}^{\infty}\left(\sum_{n=0}^{\min(k,i)} N_n I^{i-n}\right) t^i. \end{aligned}$$

In particular, then, if $m > k$ we have

$$\begin{aligned} N_m t^m &= N^* \cap M t^m \\ &= \left(\sum_{n=0}^{k} N_n I^{m-n}\right) t^m. \end{aligned}$$

Thus for any $m > k$ we have $MI^m \cap N = N_m = \sum_{n=0}^{k} N_n I^{m-n} \subseteq NI^{m-k}$. This gives the result on taking $m = k+1$ (but in fact is stronger). ■

****

Corollary 7.5 *Let R be a Noetherian ring, M a finitely generated R-module and I an ideal of R. Let*

$$D = \bigcap_{n=1}^{\infty} MI^n.$$

Then $DI = D$.

Proof. For some m we have $MI^m \cap D \leq DI$. Result follows since $DI \leq D \leq MI^m$. ■

What can we deduce from $D = DI$?

Theorem 7.6 ('Cayley-Hamilton') *Let R be any ring. Let M be a finitely generated R-module, Q an ideal of R, and $\phi : M \to M$ a module endomorphism. If $\phi(M) \subseteq MQ$ then there exist $a_1, \ldots, a_n \in Q$ such that*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0 \tag{4}$$

as an endomorphism of M.

Proof. Consider M as an $R[t]$-module where t acts like ϕ.

Say $M = \sum_{j=1}^{n} x_j R$. Then $MQ = \sum_{j=1}^{n} x_j Q$, so for each i there exist elements $c_{ij} \in Q$ such that

$$\phi(x_i) = \sum_{j=1}^{n} x_j c_{ij}.$$

Since $\phi(x_i) = x_i t$ this means that

$$\sum_{j=1}^{n} x_j(\delta_{ij}t - c_{ij}) = 0 \qquad (i = 1, \ldots, n)$$

(δ_{ij} = Kronecker δ). Let C be the $n \times n$ matrix (c_{ij}). The matrix $\mathbf{I}_n t - C$ over $R[t]$ has an adjoint matrix B, with

$$B \cdot (\mathbf{I}_n t - C) = \Delta I_n$$

where $\Delta = \det(\mathbf{I}_n t - C)$. i.e. there exist $b_{ki} \in R[t]$ such that

$$\sum_i b_{ki}(\delta_{ij}t - c_{ij}) = \Delta\delta_{kj} \qquad (j, k = 1, \ldots, n).$$

So we have

$$\begin{aligned} x_k\Delta &= \sum_j x_j\delta_{kj}\Delta \\ &= \sum_i b_{ki} \sum_j x_j(\delta_{ij}t - c_{ij}) = 0 \end{aligned}$$

for each k. Therefore $M\Delta = 0$.

Now expanding Δ we see that $\Delta = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$ where each a_k is a polynomial (without constant term) in the c_{ij}, whence $a_k \in Q$. The result follows since t acts as ϕ on M. ■

Corollary 7.7 *Let M be a finitely generated R-module and Q an ideal of R. If $M = MQ$ then there exists $x \in Q$ such that $M(1 - x) = 0$.*

Proof. Take $\phi = Id_M$ in the theorem and let $a_1, \ldots, a_n \in Q$ be as in (4). Then

$$M(1 + a_1 + \cdots + a_n) = 0$$

so we can take $x = -(a_1 + \cdots + a_n)$. ■

Theorem 7.8 (Krull Intersection Theorem) *Let R be a Noetherian ring and I an ideal of R. Then $D = \bigcap_{n=1}^{\infty} I^n$ satisfies $D(1 - x) = 0$ for some $x \in I$. If $I \neq R$ and R is an integral domain then $D = 0$.*

Proof. Take $M = R$ in Corollary 7.5, then take $M = D$ in the last corollary. Final claim is clear since $I \neq R$ implies $1 - x \neq 0$. ■

8 Localization

This is a convenient technique that can be used to simplify some arguments.

Proposition 8.1 *Let R be an integral domain, E its field of fractions. Let Y be a multiplicatively closed subset of R, with $1 \in Y$ and $0 \notin Y$. Set*

$$S := RY^{-1} = \left\{ry^{-1} \mid r \in R,\ y \in Y\right\} \subseteq E.$$

(i) *S is a subring of E.*

Denote by $\mathcal{I}(R)$, resp. $\mathcal{I}(S)$ the set of all ideals of R, resp. of S. Define maps ('contraction', 'expansion')

$$c : \mathcal{I}(S) \to \mathcal{I}(R); \quad J \longmapsto J \cap R$$
$$e : \mathcal{I}(R) \to \mathcal{I}(S); \quad I \longmapsto IS$$

and put $\mathcal{I}_c(R) = \{J \cap R \mid J \lhd S\}$, the set of 'contracted ideals'.

(ii) *The maps c and e induce mutually inverse bijections between $\mathcal{I}(S)$ and $\mathcal{I}_c(R)$; in other words, every ideal of S is extended from a unique deal of R, its contraction, and every contracted ideal of R is the contraction of a unique ideal of S, its extension. Both c and e respect inclusion, sums and intersections.*

(iii) *A prime ideal P of R is in $\mathcal{I}_c(R)$ if and only if $P \cap Y = \varnothing$.*

(iv) *c maps prime ideals of S to prime ideals of R, and e maps prime ideals in $\mathcal{I}_c(R)$ to prime ideals of S.*

(v) *Suppose that $Y = R \setminus Q$ where Q is a prime ideal of R. Then S has exactly one maximal ideal, namely $e(Q) = QS$. The prime ideals of S correspond bijectively via c with the prime ideals of R contained in Q.*

Proof. (i) Easy to see that S is closed under multiplication and that $1 \in S$. And

$$ay^{-1} - bz^{-1} = (az - by)(yz)^{-1}. \tag{5}$$

(ii) Let $J \lhd S$. If $a = ry^{-1} \in J$ ($r \in R$, $y \in Y$) then $r = ay \in J \cap R = c(J)$ so $a = ry^{-1} \in c(J)S = ec(J)$; thus $J \subseteq ec(J)$, and the reverse inclusion is clear. So $ec(J) = J$. It follows that e is onto and c is $1-1$.Now let $I = c(J) \in \mathcal{I}_c(R)$. Then $ce(I) = cec(J) = c(J) = I$, so e is $1-1$. Last part: Ex. sheet!

(iii) $P \in \mathcal{I}_c(R)$ iff $P = PS \cap R$, i.e. iff $PS \cap R \subseteq P$ (reverse inclusion always holds). Now $PS = PY^{-1}$ – this holds for any ideal P of R, and follows from (5). so the condition is: $PY^{-1} \cap R \subseteq P$. If $P \cap Y \neq \varnothing$ then $1 \in PY^{-1} \cap R$. Suppose $PY^{-1} \cap R \not\subseteq P$; say $xy^{-1} = r \in R \setminus P$ with $x \in P$ and $y \in Y$. Then $ry = x \in P$ so $y \in P \cap Y$.

(iv) Obviously if Q is a prime ideal of S then $c(Q) = Q \cap R$ is a prime ideal of R. Suppose $P = c(J)$ is prime in R. Then $e(P) = ec(J) = J$. If $(ay^{-1})(bz^{-1}) \in J$ then $ab \in J \cap R = P$ so $a \in P$ or $b \in P$, whence one of ay^{-1}, bz^{-1} lies in $PS = e(P)$. So $e(P)$ is prime.

(v) If J is a maximal ideal of S then $J = ec(J)$ and $c(J)$ is a contracted prime ideal, so $c(J) \subseteq Q$ by (iii). Therefore $J \subseteq e(Q)$, and so $J = e(Q)$. The final claim is immediate from (iii) and (iv). ∎

Corollary 8.2 *If R is Noetherian then S is Noetherian.*

Proof. A strictly ascending chain in $\mathcal{I}(S)$ contracts to a strictly ascending chain in $\mathcal{I}(R)$. ■

Remarks. (1) In the case $Y = R \setminus Q$ where Q is a prime ideal of R, one writes $RY^{-1} = R_Q$: this is called the *localization of R at Q*. If $Q \neq 0$, R_Q is a *local ring*, which means a ring with exactly one maximal ideal, which is not zero (i.e. the ring is not a field). What happens if $Q = 0$?

(2) Suppose S is a ring and M is an ideal of S. Then M is the unique maximal ideal (and S is local, or a field) if and only if $S \setminus M$ *is exactly the set of invertible elements*. Indeed, if $x \in S \setminus M$ is not invertible then xS is contained in a maximal ideal different from M; while if $L \neq M$ is a maximal ideal then $L \not\subseteq M$ and if $x \in L \setminus M$ then x is not invertible.

Example: $R = \mathbb{Z}$, $Q = 2\mathbb{Z}$: then R_Q is the ring of rational numbers with odd denominators.

(2) All of this works without assuming that R is an integral domain: one defines RY^{-1} as a set of equivalence classes on $R \times Y$, to obtain an R-algebra that in general does not contain R. This is called the *localization* of R w.r.t. Y. (Easy but requires a lot of routine verification.)

Proposition 8.3 *Let I and J be ideals in an integral domain R. If $IR_M \subseteq JR_M$ for every maximal ideal M of R then $I \subseteq J$.*

Proof. Suppose $a \in I \setminus J$ and let M be a maximal ideal containing $\{x \in R \mid ax \in J\}$. If $IR_M \subseteq JR_M$ then $a = by^{-1}$ for some $b \in J$ and $y \in R \setminus M$, but then $ay \in J$ so $y \in M$, contradiction! ■

9 Integral extensions

Let R be a subring of a ring S – we say '$R \subseteq S$ is a ring extension'. An element x of S is *integral* over R if x satisfies a monic polynomial equation over R, i.e. if there exist $a_1, \ldots, a_n \in R$ ($n \geq 1$) such that

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0. \tag{6}$$

The *integral closure* of R in S is the set $\{x \in S \mid x \text{ is integral over } R\}$. We say that S *is integral over* R, or $R \subseteq S$ is an *integral extension*, if S is equal to the integral closure of R in S.

Lemma 9.1 *Let $R \subseteq S$ be an integral ring extension where S is an integral domain. If $I \lhd S$ and $I \cap R = 0$ then $I = 0$.*

Proof. Let $0 \neq x \in I$. Then x satisfies an equation (6), which can be rearranged as $x \cdot h(x) = -a_n$, so $a_n \in I \cap R$. If the equation is chosen to have minimal degree then $a_n \neq 0$. ■

Lemma 9.2 *Let $x \in S$. Then x is integral over R if and only if there exists a finitely generated R-submodule M of S such that $1 \in M$ and $Mx \subseteq M$.*

Proof. Suppose (6) holds with each $a_i \in R$. Let

$$M = R + xR + \cdots + x^{n-1}R \subseteq S.$$

It follows from (6) that $Mx \subseteq M$.

Suppose conversely that M exists as described. The action of x is an R-module endomorphism ϕ of M. By the Cayley-Hamilton Theorem, there exists a monic polynomial f over R such that $f(\phi) = 0$. Then $M \cdot f(x) = f(\phi)(M) = 0$. This implies $f(x) = 0$ since $1 \in M$. ■

Proposition 9.3 *Let R be a subring of a ring S and suppose that $S = R[x_1, \ldots, x_k]$ is finitely generated as an R algebra. Then the following are equivalent:*

(a) x_i is integral over R for $i = 1, \ldots, k$;

(b) S is integral over R;

(c) S is finitely generated as an R-module.

Proof. (c) implies (b) by Lemma 9.2 (taking $M = S$). Obviously (b) implies (a).

Suppose that (a) holds. By Lemma 9.2 there exist finitely generated R-submodules $M_1, \ldots, M_k$ of S such that $M_i x_i \subseteq M_i$ and $1 \in M_i$ for each i. Say $M_i = Z_i R$ where Z_i is a finite set; we may assume that $1 \in Z_i$. Then $Z := Z_1 Z_2 \ldots Z_k$ is finite and $ZR \supseteq 1.R = R$. Since $Z_i x_i \subseteq M_i = Z_i R$, we have $ZRx_i \subseteq ZR$ for each i.

As ZR contains R and $ZRx_i \subseteq ZR$ for each i it follows that $ZR \supseteq R[x_1, \ldots, x_k]$. Thus $S = ZR$ and (c) holds. ■

Corollary 9.4 *Let R be a subring of a ring S and let T be the integral closure of R in S. Then T is a subring of S.*

Proof. Let $x, y \in T$. The subalgebra $R[x, y]$ of S is integral over R by (a)$\Longrightarrow$(b). Hence in particular xy and $x - y$ are in T. The result follows. ■

Corollary 9.5 *Let $R \subseteq T \subseteq S$ be rings. If T is integral over R and S is integral over T then S is integral over R.*

Proof. Let $x \in S$. Then x satisfies an equation (6) with $a_1, \ldots, a_n \in T$. Let $U = R[a_1, \ldots, a_n]$ be the R-subalgebra of T generated by the a_i. As each a_i is integral over R, the Proposition shows that U is finitely generated as an R-module. Say $U = XR$ where X is finite.

Now x is integral over U, so for the same reason the U-subalgebra $U[x]$ of S is finitely generated as a U-module. Say $U[x] = YU$ where Y is finite.

Then $U[x] = YU = YXR$, a finitely generated R-module. Now take $M = U[x]$ in Lemma 9.2 to infer that x is integral over R. ■

Prime ideals in integral extensions

Let $R \subseteq S$ be a ring extension. If I is an ideal of S we have

$$R/(I \cap R) \cong (R + I)/I \subseteq S/I.$$

Identifying $R/(I \cap R)$ with $(R + I)/I$ we will think of S/I as an extension ring of $R/(I \cap R)$. If S is integral over R then S/I will be integral over $R/(I \cap R)$ – just reduce the coefficients in (6) modulo I.

We assume for the rest of this subsection that $R \subseteq S$ is an *integral ring extension.*

Lemma 9.6 *(i) Assume that S is an integral domain. Then S is a field if and only if R is a field.*

(ii) Let Q be a prime ideal of S. Then Q is a maximal ideal of S if and only if $Q \cap R$ is a maximal ideal of R.

Proof. (i) Suppose that R is a field, and let $0 \neq x \in S$. Then $xS \cap R \neq 0$, by Lemma 9.1 Say $0 \neq r = xs \in R$. Then $r^{-1}s.x = 1$ so x is invertible in S.

Now suppose that S is a field and let $0 \neq y \in R$. Put $x = y^{-1}$. In the notation of (6) we see that

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

whence $y^{-1} \in R$.

(ii) S/Q is an integral domain and an integral extension of $R/(Q \cap R)$. Result follows by (i) since Q is maximal iff S/Q is a field, $Q \cap R$ is maximal iff $R/(Q \cap R)$ is a field. ■

An ideal P of R is said to be *contracted* if $P = Q \cap R$ for some ideal Q of S, in which case P is the *contraction* of Q.

Proposition 9.7 *(i) Every prime ideal of R is the contraction of a prime ideal of S.*

(ii) Let $Q \subseteq Q'$ be prime ideals of S. Then $Q \cap R = Q' \cap R$ if and only if $Q = Q'$.

Proof. (i) Let $P \lhd R$ be prime, and put $Y = R \setminus P$. There exist ideals $I \lhd S$ with $I \cap Y = \varnothing$, for example $I = 0$. Let Q be maximal among such ideals of S – this exists by Zorn's Lemma. Then $Q \cap R \subseteq P$.

(a) Q is prime: for Y is multiplicatively closed and $0 \notin Y$.

(b) $Q \cap R = P$.

To prove **(b)**, suppose $x \in P \smallsetminus Q$. Then $xS + Q > Q$ so $xS + Q$ meets Y; say $xs - y \in Q$ where $s \in S$ and $y \in Y$. Now s satisfies an equation

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

with each $a_i \in R$. Since $y \equiv xs \pmod{Q}$, multiplying this equation by x^n and replacing xs by y gives

$$y^n + xa_1 y^{n-1} + \cdots + x^{n-1} a_{n-1} y + x^n a_n \equiv 0 \pmod{Q}.$$

The left-hand side of this equation is $y^n + xw$ where $w = a_1 y^{n-1} + \cdots + x^{n-1} a_n \in R$, so

$$y^n + xw \in Q \cap R \subseteq P.$$

But $x \in P$ and P is prime, so $y \in P$, a contradiction!

It follows that $P \subseteq Q$.

(ii) Suppose that $Q \cap R = Q' \cap R$. Note that

$$(Q + R) \cap Q' = Q + (R \cap Q') = Q$$

by the modular law. So writing $- : S \to S/Q$ for the quotient map we have $\overline{Q'} \cap \overline{R} = \overline{Q} = 0$, and we have to show that this implies $\overline{Q'} = 0$. Replacing S by $\overline{S}$ we reduce to the case where S is an integral domain, Q' is a prime ideal with $Q' \cap R = 0$, and we have to prove that $Q' = 0$. But this is immediate from Lemma 9.1. ■

Theorem 9.8 ('Going-up Theorem') *Let $R \subseteq S$ be an integral ring extension and $P_1 < P_2 < \cdots < P_t$ a finite chain of prime ideals in R. Then there exist prime ideals $Q_1 < Q_2 < \cdots < Q_t$ of S such that $Q_i \cap R = P_i$ for each i. Moreover, if $k < t$ and $Q_1 < Q_2 < \cdots < Q_k$ are given with $Q_i \cap R = P_i$ for $1 \leq i \leq k$, then $Q_{k+1}, \ldots, Q_t$ can be chosen to satisfy the given conditions.*

Proof. By Proposition 9.7, P_1 is the contraction of a pime ideal Q_1. Let $1 \leq k < t$ and suppose that $Q_1 < Q_2 < \cdots < Q_k$ are prime ideals of S with $Q_i \cap R = P_i$ for $1 \leq i \leq k$.

For simplicity put $Q = Q_k$ and $P = P_{k+1}$. Note that

$$(P + Q) \cap R = P + (Q \cap R) = P + P_k = P.$$

Write $- : S \to S/Q$. Then $\overline{S}$ is integral over $\overline{R}$, so $\overline{P}$ is the contraction of some prime ideal L of $\overline{S}$. Say $L = Q'/Q$. Then

$$P + Q = (Q + R) \cap Q' = Q + (R \cap Q')$$

and so

$$P = (P + Q) \cap R = (Q + (R \cap Q')) \cap R = R \cap Q'$$

(using the modular law again). Setting $Q_{k+1} = Q'$ we get $Q_k \leq Q_{k+1}$ and $Q_{k+1} \cap R = P_{k+1}$. The inclusion $Q_k \leq Q_{k+1}$ is obviously strict since $P_k < P_{k+1}$.

The result follows by induction on k. ■

Corollary 9.9 *Let $R \subseteq S$ be an integral ring extension.*

(i) A strictly ascending chain of prime ideals of length t in R is the contraction of a strictly ascending chain of prime ideals of length t in S.

(ii) A strictly ascending chain of prime ideals of length t in S contracts to a strictly ascending chain of prime ideals of length t in R.

Proof. (i) Follows from Going-up Theorem. (ii) Follows from Proposition 9.7(ii). ■

The maximal length of a chain of prime ideals in a ring is called the *Krull dimension*. The corollary shows that *Krull dimension is unchanged on passing to an integral ring extension.*

Warning *Contracted and extended primes in ring extensions*

We have considered two kinds of ring extensions $R \subseteq S$: (a) when $S = RY^{-1}$ is a *localization* of R, and (b) when S is *integral* over R. The rules concerning contracted and extended ideals are different in the two cases – don't confuse them!

(a) **Localization**: every ideal of S is extended; extension and contraction give a bijection between prime ideals of R not meeting Y and prime ideals of S.

(b) **Integral extension**: every prime ideal is contracted from a prime ideal of S, but not necessarily from a unique one. The extension of a prime ideal of R need not be prime. Example: $5\mathbb{Z} = \mathbb{Z} \cap (2+i)\mathbb{Z}[i] = \mathbb{Z} \cap (2-i)\mathbb{Z}[i]$.

**********(omitted: **not examinable**)**********

Jacobson rings, again

Theorem 9.10 *Let $R \subseteq S$ be an integral ring extension. If R is a Jacobson ring then S is a Jacobson ring.*

Proof. Let Q be a prime ideal of S. Then S is integral over $(R+Q)/Q \cong R/(R \cap Q)$, so replacing S by S/Q and R by $(R+Q)/Q$ we may suppose that S is an integral domain, and have to show that $J(S) = 0$.

Let $0 \neq b \in S$. Then $0 \neq bs \in R$ for some $s \in S$ by Lemma 9.1. The Jacobson property of R implies that $bs \notin M$ for some maximal ideal M of R. Now $M = Q \cap R$ for some prime ideal Q of S, by Proposition 9.7, and Q is a maximal ideal of S by Lemma 9.6. If $b \in Q$ then $bs \in Q \cap R = M$, so $b \notin Q$. Hence $b \notin J(S)$. ■

Theorem 9.11 *Let A be a Jacobson ring and S a finitely generated A-algebra. Then S is a Jacobson ring.*

Before proving this we need

Lemma 9.12 *Let R be an integral domain. For $y \in R$ put*

$$\mathcal{M}(y) = \left\{ M \underset{\max}{\lhd} R \mid y \notin M \right\}.$$

If $J(R) = 0$ and $y \neq 0$ then $\bigcap \mathcal{M}(y) = 0$.

Proof. Note that

$$y \cdot \bigcap \mathcal{M}(y) \subseteq \bigcap \left\{ M \underset{\max}{\lhd} R \mid y \in M \right\} \cap \bigcap \mathcal{M}(y) = J(R).$$

■

Lemma 9.13 *Let R be an integral domain, $0 \neq y \in R$, and let S be a subring of the field of fractions of R with*

$$R \subseteq S \subseteq R[y^{-1}].$$

If $J(R) = 0$ then $J(S) = 0$.

Proof. Let $0 \neq a \in S$. Then $b := ay^n \in R \setminus \{0\}$ for some $n \geq 0$. By the preceding Lemma, there exists a maximal ideal M of R such that $y \notin M$ and $b \notin M$. Let $M_1 = MR[y^{-1}]$. Then $R \cap M_1 = M$ by Prop. 8.1, hence in particular $b \notin M_1$. It follows that $a = by^{-n} \notin M_1$.

Since $yR + M = R$ we can find $r \in R$ and $v \in M$ such that $yr + v = 1$. Then $y^{-1} = r + vy^{-1} \in R + M_1$; since $R + M_1$ is a subring of $R[y^{-1}]$ it follows that $R + M_1 = R[y^{-1}]$.

Then

$$S = (R + M_1) \cap S = R + (M_1 \cap S),$$

so

$$\frac{S}{S \cap M_1} \cong \frac{R}{R \cap M_1} = \frac{R}{M}$$

is a field, whence $S \cap M_1$ is a maximal ideal of S. As $a \notin S \cap M_1$ we see that $a \notin J(S)$. ■

Proof of Theorem 9.11. Now S is an A-algebra. Let R be the image of A in S. Then R is again a Jacobson ring, and $S = R[x_1, \ldots, x_k]$ for some finite k. Arguing by induction on k, it will suffice to show that if R is Jacobson and $S = R[x]$ then S is Jacobson. As in the previous theorem, we may assume that S is an integral domain, and only have to show that then $J(S) = 0$.

Case 1. Where x satisfies no polynomial equation over R. In this case, $S = R[x]$ is the polynomial ring over R. Let

$$0 \neq b = c_0 + c_1 x + \cdots + c_m x^m \in S$$

where $c_j \in R$ for each j and $c_m \neq 0$ (here $m \geq 0$). Let M be a maximal ideal of R with $c_m \notin M$, and write $- : S \to S/MS$ for the quotient map. Then

$\overline{S} = \overline{R}[\overline{x}]$ and $\overline{b} \neq 0$: here we are using the assumption that S is the polynomial ring; (check this!). Since $\overline{R}$ is a field, $J(\overline{S}) = 0$. We have proved this before, but this case is very easy to prove directly (Exercise, Sheet 3).

Let $\overline{L} = L/MS$ be a maximal ideal of $\overline{S}$ with $\overline{b} \notin \overline{L}$. Then $b \notin L$ and $L \underset{\max}{\lhd} S$. Hence $b \notin J(S)$.

Case 2. Where x satisfies an equation

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with each $a_j \in R$; we may assume that $a_0 \neq 0$ and $n \geq 1$. Let $c = a_0 x \in S$. Multipying the equation by a_0^{n-1} we see that c is integral over R. Therefore $R_1 := R[c]$ is integral over R by Proposition 9.3, and so R_1 is a Jacobson ring, by Theorem 9.10.

Now

$$R_1 = R[c] \subseteq S = R[a_0^{-1}c] \subseteq R_1[a_0^{-1}]$$

(inside the field of fractions of S). Applying Lemma 9.13 with R_1 for R and a_0 for y, we deduce that $J(S) = 0$.

This completes the proof.

****

'**Normalization**'

Lemma 9.14 *Let $0 \neq f(t_1, \ldots, t_p, t) \in F[t_1, \ldots, t_p, t]$ be a non-zero polynomial in $p+1$ variables over a field F. Then there exist $q_1, \ldots, q_p \in \mathbb{N}$ such that*

$$f(t_1 + t^{q_1}, \ldots, t_p + t^{q_p}, t) = ct^m + h(t_1, \ldots, t_p, t) \tag{7}$$

where $0 \neq c \in F$ and the degree of h as a polynomial in t over $F[t_1, \ldots, t_p]$ is at most $m - 1$.

Proof. Say

$$f = \sum_{i=1}^{s} c_i t_1^{e(i,1)} \ldots t_p^{e(i,p)} t^{e(i,0)}$$

with each $c_i \neq 0$, where the $(p+1)$-tuples $\mathbf{e}(i) = (e(i,1), \ldots, e(i,p), e(i,0))$ $(i = 1, \ldots, s)$ are distinct. Given $\mathbf{q} \in \mathbb{N}^p$ we have

$$(t_1 + t^{q_1})^{e(i,1)} \ldots (t_p + t^{q_p})^{e(i,p)} t^{e(i,0)} = t^{m(\mathbf{q}, \mathbf{e}(i))} + g_{\mathbf{q}, \mathbf{e}(i)}$$

where

$$m(\mathbf{q}, \mathbf{e}(i)) = q_1 e(i,1) + \cdots + q_p e(i,p) + e(i,0)$$

and $g_{\mathbf{q}, \mathbf{e}(i)}$ has degree at most $m(\mathbf{q}, \mathbf{e}(i)) - 1$ in t.

Suppose we can choose $\mathbf{q}$ so that the numbers $m(\mathbf{q}, \mathbf{e}(i))$ are all distinct, and the biggest one is $m(\mathbf{q}, \mathbf{e}(j))$. Then we get (7) with $m = m(\mathbf{q}, \mathbf{e}(j))$ and $c = c_j$.

To show that suitable $\mathbf{q}$ exist, consider

$$\prod_{1\le i<j\le s} (m(\mathbf{q},\mathbf{e}(i)) - m(\mathbf{q},\mathbf{e}(j))$$

as a polynomial in variables $q_1,\dots,q_p$ over $\mathbb{Z}$. If this vanishes for every $\mathbf{q}\in\mathbb{N}^p$ it must be the zero polynomial (Ex. Sheet 5). But it isn't, since for $i<j$ the tuples $\mathbf{e}(i)$ and $\mathbf{e}(j)$ are distinct. ■

Theorem 9.15 ('Noether's normalization Lemma'). *Let $S=F[x_1,\dots,x_n]$ be a finitely generated F-algebra where F is a field. Suppose that S is an integral domain. Then there exist $y_1,\dots,y_k\in S$, with $k\le n$, such that $y_1,\dots,y_k$ are algebraically independent over F and S is integral over $F[y_1,\dots,y_k]$ (we allow $k=0$, when $F[y_1,\dots,y_k]=F$).*

Of course, to say that $y_1,\dots,y_k$ are *algebraically independent* over F means that $g(y_1,\dots,y_k)\neq 0$ when $g\neq 0$ is any polynomial over F in k variables. This is equivalent to the statement: $\pi_{\mathbf{y}} : F[t_1,\dots,t_k]\to F[y_1,\dots,y_k]$ *is an isomorphism*, where $\pi_{\mathbf{y}}(g)=g(\mathbf{y})$.

Proof. If $n=0$ there is nothing to prove. Suppose $n\ge 1$. Arguing by induction on n, we may suppose that $R:=F[x_1,\dots,x_{n-1}]$ is integral over $F[y_1,\dots,y_l]$ where $y_1,\dots,y_l$ are algebraically independent over F and $l\le n-1$.

Now $S=R[x]$ where $x=x_n$.

Case 1. Suppose that $y_1,\dots,y_l,x$ are algebraically independent. Put $k=l+1$ and $y_k=x$. The integral closure of $F[y_1,\dots,y_k]$ then contains both R and x, so it is equal to S.

Case 2. $y_1,\dots,y_l,x$ are not algebraically independent. Then x satisfies a polynomial equation with coefficients in R, which we write as $f(x_1,\dots,x_{n-1},x)=0$ where f is a non-zero polynomial in n variables over F.

Taking $p=n-1$ in the Lemma and setting $z_i=x_i-x^{q_i}$ for $i=1\dots n-1$ we get

$$0=f(z_1+x^{q_1},\dots,z_{n-1}+x^{q_{n-1}},x)=cx^m+h(z_1,\dots,z_{n-1},x),$$

where h has degree at most $m-1$ in x, and $0\neq c\in F$. Multiplying this by c^{-1} we see that x is integral over $F[z_1,\dots,z_{n-1}]=R_1$, say. Since $x_i=z_i+x^{q_i}$ for each i, we have $R_1[x]=S$, and so S is integral over R_1.

Now by inductive hypothesis again, we may suppose that R_1 is integral over $F[y_1',\dots,y_s']$ where $y_1',\dots,y_s'$ are algebraically independent over F and $s\le n-1$. It follows that S is integral over $F[y_1',\dots,y_s']$. ■

This is a very useful result! If we want to prove that all integral domains that are finitely generated F-algebras have some property, we only have to check (a) that polynomial rings have it and (b) that it's preserved by integral extensions.

10 Dimensions

What is the dimension of a vector space V? This is usually defined in terms of a basis, but we would like to think of it geometrically. We can say, for example, that $\dim V = n$ if there is a chain of subspaces

$$V = V_0 \supset V_1 \supset \cdots \supset V_n \tag{8}$$

such that $\dim(V_{i-1}/V_i) = 1$ for each i, and $V_n = 0$. This still needs a definition of 'codimension one'; for example, $\dim(W/U) = 1$ iff U is the solution-set in W of a non-trivial linear equation. Another approach is to say: there is a chain of subspaces (8) of length n but no such chain of length $n+1$.

Let's try to generalize this to *algebraic sets*. We could naively repeat the definition, simple replacing 'vector space' by 'algebraic set' and 'subspace' by 'algebraic subset'. But this wouldn't be much good: let X and Y be the x-axis and y-axis in $\mathbb{R}^2$ and consider $V = X \cup Y$. Then $V \supset X \supset \varnothing$ but we'd like to say that V is one-dimensional. This suggests that we ought to avoid *reducible* algebraic sets.

Definition (1) Let V be an irreducible algebraic set. Then $\dim V = n$ if there is a chain (8) of irreducible algebraic subsets (V_i) of length n, and no such chain of length $n+1$.

In general, if V is an algebraic set one defines $\dim V = \sup\{\dim W \mid W \subseteq V, W \text{ irreducible}\}$.

Alternatively, we might like to say that U has *codimension one* in W if U is the solution-set in W of one non-trivial equation:

Definition (2) Let $W = \mathcal{V}(I)$ be an irreducible algebraic set and U an algebraic subset. Then U has *codimension one in* W if $U = \mathcal{V}(I + fR)$ where $f \notin \mathcal{I}(W)$.

Here $R = F[t_1, \ldots, t_k]$ where W and U are algebraic sets in F^n (U is called a *hypersurface* in W).

It does not seem obvious that the two definitions are compatible: is it necessarily the case that $\dim W = 1 + \dim U$ if $W \subseteq U$ are as in Definition (2)? Do we get the right answer for $\dim V$ when $V = F^n$? To examine these questions we go back to algebra.

From now on, R is a *Noetherian ring*.

Definition Let R be a ring. The *Krull dimension* $\dim(R)$ of R is the biggest integer n such that R contains a chain of prime ideals

$$P_0 < P_1 < \cdots < P_n. \tag{9}$$

(or ∞ if there is no maximal such n).

Remark We have seen in Proposition 8.1 that if S is an ID and Q is a prime ideal of S, then chains of prime ideals of S contained in Q corrrespond to chains of prime ideals in the local ring S_Q. Applying this with $S = R/P_0$ and $Q = P_n/P_0$, we deduce that $\dim(R)$ is the supremum of the dimensions $\dim\big((R/P)_{M/P}\big)$ where P ranges over minimal primes of R and M ranges over maximal ideals containing P. So we can often concentrate on the case of *local rings*.

Suppose $R = F[t_1, \ldots, t_k]$ and $\overline{R} = R/I$ where $I = \mathcal{I}(V)$ and V is an algebraic set. Let's assume that F is algebraically closed. Then a chain (9) in R with $I \subseteq P_0$ corresponds to a chain $V \supseteq V_0 \supset V_1 \supset \cdots \supset V_n$ of irreducible algebraic subsets $V_i = \mathcal{V}(P_i)$ of V, and conversely. So $\dim V = \dim(\overline{R})$. Thus we have translated Definition (1) into algebra.

We have already seen the following corollary to the 'Going-up Theorem':

Theorem 10.1 *If $R \subseteq S$ is an integral ring extension then* $\dim(S) = \dim(R)$.

With Noether's Normalization Lemma, this reduces the dimension theory of finitely generated algebras over fields to the special case of *polynomial rings*. 'Obviously' $F[t_1, \ldots, t_n]$ should have dimension n: the algebraic set corresponding to the ideal 0 is F^n. This is true, but to prove it needs a bit more work. In fact it follows by induction from the general

Theorem 10.2 *Let R be a Noetherian ring. Then* $\dim(R[t]) = 1 + \dim(R)$.

It's easy to see that $\dim(R[t]) > \dim(R)$ if the latter is finite (Ex. sheet). Before proving the reverse direction, we will take a detour suggested by Definition (2).

Height of a prime ideal

The *height* $h(P)$ of a prime ideal P is the supremum of the lengths of chains of prime ideals contained in P; that is, $h(P) = n$ if there is a chain (9) with $P_n = P$, and n is as big as possible (as usual, we set $h(P) = \infty$ if there is no biggest such n).

Thus

$$\begin{aligned}\dim(R) &= \sup\left\{h(P) \mid P \underset{\text{pr}}{\lhd} R\right\} \\ &= \sup\left\{h(M) \mid M \underset{\max}{\lhd} R\right\}.\end{aligned}$$

Now to determine $h(P)$ we only need to consider prime ideals contained in P. To do this, we can simplify the ring R by localizing at P.

Assume for now that R is an integral domain. Fix a prime ideal P of R. By the remark above, the local ring R_P has exactly one maximal ideal, namely PR_P, and

$$h(P) = h(PR_P) = \dim(R_P).$$

Recall also that *R_P is Noetherian if R is Noetherian.*

Recall that a *minimal prime* of an ideal I is a prime ideal P minimal w.r.t. $P \supseteq I$.

Lemma 10.3 *Let R be a Noetherian local ring with maximal ideal P. Let I be a proper ideal of R. The following are equivalent:*
(a) P is a minimal prime of I;
(b) $P = \mathrm{rad}(I)$;
(c) $P^q \subseteq I$ for some $q \in \mathbb{N}$.

Proof. Recall that $\mathrm{rad}(I)$ is the intersection of the minimal primes of I. As every prime ideal is contained in the unique maximal ideal P, if P is a minimal prime of I then P is in fact the only minimal prime of I, so (a) implies (b) We know that $\mathrm{rad}(I)/I$ is nilpotent as long as R is Noetherian, so (b) implies (c). If (c) holds and $Q \geq I$ for some prime ideal Q then $Q \geq P$, so $Q = P$ as P is maximal. Thus (a) holds. ■

Length of a module

Let M be an R-module. We say that M has *length* $\lambda(M) = n$ if there is a chain of submodules

$$M = M_0 > M_1 > \cdots > M_n = 0,$$

and n is as big as possible, $\lambda(M) = \infty$ if there is no biggest such n. (For example $\lambda(V) = \dim V$ if V is a vector space over a field).

Lemma 10.4 *If N is a submodule of M then $\lambda(M) = \lambda(N) + \lambda(M/N)$.*

Proof. Ex. Sheet. ■

Modules don't usually have finite length. But:

Lemma 10.5 *Let M be a Noetherian R-module. Suppose that $MP^k = 0$ for some maximal ideal P of R. Then $\lambda(M)$ is finite.*

Proof. Consider $V_i = MP^{i-1}/MP^i$. Since $V_iP = 0$, V_i is a vector space over the field $F = R/P$, and the R-submodules of V_i are exactly its F-subspaces. So $\lambda(MP^{i-1}/MP^i) = \dim_F(V_i) < \infty$ since V_i is finitely generated as an R-module, hence also as a vector space over F. The result now follows from the preceding lemma. ■

The 'Principal Ideal Theorem'

Theorem 10.6 ('Krull's Principal Ideal Theorem') *Let R be a Noetherian ring and let $a \in R$. If $aR \neq R$ and P is a minimal prime of aR then $h(P) \leq 1$.*

Proof. We start with some reductions. Suppose $h(P) > 1$. Then there exist prime ideals $P_0 < P_1 < P$. In the integral domain $\overline{R} = R/P_0$, the prime ideal $\overline{P} = P/P_0$ has height at least 2, and is a minimal prime of $\overline{a}\overline{R}$. So replacing R by $\overline{R}$ we may as well assume that R is an integral domain.

Now we can embed R in the local ring R_P. The correspondence between primes of R contained in P and primes of R_P shows (a) that PR_P is a minimal prime of aR_P, and (b) that $h(P) = h(R_P)$. So we may replace R by PR_P, and so assume that R *is a local integral domain with unique maximal ideal* P.

Now Lemma 10.3 shows that

$$P^k \leq aR$$

for some k. If $a = 0$ then $P = 0$ has height 0 and we are done; so we may suppose that $a \neq 0$.

Now suppose we have $0 < P_1 \leq P$ for some prime ideal P_1. We will prove that $P_1 = P$. Choose $b \in P_1$ with $b \neq 0$, and set $B = bR$. Note that then $B \leq P_1$.

We apply the Artin-Rees Lemma to the pair of R-modules $B \leq R$ and the ideal aR. This shows that for some positive integer q,

$$a^{q+1}R \cap B \leq Ba.$$

Then putting $D = a^qR \cap B$ we have

$$a^{q+1}R \cap B = a^{q+1}R \cap Ba = Da,$$

since R is an integral domain and $a \neq 0$.

Now $Da \leq D \leq B$ and $Da \leq Ba \leq B$. Also $BP^k \leq Ba$ and $BP^{qk} \leq Ba^q \leq D$. So by Lemma 10.5 both B/Ba and B/D have finite length. We also have

$$\frac{B}{Ba} = \frac{bR}{baR} \cong \frac{R}{aR} \cong \frac{a^qR}{a^{q+1}R},$$
$$\frac{B}{D} \cong \frac{Ba}{Da};$$

these isomorphisms are induced by multiplication by the non-zero elements b, a^q and a respectively.

It follows that Ba/Da has finite length, and we have

$$\begin{aligned}\lambda(B/Ba) + \lambda(Ba/Da) &= \lambda(B/Da) \\ &= \lambda(B/D) + \lambda(D/Da) \\ &= \lambda(Ba/Da) + \lambda(D/Da).\end{aligned}$$

Thus $\lambda(R/aR) = \lambda(B/Ba) = \lambda(D/Da)$.

But

$$\frac{D}{Da} = \frac{a^q R \cap B}{a^{q+1} R \cap B} \cong \frac{(a^q R \cap B) + a^{q+1} R}{a^{q+1} R} \leq \frac{a^q R}{a^{q+1} R} \cong \frac{R}{aR}.$$

As the two outer modules have the same, finite, length, this now implies that

$$(a^q R \cap B) + a^{q+1} R = a^q R.$$

Therefore

$$a^q = c + a^{q+1} r$$

for some $c \in B$ and $r \in R$. Then $a^q(1 - ar) = c \in B \leq P_1$. But $1 - ar \notin P_1$ since $a \in P$ and $P_1 \leq P$, consequently $a \in P_1$. Thus $aR \leq P_1 \leq P$ as; as P is minimal over aR we conclude that $P_1 = P$, as claimed. ■

This looks like a rather technical result. But we will get a lot of mileage out of it.

Theorem 10.7 *Let R be a Noetherian ring and let I be a proper ideal of R. If P is a minimal prime of I and I can be generated by d elements then $h(P) \leq d$.*

Proof. As in the preceding proof, we immediately reduce to the case where R is a local ring with unique maximal ideal P. Then $P = \mathrm{rad}(I)$. Now we argue by induction on d. If $d \leq 1$ the result is just the PIT. Assuming that $h(P) > d \geq 2$, we aim to derive a contradiction.

Say $I = \sum_{i=1}^{d} a_i R$. Since $h(P) > d$ there exists a prime ideal $P_1 < P$ with $h(P_1) \geq d$. We choose P_1 to contain as many as possible of $a_1, \ldots, a_d$. Of course P_1 can't contain all of them because P is minimal over $\sum_{i=1}^{d} a_i R$; wlog we suppose that $a := a_d \notin P_1$. Then P is minimal over $P_1 + aR$, since if $P_1 + aR \leq Q < P$ we could replace P_1 by Q, which contains more of the a_i. Therefore $P = \mathrm{rad}(P_1 + aR)$.

Hence for some $q \in \mathbb{N}$ we have $a_i^q \in P_1 + aR$ $(i = 1, \ldots, d-1)$. Thus

$$a_i^q = b_i + ar_i$$

with $b_i \in P_1$ and $r_i \in R$. Put $J = \sum_{i=1}^{d-1} b_i R$. Applying the inductive hypothesis, we infer from $h(P_1) \geq d$ that P_1 is *not* minimal over J; so $P_1 > Q \geq J$ for some prime ideal Q.

Now the ideal $J + aR$ contains a and a_i^q for $i = 1, \ldots, d-1$, so $I \subseteq \mathrm{rad}(J + aR)$. It follows that $P = \mathrm{rad}(I) \leq \mathrm{rad}(J + aR) \leq \mathrm{rad}(Q + aR)$, and hence that P is a minimal prime of $Q + aR$. Therefore P/Q is a minimal prime of $(Q + aR)/Q$.

Now the PIT shows that $h(P/Q) \leq 1$. But we have $P/Q > P_1/Q > Q/Q = 0$, the desired contradiction. ■

Corollary 10.8 *Every prime ideal of R has finite height.*

Proof. Each prime ideal is a minimal prime of itself, and is finitely generated because R is Noetherian. ■

Remark This does *not* imply that $\dim(R)$ is finite! (See ex. sheet 4.)

Corollary 10.9 *Let P be a prime ideal of R, with $h(P) = d$. Then there exist $a_1, \ldots, a_d \in P$ such that P is a minimal prime of $\sum_{i=1}^{d} a_i R$.*

Proof. If $d = 0$ then P is a minimal prime of 0. Suppose that $d \geq 1$. We will recursively find $a_1, a_2, \ldots \in P$ such that every minimal prime of the ideal $A_i = \sum_{j=1}^{i} a_j R$ has height i.

Suppose this holds for $i = d$. Then $A_d \leq Q \leq P$ for some minimal prime Q of A_d; if $Q < P$ then $d = h(P) > h(Q) = d$, contradiction; so $P = Q$ is indeed minimal over A_d.

The construction goes like this. Start with $A_0 = 0$. Let $0 \leq i < d$ and suppose we have found A_i. Let $Q_1, \ldots, Q_k$ be the minimal primes of A_i, each supposed to have height i. Then $P \not\subseteq Q_j$ for each j, since $i < d$. It follows that $P \not\subseteq \bigcup_{j=1}^{k} Q_j$ (Ex. Sheet 1). Let $a_{i+1} \in P \setminus \bigcup_{j=1}^{k} Q_j$. We have to show that if Q is any minimal prime of A_{i+1} then $h(Q) = i + 1$. Certainly $h(Q) \leq i + 1$, by Theorem 10.7. On the other hand, Q contains Q_j for some j and $a_{i+1} \in Q \setminus Q_j$, so $Q > Q_j$. Therefore $h(Q) \geq 1 + h(Q_j) = 1 + i$. This completes the proof. ∎

Theorem 10.10 *Let R be a Noetherian ring and $a \in R$.*

(i) If a is neither a zero-divisor nor a unit then $\dim(R/aR) \leq \dim(R) - 1$.
(ii) If Q is a prime ideal of R and $a \in Q$ then $h(Q) \leq \dim(R/aR) + 1$.
(iii) If R is local and a is neither a zero-divisor nor a unit then $\dim(R) = \dim(R/aR) + 1$.

Proof. Write $- : R \to R/aR = \overline{R}$ for the quotient map.

(i) Suppose $\overline{P_0} < \overline{P_1} < \cdots < \overline{P_m} = \overline{P}$ is a chain of primes in $\overline{R}$, with each P_i a prime ideal of R containing aR (of course, every prime of $\overline{R}$ is of the form $\overline{Q}$ for some prime Q of R containing aR). As a is not a zero-divisor and $a \in P_0$ it follows that P_0 is not a minimal prime ideal of R. So $P_0 > Q$ for some prime ideal Q, whence $m + 1 \leq h(P) \leq \dim(R)$. Hence $\dim(\overline{R}) + 1 \leq \dim(R)$.

(ii) Put $n = h(\overline{Q})$. By the preceding Corollary, there exist $\overline{a_1}, \ldots, \overline{a_n} \in \overline{Q}$ such that $\overline{Q}$ is a minimal prime of $\sum_{i=1}^{n} \overline{a_i}\overline{R}$. Then Q is a minimal prime of $aR + \sum_{i=1}^{n} a_i R$, and so by Theorem 10.7

$$h(Q) \leq n + 1 \leq \dim(R/aR) + 1.$$

(iii) If R is local we take Q to be the unique maximal ideal. Then $a \in Q$ since $aR \neq R$ and the result follows from (i) and (ii) since now $\dim(R) = h(Q)$. ∎

Remark Part (iii) is not always true if R is not assumed to be a local ring. But it is OK in the special case where $R = R_1[t]$ and $a = t$: this is the content of Theorem 10.2.

Now we can complete the

Proof of Theorem 10.2. R is a Noetherian ring, and we have to show that $\dim(R[t]) = 1 + \dim(R)$. Since $R[t]/tR \cong R$, part (i) of Theorem 10.10 shows that $\dim(R[t]) \geq 1 + \dim(R)$.

For the reverse inequality, let M be a maximal ideal of $S = R[t]$. We have to show that $h(M) \leq 1 + \dim(R)$.

First we reduce to the case where R is an integral domain: we have $h(M) = h(M/P_0)$ for some minimal prime ideal P_0 of S. Now $R[t]/(P_0 \cap R)R[t] \cong (R/(P_0 \cap R))[t]$ is an integral domain, so $(P_0 \cap R)R[t]$ is prime and hence equal to P_0. Thus $S/P_0 \cong (R/(P_0 \cap R))[t]$, and replacing R by $R/(P_0 \cap R)$ we may suppose that R is an integral domain.

Next, let $Y = R \setminus (M \cap R)$. By Proposition 8.1, we have inclusion-preserving bijections between the sets

- prime ideals of SY^{-1} and prime ideals of S not meeting Y;
- prime ideals of RY^{-1} and prime ideals of R not meeting Y,

given by $P \longmapsto P \cap S$, respectively $P \longmapsto P \cap R$. It follows that (a) $h(M) = h(MY^{-1})$, (b) $MY^{-1} \cap RY^{-1}$ is a maximal ideal in RY^{-1}, and (c) $\dim(RY^{-1}) \leq \dim(R)$. Replacing R by its localization RY^{-1} and S by $SY^{-1} = RY^{-1}[t]$, we may therefore suppose that $M \cap R$ is a maximal ideal of R and every element of $R \setminus (M \cap R)$ is invertible in R.

In view of Theorem 10.10(ii), it will suffice to find an element $a \in M$ such that $\dim(S/aS) \leq \dim(R)$.

If $t \in M$ we take $a = t$ and have $S/aS \cong R$. If $t \notin M$ then $M + tS = S$ so $1 - tf(t) \in M$ for some $f(t) \in S$, and clearly $f(t) \neq 0$. Choosing f of minimal degree we have

$$b := c_n t^n + \cdots + c_1 t - 1 \in M$$

where $n \geq 1$ and $c_n \notin M$, so c_n is invertible. Now let $a = c_n^{-1} b = g(t)$, say. Then $a \in M$, and

$$\frac{S}{aS} = \overline{R}[\tau]$$

where $\overline{R} = (R + aS)/aS$ (isomorphic to R in fact, but no matter), and $\tau = t + aS$ satisfies $g(\tau) = 0$. Thus S/aS is integral over $\overline{R}$, whence $\dim(S/aS) \leq \dim(\overline{R}) \leq \dim(R)$.

■

Now if F is a field then $\dim(F) = 0$. Arguing by induction on n we infer

Theorem 10.11 $\dim(F[t_1, \ldots, t_n]) = n$.

So we see that the *affine n-space* F^n – the vector space considered as an algebraic set – does indeed have dimension n as an algebraic set.

Transcendental dimension

Proposition 10.12 *Let $E \supseteq F$ be fields. Let X and Y be algebraically independent subsets of E such that E is algebraic over $F(X)$. If X is finite then so is Y and $|Y| \leq |X|$.*

Proof. We may suppose that $|Y| \geq |X|$. Say $X = \{x_1, \ldots, x_d\}$, and let $y = y_1 \in Y$. Then y satisfies a monic polynomial equation over $F(X)$, and clearing denominators we get an equation

$$f_0(x_1, \ldots, x_d)y^n + \cdots + f_n(x_1, \ldots, x_d) = 0;$$

here each f_i is a polynomial over F, and at least one of the f_i is not constant since y is not algebraic over F. Say x_1 occurs with positive degree in f_i. Then the equation can be rewritten as

$$g_0(y, x_2, \ldots, x_d)x_1^m + \cdots + g_m(y, x_2, \ldots, x_d) = 0$$

where $g_0 \neq 0$. Thus x_1 is algebraic over $F(y, x_2, \ldots, x_d)$, and it follows that E is algebraic over $F(y_1, x_2, \ldots, x_d)$.

Suppose $y_1, \ldots, y_e$ are distinct elements of Y where $e \leq d$, and we have shown that after relabelling the x_i in a suitable order, E is algebraic over $F(y_1, y_2, \ldots, y_{e-1}, x_e, \ldots, x_d)$. Then y_e is algebraic over this field, but not algebraic over $F(y_1, y_2, \ldots, y_{e-1})$; arguing as above, we deduce that one of the x_j with $j \geq e$ is algebraic over $F(y_1, y_2, \ldots, y_{e-1}, y_e, X^*)$ where $X^* = \{x_e, \ldots, x_d\} \setminus \{x_j\}$. Re-labelling the x's we may suppose that $j = e$, and so obtain: E is algebraic over $F(y_1, y_2, \ldots, y_e, x_{e+1}, \ldots, x_d)$.

It follows by induction that E is algebraic over $F(y_1, y_2, \ldots, y_d)$. In particular every element of Y is algebraic over $F(y_1, y_2, \ldots, y_d)$, and as Y is algebraically independent this implies that $Y = \{y_1, y_2, \ldots, y_d\}$. ■

Let E be an extension field of a field F. A subset X of E is a *transcendence basis* for E over F if (i) X is algebraically independent over F and (ii) E is algebraic over $F(X)$. Proposition 10.12 shows that if E has a finite transcendence basis X, then every transcendence basis has the same cardinality $|X|$. This cardinality is called the *transcendence degree* of E over F, and is denoted $td(E/F)$. (In general field theory it's usual to consider possibly infinite subsets and define $td(E/F)$ to be a possibly infinite cardinal; this need not concern us.)

If R is an integral domain and an F-algebra, then $td(R/F)$ is defined to be $td(E/F)$ where E is the field of fractions of R.

Exercise: If it's finite, then $td(R/F)$ is the size of any maximal algebraically independent (over F) subset of R.

Theorem 10.13 *Let R be an integral domain and a finitely generated F-algebra. Then $td(R/F) = \dim(R) < \infty$.*

Proof. By Noether's Normalization Lemma, R is integral over a subring $S = F[x_1, \ldots, x_d]$ where $x_1, \ldots, x_d$ are algebraically independent over F. Then $S \cong F[t_1, \ldots, t_d]$, and the preceding Theorem gives $d = \dim(S)$. Now $\dim(R) = \dim(S)$ by Theorem 10.1.

Finally, $d = td(R/F)$ because $\{x_1, \ldots, x_d\}$ is a maximal algebraically independent subset of R. ■

In terms of algebraic geometry, this can be interpreted as follows. Let $V \subseteq F^n$ be an algebraic set. An element $x = f(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ defines a function $e_x : V \to F$ by evaluation, and $e_x = e_y$ precisely when $x - y \in \mathcal{I}(V) = I$; so for $\overline{x} \in F[t_1, \ldots, t_n]/I = R$ we can define a function $e_{\overline{x}}$ on V by $e_{\overline{x}} = e_x$ where $\overline{x} = xI$. In this way, R can be thought of as the ring of polynomial functions on V (it is also called the *co-ordinate ring* of V, since it is generated by the co-ordinate functions $e_{\overline{t_i}}$).

Now the theorem says: if V is irreducible, then $\dim(V)$ is equal to the maximal number of independent polynomial functions defined on V – and it tells us what we should mean by 'independent' in this context.

11 Appendix: Zorn's Lemma

This is a set-theoretic principle: it is a form of the Axiom of Choice that is particularly convenient for application in algebra. In order to prove various general existence statements about rings and modules we just have to accept it as an axiom. In many of our results, we can use the Noetherian hypothesis instead.

Let S be a non-empty *partially ordered* set: a set with a binary relation $\leq$ that is reflexive, transitive and satisfies $a = b \iff (a \leq b \text{ and } b \leq a)$.

If $a \in T \subseteq S$ then a is said to be 'maximal in T' if

$$\forall b \in T.\ (a \leq b \Longrightarrow b = a).$$

An element $c \in S$ is an *upper bound* for T if

$$\forall b \in T.\ b \leq c.$$

A subset T of S is a *chain* if T is totally ordered by $\leq$, i.e.

$$\forall x, y \in T.\ (x \leq y \text{ or } y \leq x).$$

The partially ordered set $(S, \geq)$ is said to be *inductively ordered* if *every chain in S has an upper bound in S.*

Zorn's Lemma *If S is inductively ordered then S has a maximal element.*

This is often applied to the case where S is a collection of subsets of some set X, and $a \leq b$ means $a \subseteq b$. In this case, we can sometimes verify that S is inductively ordered by checking that the union of a chain in S still belongs to S. Typical example: S is the set of ideals I in a ring R such that $I \cap Y = \varnothing$, where Y is some given non-empty subset of R. Taking $Y = \{1\}$ for example shows that maximal (i.e. maximal proper) ideals exist.