B2.2: Commutative Algebra

Nikolay Nikolov

Hilary term, 2018

All rings in this course will be assumed commutative and containing an identity element. For a ring R we denote by $R[t_1, \dots, t_k]$ the polynomial ring in indeterminates t_i with coefficients in R. A subset S of R is said to be *multiplicatively closed* if $1 \in S$ and whenever $x, y \in S$ then $xy \in S$.

Zorn's Lemma

A partial order $\leq$ on a set X is a reflexive transitive relation such that $a \leq b$ and $b \leq a$ implies $a = b$.

A chain C in a partially ordered set X is a subset $C \subseteq X$ which is totally ordered, i.e. for any $x, y \in C$ we have $a \leq b$ or $b \leq a$. 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 1 (Zorn's Lemma) *Let $(X, \leq)$ be a 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 unital ring R: Let X be the set of all ideals of R different from 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 the lemma is satisfied. Therefore X has maximal elements, i.e. maximal ideals.

1 Introduction

Commutative algebra has developed under the unfluence of two major subjects: Algebraic Number Theory and Algebraic Geometry.

Recall that an ideal I of a ring R is prime if R/I is a domain, or equivalently whenever the complement $R \backslash I$ is multiplicatively closed.

The main object of study in Algebraic Number theory is the ring of integers $\mathcal{O}$ of a finite extension field K of $\mathbb{Q}$. The ring $\mathcal{O}$ is an example of a Dedekind domain: all nonzero prime ideals are maximal (in fact of finite index in $\mathcal{O}$), and moreover every ideal of $\mathcal{O}$ has a unique factorization into a product of prime ideals.

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

Let $Y \subseteq R$ be a collection of polynomials from R and define

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

This is just the subset in F^k 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.

Definition 2 *A set $U \subseteq F^k$ 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).*

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

Definition 3 *Let $Z \subseteq F^k$ be any subset. Define*

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

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 4 *For ideals $I \subseteq I' \subseteq R$ and subsets $Z \subseteq Z' \subseteq F^k$ we have*

(1) $\mathcal{V}(\mathcal{I}(Z)) \supseteq Z$, moreover there is equality if Z is an algebraic set.

(2) $\mathcal{I}(\mathcal{V}(I)) \supseteq I$,

(3) $\mathcal{V}(I) \supseteq \mathcal{V}(I')$,

(4) $\mathcal{I}(Z) \supseteq \mathcal{I}(Z')$.

Proof. Exercise.

The above proposition shows that $\mathcal{I}$ and $\mathcal{V}$ are order reversion maps between the set of ideals of R and the algebraic subsets of F^k. Moreover (1) shows that $\mathcal{V}$ is surjective while $\mathcal{I}$ 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.

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 5 *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. $\square$

Definition 6 *An R-module M is said to be Noetherian if it satisfies any of the three equivalent conditions of Lemma 5.*

Proposition 7 *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 8 *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 9 *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 10 *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 clearly M is finitely generated as a module. Conversely, soppose 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 11 (Hilbert's Basis Theorem) *Let R be a Noetherian ring. Then the polynomial ring $R[t]$ is Noetherian.*

Let $A \leq B$ be two rings. We say that B is finitely generated as A-algebra (or that B is finitely generated as a ring over A) if there exists elements $b_1, \dots, b_k \in B$ such that $B = A[b_1, \dots, b_k]$ meaning that B is the smallest ring containing A and all b_i. 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.

Corollary 12 *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 $R[t_1, \dots, t_k]$ and with Theorem 11 and induction on k we deduce that $R[t_1, \dots, t_k]$ is a Noetherian ring. Therefore S is a Noetherian ring.

In particular this implies that the polynomial ring $F[t_1, \dots, t_k]$ is a Noetherian ring for any field F. This has the following central application to algebraic geometry.

Corollary 13 *Let $X \subseteq F[t_1, \dots, t_k]$ be any subset. Then there is a finite subset $Y \subseteq X$ such that $\mathcal{V}(X) = \mathcal{V}(Y)$.*

Proof. Let $I = \langle X \rangle$ be the ideal generated by X in $R = F[t_1, \dots, t_k]$. Since R is a Noetherian ring the ideal I is finitely generated and hence $I = \langle Y \rangle$ for some finite subset Y of X. Then $\mathcal{V}(X) = \mathcal{V}(Y)$. $\square$

Proof of Theorem 11.

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 ideal of R generated by all leading coefficients of all non-zero polynomials in I. Then M is finitely generated ideal and hence there are some polynomials $p_1, \dots, p_k \in I$ such that p_i has leading coefficient c_i and $M = \sum_i Rc_i$. Let $N = \max\{\deg p_i \mid 1 \leq i \leq k\}$ and let $K = I \cap \big(R \oplus Rt \oplus \cdots \oplus Rt^N\big)$. Note that K is an R-submodule of the Noetherian R-module R^N and hence 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 the converse. 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 finitely generated ideal of $R[t]$. Therefore $R[t]$ is a Noetherian ring. $\square$

3 The Nilradical

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

Theorem 14 *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 X be the set of bad ideals and since R is Noetherian there is a maximal element of X, 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 an 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. $\square$

Let I be any ideal of a Noetherian ring R. By appying the above theorem to the quotient ring R/I we deduce that there is a finite collection $\{P_1, \ldots, P_n\}$ of prime ideals P_i of R which are minimal subject to $I \subseteq P_i$. We will refer to $\{P_1, \ldots, P_n\}$ as the *minimal primes of the ideal I*.

An element $x \in R$ is nilpotent if $x^n = 0$ for some n. An ideal I is said to be nilpotent if $I^n = 0$ for some $n \in \mathbb{N}$.

The set $\{x \in R |\ x \text{ nilpotent}\}$ of all nilpotent elements of R is an ideal of R (exercise).

Definition 15 *The nilradical of a ring R denoted by* $\mathrm{nilrad}(R)$ *is the set of all nilpotent elements of R.*

The nilradical may not be nilpotent: consider the ideal generated by $t_1, t_2, \ldots$ in the ring $\bigoplus_{k=1}^{\infty} \mathbb{R}[t_k]/(t_k)^k$. However

Proposition 16 *Let I be an ideal of a ring R consisting of nilpotent elements (such ideal is called a nil ideal). Suppose that I is finitely generated as an ideal. Then I is nilpotent.*

Proof. Let $x_i \in I$ such that $I = \langle x_1, \ldots, x_k \rangle = Rx_1 + Rx_2 + \cdots Rx_k$. Let $x_i^{n_i} = 0$ for some integers $n_i \in \mathbb{N}$ and take $m = n_1 + \cdots n_k$. Now

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

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 $I^n = 0$.

Corollary 17 *The nilradical of a Noetherian ring is nilpotent.*

There is another very useful characterization of the nilradical.

Theorem 18 (Krull's theorem) *For any ring R,* $\mathrm{nilrad}(R)$ *is the intersection of all prime ideals of R.*

Proof. 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 $\mathrm{nilrad}(R) \subseteq X := \cap\{P \mid P \text{ prime ideal of } R\}$. 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 problem sheet 1 Q1 there is a prime ideal P such that $P \cap S = \emptyset$. So $x \notin X$. Thus $X \subseteq \mathrm{nilrad}(R)$ and so $\mathrm{nilrad}(R) = X$.

Definition 19 *Let I be an ideal of R. The radical of I is defined to be*

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

So by definition $\mathrm{rad}(I)/I = \mathrm{nilrad}(R/I)$ from where we see by Theorem 18 the first part of the following.

Corollary 20 *Let I be an ideal of a ring R. Then*

(1) $\mathrm{rad}(I) = \cap\{P \mid P$ *prime ideal of* R *with* $I \subseteq P\}$

(2) If R is Noetherian then $\mathrm{rad}(I) = P_1 \cap \cdots \cap P_k$ *for some prime ideals P_i of R. There exists some $n \in \mathbb{N}$ such that* $\mathrm{rad}(I)^n \subseteq I$.

Proof. It remains to prove (2). By considering R/I and applying Theorem 14 we deduce that there are finitely many prime ideals, say $P_1, \ldots, P_k$ minimal subject to $I \subseteq P_i$ and every prime ideal Q above I contains some P_i. It is now clear that $r(I) = P_1 \cap \cdots \cap P_k$. The last part follows from Corollary 17 applied to the nil ideal $r(I)/I$ of the Noetherian ring R/I.

3.1 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 21 *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) $\mathrm{rad}\, \mathcal{I}(Z) = \mathcal{I}(Z)$ *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 $W = \mathcal{V}(t_1 t_2)$ 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 22 *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 23 *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 $\mathcal{I}(W_i)$ is strictly larger than $\mathcal{I}(W)$ and we can take $f_i \in \mathcal{I}(W_i) \backslash \mathcal{I}(W)$. Then the polynomial $f_1 f_2$ vanishes on both W_1 and W_2 hence it vanishes on W and so $f_1 f_2 \in \mathcal{I}(W)$. 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 24 *Every algebraic set is a union of finitely many irreducible algebric sets.*

Proof. Problem sheet 2.

Suppose W is an algebraic set and $W = V_1 \cup \cdots \cup V_n$ where V_i are irreducible algebraic sets and n is minimal possible. Then $V_i \nsubseteq V_j$ for any i, j otherwise we may omit V_i from the union. 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 $\mathcal{I}(W)$. Since $V_i = \mathcal{V}(P_i)$ it follows that the irreducible sets V_i in the minimal decomposition $W = V_1 \cup \cdots \cup V_n$ are determined uniquely by W and we refer to them as the *irreducible components* of 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

We start with a technical result.

Proposition 25 *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.*

Proof. Suppose that $C = \sum_{i=1}^n B y_i$ 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 Theorem 11 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 $C = M$. So C is finitely generated as B_0-module and in particular C is a Noetherian B_0-module. Its submodule B is therefore also a Noetherian B_0-module and hence it is finitely generated as a B_0-module. In particular there are elements $l_s \in B$ such that $C = \sum_{s=1}^{r} B_0 l_i$. Then the set of all b_{ij}, b_{jkl}, l_s for all possible i, j, k, l, s generates B as an A-algebra. $\square$

4.1 Field extensions

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. The following is mostly part A material.

Proposition 26 *Let E/F be a field extension such that $E = F(x)$ for some element $x \in E$ (meaning that E is the smallest field containing F and x). The following are equivalent*

(1) E/F is a finite extension.

(2) x is algebraic over F.

(3) E is generated by x as an F-algebra.

(4) E is finitely generated as an F-algebra.

Proof. The equivalence of (1),(2) and (3) is part A material. Clearly(3) implies (4). It remains to prove that (4) implies (2).

Suppose 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 $g_i = p_i(x)/q_i(x)$, $i = 1, \ldots, k$ where $p_i, q_i \in F[x]$ are polynomials in x. Let $r(x) = \prod_{i=1}^{k} q_i$ and consider the element $a = 1/(xr(x) + 1) \in E$. Then

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

for some polynomial $f \in F[t_1, \ldots, t_k]$. By muliplying with appropriate power of r to clear the denominators on RHS we reach the equation $a = s(x)/r(x)^n$ for some $n \in \mathbb{N}$ and polynomial $s(x) \in F[x]$. Thus $r(x)^n = s(x)(xr(x) + 1)$ which is impossible since $xr(x) + 1$ is coprime to $r(x)^n$.

Theorem 27 (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 $E = F[x_1, \ldots, x_k]$ and argue by induction on k. The case $k = 1$ is the above Proposition 26. Assuming the result is true for $k - 1$ consider the sequence of fields $F \subseteq F' \subseteq E$ where $F' = F(x_1)$. We have that E is finitely generated as F'-algebra by $k-1$ elements and hence by the induction hypothesis E/F' is finite. So E is finitely generated as F'-module and by Propostion 25 F' is finitely generated as F-algebra. Now Proposition 26 gives that F'/F is finite and therefore $[E : F] = [E : F'][F' : F]$ is finite. $\square$

Corollary 28 *Let F be a field and let R be a finitely generated F-algebra. Let M be a maximal ideal of R. Then $\dim_F R/M$ is finite.*

Proof. R/M is a field which is finitely generated as F-algebra.

The next corollary describes the maximal ideals of polynomial rings over algebraically closed fields. First we need some notation.

Let F be a field and let $R = F[t_1, \ldots, t_k]$ be a polynomial ring. Let $\mathcal{M}$ denote the set of maximal ideals of R and define a map $\mu : F^k \to \mathcal{M}$ by

$$\mu(a_1, \ldots, a_k) := \sum_{i=1}^{k} R(t_i - a_i) = \langle t_1 - a_1, \ldots, t_k - a_k \rangle$$

It is easy to check that $\mu(a_1, \ldots, a_k) \in \mathcal{M}$ and that the map μ is injective.

Corollary 29 *Assume that the field F is algebraically closed. Then μ is bijective.*

Proof. It remains to show that μ is surjective. Let M be a maximal ideal of R. By Corollary 28 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 $\mu(a_1, \ldots, a_k) \subseteq M$ and hence $M = \mu(a_1, \ldots, a_k)$.

Corollary 30 *Let R be a polynomial ring over algebraically closed field F. Let I be an ideal of R. Then $\mathcal{V}(I) = \emptyset$ if and only if $I = R$. Moreover $\mathbf{a} \in F^k$ belongs to $\mathcal{V}(I)$ if and only if $I \subseteq \mu(\mathbf{a})$.*

Proof. If $R = I$ then $1 \in I$ and so $\mathcal{V}(I) = \emptyset$. Conversely if $I \neq R$ there is a maximal ideal $M \in \mathcal{M}$ such that $I \subseteq M$. By Corollary 29 $M = \mu(\mathbf{a})$ for some $\mathbf{a} \in F^k$. Notice that $\mathcal{I}\{\mathbf{a}\} = \mu(\mathbf{a})$. So if $f \in I$ then $f \in \mu(\mathbf{a})$ and hence $f(\mathbf{a}) = 0$. Thus $\mathbf{a} \in \mathcal{V}(I)$ and so $\mathcal{V}(I) \neq \emptyset$. The second part follows by the same argument. □

So the points of the algebraic set $\mathcal{V}(I)$ correspond to the maximal ideals of R which contain I.

It remains to identify $\mathcal{I}(\mathcal{V}(I))$.

Theorem 31 (The Nullstellensatz) *Let F be an algebraically closed field and let $R = F[t_1, \ldots, t_k]$. Let I be an ideal of R. 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 $zf - 1 = -1$ is not zero. Hence by Corollary 30 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 ramains 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. □

Corollary 32 *Let F and R be as in Theorem 31 and let I be an ideal of R. Then* $\mathrm{rad}(I)$ *is an intersection of maximal ideals of R.*

Proof. Let U be the intersection of all maximal ideals of R which contain I. Clearly $\mathrm{rad}(I) \subseteq U$ (since $\mathrm{rad}(I)$ is the intersection of all prime ideals of R which contain I).

Suppose now $f \notin \mathrm{rad}(I)$. By Theorem 31 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 $U \subseteq \mathrm{rad}(I)$ and so we have equality $U = \mathrm{rad}(I)$. $\square$

This leads us to the following definition.

Definition 33 *The Jacobson radical $J(R)$ of a ring R is defined to be the intersection of all maximal ideals of R.*

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

Definition 34 *A ring R is said to be a Jacobson ring if $J(R/I) = \mathrm{rad}(I)/I =$* $\mathrm{nilrad}(R/I)$ *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 32 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.

5 The Cayley-Hamilton Theorem, Nakayama's lemma

Theorem 35 *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 $a_1, \ldots, a_n \in I$ such that the module homomorphism*

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

as a map on M.

Proof. Let $x_1, \ldots, x_n \in M$ be generators of M, so $M = \sum_{i=1}^n Rx_i$. There exist $c_{i,j} \in I$ such that $\phi(x_i) = \sum_{j=1}^n c_{ji}x_j$. Let $C = (c_{i,j})$ and consider C as a matrix in $M_n(R[t])$. Let $p = p(t) = \det(t \cdot \mathbf{I}_n - C)$ be the characteristic polynomial of C and note that $p(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ where $a_i \in I$ since a_i is a polynomial in the coefficients $c_{i,j}$ of C. From the Cayley-Hamilton theorem in part A we have $p(C) = 0$ and hence $p(\phi)$ is the zero map on M because ϕ acts as C on M.

Corollary 36 (Nakayama's Lemma) *Let M be a finitely generated R-module and let I be an ideal of R such that $M = IM$. Then there exists $x \in I$ such that $(1 + x)M = 0$.*

Proof. Take $\phi = \mathrm{Id}_M$ in Theorem 35. Then there exist $a_i \in I$ such that $(1 + a_1 + \cdots + a_n)M = 0$ and we can take $x = \sum_{i=1}^n a_i$.

The above corollary has an important special case (which is sometimes also stated as Nakayama's lemma).

Corollary 37 *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. Problem sheet 3.

Corollary 38 *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 37 to the module M/N. □

These results is particularly useful for local rings.

Definition 39 *A ring R is a local ring if R has a unique maximal ideal.*

It is clear that if R is a local ring with maximal ideal I then $I = J(R)$ is the Jacobson radical of R. We have that the elements of $R \backslash I$ are the units of R. The last corollary then implies that in order to generate a Noetherian module M over a local ring R is is sufficient to generate the quotient M/IM. In turn M/IM is a vector space over the field R/I and the problem of generating M reduces to linear algebra in M/IM.

6 Localization

Now we describe a technique which often helps to simplify arguments and reduce them to the case of local rings. Let R be a domain, that is a ring without zero divisors. Let Y be a multiplicativley closed subset of R which contains 1 and such that $0 \notin Y$. Let E be the field of fractions of R.

Definition 40 *We define*

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

For an ideal I of R we define $e(I) := SI = \{xy^{-1} \mid x \in I,\ y \in Y\}$.

It is easy to check that $S = Y^{-1}R$ is a ring and that $e(I)$ is an ideal of S.

For example when $R = \mathbb{Z}$ and $Y = \{2^k \mid k = 0, 1, 2 \ldots\}$ then $Y^{-1}R$ is the ring of rational numbers with denominators which are a power of 2. Now if $I = 3\mathbb{Z}$ then $e(I) = 3S = \{\frac{3n}{2^k} \mid n \in \mathbb{Z}, k = 0, 1, 2, \ldots\}$.

For an ideal J of S we define $c(J) := R \cap J$, this is an ideal of R, the *contraction* of the ideal J.

Let $\mathcal{R}$ and $\mathcal{S}$ denote the set of ideals of R and S respectively. We can regard $e : \mathcal{R} \to \mathcal{S}$ and $c : \mathcal{S} \to \mathcal{R}$ as maps between $\mathcal{R}$ and $\mathcal{S}$. Let $\mathcal{R}_c$ denote the set $\{J \cap R \mid J \in \mathcal{S}\}$, the image of the contraction map c.

Proposition 41

(1) The maps c and e are mutually inverse bijections between $\mathcal{S}$ and $\mathcal{R}_c$. Both c and e respect inclusion and intersection of ideals. In addition e respects sums of ideals.

(2) The prime ideals in R_c are precisely the prime ideals P of R such that $P \cap Y = \emptyset$.

(3) e maps prime ideals from $\mathcal{R}_c$ to prime ideals of S, c maps prime ideals of S to prime ideals of R.

Proof. Part (1) is an easy exercise. For part (2), suppose $P = c(J)$ is a contracted prime ideal of R. If $y \in P \cap Y$ then $y \in J$ but $y^{-1} \in S$ and so $1 \in J$, giving $J = S$ and $P = R \cap S = R$ contradiction. So $P \cap Y = \emptyset$. Conversely if P is a prime ideal of R such that $P \cap Y = \emptyset$ then let $J = e(P)$ and consider $c(J) = P \cap J$. Clearly $P \subseteq c(J)$. Suppose $x \in c(J)$, thus $x \in R$

and $x = py^{-1}$ for some $p \in P$ and $y \in Y$. Hence $p = xy$ with $y \notin P$, hence $x \in P$ because P is prime. Therefore $P = c(J) = ce(P)$ proving (2).

For part (3): If J is a prime ideal of S then $c(J) = J \cap R$ is a prime ideal of R.

Now suppose P is a prime ideal of R with $P \cap Y = \emptyset$. We want to show that $e(P) = SP = Y^{-1}P$ is a prime ideal of S. Suppose $r_1, r_2 \in R$, $y_1, y_2 \in Y$ with $(r_1 y_1^{-1})(r_2 y_2^{-1}) \in e(P)$. Hence $r_1 r_2 (y_1 y_2)^{-1} = py^{-1}$ for some $p \in P, y \in Y$. This gives $y_1 y_2 p = y r_1 r_2 \in P$ and then either $r_1 \in P$ or $r_2 \in P$ since P is prime and $y \notin P$. Hence either $r_1/y_1 \in e(P)$ or $r_2/e_2 \in e(P)$. Therefore $e(P)$ is a prime ideal. $\square$

Corollary 42 *Suppose $Y = R \backslash P$ for some prime ideal P of R. Let $S := Y^{-1}R$. Then S has precisely one maximal ideal, namely $e(P) = SP$. The prime ideals of S correspond bijectively via c to the prime ideals of R contained in P.*

Proof. Let M be a maximal ideal of S. Now $M = ec(M)$ and $c(M) = R \cap M$ is a prime ideal of R disjoint from Y, hence $c(M) \subseteq P$. Thus $M = ec(M) \subseteq e(P)$ and by maximality $M = e(P)$. So $e(P)$ is the unique maximal ideal of S. The rest of the claims follow from Proposition 41 (2) and (3).

Corollary 43 *If R is Noetherian then $S = Y^{-1}R$ is also Noetherian.*

Proof. A strictly ascending chain of ideals in $\mathcal{S}$ contracts to a strictly ascending chain of ideals in $\mathcal{R}_c$. $\square$

Definition 44 *When P is a prime ideal of R and $Y = R \backslash P$ we write R_P for $Y^{-1}R$ and call this the* localization *of R at P. By Corollary 42 R_P is a local ring whose prime ideals correspond bijectively to the prime ideals of R contained in P.*

For example when $R = \mathbb{Z}$ and $P = 2\mathbb{Z}$ then $\mathbb{Z}_{2\mathbb{Z}}$ is the ring of rational numbers with odd denominators which has a unique maximal ideal $2\mathbb{Z}_{2\mathbb{Z}}$.

Proposition 45 *Let I and J be ideals in a domain R. Suppose that $IR_M \subseteq JR_M$ for each maximal ideal M of M. Then $I \subseteq J$.*

Proof. 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 there is some maximal ideal M of R with $L \subseteq M$. Now $a \in IR_M \subseteq JR_M$ and so $a = xy^{-1}$ with $x \in J$ and $y \notin M$. But then $ay = x \in J$ and so $y \in L \subseteq M$, contradiction. Hence $I \subseteq J$. $\square$

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 46 *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*

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

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.

Proposition 47 *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 (1) 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 $a_n \in I \cap R$. $\square$

Proposition 48 *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 (1). 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 35 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. $\square$.

Definition 49 *The integral closure of R in S is the set of all elements of S which are integral over R.*

Corollary 50 *Let C be the integral closure of R in S. Then C is a subring of S.*

Proof. 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 48 now gives that $x+y$ and $xy \in C$. □

Proposition 51 *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 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Let $S' := R[a_1, \ldots, a_n] \subseteq S$. Since each a_i is integral over R the argument of Proposition 48 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 48 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 52 *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 $x \in S \backslash \{0\}$ and let

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

with $a_i \in R$ and n minimal possible. Then $a_n \neq 0$ and we can rewrite the above equation as $xy = -a_n$ where $y = x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1} \in S$. Since R is a field the element a_n is invertible in R and thus $-y a_n^{-1}$ is an inverse for x in S. So 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 (1) 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. $\square$

Proposition 53 *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. Choose an ideal P of S maximal subject to the condition $P \cap Y = \emptyset$, such an ideal P exists by Zorn's Lemma. 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 47 we must have that P_2/P_1 is the zero ideal, hence $P_1 = P_2$. $\square$

Theorem 54 *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 Proposition 53. 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 $P_1 \cap R = Q_1$ then 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 Proposition 53 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 54 and Proposition 53 (b) together give the following.

Corollary 55 *Let $R \subseteq S$ be an integral extension. A strictly increasing chain of prime ideals of S intersects R in a strictly increasing chain of prime ideals of R. 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 56 *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*

$$\emptyset \neq V_n \subset V_{n-1} \subset \cdots \subset V_0 = V \tag{2}$$

of irreducible algebraic sets V_i*.*

More generally when V *is reducible 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 (2). 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 57 *Let* R *be a ring. The Krull dimension of* R *denoted by* $\dim R$ *is the largest* n *such that there is a chain*

$$P_0 \subset P_1 \subset \cdots \subset P_n \tag{3}$$

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

So we see that for an algebraic set $V \subseteq F^k$ we have $\dim V = \dim R/\mathcal{I}(V)$ where $R = F[t_1, \ldots, t_k]$.

Corollary 55 now implies the following.

Proposition 58 *Let* $R \subseteq S$ *be an integral extension. Then* $\dim R = \dim S$*.*

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

Definition 59 *Let* P *be a prime ideal of a ring* R*. The height,* $ht(P)$ *of* P *is defined to be the largest integer* n *such that there is chain*

$$P_0 \subset \cdots \subset P_n = P$$

of prime ideals P_i *terminating at* P*.*

So $\dim R$ is the maximum of the heights of its prime ideals. It turns out that $ht(P) < \infty$ for every prime ideal P of a Noetherian ring R but we won't prove this here.

Our next aim is 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 60 *Let $F \subseteq E$ be a field extension. Elements $x_1, \dots x_k \in E$ are said to be algebraically dependent over F if there is a non-zero polynomial $f \in F[t_1, \dots, t_k]$ such that $f(x_1, \dots, x_k) = 0$.*

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

Definition 61 *With $F \subseteq E$ as above the set $X := \{x_1, \dots, x_n\}$ 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 $E = F(c_1, \dots, c_m)$ is finitely generated as a field over F then there is a finite subset $X \subseteq \{c_1, \dots, c_m\}$ which is a transcendence basis for E/F. What needs proving is the analogue of fundamental property of bases of a vector space:

Proposition 62 *Any two transcendence bases for E over F have the same size.*

Proof. Let $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_m\}$ be two transcendence bases for E over F. Suppose that $m > n$.

By the maximality of X we have that E is algebraic over $L := F(x_1, \dots, x_n)$ and therefore there is a non-zero polynomial $f \in F[t_1, \dots, t_{n+1}]$, such that $f(x_1, \dots, x_n, y_1) = 0$. We can further assume that f has as small degree as possible. Now $f \notin F[t_{n+1}]$, because y_1 is transcendental over F. Hence there is some t_j with $j \leq n$, say t_1, which appears in a nonzero monomial of f. Rewriting f as a polynomial in t_1 with coefficients in $F[t_2, \dots, t_{n+1}]$ gives that x_1 is algebraic over the subfield $L_1 := F(y_1, x_2, \dots, x_n)$. Hence L is algebraic over L_1 and E is algebraic over L, therefore E is algebraic extension of L_1.

Now y_2 is algebraic over L_1 and in the same way we deduce that there is some $x_j, j > 1$, for example x_2 such that x_2 is algebraic over $L_2 := F(y_1, y_2, x_3, \dots, x_n)$ and as a consequence E is algebraic over L_2. We can continue in the same way replacing each successive x_i with y_i until we reach the situation where E is algebraic over the subfield $L_n := F(y_1, \dots, y_n)$. But then y_{n+1} is algebraic over L_n which is contradiction to Y being transcendental over F. So $n \geq m$ and by exchanging the roles of X and Y we get $m \geq n$ and therefore $m = n$. $\Box$

Definition 63 *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, known as Noether's Normalization Lemma is very useful in simplifying many proofs by reducing them to polynomial rings.

Lemma 64 (Noether's Normailization Lemma) *Let $R = F[y_1, \ldots, y_n]$ be a finitely generated as an algebra over a subfield F. Assume that R is a domain. There exists an algebraically independent set $\{x_1, \ldots, x_k\} \subset R$ over F such that R is integral over $F[x_1, \ldots, x_k]$.*

Proof. We will prove the lemma in the case when the field F is infinite.

We argue by induction on n, the case $n = 0$ being trivially true. Suppose the lemma is true for $R[y_1, \ldots, y_{n-1}]$ and we can find $x_1, \ldots, x_s$, $(s \leq n-1)$, which are algebraically independent over F and such that $F[y_1, \ldots, y_{n-1}]$ is integral over $F[x_1, \ldots, x_s]$.

Suppose first that $x_1, \ldots, x_s, y_n$ are still algebraically independent. Take $k = s + 1$, $x_{s+1} = y_n$. Now $y_1, \ldots, y_n$ are integral over $F[x_1, \ldots, x_k]$ and we are done.

So we may assume that $f(x_1, \ldots, x_s, y_n) = 0$ for some nonzero polynomial $f \in F[t_1, \ldots, t_{s+1}]$ in $s+1$. Let g be the sum of all monomials of highest degree m in f. Since F is infinite there exist $c_i \in F \backslash \{0\}$ with $g(c_1, \ldots, c_{s+1}) \neq 0$. Since g is homogeneous we can consider $g(c_1, \ldots c_{s+1})/c_{s+1}^m$ and by replacing each c_i by c_i/c_{s+1} we may assume $c_{s+1} = 1$. Let $b := g(c_1, \ldots, c_s, 1) \in F \backslash \{0\}$.

Let $z_i := x_i - c_i y_n$. We have

$$0 = f(x_1, \ldots, x_s, y_n) = f(z_1 + c_1 y_n, \ldots, z_s + c_s y_n, y_n) = b y_n^m + h(z_1, \ldots, z_s, y_n),$$

where h is a polynomial whose degree in y_n is at most $m-1$. Dividing by $b \neq 0$ we conclude that y_n is integral over $R' := F[z_1, \ldots, z_s]$. Since $x_i \in R'[y_n]$ it follows that $F[x_1, \ldots, x_s]$ is integral over R' and hence R is integral over R'. The ring R' is generated as an F-algebra by $s < n$ elements and so by the induction hypothesis there exist elements $x'_1, \ldots x'_k$ which are algebraically independent set over F and R' is integral over $F[x'_1, \ldots, x'_k]$. In turn R is integral over R' and by Proposition 51 R is integral over $F[x'_1, \ldots, x'_k]$. $\square$

Proposition 65 *Let R be a domain which is finitely generated as an algebra over a field F. Let $P \neq \{0\}$ be a prime ideal of R. Then* $\mathrm{tr.deg}_F R > \mathrm{tr.deg}_F R/P$.

Proof. Let $k = \mathrm{tr.deg}_F \bar{R}$ and let $\{\bar{x}_1, \ldots, \bar{x}_k\}$ be a transcendence basis of $\bar{R}$ over F. 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 $\mathrm{tr.deg}_F R \geq k$. Suppose for the sake of contradiction that $\mathrm{tr.deg}_F R = k$. This implies that R is algebraic over its subring $L := F[x_1, \ldots, x_k]$. Suppose $R = L[y_1, \ldots, y_n]$ for some elements $y_i \in R$. Note that since $\bar{x}_1, \ldots, \bar{x}_k$ are algebraically independent we have $L \cap P = \{0\}$. Let $Y = L \backslash \{0\}$ this is a multiplicatively closed subset of R such that $Y \cap P = \emptyset$. Consider the localization $S := Y^{-1}R$ and let $T := e(P) = SP$. By Proposition 41 we have that $T \neq \{0\}$ is a prime ideal of S. Let $E := Y^{-1}L = F(x_1, \ldots, x_k)$ be the field of fractions of L. Then $S = Y^{-1}R = E[y_1, \ldots, y_n]$. Each of the elements y_i is algebraic over E and so S is a finite field extension of E. This contradicts the fact that $T = e(P)$ is a nonzero prime ideal of S.

Therefore $\mathrm{tr.deg}_F \bar{R} < \mathrm{tr.deg}_F R$ as claimed. $\square$

Theorem 66 *Let R be a domain which is finitely generated as an algebra over its subfield F. Then* $\dim R = \mathrm{tr.deg}_F R$.

Proof. By Theorem 64 there exists an algebraically independent set $\{x_1, \ldots x_k\} \subset R$ such that R is integral over its subring $K := R[x_1, \ldots, x_k]$. We have $\dim R = \dim K$ and since the field of fractions of R is algebraic over $R(x_1, \ldots, x_k)$ we have $k = \mathrm{tr.deg}_F R$. Now consider the chain of ideals of K

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

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

Suppose for the sake of contradiction that $\dim R > k$ and let $\{0\} = P_0 \subset P_1 \subset \cdots P_{k+1}$ be a chain of $k+2$ non-zero ideals of R. Let $R_i := R/P_i$, this is a domain which is a finitely generated algebra over F and by Proposition 65 we have $\text{tr.deg}_F R > \text{tr.deg}_F R_1 > \cdots > \text{tr.deg} R_{k+1} \geq 0$. So $\text{tr.deg} R > k$, contradiction. Hence $\dim R = k = \text{tr.deg}_F R$. $\square$

Corollary 67 *Let F be a field, and $R = F[t_1, \ldots, t_k]$ be a polynomial ring. Then* $\dim R = k$.

Corollary 68 *Let F be an algebraically closed field and let $V \subseteq F^k$ be an algebraic set. Then* $\dim V \leq k$ *with equality if and only if* $V = F^k$.

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

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. Let $P = \mathcal{I}(V)$. Since $V \neq F^k$ the prime ideal P is not zero. But then

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

by Proposition 65. $\square$

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.

Theorem 69 *Let R be a Noetherian ring of dimension 0. Then* $R/\text{nilrad}(R)$ *is isomorphic to a finite direct product of fields.*

Proof. By Proposition 14 R has finitely many minimal prime ideals, say $P_1, \ldots, P_n$ and $\text{nilrad} R = \cap_{i=1}^n P_i$ is nilpotent. Let $Q_j := \cap_{i \neq i} P_i$. Since $\dim R = 0$ each P_j is a maximal ideal of R and so $P_i \not\subseteq P_i$ for any $i \neq j$. Given j for each $i \neq j$ choose $a_i \in P_i \backslash P_j$ and then $\prod_{i \neq j} a_i$ belongs to Q_j but not to P_j. So $Q_j \not\subseteq P_j$ and hence $Q_j + P_j = R$. This holds for any j and by the Chinese remainder theorem

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

Now each R/P_i is a field by the maximality of P_i. $\square$

Conversely, a ring R such that $\mathrm{nilrad}R$ is a nilpotent finitely generated ideal and $R/\mathrm{nilrad}R$ is a 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.

Definition 70 *Let R be a domain. We say that R is integrally closed if R is integerally closed in its field of fractions E, that is any $x \in E$ which is integral over R must satisfy $x \in R$.*

For example $\mathbb{Z}$ and more generally any PID is an integrally closed domain, see the proof of Proposition 72 below.

Definition 71 *A Noetherian domain R is said to be a Dedekind domain if* $\dim R = 1$ *and R is integrally closed.*

Examples of Dedekind domains are all principal ideal domains.

Proposition 72 *Let R be a PID which is not a field. Then R is a Dedekind domain.*

Proof. Any nonzero prime ideal P of R is maximal, thus a maximal chain of prime ideals is provided by $\{0\} \subset P$. Hence $\dim R = 1$. It remains to show that R is integrally closed. Let K be the field of fractions of R and let $x = yz^{-1} \in K$ be integral over R where $y, z \in R$ and $z \neq 0$. We will prove that $x \in R$. We may assume that y and z are coprime elements of R. Suppose x satisfies the equaition (1) with $a_i \in R$. Multiply by z^n to clear denominators and reach $y^n + a_1 y^{n-1} z + \cdots + a_n z^n = 0$. This gives that z divides y^n and since y and z are assumed coprime it follows that z is a unit of R. Thus $x = yz^{-1} \in R$ and R is integrally closed. $\square$

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 R be the integral closure of $\mathbb{Z}$ in E. Then R is a domain and since R is integral over $\mathbb{Z}$ we have $\dim R = \dim \mathbb{Z} = 1$. Moreover it can be proved that $(R, +)$ is a finitely generated abelian group, thus R is a Noetherian $\mathbb{Z}$-module, hence a Noetherian R-module and hence R is a Noetherian ring. An important characterisation of Dedekind domains is that their ideals have unique factorization property.

Theorem 73 *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. Let $I \neq \{0\}$ be an ideal of R. Let $P_1, \ldots, P_n$ be the minimal primes of I. Choose some P_i and consider the localization R_{P_i}. Then R_{P_i} is a local Noetherian domain of dimension 1. Since R is integrally closed so is R_{P_i} by Problem sheet 4. Now we can apply the last problem in Sheet 4 which gives that R_{P_i} is a PID in which every nonzero ideal is a power of its maximal ideal $e(P_i) = P_i R_{P_1}$. Hence there is an integer $n_i \in \mathbb{N}$ such that $e(I) = IR_{P_i} = e(P_i)^{n_i}$.

Let $J = P_1^{n_1} \cdots P_k^{n_k}$. Now observe that for $j \neq i$ we have $P_j R_{P_i} = R_{P_i}$ and so $JR_{P_i} = (P_i)^{n_i} R_{P_i} = IR_{P_i}$. On the other hand if Q is a non-zero prime ideal different from any of the P_i then $I \not\subseteq Q$ and so $IR_Q = R_Q = JR_Q$. Therefore $IR_M = JR_M$ for every maximal prime ideal M of R. By Proposition 45 we have $I = J$ is a product of prime ideals. The same arguments shows that the integers n_i and the prime ideals P_i are uniquely determined by I. $\square$

There is a converse to Theorem 73: A domain all of whose ideals are product of prime ideals is necessarily a Dedekind domain. We won't prove this here, instead we shall prove some other results.

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 74 *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 $U := \prod_{i=1}^m P_i^{u_i}$. We have $UI = J$ and so I divides J. $\square$

Proposition 75 *Let R be a Dedekind domain. Then every ideal of R can be generated by at most 2 elements.*

Proof. Let $a \in I\backslash\{0\}$ and let $J = Ra$. We can factorize $J = \prod_{i=1}^m P_i^{s_i}$ for some prime ideals P_i and $s_i \in \mathbb{N}$. Since $J \subseteq I$ we must have $I = \prod_{i=1}^m P_i^{n_i}$ for some integers $0 \leq n_i \leq s_i$.

We have $I/J \simeq \prod_{i=1}^m P_i^{n_i}/P_i^{s_i}$ by the Chinese Remainder theorem. Let us choose $b_i \in P_i \backslash P_i^2$. This gives $Rb_i^{n_i} + P_i^{s_i} = P_i^{n_i}$ and so each $P_i^{n_i}/P_i^{s_i}$ is a principal ideal in $R/P_i^{s_i}$. Hence I/J is a principal ideal generated say by $b + J$ in the ring R/J. Then $I = Rb + J = \langle a, b\rangle$. $\square$

9.1 Fractional ideals and the ideal class group

We know that a PID is a Dedekind domain, but not every Dedekind domain R is a PID. How can we measure the failure of R to be a PID?

Definition 76 *Let R be a Dedekind domain with field of fractions K. A* fractional ideal *of K is a subset of the form αI where $\alpha \in K\backslash\{0\}$ and I is a nonzero ideal of R. Denote by $\mathcal{F}$ the set of all fractional ideals of K.*

It is clear that if αI and βJ are fractional ideals of K then so is their product $\alpha\beta IJ$. The fractional ideal R plays the role of identity since $\alpha I \cdot R = \alpha I$ for each $\alpha I \in \mathcal{F}$. We now show that every fractional ideal has an inverse, thus making $\mathcal{F}$ into abelian group.

Theorem 77 *Let $L \in \mathcal{F}$ be a fractional ideal of K. Then L has an inverse L^{-1}, namely a fractional ideal $L^{-1} \in \mathcal{F}$ such that $LL^{-1} = R$.*

Proof. Suppose $L = \alpha I$ for an ideal I of R and nonzero $\alpha \in K$. Choose any nonzero element $x \in I$. Since $Rx \subseteq I$ by Proposition 74 we must have $Rx = IJ$ for some ideal J of R. Define $L^{-1} := \alpha^{-1}x^{-1}J$. Then $L^{-1}L = \alpha^{-1}\alpha x^{-1}IJ = x^{-1}IJ = x^{-1}xR = R$. $\square$

This shows that $\mathcal{F}$ is an abelian group under multiplication. We have the subgroup of principal ideals $\mathcal{P} := \{\alpha R |\ \alpha \in K\backslash\{0\}\}$ and so we can define

Definition 78 *The ideal class group of a Dedekind domain is the quotient* $\mathcal{C} := \mathcal{F}/\mathcal{P}$ *of fractional ideals modulo principal ideals.*

Thus R is a PID if and only if $\mathcal{C} = \{0\}$. One of the major results in Algebraic number theory is that $|\mathcal{C}|$ is finite when R is a ring of integers. The proof relies on geometric arguments specific to rings of integers, in particular their realization as a lattice in Euclidean space and lies outside the scope of this course.