B2.2 Commutative Algebra

Damian Rössler

Oxford, Hilary Term

Introduction

Commutative algebra is the study of commutative rings, with a focus on the commutative rings which arise in algebraic geometry.

As will be explained in the Part C course Introduction to Schemes, a commutative ring corresponds to an affine scheme and in this sense, commutative algebra is a part of the theory of schemes.

Affine schemes are generalisations of affine varieties over fields.

The class of rings, which arise from affine varieties over fields (as their coordinate rings) is the class of finitely generated algebras over fields, ie quotients of polynomial rings $K[x_1, \ldots, x_k]$, where K is a field.

In the context of schemes, the most commonly studied affine schemes are those which are of finite type over a noetherian affine scheme.

The corresponding class of rings is then the class of rings, which are finitely generated over a noetherian ring.

This class is the prime object of study of this course.

Some history. Up to the end of the nineteenth century, one mainly studied finitely generated algebras over fields given by explicit equations (ie by polynomials generating an ideal I, when the algebra has the presentation $K[x_1, \ldots, x_k]/I$). The study of commutative rings in abstracto only started in the 1930s and it gathered a lot of momentum in the 1960s, when many geometric techniques became available through the theory of schemes.

Preamble

All rings in these lectures are commutative unitary rings. A ring will be short for a commutative unitary ring.

We assume that the reader is familiar with the content of the part A course Rings and Modules.

The basic reference for this course is the book

Introduction to Commutative Algebra by M. F. Atiyah and I. G MacDonald. Perseus Books.

For (a lot) more material and more explanations on the material presented here, see the book

Commutative Algebra with a View Toward Algebraic Geometry by D. Eisenbud. Springer, Graduate Texts in Mathematics 150.

We now review some terminology.

Let R be a ring. If $I \subseteq R$ is an ideal in R, we shall say that I is *non trivial* if $I \neq R$ (this is not entirely standard terminology).

The ideal I is *principal* if it can be generated by one element as an R-module.

We shall write $R^* := R \backslash \{0\}$.

An element $r \in R$ is said to be *nilpotent* if there exists an integer $n \geq 1$ such that $r^n = r \cdot r \cdots r \, (n\text{-times}) = 0$.

The ring R is *local* if it has a single maximal ideal.

The *prime ring* of a ring R is the image of the unique ring homomorphism $\mathbb{Z} \to R$ (which sends $n \in \mathbb{Z}$ to the corresponding multiple of $1 \in R$).

If R, T are rings, then T is said to be a *R-algebra* if there is a homomorphism of rings $R \to T$.

If $\phi_1 : R \to T_1$ and $\phi_2 : R \to T_2$ are two R-algebras, a *homomorphism of R-algebras* is a homomorphism of rings $\lambda : T_1 \to T_2$ such that $\lambda \circ \phi_1 = \phi_2$.

A R-algebra $\phi : R \to T$ is said to be *finitely generated* if there exists an integer $k \geq 0$ and a surjective homomorphism of R-algebras

$$R[x_1, \ldots, x_k] \to T.$$

If M is an R-module and $S \subseteq M$ is a subset of M, we write

$$\mathrm{Ann}(S) := \{r \in R \,|\, rm = 0 \,\text{for all}\, m \in S\}$$

The set $\mathrm{Ann}(S)$ is an ideal of R, called the *annihilator* of S.

If $I, J \subseteq R$ are ideals in R, we shall write

$$(I : J) := \{r \in R \mid rJ \subseteq I\}.$$

Let

$$\cdots \to M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} \cdots$$

be a sequence of R-modules such that $d_{i+1} \circ d_i = 0$ for all $i \in \mathbb{Z}$.

Such a sequence is called a *complex* of R-modules.

We shall say that the complex is *exact* if $\ker(d_{i+1}) = \mathrm{Im}(d_i)$ for all $i \in \mathbb{Z}$.

For the record, we recall the following two basic results:

Theorem 0.1 (Chinese remainder theorem)

Let R be a ring and let $I_1, \ldots, I_k$ be ideals of R. Let

$$\phi : R \to \prod_{i=1}^{k} R/I_i$$

be the ring homomorphism such that $\phi(r) = \prod_{i=1}^{k}(r \pmod{I_i})$ for all $r \in R$.

Then $\ker(\phi) = \cap_{i=1}^{k} I_i$.

Furthermore the map ϕ is surjective iff $I_i + I_j = R$ for any $i, j \in \{1, \ldots, k\}$ such that $i \neq j$. In that case, we have $\cap_{i=1}^{k} I_i = \prod_{i=1}^{k} I_i$.

(for the proof see Prop. 10 in AT).

Proposition 0.2 (Euclidean division)

Let R be a ring. Let $P(x), T(x) \in R[x]$.

Suppose that the leading coefficient of $T(x)$ is a unit of R.

Then there exist unique polynomials $Q(x), J(x) \in R[x]$ such that

$$P(x) = Q(x)T(x) + J(x)$$

and $\deg(J(x)) < \deg(T(x))$.

We shall also need the following result from set theory.

A *partial order* on a set S is a relation $\leq$ on S, such that

- (reflexivity) $s \leq s$ for all $s \in S$;

- (transitivity) if $s \leq t$ and $t \leq r$ for $s, t, r \in S$ then $s \leq r$;

- (antisymmetry) if $s \leq t$ and $t \leq s$ for $t, s \in S$ then $s = t$.

If we also have

- (connexity) for all $s, t \in S$, either $s \leq t$ or $t \leq s$

then the relation $\leq$ is said to be a *total order* on S.

Let $T \subseteq S$ be a subset and let $b \in S$. We say that b is an *upper bound* for T if $t \leq b$ for all $t \in T$.

An element $s \in S$ is said to be a *maximal element* of S if for all $t \in S$, we have $s \leq t$ iff $s = t$.

An element $s \in S$ is said to be a *minimal element* of S if for all $t \in S$, we have $t \leq s$ iff $s = t$.

Proposition 0.3 (Zorn's lemma)

Let $\leq$ be a partial order on a non-empty set S.

Suppose that for every subset $T \subseteq S$, which is totally ordered, there is an upper bound for T in S.

Then there exists a maximal element in S.

Proof. Omitted. See any first course on set theory. Zorn's lemma is a consequence of the axiom of choice. $\square$

On the next slide we shall see a classical application of Zorn's lemma.

Lemma 1

Let R be a ring. If $I \subseteq R$ be a non trivial ideal. Then there is a maximal ideal $M \subseteq R$ such that $I \subseteq M$.

Proof. Let $\mathcal{S}$ be the set of all non trivial ideals containing I.

Endow $\mathcal{S}$ with the relation given by inclusion.

If $\mathcal{T} \subseteq \mathcal{S}$ is a totally ordered subset, then $\mathcal{T}$ has the upper bound $\cup_{J \in \mathcal{T}} J$.

Hence, by Zorn's lemma, there is a maximal element M in $\mathcal{S}$.

By definition, the ideal M has the property that whenever J is a non trivial ideal containing I and $M \subseteq J$, then $M = J$.

If J is an ideal of R, which does not contain I, then we cannot have $M \subseteq J$ (since M contains I).

We conclude that for any non trivial ideal J of R, we have $M = J$ if $M \subseteq J$.

Ie M is a maximal ideal of R, which contains I. $\square$

END OF LECTURE 1

The nilradical and the Jacobson radical

Definition 0.4

Let R be a ring. The nilradical of R is the set of nilpotent elements of R.

The nilradical is obviously an ideal.

Examples. The nilradical of a domain is the zero ideal. The nilradical of $\mathbb{C}[x]/(x^n)$ is (x).

A ring R is called *reduced* if its nilradical is $\{0\}$.

The nilradical captures the "infinitesimal part" of a ring.

In the classical algebraic geometry of varieties, the coordinate rings were always assumed to be reduced, and nilradicals did not play a role.

Part of the strength of scheme theory is that it allows the presence of infinitesimal phenomena.

Proposition 0.5

Let R be a ring. The nilradical of R is the intersection of all the prime ideals of R.

Proof. Suppose that $f \in R$ is a nilpotent element. Let $\mathfrak{p} \subseteq R$ be a prime ideal.

Some power of f is 0, which is an element of $\mathfrak{p}$. In particular, $f \pmod{\mathfrak{p}} \in A/\mathfrak{p}$ is a zero-divisor.

Since $\mathfrak{p}$ is a prime ideal, the ring $A/\mathfrak{p}$ is a domain and so $f \pmod{\mathfrak{p}} = 0 \pmod{\mathfrak{p}}$.

In other words, $f \in \mathfrak{p}$. We conclude that f is in the intersection of all the prime ideals of R.

Conversely, suppose that $f \in R$ is not nilpotent.

Let Σ be the set of non trivial ideals I of R, such that for all $n \geq 1$ we have $f^n \notin I$.

The set Σ is non-empty, since $(0) \in \Sigma$.

If we endow this set with the relation of inclusion, we may conclude from Zorn's lemma that Σ contains a maximal element M.

We claim that M is a prime ideal.

To prove this, suppose that $x, y \in R$ and that $x, y \notin M$.

Note that the ideal $(x) + M$ (resp. $(y) + M$) strictly contains M and hence cannot belong to Σ (by the maximality property of M).

Hence there are integers $n_x, n_y \geq 1$ such that $f^{n_x} \in (x) + M$ and $f^{n_y} \in (y) + M$.

In other words, $f^{n_x} = a_1 x + m_1$, where $a_1 \in R$ and $m_1 \in M$ and $f^{n_y} = a_2 y + m_2$, where $a_2 \in R$ and $m_2 \in M$.

Thus

$$f^{n_x + n_y} = a_1 a_2 xy + m_3$$

where $m_3 \in M$.

Hence $xy \notin M$, for otherwise we would have $f^{n_x+n_y} \in M$, which is not possible since $M \in \Sigma$.

Since $x, y \in R$ were arbitrary, we conclude that M is a prime ideal.

Since $M \in \Sigma$, for all $n \geq 1$ we have $f^n \notin M$.

In particular we have $f \notin M$. In other words, we have exhibited a prime ideal in R, which does not contain f.

In particular, f does not lies in the intersection of all the prime ideals of R. $\square$

Let $I \subseteq R$ be an ideal.

Let $q : R \to R/I$ be the quotient map and let $\mathcal{N}$ be the nilradical of R/I.

The *radical* $\mathfrak{r}(I)$ *of* I is defined to be $q^{-1}(\mathcal{N})$.

From the definitions, we see that the nilradical of R coincides with the radical $\mathfrak{r}((0))$ of the 0 ideal.

From the previous proposition, we see that the radical of I has the two equivalent descriptions:

- it is the set of elements $f \in R$ such that there exists an integer $n \geq 1$ such that $f^n \in I$;

- it is the intersection of the prime ideals of R, which contain I.

An ideal, which coincides with its own radical is called a *radical ideal*.

Definition 0.6

Let R be a ring. The Jacobson radical of R is the intersection of all the maximal ideals of R.

By definition, the Jacobson radical of R contains the nilradical of R.

Let $I \subseteq R$ be a non trivial ideal.

Let $q : R \to R/I$ be the quotient map and let $\mathcal{J}$ be the Jacobson radical of R/I.

The *Jacobson radical of I* is defined to be $q^{-1}(\mathcal{J})$.

By definition, this coincides with the intersection of all the maximal ideals containing I.

Again by definition, the Jacobson radical of I contains the radical of I.

Proposition 0.7 (Nakayama's lemma)

Let R be a ring. Let M be a finitely generated R-module.

Let I be an ideal of R, which is contained in the Jacobson radical of R.

Suppose that $IM = M$.

Then $M \simeq (0)$.

Proof. Suppose for contradiction that $M \neq (0)$.

Let $x_1, \ldots, x_s$ be a set of generators of M and suppose that s is minimal.

By assumption, there are elements $a_1, \ldots, a_s \in I$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s$$

so that $(1 - a_s)x_s$ lies in the submodule M' generated by $x_1, \ldots, x_{s-1}$.

Now the element $1 - a_s$ is a unit.

Indeed, if $1 - a_s$ were not a unit then it would be contained in a maximal ideal $\mathfrak{m}$ of R and by assumption $a_s \in \mathfrak{m}$ so that we would have $1 \in \mathfrak{m}$, which is contradiction.

Hence

$$x_s = ((1 - a_s)^{-1} a_1) x_1 + \cdots + ((1 - a_s)^{-1} a_{s-1}) x_{s-1}. \tag{1}$$

Thus M has $s - 1$ generators, which is a contradiction.

Hence $M \simeq (0)$. $\square$

Corollary 0.8

Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module.

Let $x_1, \ldots, x_s \in M$ be elements of M and suppose that the elements

$$x_1 \,(\mathrm{mod}\, \mathfrak{m}), \ldots, x_s \,(\mathrm{mod}\, \mathfrak{m}) \in M/\mathfrak{m}M$$

generate the $R/\mathfrak{m}$-module $M/\mathfrak{m}M$.

Then the elements $x_1, \ldots, x_s$ generate M.

Proof. Let $M' \subseteq M$ be the submodule generated by $x_1, \ldots, x_s$.

By assumption, we have $M' + \mathfrak{m}M = M$ so that

$$\mathfrak{m}(M/M') = M/M'.$$

By Nakayama's lemma, we thus have $M/M' \simeq (0)$, ie $M = M'$. □

Definition 0.9

A ring R is called a Jacobson ring if for all the non trivial ideals I of R, the Jacobson radical of I coincides with the radical of I.

From the definition, we see that any quotient of a Jacobson ring is also Jacobson.

It is easy to see that the ring $\mathbb{Z}$ is Jacobson, and that any field is Jacobson.

So is $K[x]$, if K is a field, and in fact so is any finitely generated algebra over a Jacobson ring.

On the other hand, a local domain is never Jacobson.

So for instance the ring of p-adic integers $\mathbb{Z}_p$ (where p is a prime number) is not Jacobson.

END OF LECTURE 2

The spectrum of a ring

Let R be a ring. We shall write $\mathrm{Spec}(R)$ for the set of prime ideals of R.

If $\mathfrak{a} \subseteq R$ is an ideal, we define

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(R) \,|\, \mathfrak{p} \supseteq \mathfrak{a}\}$$

Lemma 2

The symbol $V(\bullet)$ has the following properties:

- $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cdot \mathfrak{b})$;
- $\bigcap_{i \in I} V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$;
- $V(R) = \emptyset$; $V((0)) = \mathrm{Spec}(R)$.

Proof. Straightforward. □

An immediate consequence of the last lemma is that the sets $V(\mathfrak{a})$ (where $\mathfrak{a}$ is an ideal of R) form the closed sets of a topology on $\mathrm{Spec}(R)$.

This topology is called the *Zariski topology*.

The closed points in $\mathrm{Spec}(R)$ are precisely the maximal ideals of R.

If R is the coordinate ring of an affine variety W over an algebraically closed field, the closed points correspond to the points of the variety, whereas the other prime ideals correspond to the irreducible closed subvarieties of W.

From the definitions, we see that R is a Jacobson ring iff the closed points are dense in any closed set of $\mathrm{Spec}(R)$.

If $\phi : R \to T$ is a homomorphism of rings, there a map

$$\mathrm{Spec}(\phi) : \mathrm{Spec}(T) \to \mathrm{Spec}(R)$$

given by the formula

$$\mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p}).$$

If $\mathfrak{a}$ is an ideal in R and $\mathfrak{b}$ is the ideal generated in T by $\phi(\mathfrak{a})$, we clearly have $\mathrm{Spec}(\phi)^{-1}(V(\mathfrak{a})) = V(\mathfrak{b})$, so that $\mathrm{Spec}(\phi)$ is a continuous map for the Zariski topologies on source and target.

Lemma 3

Let $\phi : R \to T$ be a surjective homomorphism of rings.

Then $\mathrm{Spec}(\phi)$ is injective and the image of $\mathrm{Spec}(\phi)$ is $V(\ker(\phi))$.

The map $\mathrm{Spec}(\phi)$ is a homeomorphism onto its image.

Proof. Straightforward. See the notes for details. □

Lemma-Definition 0.10

Let $f \in R$. The set

$$D_f(R) = D_f = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid f \notin \mathfrak{p}\}$$

is open in $\operatorname{Spec}(R)$.

The open sets of $\operatorname{Spec}(R)$ of the form D_f form a basis for the Zariski topology of $\operatorname{Spec}(R)$.

Furthermore, the topology of $\operatorname{Spec}(R)$ is quasi-compact.

The open sets of the form D_f are often called *basic open sets* (in $\operatorname{Spec}(R)$).

Recall that a set B of open sets of a topological space X is said to be a *basis* for the topology of X if every open set of X can be written as a union of open sets in B.

A topological space X is called *quasi-compact* if: for every family $(U_{i \in I})$ of open sets in X such that $\bigcup_{i \in I} U_i = X$ there exists a finite subset $I_0 \subseteq I$ such that $\bigcup_{i \in I_0} U_i = X$.

Proof. We first prove that D_f is open. To see this, just notice that the complement of D_f in $\mathrm{Spec}(R)$ is precisely $V((f))$, where (f) is the ideal generated by f.

We now prove that the open sets of $\mathrm{Spec}(R)$ of the form D_f form a basis for the Zariski topology of $\mathrm{Spec}(R)$.

Let $\mathfrak{a}$ be an ideal. We have to show that

$$\mathrm{Spec}(R)\backslash V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(R) \,|\, \mathfrak{p} \not\supseteq \mathfrak{a}\} = \bigcup_{i \in I} D_{r(i)}$$

for some index set I and some function $r : I \to R$. Let $r : I \to \mathfrak{a}$ be an enumeration of a set of generators of $\mathfrak{a}$. In view of of the properties of the symbol $V(\bullet)$, we have the required equality.

Finally, we show that $\mathrm{Spec}(R)$ is quasi-compact.

In view of the fact that the open sets of $\mathrm{Spec}(R)$ of the form D_f form a basis, we only need to show that if

$$\mathrm{Spec}(R) = \bigcup_{i \in I} D_{r(i)} \tag{2}$$

where $r : I \to R$ is a some function, then there is a finite subset $I_0 \subseteq I$ such that $\mathrm{Spec}(R) = \bigcup_{i \in I_0} D_{r(i)}$.

Now notice that the equality (2) is equivalent to the equality

$$\bigcap_{i \in I} V((r(i))) = V((r(I))) = \emptyset \tag{3}$$

where we have used the short-hand $(r(I))$ for the ideal generated by all the $r(i)$.

Now the equality $V((r(I))) = \emptyset$ says that no prime ideal contains $(r(I))$.

This is only possible if $(r(I)) = R$, for otherwise $(r(I))$ would be contained in at least one maximal ideal and maximal ideals are prime.

Now choose a finite subset $I_0 \subseteq I$ and a map $c : I_0 \to R$ such that $1 = \sum_{i \in I_0} c(i) \cdot r(i)$.

We then have $\sum_{i \in I_0}(r(i)) = R$ and thus $\bigcap_{i \in I_0} V((r(i))) = \emptyset$, which is what we want. $\square$

Lemma 4

Let $\mathfrak{a}, \mathfrak{b}$ be ideals in R. Then $V(\mathfrak{a}) = V(\mathfrak{b})$ if and only if $\mathfrak{r}(\mathfrak{a}) = \mathfrak{r}(\mathfrak{b})$.

Proof. This is a consequence of the fact that the radical of an ideal is the intersection of all the prime ideals containing it. $\square$

So the Zariski topology "does not see the nilradical".

In particular, there is a one to one correspondence between radical ideals in R and closed subsets of $\mathrm{Spec}(R)$.

The closed subsets corresponding to prime ideals are called *irreducible*.

If R is the coordinate ring of an affine variety W over an algebraically closed field, the radical ideals correspond to the closed (but not necessarily irreducible) subvarieties of W.

Remark 0.11

Let R be a commutative ring and let $\mathfrak{a}, \mathfrak{b}$ be two ideals in R. Then we have

$$(\mathfrak{a} \cap \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$$

and thus $\mathfrak{r}(\mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{r}(\mathfrak{a} \cap \mathfrak{b})$. In particular, we have

$$V(\mathfrak{a} \cdot \mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}).$$

Note that if $\mathfrak{a}$ and $\mathfrak{b}$ are radical ideals then $\mathfrak{a} \cap \mathfrak{b}$ is also a radical ideal, whereas $\mathfrak{a} \cdot \mathfrak{b}$ might not be.

END OF LECTURE 3

Localisation

Let R be a ring. A subset $S \subseteq R$ is said to be a *multiplicative set* if $1 \in S$ and if $xy \in S$ whenever $x, y \in S$.

A basic example of a multiplicative set is the set $\{1, f, f^2, f^3, \dots\}$, where $f \in R$.

Let $S \subseteq R$ be a multiplicative subset.

We define a relation $\sim$ on $R \times S$ as follows. If $(a, s), (b, t) \in R \times S$ then $(a, s) \sim (b, t)$ iff there exists $u \in S$ such that $u(ta - sb) = 0$.

The relation $\sim$ is an equivalence relation and we define

$$S^{-1}R = (R \times S)/\sim,$$

ie $S^{-1}R$ is the set of equivalence classes of $R \times S$ under $\sim$.

If $a \in R$ and $s \in S$, we write a/s for the image of (a, s) in $S^{-1}R$.

We define a map $+ : S^{-1}R \times S^{-1}R \to S^{-1}R$ by the rule

$$(a/s, b/t) \mapsto (at + bs)/(st).$$

We also define a map $\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R$ by the rule

$$(a/s, b/t) \mapsto (ab)/(ts).$$

These two maps provide $S^{-1}R$ with the structure of a commutative unitary ring, whose identity element is $1/1$.

The 0 element in $S^{-1}R$ is then the element $0/1$.

There is natural ring homomorphism from R to R_S, given by the formula $r \mapsto r/1$.

By construction, if $r \in S$, the element $r/1$ is invertible in R, with inverse $1/r$.

We shall see in Lemma-Definition 0.12 below that $S^{-1}R$ is the "minimal extension" of R making every element of S invertible.

Note that if R is a domain, the fraction field of R is the ring $R_{R\setminus 0}$.

Note also that if R is a domain and $0 \notin S$, then $S^{-1}R$ is a domain and $S^{-1}R$ is naturally a subring of the fraction field of R.

Indeed suppose that R is domain and that $(a/s)(b/t) = 0$, where $a, b \in R$ and $s, t \in S$. Then by definition we have $u(ab) = 0$ for some $u \in S$, which implies that $ab = 0$ so that either $a = 0$ or $b = 0$, in particular either $a/s = 0/1$ or $b/t = 0/1$.

More generally, the kernel of the natural map $R \to S^{-1}R$ is $\cup_{s\in S}\mathrm{Ann}(\{s\})$.

If M is an R-module, we may carry out a similar construction.

We define a relation $\sim$ on $M \times S$ as follows. If $(a, s), (b, t) \in M \times S$ then $(a, s) \sim (b, t)$ iff there exists $u \in S$ such that $u(ta - sb) = 0$.

The relation $\sim$ is again an equivalence relation and we define $S^{-1}M$ to be $(M \times S)/\sim$, ie $S^{-1}M$ is the set of equivalence classes of $M \times S$ under $\sim$.

If $a \in M$ and $s \in S$, we again write a/s for the image of (a, s) in $S^{-1}M$.

We define a map $+ : S^{-1}M \times S^{-1}M \to S^{-1}M$ by the rule

$$(a/s, b/t) \mapsto (at + bs/(st).$$

This is also well-defined.

Similarly, we define the map $\cdot : S^{-1}R \times S^{-1}M \to S^{-1}M$ by the rule

$$(a/s, b/t) \mapsto (ab)/(ts).$$

Again, this is well-defined. One checks that these two maps provide $S^{-1}M$ with the structure of a $S^{-1}R$-module.

The 0 element in $S^{-1}M$ is then the element $0/1$.

The $S^{-1}R$-module $S^{-1}M$ carries a natural structure of R-module via the natural map $R \to S^{-1}R$ and there a natural map of R-modules $M \to S^{-1}M$, given by the formula $m \mapsto m/1$.

We shall often write $R_S := S^{-1}R$ and $M_S := S^{-1}M$.

The ring R_S (resp. the R-module M_S) is called the *localisation of the ring R at S* (resp. *localisation of the R-module M at S*).

Lemma-Definition 0.12

Let $\phi : R \to R'$ be a ring homomorphism. Let $S \subseteq R$ be a multiplicative subset.

Suppose that $\phi(S)$ consists of units of R'.

Then there is a unique ring homomorphism

$$\phi_S = S^{-1}\phi : R_S \to R'$$

such that

$$\phi_S(r/1) = \phi(r)$$

for all $r \in R$.

Proof. Unwind the definitions. See the notes for details. □

There is a similar result for modules:

Lemma 5

Let R be a ring and let $S \subseteq R$ be a multiplicative subset.

Let M be a R-module and suppose for each $s \in S$, the "scalar multiplication by s" map $M \to M$ is an isomorphism.

Then there is a unique structure of R_S-module on M such that

$$(r/1)m = rm$$

for all $m \in M$ and $r \in R$.

Proof. Left to the audience. □

We also record the following important fact.

Lemma 6

Let R be a ring and let $f \in R$. Let $S = \{1, f, f^2, \dots\}$. Then the ring R_S is finitely generated as a R-algebra.

Proof. The R-algebra $T := R[x]/(fx - 1)$ has the universal property of R_S and so must be isomorphic to R_S. For a more down to earth proof, see the notes. □

In view of Lemma on the last slide, if R is a ring and $\phi : N \to M$ is a homomorphism of R-modules, there is a unique homomorphism of R_S-modules $\phi_S : N_S \to M_S$ such that $\phi(n/1) = \phi(n)/1$ for all $n \in N$.

We verify on the definitions that if $\psi : M \to T$ is another homomorphism of R-modules then, we have $(\psi \circ \phi)_S = \psi_S \circ \phi_S$.

Lemma 7

Let R be a ring and let $S \subseteq R$ be a multiplicative subset. Let

$$\cdots \to M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} \cdots$$

be an exact complex of R-modules.

Then the sequence

$$\cdots \to M_{i,S} \xrightarrow{d_{i,S}} M_{i+1,S} \xrightarrow{d_{i+1,S}} \cdots$$

is also exact.

Proof. Let $m/s \in M_{i,S}$ (with $m \in M_i$ and $s \in S$) and suppose that $d_{i,S}(m/s) = (1/s)d_{i,S}(m/1) = 0$.

Then $d_{i,S}(m/1) = d_i(m)/1 = 0$ so that there is a $u \in S$, such that $u \cdot d_i(m) = d_i(um) = 0$.

Now by assumption there is an element $p \in M_{i-1}$ such that $d_{i-1}(p) = um$.

Then we have $d_{i-1,S}(p/(us)) = m/s$. $\square$

Let R be a ring and let $\mathfrak{p}$ be a prime ideal in R. Then the set $R\backslash\mathfrak{p}$ is a multiplicative subset.

Indeed, $1 \notin \mathfrak{p}$ for otherwise $\mathfrak{p}$ would be equal to R and if $x, y \notin \mathfrak{p}$ then $xy \notin \mathfrak{p}$, for otherwise either x or y would lie in $\mathfrak{p}$.

We shall use the shorthand $R_{\mathfrak{p}}$ for $R_{R\backslash\mathfrak{p}}$.

If M is a R-module, we shall use the shorthand $M_{\mathfrak{p}}$ for $M_{R\backslash\mathfrak{p}}$. If $\phi : M \to N$ is a homomorphism of R-modules, we shall write $\phi_{\mathfrak{p}}$ for $\phi_{R\backslash\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$.

Lemma 8

Let R be a ring and let $S \subseteq R$ be a multiplicative subset.

Let $\lambda : R \to R_S$ be the natural ring homomorphism.

Then the prime ideals of R_S are in one-to-one correspondence with the prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p} \cap S = \emptyset$.

If $\mathfrak{q}$ is a prime ideal of R_S then the corresponding ideal of R is $\lambda^{-1}(\mathfrak{q})$.

If $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$ then the corresponding prime ideal of R_S is $\iota_{\mathfrak{p},S}(\mathfrak{p}_S) \subseteq R_S$, where $\iota_{\mathfrak{p}} : \mathfrak{p} \to R$ is the inclusion map.

Furthermore, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is then the ideal generated by $\lambda(\mathfrak{p})$ in R_S.

The proof is straightforward but requires a lot of trivial verifications. See the notes for details.

Note the following rewording of part of the last lemma:

$\mathrm{Spec}(\lambda)(\mathrm{Spec}(R_S))$ consists of the prime ideals in $\mathrm{Spec}(R)$, which do not meet S.

In particular, in the notation of Lemma-Definition 0.10,

$$\mathrm{Spec}(\lambda)(\mathrm{Spec}(R_S)) = D_f(R)$$

if $S = \{1, f, f^2, f^3, \dots\}$.

Lemma 9

Let R be a ring and let $\mathfrak{p} \subseteq R$ be a prime ideal. Then the ring $R_{\mathfrak{p}}$ is a local ring. If $\mathfrak{m}$ is the maximal ideal of $R_{\mathfrak{p}}$ and $\lambda : R \to R_{\mathfrak{p}}$ is the natural homomorphism of rings, then $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$.

Proof. By the last lemma, the prime ideals of $R_{\mathfrak{p}}$ correspond to the prime ideals of R which do not meet $R \backslash \mathfrak{p}$, ie to the prime ideals of R which are contained in $\mathfrak{p}$.

This correspondence preserves the inclusion relation, so every prime ideal of $R_{\mathfrak{p}}$ is contained in the prime ideal corresponding to $\mathfrak{p}$.

Now let I be a maximal ideal of $R_{\mathfrak{p}}$.

Since I is contained in the prime ideal corresponding to $\mathfrak{p}$, it must coincide with this ideal by maximality.

So the prime ideal $\mathfrak{m}$ corresponding to $\mathfrak{p}$ is maximal and it is the only maximal ideal of $R_{\mathfrak{p}}$.

By the last lemma, we have $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$. $\square$

Lemma 10

Let R be a ring. Let

$$\cdots \to M_i \stackrel{d_i}{\to} M_{i+1} \stackrel{d_{i+1}}{\to} \cdots \tag{4}$$

be a complex of R-modules. Then the complex (4) is exact iff the complex

$$\cdots \to M_{i,\mathfrak{p}} \stackrel{d_{i,\mathfrak{p}}}{\to} M_{i+1,\mathfrak{p}} \stackrel{d_{i+1,\mathfrak{p}}}{\to} \cdots \tag{5}$$

is exact for all the maximal ideals $\mathfrak{p}$ of R.

Proof. "$\Rightarrow$": already proved.

"$\Leftarrow$": Suppose that the complex (4) is not exact.

Then $\ker(d_{i+1})/\mathrm{Im}(d_i) \neq 0$ for some $i \in \mathbb{Z}$. We already know that there is a natural isomorphism

$$(\ker(d_{i+1})/\mathrm{Im}(d_i))_{\mathfrak{p}} \simeq \ker(d_{i+1})_{\mathfrak{p}}/\mathrm{Im}(d_i)_{\mathfrak{p}}$$

for all the prime ideals $\mathfrak{p}$ in R.

In particular, if $(\ker(d_{i+1})/\mathrm{Im}(d_i))_{\mathfrak{p}} \neq 0$ for some prime ideal $\mathfrak{p}$, then the complex (5) is not exact for that choice of prime ideal.

Since $\ker(d_{i+1})/\mathrm{Im}(d_i) \neq 0$, we see that there is an element $a \in \ker(d_{i+1})/\mathrm{Im}(d_i)$ such that $\mathrm{Ann}(a) \neq R$ (any non zero element of $\ker(d_{i+1})/\mathrm{Im}(d_i)$ will do).

Let $\mathfrak{p}$ be a maximal ideal of R, which contains $\mathrm{Ann}(a)$.

Then $(\ker(d_{i+1})/\mathrm{Im}(d_i))_{\mathfrak{p}} \neq 0$ for otherwise there would be an element $u \in R\backslash\mathfrak{p} \subseteq R\backslash\mathrm{Ann}(a)$ such that $ua = 0$, which is a contradiction. $\square$

END OF LECTURE 4

Primary decomposition

In this section, we study a generalisation of the decomposition of integers into products of prime numbers.

In a geometric context (ie for affine varieties over algebraically closed fields) this generalisation also provides the classical decomposition of a subvariety into a disjoint union of irreducible subvarieties.

Applied to the ring of polynomials in one variable over a field, it yields the decomposition of a monic polynomial into a product of irreducible monic polynomials.

Let R be a ring.

Proposition 0.13

(i) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be prime ideals of R. Let I be an ideal of R. Suppose that $I \subseteq \cup_{i=1}^{k} \mathfrak{p}_i$. Then there is $i_0 \in \{1, \ldots, k\}$ such that $I \subseteq \mathfrak{p}_{i_0}$.*
(ii) *Let $I_1, \ldots, I_k$ be ideals of R and let $\mathfrak{p}$ be a prime ideal of R. Suppose that $\mathfrak{p} \supseteq \cap_{i=1}^{k} I_i$. Then there is $i_0 \in \{1, \ldots, k\}$ such that $\mathfrak{p} \supseteq I_{i_0}$. If $\mathfrak{p} = \cap_{i=1}^{k} I_i$, then there is a $i_0 \in \{1, \ldots, k\}$ such that $\mathfrak{p} = I_{i_0}$.*

Proof. Skipped. See the notes. □

Definition 0.14

An ideal I of R is primary if it is non trivial and all the zero-divisors of R/I are nilpotent.

In other words, I is primary if the following holds: if $xy \in I$ and $x, y \notin I$ then $x^l \in I$ and $y^n \in I$ for some $l, n > 1$ (in other words, $x, y \in \mathfrak{r}(I)$).

From the definition, we see that every prime ideal is primary.

Example. The ideals (p^n) of $\mathbb{Z}$ are primary if p is prime and $n > 0$.

Lemma 11

Suppose that I is a primary ideal of R. Then $\mathfrak{r}(I)$ is a prime ideal.

Proof. Let $x, y \in R$ and suppose that $xy \in \mathfrak{r}(I)$.

Then there is $n > 0$ such that $x^n y^n \in I$ and thus

- either $x^n \in I$ or $y^n \in I$;

- or $x^{nl}, y^{nk} \in I$ for some $l, k \geq 1$.

Hence either x or y lies in $\mathfrak{r}(I)$. $\square$

The previous Lemma justifies the following terminology.

If $\mathfrak{p}$ is a prime ideal and I is a primary ideal, we say that I is $\mathfrak{p}$-*primary* if $\mathfrak{r}(I) = \mathfrak{p}$.

Note that if the radical of an ideal is prime, it does not imply that this ideal is primary. For counterexamples, see AT, beginning of chapter 4.

We have however the following result:

Lemma 12

Let J be an ideal of R. Suppose that $\mathfrak{r}(J)$ is a maximal ideal. Then J is primary.

Proof. From the assumptions, we see that the nilradical $\mathfrak{r}(R/J)$ of R/J is maximal. Since any prime ideal of R/J contains $\mathfrak{r}(R/J)$, we see that $\mathfrak{r}(R/J)$ is the only prime ideal of R/J. Since any non-unit of R/J is contained in a maximal ideal, we deduce that $\mathfrak{r}(R/J)$ is precisely the set of non-units of R/J. In particular, the zero divisors of R/J lies in $\mathfrak{r}(R/J)$. In particular, J is primary. □

Lemma 13

Let I be a $\mathfrak{p}$-primary ideal and $x \in R$.

(i) *If $x \in I$ then $(I : x) = R$.*

(ii) *If $x \notin I$ then $\mathfrak{r}(I : x) = \mathfrak{p}$.*

(iii) *If $x \notin \mathfrak{p}$ then $(I : x) = I$.*

Proof. (i) and (iii) follow directly from the definitions. We prove (ii).

Suppose that $y \in \mathfrak{r}(I : x)$.

By definition, this means that for some $n > 0$, we have $xy^n \in I$. As $x \notin I$, we see that $y^{ln} \in I$ for some $l > 0$ so that $y \in \mathfrak{r}(I) = \mathfrak{p}$.

Hence $\mathfrak{r}(I : x) \subseteq \mathfrak{p}$.

Now consider that we have $I \subseteq \mathfrak{r}(I : x) \subseteq \mathfrak{p}$.

Applying the operator $\mathfrak{r}(\bullet)$, we see that we have

$$\mathfrak{r}(I) = \mathfrak{p} \subseteq \mathfrak{r}(\mathfrak{r}(I : x)) = \mathfrak{r}(I : x) \subseteq \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$$

so that $\mathfrak{r}(I : x) = \mathfrak{p}$. $\square$

Lemma 14

Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{q}_1 \ldots, \mathfrak{q}_k$ be $\mathfrak{p}$-primary ideals. Then $\mathfrak{q} := \cap_{i=1}^{k} \mathfrak{q}_i$ is also $\mathfrak{p}$-primary.

Proof. We compute

$$\mathfrak{r}(\mathfrak{q}) = \cap_{i=1}^{k} \mathfrak{r}(\mathfrak{q}_i) = \mathfrak{p}.$$

In particular, $\mathfrak{q}$ is $\mathfrak{p}$-primary if it is primary.

We verify that $\mathfrak{q}$ is primary.

Suppose that $xy \in \mathfrak{q}$ and that $x, y \notin \mathfrak{q}$.

Then then there are $i, j \in \{1 \ldots, k\}$ such that $x \notin \mathfrak{q}_i$ and $y \notin \mathfrak{q}_j$. Hence there are $l, t > 0$ such $y^l \in \mathfrak{q}_i$ and $x^t \in \mathfrak{q}_j$.

In other words,

$$x, y \in \mathfrak{r}(\mathfrak{q}_i) = \mathfrak{r}(\mathfrak{q}_j) = \mathfrak{p} = \mathfrak{r}(\mathfrak{q}).$$

□

We shall say that an ideal I of R is *decomposable* if there exists a sequence $\mathfrak{q}_1 \ldots, \mathfrak{q}_k$ of primary ideals in R such that $I = \cap_{i=1}^{k} \mathfrak{q}_i$.

Such a sequence is called a *primary decomposition* of I.

A primary decomposition as above is called *minimal* if

(a) all the $\mathfrak{r}(\mathfrak{q}_i)$ are distinct;

(b) for all $i \in \{1, \ldots, k\}$ we have $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$.

Note that any primary decomposition can be reduced to a minimal primary decomposition in the following way:

- first use the last lemma to replace the sets of primary ideals with the same radical by their intersection; then (a) is achieved;

- then successively throw away any primary ideal violating (b).

In general, not all ideals are decomposable. We shall see later that all ideals are decomposable if R is noetherian.

END OF LECTURE 5

The following theorem examines what part of primary decompositions are unique.

Theorem 0.15

Let I be a decomposable ideal. Let $\mathfrak{q}_1 \ldots, \mathfrak{q}_k$ be primary ideals and let $I = \cap_{i=1}^{k} \mathfrak{q}_i$ be a minimal primary decomposition of I. Let $\mathfrak{p}_i := \mathfrak{r}(\mathfrak{q}_i)$ (so that $\mathfrak{p}_i$ is a prime ideal).

Then the following two sets of prime ideals coincide

- the set $\{\mathfrak{p}_i\}_{i \in \{1,\ldots,k\}}$;

- the ideals among the ideals of the type $\mathfrak{r}(I : x)$ (where $x \in R$), which are prime.

Proof. Let $x \in R$. Note that $(I : x) = \cap_{i=1}^{k}(\mathfrak{q}_i : x)$ and $\mathfrak{r}(I : x) = \cap_{i=1}^{k}\mathfrak{r}(\mathfrak{q}_i : x)$.

Hence by Lemma 13, we have $\mathfrak{r}(I : x) = \cap_{i, x \notin \mathfrak{q}_i}\mathfrak{p}_i$.

Now suppose that $\mathfrak{r}(I : x)$ is a prime ideal.

Then $\mathfrak{r}(I : x) = \mathfrak{p}_{i_0}$ for some $i_0 \in \{1, \ldots, k\}$ by Proposition 0.13.

Conversely, note that for any $i_0 \in \{1, \ldots, k\}$, there exists an $x \in R$, such that $x \notin \mathfrak{q}_{i_0}$ and such that $x \in \mathfrak{q}_i$ for all $i \neq i_0$.

This follows from the minimality of the decomposition.

For such an x, we have $\mathfrak{r}(I : x) = \mathfrak{p}_{i_0}$ by the above. $\square$

As a consequence of Theorem 0.15, we can associate with any decomposable ideal I in R a uniquely defined set of prime ideals.

Note that the intersection of these prime ideals is the ideal $\mathfrak{r}(I)$.

Another consequence is that any radical decomposable ideal has a unique minimal primary decomposition by prime ideals.

Examples. If $n = \pm p_1^{n_1} \cdots p_k^{n_k} \in \mathbb{Z}$, where the p_i are distinct prime numbers, a primary decomposition of (n) is given by

$$(n) = \cap_{i=1}^{k} (p^{n_i})$$

(apply the Chinese Remainder Theorem). The set of prime ideals associated to this decomposition is of course $\{(p_1), \ldots, (p_k)\}$.

A more complex example is the ideal $(x^2, xy) \subseteq \mathbb{C}[x, y]$.

Here

$$(x^2, xy) = (x) \cap (x, y)^2$$

is a primary decomposition and the associated set of prime ideals is $\{(x), (x, y)\}$.

For a justification, see the notes.

Lemma 15

Let I be a decomposable ideal.

Let $\mathcal{S}$ be the set of prime ideals associated with some (and hence any) minimal primary decomposition of I.

Let $\mathcal{I}$ be the set of all the prime ideals of R, which contain I.

View $\mathcal{S}$ (resp. $\mathcal{I}$) as partially ordered by the inclusion relation.

Then the minimal elements of $\mathcal{S}$ coincide with the minimal elements of $\mathcal{I}$.

Proof. Clearly the minimal elements of $\mathcal{I}$ are also minimal elements of $\mathcal{S}$.

We only have to show that the minimal elements of $\mathcal{S}$ are also minimal in $\mathcal{I}$.

Let $\mathcal{S}_{\min} \subseteq \mathcal{S}$ (resp. $\mathcal{I}_{\min} \subseteq \mathcal{I}$) be the set of minimal elements of $\mathcal{S}$ (resp. $\mathcal{I}$).

Note first that by Theorem 0.15, we have $\mathfrak{r}(I) = \cap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}$ and thus we also have $\mathfrak{r}(I) = \cap_{\mathfrak{p} \in \mathcal{S}_{\min}} \mathfrak{p}$.

Now let $\mathfrak{p}_0 \in \mathcal{S}_{\min}$. Suppose for contradiction that $\mathfrak{p}_0 \notin \mathcal{I}_{\min}$.

Then there exists an element $\mathfrak{p}_0' \in \mathcal{I}$ such that $\mathfrak{p}_0' \subsetneq \mathfrak{p}_0$.

On the other hand, we have $\mathfrak{p}_0' \supseteq I$, so that $\mathfrak{p}_0' \supseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathcal{S}_{\min}$ by Proposition 0.13.

We conclude that $\mathfrak{p}_0 \supsetneq \mathfrak{p}$, which contradicts the minimality of $\mathfrak{p}_0$. $\square$

In the second example given before Lemma 15, the set $\mathcal{S}_{\min}$ consists only of (x).

The elements of $\mathcal{S}_{\min}$ are called the *isolated* prime ideals whereas the elements of $\mathcal{S} \backslash \mathcal{S}_{\min}$ are called the *embedded* prime ideals.

This terminology is justified by algebraic geometry.

Note the following important fact:

if I is a decomposable radical ideal, then there is a minimal primary decomposition of I, which consist of the primes ideals which are minimal among all the prime ideals containing I.

In particular, all the associated prime ideals of a decomposable radical ideal are isolated.

Note. One can show that all the minimal primary decompositions of a decomposable radical ideal coincide. See notes for more details (but no proof).

END OF LECTURE 6

Noetherian rings

Let R be a ring.

We say that R is *noetherian* if every ideal of R is finitely generated.

In other words, if $I \subseteq R$ is an ideal of R, then there are elements $r_1, \ldots, r_k$ such that $I = (r_1, \ldots, r_k)$.

Examples. Fields and PIDs are noetherian (why?). In particular, $\mathbb{Z}$ and $\mathbb{C}$ are noetherian, and so is $K[x]$, for any field K.

We shall see that "most" rings that one encounters are noetherian. In fact any finitely generated algebra over a noetherian ring is noetherian (see below).

We begin with some generalities.

Lemma 16

Let R be a noetherian ring. Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending sequence of ideals.

Then there exists a $k \geq 1$ such that $I_k = I_{k+i} = \cup_{t=1}^{\infty} I_t$ for all $i \geq 0$.

Proof. The set $\cup_{t=1}^{\infty} I_t$ is clearly an ideal (verify) and it is finitely generated by assumption. A given finite set of generators for $\cup_{t=1}^{\infty} I_t$ lies in I_k for some $k \geq 1$. The conclusion follows. □

Lemma 17

Let R be a noetherian ring and $I \subseteq R$ an ideal.

Then the quotient ring R/I is noetherian.

Proof. Let $q : R \to R/I$ be the quotient map. Let J be an ideal of R/I. The ideal $q^{-1}(J)$ is finitely generated by assumption and the image by q of any set of generators of $q^{-1}(J)$ is a set of generators for J. □

Lemma 18

Let R be a noetherian ring and let $S \subseteq R$ be a multiplicative subset.

Then the ring R_S is noetherian.

Proof. Let $\lambda : R \to R_S$ be the natural ring homomorphism. In the proof of Lemma 8, we showed that for any ideal I of R_S, the ideal generated by $\lambda(\lambda^{-1}(I))$ is I (see (ii) in the proof). The image of any finite set of generators of $\lambda^{-1}(I)$ under λ is thus a finite set of generators for I. □

Lemma 19

Let R be a noetherian ring.

Let M be a finitely generated R-module.

Then any submodule of M is also finitely generated.

Proof. Omitted. See the notes. □

Lemma 20

Let R be a noetherian ring. If $I \subseteq R$ is an ideal, then there is an integer $t \geq 1$ such that $\mathfrak{r}(I)^t \subseteq I$. In particular, some power of the nilradical of R is the 0 ideal.

Proof. By assumption, we have $\mathfrak{r}(I) = (a_1 \ldots, a_k)$ for some $a_1, \ldots, a_k \in R$.

By assumption again, there is an integer $n \geq 1$ such that $a_i^n \in I$ for all $i \in \{1, \ldots, k\}$.

Let $t = k(n-1)+1$. Then $\mathfrak{r}(I)^t \subseteq (a_1^n \ldots, a_k^n) \subseteq I$. □

The following simple but remarkable result will be used later to give a simple proof of the so-called weak Nullstellensatz.

It also has several other applications (see exercises).

Theorem 0.16 (Artin-Tate)

Let T be a ring and let $R, S \subseteq T$ be subrings.

Suppose that $R \subseteq S$ and that R is noetherian. Suppose that T is finitely generated as a R-algebra and that T is finitely generated as a S-module.

Then S is a finitely generated as a R-algebra.

Proof. Let $r_1, \ldots, r_k$ be generators of T as a R-algebra.

Let $t_1, \ldots, t_l$ be a generators of T as an S-module.

By assumption, for any $a \in \{1, \ldots, k\}$, we can write

$$r_a = \sum_{j=1}^{l} s_{ja} t_j$$

where $s_j \in S$. Similarly, for any $a, b \in \{1, \ldots, k\}$, we can write

$$t_b t_d = \sum_{j=1}^{l} s_{jbd} t_j$$

where $s_{jbd} \in S$.

Let S_0 be the R-subalgebra of S generated by all the s_{ja} and s_{jbd}.

Using the two formulae above, we see that T is finitely generated as a S_0-module, with generators $t_1, \ldots, t_l$.

Furthermore, S_0 is a finitely generated R-algebra by construction.

The R-algebra S is naturally a S_0-algebra, in particular a S_0-module, and it is a S_0-submodule of T.

Since R is noetherian, S_0 is also noetherian as a consequence of the Hilbert basis theorem (the next theorem) and since S is a submodule of a finitely generated S_0-module, S is also finitely generated as a S_0-module by Lemma 19.

In particular S is a finitely generated S_0-algebra, and since S_0 is finitely generated over R, so is S. $\square$

Theorem 0.17 (Hilbert basis theorem)

Suppose that R is noetherian. Then the polynomial ring $R[x]$ is also noetherian.

Proof. Let $I \subseteq R[x]$ be an ideal. The leading coefficients of the polynomials in I form an ideal J of R (check).

Since R is noetherian, J has a finite set of generators, say $a_1, \ldots, a_k$.

For each $i \in \{1, \ldots, k\}$, choose $f_i \in I$ such that
$f_i(x) = a_i x^{n_i} + (\text{terms of lower degree})$.

Let n be the maximum of the n_i.

Let $I' = (f_1(x), \ldots, f_k(x)) \subseteq I$ be the ideal generated by the $f_i(x)$.

Now let $f(x) = ax^m + (\text{terms of lower degree})$ be any polynomial in I.

By construction, we have $a = r_1 a_1 + \cdots + r_k a_k$ for some $r_1, \ldots, r_k \in R$.

Suppose first that $m \geq n$. The polynomial

$$f(x) - r_1 f_1(x) x^{m-n_1} + \cdots + r_k f_k(x) x^{m-n_k}$$

is then of degree $< m$ (the leading terms cancel) and it also lies in I.

Applying the same procedure to this polynomial we obtain a new polynomial of degree $< m - 1$ and we keep going in the same way until we obtain a polynomial of degree $< n$.

Let M is the R-submodule of $R[x]$, generated by $1, x, x^2, \ldots, x^{n-1}$.

We have expressed the polynomial $f(x)$ as an element of $M \cap I + I'$.

If $m < n$ then we have $f(x) \in M \cap I$ so that we also have $f(x) \in M \cap I + I'$.

Since $f(x)$ was arbitrary, we have shown that

$$I = M \cap I + I'.$$

Now $M \cap I$ is an R-submodule of $M \simeq R^n$ and is thus finitely generated (as an R-module) by Lemma 19.

If we let $g_1(x), \ldots, g_t(x) \in M \cap I$ be a set of generators, then the set $g_1(x), \ldots, g_t(x), f_1(x), \ldots, f_k(x)$ is clearly a set of generators of I (as an ideal). $\square$

From Theorem 0.17, we deduce that $R[x_1, \ldots, x_k]$ is noetherian for any $k \geq 0$.

From this and Lemma 17, we deduce that *every finitely generated algebra over a noetherian ring is noetherian.*

Proposition 0.18 (Lasker-Noether)

Let R be a noetherian ring. Then every ideal of R is decomposable.

Proof. Omitted. See the notes. The proof is in two steps.

Say that an idea I is *irreducible* if whenever I_1, I_2 are ideals of R and $I = I_1 \cap I_2$, we have either $I = I_1$ or $I = I_2$.

The first step of the proof is to show that any ideal can be written as an intersection of irreducible ideals.

The second step is to show that any irreducible ideal is primary. □

Note. A primary ideal is not necessarily irreducible. See exercises.

Let R be a noetherian ring and let $I \subseteq R$ be a radical ideal.

As explained after Theorem 0.15, a consequence of Proposition 0.18 is that there is a unique set $\{\mathfrak{q}_1 \ldots, \mathfrak{q}_k\}$ of prime ideals in R such that $I = \cap_{i=1}^{k} \mathfrak{q}_i$ and such that

- all the $\mathfrak{q}_i$ are distinct;

- for all $i \in \{1, \ldots, k\}$ we have $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$.

Furthermore, the $\mathfrak{q}_i$ are precisely the prime ideals, which are minimal among all the prime ideals containing I.

In terms of the spectrum of R, $V(I)$ is the union of the $V(\mathfrak{q}_i)$.

If R is the coordinate ring of an affine variety over an algebraically closed field, this decomposition is the classical decomposition of a closed subvariety into its irreducible components.

END OF LECTURE 7

Integral extensions

The notion of integral extension of rings is a generalisation of the notion of algebraic extension of fields.

Let B be a ring and let $A \subseteq B$ be a subring. Let $x \in B$.

We shall say that b is *integral* over A if there is a monic polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ such that

$$P(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

We shall say that b is *algebraic* over A if there is a polynomial $Q(x) \in A[x]$ (not necessarily monic) such that $Q(b) = 0$.

Note that if A is a field, b is algebraic over A iff it is integral over A but this is not true in general.

If $S \subseteq B$ is a subset, we write $A[S]$ for the intersection of all the subrings of B which contain A and S.

Note that $A[S]$ is naturally an A-algebra.

Abusing notation slightly, we shall write $A[b]$ for $A[\{b\}]$ and more generally $A[b_1, \ldots, b_k]$ for $A[\{b_1, \ldots, b_k\}]$.

Note that we have the explicit description

$$A[b_1, \ldots, b_k] := \{Q(b_1, \ldots, b_k) \mid Q(x_1, \ldots, x_k) \in A[x_1, \ldots, x_k]\}$$

and that we have

$$A[b_1, \ldots, b_k] = A[b_1][b_2] \ldots [b_k].$$

Proposition 0.19

Let R be a ring and let M be a finitely generated R-module.

Let $\phi : M \to M$ be a homomorphism of R-modules.

Then there exists a monic polynomial $Q(x) \in R[x]$ such that $Q(\phi) = 0$.

Proof. Omitted. See the notes.

The mechanism of the proof is to reduce to statement to a free finitely generated R-module, where R is a ring a polynomials.

One can then apply the usual Cayley-Hamilton theorem. □

Proposition 0.20

Let A be a subring of the ring B.

Let $b \in B$ and let C be a subring of B containing A and b.

(i) *If the element $b \in B$ is integral over A then the A-algebra $A[b]$ is finitely generated as a A-module.*

(ii) *If C is finitely generated as an A-module then b is integral.*

Proof.

(i): if b is integral over A, we have

$$b^n = -a_{n-1}b^{n-1} - \cdots - a_1 b - a_0$$

for some $a_i \in A$ (where $i \in \{0, \ldots, n-1\}$).

Hence b^{n+k} is in the A-submodule of B generated by $1, b, b^2, \ldots, b^{n-1}$ for all $k \geq 0$.

In particular $A[b]$ is generated by $1, b, b^2, \ldots, b^{n-1}$ as an A-module.

(ii): Let $\phi : C \to C$ be the homomorphism of A-modules such that $\phi(v) = b \cdot v$ for all $v \in C$.

By Proposition 0.19, there a polynomial $Q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ such that $Q(\phi) = 0$.

Hence $Q(\phi)(1) = b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$.

In particular, b is integral over A. $\square$

The following lemma and its proof is a generalisation of the tower law.

Lemma 21

Let $\phi : R \to T$ be a homomorphisms of rings and let N be a T-module.

If T is finitely generated as a R-module and N is finitely generated as a T-module, then N is finitely generated as a R-module.

Proof. Let $t_1, \ldots, t_k \in T$ be generators of T as a R-module and let $l_1, \ldots l_s$ be generators of N as a T-module.

Then the elements $t_i l_j$ are generators of N as a R-module. □

Corollary 0.21 (of Proposition 0.20)

Let A be a subring of B.

Let $b_1, \ldots, b_k \in B$ be integral over A.

Then the subring $A[b_1, \ldots, b_k]$ is finitely generated as a A-module.

Proof. By Proposition 0.20 (i), $A[b_1]$ is finitely generated as an A-module, $A[b_1, b_2] = A[b_1][b_2]$ is finitely generated as a $A[b_1]$-module etc.

Hence by Lemma 21, $A[b_1, \ldots, b_k]$ is finitely generated as a A-module. □

Corollary 0.22 (of Corollary 0.21 and Proposition 0.20)

Let A be a subring of the ring B.

The subset of elements of B, which are integral over A, is a subring of B.

Proof. Let $b, c \in B$. Then $b + c, bc \in A[b, c]$ and $A[b, c]$ is a finitely generated A-module by Corollary 0.21.

Hence $b + c$ and c are integral over A by Proposition 0.20 (ii). $\square$

Let $\phi : A \to B$ be a ring homomorphism (in other words B is an A-algebra).

We shall say that B is *integral over* A (or an *integral A-algebra*) if all the elements of B are integral over the ring $\phi(A)$.

We shall say that B is *finite over* A (or a *finite A-algebra*) if B is a finitely generated $\phi(A)$-module.

Proposition 0.20 and Corollary 0.21 show that B is a finite A-algebra iff B is a finitely generated integral A-algebra.

If A is a subring of a ring B, the set of elements of B, which are integral over A, is called the *integral closure* of A in B.

This set is a subring of B by Corollary 0.22.

If A is a domain and K is the fraction field of K, we say that A is *integrally closed* if the integral closure of A in K is A.

Example. $\mathbb{Z}$ and $K[x]$ are integrally closed, if K is a field. Fields are obviously integrally closed. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is the ring of Gaussian integers $\mathbb{Z}[i]$ (see exercises).

Lemma 22

Let $A \subseteq B \subseteq C$, where A is a subring of B and B is a subring of C.

If B is integral over A and C is integral over B, then C is integral over A.

Proof. Let $c \in C$. By assumption, we have

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$$

for some $b_i \in B$.

Let $B' = A[b_1, \ldots, b_{n-1}]$.

Then c is integral over B' and so $B'[c]$ is finitely generated as a B'-module by Proposition 0.20 (i).

Hence $B'[c]$ is finitely generated as a A-module by Corollary 0.21 and Lemma 21.

Hence c is integral over A by Proposition 0.20 (ii). $\square$

Let $A \subseteq B \subseteq C$, where A is a subring of B and B is a subring of C.

A consequence of the previous lemma is that the integral closure in C of the integral closure of A in B is the integral closure of A in C.

Lemma 23

Let A be a subring of B. Let S be a multiplicative subset of A.

Suppose that B is integral (resp. finite) over A.

Then the the natural ring homomorphism $A_S \to B_S$ makes B_S into an integral (resp. finite) A_S-algebra.

Proof. Omitted. This is straightforward. See the notes. □

END OF LECTURE 8

Theorem 0.23 (part of the Going Up Theorem)

Let A be a subring of a ring B and let $\phi : A \to B$ be the inclusion map.

Suppose that B is integral over A.

Then $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

To prove Theorem 0.23, we shall need the following lemma.

Lemma 24

Suppose that C is a subring of a ring D. Suppose that D (and hence C) is a domain and that D is integral over C.

Then D is a field if and only if C is a field.

Proof.

"$\Leftarrow$": Suppose that C is a field. Let $d \in D^*$. We need to show that d has an inverse in D.

Let $\phi : C[t] \to D$ be the C-algebra map sending t on d. The kernel of this map is a prime ideal, since D is integral.

Since non-zero prime ideals in $C[t]$ are maximal (because C is a field), we conclude that the image of ϕ contains an inverse of d.

"$\Rightarrow$": Suppose that D is a field.

Let $c \in C^*$. We only have to show that the inverse $c^{-1} \in D$ lies in C.

Let $e_c : C[c, 1/c] \to C[c, 1/c]$ be the map such that $e_c(z) = z/c$ for all $z \in C[c, 1/c]$.

By Proposition 0.19 and Proposition 0.20 (i), there is a polynomial $P(t) = t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_0 \in C[t]$ such that $P(e_c) = 0$.

In particular, we have $P(e_c)(1) = P(1/c) = 0$.

Thus we have $c^{n-1} \cdot P(1/c) = 0$, ie

$$c^{-1} + a_{n-1} + \cdots + a_0 \cdot c^{n-1} = 0$$

which implies that $c^{-1} \in C$. $\square$

We record the following consequence of Lemma 24:

Corollary 0.24 (of lemma 24)

Let A be a subring of a ring B and let $\phi : A \to B$ be the inclusion map.

Suppose that B is integral over A.

Let $\mathfrak{q}$ be a prime ideal if B.

Then $\mathfrak{q} \cap A$ is a maximal ideal of A iff $\mathfrak{q}$ is a maximal ideal of B.

Proof. The induced map $A/(\mathfrak{q} \cap A) \to B/\mathfrak{q}$ is injective and makes $B/\mathfrak{q}$ into an integral $A/(\mathfrak{q} \cap A)$-algebra.

Since both $A/(\mathfrak{q} \cap A)$ and $B/\mathfrak{q}$ are domains, the conclusion follows from Lemma 24. $\square$

Proof. (of Theorem 0.23) Write $B_{\mathfrak{p}}$ for the localisation $B_{\phi(A\setminus\mathfrak{p})}$ of the ring B at the multiplicative set $\phi(A\setminus\mathfrak{p})$.

Note that $B_{\mathfrak{p}}$ is isomorphic to the localisation of B at $\mathfrak{p}$, when B is viewed as an A-module.

By Lemma-Definition 0.12, we thus obtain a unique ring homomorphism $\phi_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ such that $\phi_{\mathfrak{p}}(a/1) = \phi(a)/1$.

Write $\lambda_A : A \to A_{\mathfrak{p}}$ and $\lambda_B : B \to B_{\mathfrak{p}}$ for the natural ring homomorphisms.

We have $\lambda_B \circ \phi = \phi_{\mathfrak{p}} \circ \lambda_A$.

We thus obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}(B_{\mathfrak{p}}) & \xrightarrow{\mathrm{Spec}(\lambda_B)} & \mathrm{Spec}(B) \\ \downarrow{\scriptstyle \mathrm{Spec}(\phi_{\mathfrak{p}})} & & \downarrow{\scriptstyle \mathrm{Spec}(\phi)} \\ \mathrm{Spec}(A_{\mathfrak{p}}) & \xrightarrow{\mathrm{Spec}(\lambda_A)} & \mathrm{Spec}(A) \end{array}$$

By Lemma 9, $\mathfrak{p}$ is the image of the maximal ideal $\mathfrak{m}$ of $A_\mathfrak{p}$ under the map $\mathrm{Spec}(\lambda_A)$.

Thus it is sufficient to show that there is a prime ideal $\mathfrak{q}$ in $B_\mathfrak{p}$ so that $\phi_\mathfrak{p}^{-1}(\mathfrak{q}) =: \mathrm{Spec}(\phi_\mathfrak{p})(\mathfrak{q}) = \mathfrak{m}$.

Let $\mathfrak{q}$ be any maximal ideal of $B_\mathfrak{p}$ (this exists by Lemma 1).

Note that the map $\phi_\mathfrak{p}$ is injective by Lemma 7 and thus we obtain an injective map $A_\mathfrak{p}/\phi_\mathfrak{p}^{-1}(\mathfrak{q}) \to B_\mathfrak{p}/\mathfrak{q}$.

Now consider that the ring $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ by Lemma 23, so that $B_\mathfrak{p}/\mathfrak{q}$ is also integral over $A_\mathfrak{p}/\phi_\mathfrak{p}^{-1}(\mathfrak{q})$.

By assumption, the ring $B_\mathfrak{p}/\mathfrak{q}$ is a field and so by Lemma 24, the ring $A_\mathfrak{p}/\phi_\mathfrak{p}^{-1}(\mathfrak{q})$ is also field.

In other words, $\phi_\mathfrak{p}^{-1}(\mathfrak{q})$ is a maximal ideal of $A_\mathfrak{p}$.

Since $A_\mathfrak{p}$ is a local ring, we have $\mathfrak{m} = \phi_\mathfrak{p}^{-1}(\mathfrak{q})$. $\square$

Corollary 0.25

Let $\phi : A \to B$ be a homomorphism of rings.

Suppose that B is integral over A.

Then the map $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is closed (ie it sends closed sets to closed sets).

Proof. Let $\mathfrak{a}$ be an ideal of B.

We have to show that $\mathrm{Spec}(\phi)(V(\mathfrak{a}))$ is closed in $\mathrm{Spec}(A)$.

Let $q_{\mathfrak{a}} : B \to B/\mathfrak{a}$ be the quotient map and let

$$\mu := q_{\mathfrak{a}} \circ \phi : A \to B/\mathfrak{a}.$$

Let

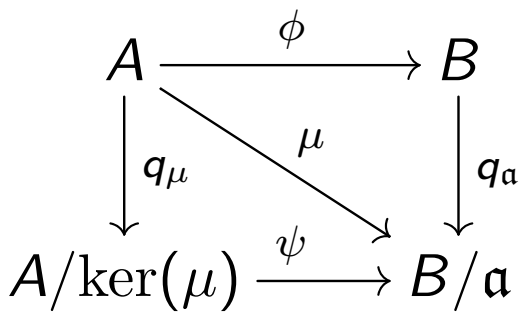
$$q_{\mu} : A \to A/\ker(\mu)$$

be the quotient map and let

$$\psi : A/\ker(\mu) \to B$$

be the ring homomorphism induced by μ.

We have the following commutative diagram:



Since B is integral over A, $B/\mathfrak{a}$ is also integral over $A/\ker(\mu)$.

Furthermore, the map ψ is injective by construction.

By Theorem 0.23, we thus have

$$\mathrm{Spec}(\psi)(\mathrm{Spec}(B/\mathfrak{a})) = \mathrm{Spec}(A/\ker(\mu)).$$

Furthermore, by Lemma 3, we have

$$\mathrm{Spec}(q_{\mathfrak{a}})(\mathrm{Spec}(B/\mathfrak{a})) = V(\mathfrak{a})$$

and

$$\mathrm{Spec}(q_{\mu})(\mathrm{Spec}(A/\ker(\mu)) = V(\ker(\mu)).$$

Thus $\mathrm{Spec}(\phi)(V(\mathfrak{a})) = V(\ker(\mu))$, which is closed. $\square$

Proposition 0.26

Let $\phi : A \to B$ be a ring homomorphism and suppose that B is finite over A.

Then the map $\mathrm{Spec}(\phi)$ has finite fibres.

Proof. Let $q : A \to A/\ker(\phi)$ be the quotient map.

The map $\mathrm{Spec}(q)$ has finite fibres by Lemma 3 (since it is injective), so we may replace A by $A/\ker(\phi)$ and suppose that A is a subring of B.

Let $\mathfrak{p}$ be a prime ideal of A.

We have to show that there are finitely many prime ideals $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Let $\bar{\mathfrak{p}}$ be the ideal of B generated by $\mathfrak{p}$.

Let $q : A \to A/\mathfrak{p}$ (resp. $\bar{q} : B \to B/\bar{\mathfrak{p}}$) be the quotient map.

Let $\psi : A/\mathfrak{p} \to B/\bar{\mathfrak{p}}$ be the ring homomorphism induced by ϕ.

By construction, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}(B/\bar{\mathfrak{p}}) & \xrightarrow{\mathrm{Spec}(\bar{q})} & \mathrm{Spec}(B) \\ \downarrow{\scriptstyle \mathrm{Spec}(\psi)} & & \downarrow{\scriptstyle \mathrm{Spec}(\phi)} \\ \mathrm{Spec}(A/\mathfrak{p}) & \xrightarrow{\mathrm{Spec}(q)} & \mathrm{Spec}(A) \end{array}$$

Since any prime ideal $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ has the property that $\mathfrak{q} \supseteq \bar{\mathfrak{p}}$, we see (using Lemma 3) that any such prime ideal lies in the image of $\mathrm{Spec}(\bar{q})$.

The corresponding prime ideals of $\mathrm{Spec}(B/\bar{\mathfrak{p}})$ are the primes ideals I such that $\psi^{-1}(I) = (0)$.

We thus have to show that $\mathrm{Spec}(\psi)^{-1}((0))$ is a finite set.

Now let $S = (A/\mathfrak{p})^*$. This is a multiplicative set.

Let

$$\lambda_{A/\mathfrak{p}} : A/\mathfrak{p} \to (A/\mathfrak{p})_S$$

and let

$$\lambda_{B/\bar{\mathfrak{p}}} : B/\bar{\mathfrak{p}} \to (B/\bar{\mathfrak{p}})_{\psi(S)}$$

be the natural ring homomorphisms.

There is also a natural ring homomorphism

$$\psi_S : (A/\mathfrak{p})_S \to (B/\bar{\mathfrak{p}})_{\psi(S)},$$

which is compatible with $\lambda_{A/\mathfrak{p}}$ and $\lambda_{B/\bar{\mathfrak{p}}}$.

We thus obtain a diagram

$$\begin{array}{ccc} \mathrm{Spec}((B/\bar{\mathfrak{p}})_{\psi(S)}) & \xrightarrow{\mathrm{Spec}(\lambda_{B/\bar{\mathfrak{p}}})} & \mathrm{Spec}(B/\bar{\mathfrak{p}}) \\ \downarrow{\scriptstyle \mathrm{Spec}(\psi_S)} & & \downarrow{\scriptstyle \mathrm{Spec}(\psi)} \\ \mathrm{Spec}((A/\mathfrak{p})_S) & \xrightarrow{\mathrm{Spec}(\lambda_{A/\mathfrak{p}})} & \mathrm{Spec}(A/\mathfrak{p}) \end{array}$$

Now notice that if $\mathfrak{q} \in \mathrm{Spec}(B/\bar{\mathfrak{p}})$ and $\psi^{-1}(\mathfrak{q}) = (0)$ then we have $\mathfrak{q} \cap \psi(S) = \emptyset$ so any such ideal lies in the image of $\mathrm{Spec}(\lambda_{B/\bar{\mathfrak{p}}})$.

It is thus sufficient to prove that the map $\mathrm{Spec}(\psi_S)$ has finite fibres.

Notice now that $A/\mathfrak{p}$ is domain (since $\mathfrak{p}$ is a prime ideal) and that $(A/\mathfrak{p})_S$ is none other than the fraction field of $A/\mathfrak{p}$.

Note further that we may assume that $\bar{\mathfrak{p}} \cap A = \mathfrak{p}$, or in other words that ψ is injective.

Indeed, if there is a prime ideal $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$, then $\bar{\mathfrak{p}} \cap A \subseteq \mathfrak{q} \cap A = \mathfrak{p}$.

Since we of course have $\bar{\mathfrak{p}} \cap A \supseteq \mathfrak{p}$ we then have $\bar{\mathfrak{p}} \cap A = \mathfrak{p}$.

So either we have $\bar{\mathfrak{p}} \cap A = \mathfrak{p}$ or there are no prime ideals $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ (in which case, there is nothing to prove - and this is contradicted by Theorem 0.23 anyway).

Now, since B is finite over A, $B/\bar{\mathfrak{p}}$ is also finite over $A/\mathfrak{p}$ and further, applying Lemma 23, we see that $(B/\bar{\mathfrak{p}})_{\psi(S)}$ is finite over $(A/\mathfrak{p})_S$.

In other words, $(B/\bar{\mathfrak{p}})_{\psi(S)}$ is a finite-dimensional $(A/\mathfrak{p})_S$-vector space.

Write $K := (A/\mathfrak{p})_S$.

If $\mathfrak{q}$ is a prime ideal in $(B/\bar{\mathfrak{p}})_{\psi(S)}$, then $(B/\bar{\mathfrak{p}})_{\psi(S)}/\mathfrak{q}$ is a domain, which is finite over the field K and it is thus a field by Lemma 24.

Thus $\mathfrak{q}$ is maximal.

So we only have to show that $(B/\bar{\mathfrak{p}})_{\psi(S)}$ has finitely many maximal ideals.

Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ be any distinct maximal ideals of $(B/\bar{\mathfrak{p}})_{\psi(S)}$.

By the Chinese remainder theorem, we have a surjective homomorphism of K-algebras

$$(B/\bar{\mathfrak{p}})_{\psi(S)} \to \prod_{i=1}^{k} (B/\bar{\mathfrak{p}})_{\psi(S)}/\mathfrak{q}_i$$

and each $(B/\bar{\mathfrak{p}})_{\psi(S)}/\mathfrak{q}_i$ is a K-algebra, which has dimension > 0 as K-vector space.

Hence $(B/\bar{\mathfrak{p}})_{\psi(S)}$ has dimension at least k as a K-vector space.

Hence there are at most $\dim_K((B/\bar{\mathfrak{p}})_{\psi(S)})$ prime (and therefore maximal) ideals in $(B/\bar{\mathfrak{p}})_{\psi(S)}$. $\square$

END OF LECTURE 9

The Noether normalisation lemma and Hilbert's Nullstellensatz

Noether's normalisation lemma shows that any finitely generated algebra over a field can be "approximated" by a polynomial ring, up to a finite injective homomorphism.

In terms of affine varieties, in say that for any affine variety, there is a finite surjective map from the variety to some affine space.

Theorem 0.27 (Noether's normalisation lemma)

Let K be a field and let R be a non zero finitely generated K-algebra.

Then there exists an injective homomorphism of K-algebras

$$K[y_1, \ldots, y_t] \to R$$

for some $t \geq 0$ (where we set $K[y_1, \ldots, y_t] = K$ if $t = 0$), such that R is finite as a $K[y_1, \ldots, y_t]$-module.

The idea of the proof is as follows.

It is easy to see that there is an injective homomorphism of algebras $K[y_1, \ldots, y_t] \to R$ so that R is algebraic over $K[y_1, \ldots, y_t]$.

The proof of the normalisation lemma basically considers such a homomorphism and tweaks it, using properties of polynomials, so that R becomes integral over $K[y_1, \ldots, y_t]$.

Proof. (of Noether's normalisation lemma). We will only prove this result in the situation where K is infinite.

Let $r_1, \ldots, r_n \in R$ be a set of generators of minimal size (ie n is minimal) for R as a K-algebra.

We proceed by induction on n.

If $n = 1$ then either $R \simeq K[x]$ or $R \simeq K[x]/I$ for some non trivial ideal I in $K[x]$.

In the first case, we may set $t = 1$ in the theorem and in the second case we may set $t = 0$.

So the theorem is proven when $n = 1$.

So suppose that $n > 1$ and that the theorem holds for $n - 1$.

Up to renumbering the generators, we may assume that there is a $k \in \{1, \ldots, n\}$ such that for all $i \in \{1, \ldots, k\}$, r_i is not algebraic over $K[r_1, \ldots, r_{i-1}]$ and such that r_{k+i} is algebraic over $K[r_1, \ldots, r_k]$ for all $i \in \{1, \ldots, n - k\}$.

Now we may assume that $k < n$, for otherwise we may set $t = k = n$ in the theorem.

The generator r_n is thus algebraic over $K[r_1, \ldots, r_{n-1}]$.

Let $P_1(x) \in K[r_1, \ldots, r_{n-1}][x]$ be a non zero polynomial (not necessarily monic) such that $P_1(r_n) = 0$.

Since $K[r_1, \ldots, r_{n-1}]$ is the image of the polynomial ring $K[x_1, \ldots, x_{n-1}]$ by the homomorphism of K-algebras sending x_i to r_i, there is a non zero polynomial

$$P(x_1, \ldots, x_n) \in K[x_1, \ldots, x_{n-1}][x_n] = K[x_1, \ldots, x_n]$$

such that $P(r_1, \ldots, r_n) = 0$.

Let $F(x_1, \ldots, x_n)$ be the sum of the monomials of degree $d := \deg(P)$ which appear in P (so that in particular $\deg(P - F) < d$).

Choose $\lambda_1, \ldots, \lambda_{n-1} \in K$ so that $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$.

Now let $u_i := r_i - \lambda_i r_n$ for all $i \in \{1, \ldots, n-1\}$.

We compute

$$\begin{aligned} & P(r_1, \ldots, r_n) \\ &= P(u_1 + \lambda_1 r_n, u_2 + \lambda_2 r_n, \ldots, u_{n-1} + \lambda_{n-1} r_n, r_n) \\ &= F(\lambda_1, \ldots, \lambda_{n-1}, 1) r_n^d + F_1(u_1, \ldots, u_{n-1}) r_n^{d-1} \\ &+ \cdots + F_d(u_1, \ldots, u_{n-1}) \\ &= 0 \end{aligned}$$

for some polynomials $F_1, \ldots, F_d$ in the u_i.

Thus

$$r_n^d + (F(\lambda_1, \ldots, \lambda_{n-1}, 1))^{-1} F_1(u_1, \ldots, u_{n-1}) r_n^{d-1} + \ldots$$

$$+ (F(\lambda_1, \ldots, \lambda_{n-1}, 1))^{-1} F_d(u_1, \ldots, u_{n-1}) = 0$$

and we see that r_n is integral over $K[u_1, \ldots, u_{n-1}]$

and the proof is complete by induction. $\square$

Noether's normalisation lemma has the following fundamental corollary.

Corollary 0.28 (weak Nullstellensatz)

Let K be a field and let R be a finitely generated K-algebra.

Suppose that R is a field.

Then R is finite over K (ie R is a finite-dimensional K-vector space).

Proof. Let

$$K[y_1, \ldots, y_t] \to R$$

be as in Noether's normalisation lemma.

Recall that by Theorem 0.23, the map $\mathrm{Spec}(R) \to \mathrm{Spec}(K[y_1, \ldots, y_t])$ is surjective.

Now $\mathrm{Spec}(R)$ has only one element, since R is a field.

Hence $\mathrm{Spec}(K[y_1, \ldots, y_t])$ has only one element.

Thus $t = 0$, because for any $t \geq 1$, $\mathrm{Spec}(K[y_1, \ldots, y_t])$ has more than one element.

We conclude that R is integral over K.

Since R is also finitely generated over K, it must be finite over K (see after Corollary 0.22). $\square$

END OF LECTURE 10

The weak Nullstellensatz has the following corollaries, which are of fundamental importance in algebraic geometry.

Corollary 0.29

Let K be an algebraically closed field. Let $t \geq 1$.

Then an ideal I of $K[x_1, \ldots, x_t]$ is maximal iff it has the form $(x_1 - a_1, \ldots, x_t - a_t)$ for some $a_1, \ldots, a_t \in K$.

A polynomial $Q(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$ lies in $(x_1 - a_1, \ldots, x_t - a_t)$ iff $Q(a_1, \ldots, a_t) = 0$.

Proof. We first prove the first statement.

"$\Leftarrow$": Note that the ideal $(x_1 - a_1, \ldots, x_t - a_t)$ is the image of the ideal $(x_1, \ldots, x_t)$ under the automorphism of $K[x_1, \ldots, x_t]$ sending x_i to $x_i - a_i$ for all $i \in \{1, \ldots, t\}$.

Now the ideal $(x_1, \ldots, x_t)$ is maximal since $K[x_1, \ldots, x_t]/(x_1, \ldots, x_t) \simeq K$.

Hence $(x_1 - a_1, \ldots, x_t - a_t)$ is also maximal.

"$\Rightarrow$": Suppose that I is maximal.

Note that $K[x_1, \ldots, x_t]/I$ is a field, which is also a finitely generated K-algebra.

Hence, by Corollary 0.28, $K[x_1, \ldots, x_t]/I$ is finite, and it particular algebraic over K. Since K is algebraically closed, this implies that $K[x_1, \ldots, x_t]/I$ is isomorphic to K as a K-algebra.

Let $\phi : K[x_1, \ldots, x_t] \to K$ be the induced homomorphism of K-algebras.

By construction, the ideal I contains the ideal

$$(x_1 - \phi(x_1), \ldots, x_t - \phi(x_t)).$$

Since the ideal $(x_1 - \phi(x_1), \ldots, x_t - \phi(x_t))$ is also maximal by the first part, we must have

$$I = (x_1 - \phi(x_1), \ldots, x_t - \phi(x_t)).$$

For the second statement, note that the homomorphism of K-algebras $\psi : K[x_1, \ldots, x_t] \to K$ such that

$$\psi(P(x_1, \ldots, x_t)) = P(a_1, \ldots, a_t)$$

is surjective and

$$\ker(\psi) \supseteq (x_1 - a_1, \ldots, x_t - a_t).$$

In particular, $\ker(\psi)$ is maximal, and we must have

$$\ker(\psi) = (x_1 - a_1, \ldots, x_t - a_t),$$

since

$$(x_1 - a_1, \ldots, x_t - a_t)$$

is maximal by the first part. $\square$

Corollary 0.30

Let K be a field. Let R be a finitely generated K-algebra.

Then R is a Jacobson ring.

Proof. Let $I \subseteq R$ be an ideal.

We need to show that the Jacobson radical of I of R coincides with the radical of I.

In other words, we need to show that the nilradical of R/I coincides with the Jacobson radical of the zero ideal in R/I.

Since R/I is also finitely generated over K, we may thus replace R by R/I and suppose that $I = 0$.

Let $f \in R$ and suppose that f is not nilpotent.

We need to show that there exists a maximal ideal $\mathfrak{m}$ in R, such that $f \notin \mathfrak{m}$.

Let $S = \{1, f, f^2, \dots\}$.

Since f is not nilpotent, we have $f^k \cdot f \neq 0$ for all $k \geq 0$ and thus the localisation R_S is not the zero ring.

Let $\mathfrak{q}$ be a maximal ideal of R_S (this exists by Lemma 1). Since R_S is a finitely generated K-algebra (see Lemma 6), the quotient $R_S/\mathfrak{q}$ is also finitely generated over K.

Thus, by Corollary 0.28, the canonical homomorphism of rings $K \to R_S/\mathfrak{q}$ (giving the K-algebra structure) makes $R_S/\mathfrak{q}$ into a finite field extension of K.

Let $\phi : R \to R_S/\mathfrak{q}$ be the homomorphism of K-algebras obtained by composing the natural homomorphism $R \to R_S$ with the homomorphism $R_S \to R_S/\mathfrak{q}$.

The image $\mathrm{Im}(\phi)$ of ϕ is a domain (since $R_S/\mathfrak{q}$ is a domain, being a field), which is integral over K and thus $\mathrm{Im}(\phi)$ is a field by Lemma 24.

Thus $\ker(\phi)$ is a maximal ideal of R.

On the other hand, $\ker(\phi)$ is by construction the inverse image of $\mathfrak{q}$ by the natural homomorphism $R \to R_S$.

Since $f/1$ is a unit in R_S, we have $f/1 \notin \mathfrak{q}$ and thus $f \notin \ker(\phi)$.

Thus we may set $\mathfrak{m} := \ker(\phi)$. $\square$

The following Corollary also contains a definition.

Corollary 0.31 (strong Nullstellensatz)

Let K be an algebraically closed field.
Let $t \geq 1$ and let $I \subseteq K[x_1, \ldots, x_t]$ be an ideal.

Let

$$Z(I) := \{(c_1, \ldots, c_t) \in K^n \mid P(c_1, \ldots, c_n) = 0 \, for \; all \; P \in I\}$$

Let $Q(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$.
Then $Q \in \mathfrak{r}(I)$ iff $Q(c_1, \ldots, c_t) = 0$ for all $(c_1, \ldots, c_t) \in Z(I)$.

The strong Nullstellensatz implies that the set of simultaneous roots of a set of polynomials determines the radical of the ideal generated by the set of polynomials.

Proof. Let $R := K[x_1, \ldots, x_t]$. The implication "$\Rightarrow$" is straightforward.

We prove the implication "$\Leftarrow$".

Let $Q(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$ and suppose that $Q(c_1, \ldots, c_t) = 0$ for all $(c_1, \ldots, c_t) \in Z(I)$.

Suppose for contradiction that $Q \notin \mathfrak{r}(I)$.

Since R is Jacobson ring (by Corollary 0.30), there exists a maximal ideal $\mathfrak{m}$ in R, such that $\mathfrak{m} \supseteq I$ and $Q \notin \mathfrak{m}$.

By Corollary 0.29, we have $\mathfrak{m} = (x_1 - a_1, \ldots, x_t - a_t)$ for some a_i (where $i \in \{1, \ldots, t\}$).

By construction, we have $P(a_1, \ldots, a_t) = 0$ for all $P \in \mathfrak{m}$ and hence for all $P \in I$.

In other words, $(a_1, \ldots, a_t) \in Z(I)$.

By the second statement in Corollary 0.29, we see that $Q(a_1, \ldots, a_t) \neq 0$.

This is a contradiction, so $Q \in \mathfrak{r}(I)$. $\square$

Jacobson rings

In this section, we collect more consequences of the weak Nullstelllensatz and we show that the property of being a Jacobson ring is a very stable property.

The Jacobson property enters the proof of Theorem 0.33 below via the following lemma.

Lemma 25

Let R be a Jacobson ring. Suppose that R is a domain.

Let $b \in R$ and let $S := \{1, b, b^2, \dots\}$.

Suppose that R_S is a field.

Then R is a field.

Proof. We know from Lemma 8 that the prime ideals of R, which do not meet b are in one to one correspondence with the prime ideals of R_S.

Since R_S is a field, there is only one such ideal in R, namely the 0 ideal.

Hence every non zero prime ideal of R meets b.

Now suppose for a moment that (0) is not a maximal ideal of R.

Since (0) is its own radical (since R is a domain) and since R is Jacobson, the ideal (0) is the intersection of all the non zero maximal ideals of R.

However, we just saw that this intersection contains b, which is a contradiction.

So (0) must be a maximal ideal of R. Hence R is a field . $\square$

Corollary 0.32

Let T be a field and let $R \subseteq T$ be a subring. Suppose that R is a Jacobson ring.

Suppose that T is finitely generated over R.

Then R is a field. In particular, T is finite over R by the Noether normalisation lemma.

Proof. Let $K \subseteq T$ be the fraction field of R. Note that by the weak Nullstellensatz T is a finite extension of K. Let $t_1, \ldots, t_k \in T$ be generators of T as a R-algebra.

Let

$$P_i(x) = x^{d_i} + (a_{i,d_i-1}/b_{i,d_i-1})x^{d_i-1} + \cdots + a_{i,0}/b_{i,0} \in K[x]$$

be a monic polynomial with coefficients in K, which annihilates t_i.

Let $b := \prod_{i=1}^{k} \prod_{j=1}^{d_i} b_{i,d_i-j}$. Let $S := \{1, b, b^2, \ldots\}$.

Then there is a natural injective homomorphism of R-algebras from R_S into K, because R is a domain. We view R_S as a sub-R-algebra of K.

By construction, T is generated by the t_i as a R_S-algebra and the elements t_i are integral over R_S.

Hence T is finite over R_S.

Also, since T is a field, it has a single prime ideal, which is maximal, and we deduce from Corollary 0.24 and Theorem 0.23 that R_S has a single prime ideal, which is maximal. Hence R_S is a field. Now Lemma 25 implies that R is a field. $\square$

Corollary 26

Let $\psi : R \to T$ be a homomorphism of rings.

Suppose that R is Jacobson and that T is a finitely generated R-algebra.

Let $\mathfrak{m}$ be a maximal ideal of T.

Then $\psi^{-1}(\mathfrak{m})$ is a maximal ideal of R and the induced map

$$R/\psi^{-1}(\mathfrak{m}) \to T/\mathfrak{m}$$

makes $T/\mathfrak{m}$ into a finite field extension of $R/\psi^{-1}(\mathfrak{m})$.

Proof. Note that $T/\mathfrak{m}$ is a field which is finitely generated over $R/\psi^{-1}(\mathfrak{m})$. Note also that $R/\psi^{-1}(\mathfrak{m})$ is a Jacobson ring since it is the quotient of a Jacobson ring. Thus Corollary 0.32 implies the result. □

Theorem 0.33

A finitely generated algebra over a Jacobson ring is Jacobson.

Proof. The beginning of the proof is similar to the proof of Corollary 0.30.

Let R be a Jacobson ring and let T be a finitely generated R-algebra.

Let $I \subseteq T$ be an ideal.

We need to show that the Jacobson radical of I of T coincides with the radical of I.

In other words, we need to show that the nilradical of T/I coincides with the Jacobson radical of the zero ideal in T/I.

Since T/I is also finitely generated over R, we may thus replace T by T/I and suppose that $I = 0$.

Let $f \in T$ and suppose that f is not nilpotent. We need to show that there exists a maximal ideal $\mathfrak{m}$ in T, such that $f \notin \mathfrak{m}$.

Let $S = \{1, f, f^2, \dots\}$. Since f is not nilpotent, we have $f^k \cdot f \neq 0$ for all $k \geq 0$ and thus the localisation T_S is not the zero ring.

Let $\mathfrak{q}$ be a maximal ideal of T_S. Since T_S is a finitely generated R-algebra (see Lemma 6), the quotient $T_S/\mathfrak{q}$ is also finitely generated over R.

Let $\phi : R \to T_S/\mathfrak{q}$ be the canonical ring homomorphism.

By Corollary 26, the kernel of ϕ is also maximal and $T_S/\mathfrak{q}$ is a finite field extension of $R/\ker(\phi)$.

Now consider the map $\Phi : T \to T_S/\mathfrak{q}$ which is the composition of the natural map $T \to T_S$ with the quotient map.

The image $\mathrm{Im}(\Phi)$ of ϕ is a R-subalgebra, and hence $R/\ker(\phi)$-subalgebra, of $T_S/\mathfrak{q}$.

Since $T_S/\mathfrak{q}$ is integral over $R/\ker(\phi)$, we see that $\mathrm{Im}(\Phi)$ is integral over $R/\ker(\phi)$ and hence $\mathrm{Im}(\phi)$ is a field by Lemma 24.

In other words, $\ker(\Phi)$ is a maximal ideal of T.

Finally, note that $\ker(\Phi)$ is by construction the inverse image of $\mathfrak{q}$ by the natural homomorphism $T \to T_S$ and that $f/1 \notin \mathfrak{q}$, since $f/1$ is a unit in T_S.

Thus we have $f \notin \ker(\Phi)$. We conclude that we may set $\mathfrak{m} := \ker(\Phi)$. □

Examples. The ring $\mathbb{Z}$ is Jacobson (prove this). Hence any finitely generated algebra over $\mathbb{Z}$ is a Jacobson ring.

END OF LECTURE 11

Dimension

The dimension of a ring R is an invariant of a ring, whose definition is inspired by algebraic geometry. If R is the coordinate ring of an affine algebraic variety over an algebraically closed field, the dimension of R is the ordinary dimension of the variety.

Here is the formal definition.

Definition 0.34

Let R be a ring. The dimension of R is

$$\dim(R) := \sup\{n \,|\, \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n,\ \mathfrak{p}_0, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)\}.$$

Let $\mathfrak{p}$ be a prime ideal of R.

The codimension (also called height) of $\mathfrak{p}$ is

$$\operatorname{ht}(\mathfrak{p}) = \sup\{n \,|\, \mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n,\ \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)\}.$$

Note that the dimension of R as well as the codimension of $\mathfrak{p}$ might be infinite.

From the definitions, we see that if $\mathfrak{q}$ is a prime ideal and $\mathfrak{q} \subsetneq \mathfrak{p}$ then we have $\mathrm{ht}(\mathfrak{p}) > \mathrm{ht}(\mathfrak{q})$, provided $\mathrm{ht}(\mathfrak{p}) < \infty$.

Let R be a ring. If N is the nilradical of R, then N is contained in every prime ideal of R and thus

$$\dim(R) = \dim(R/N)$$

and

$$\mathrm{ht}(\mathfrak{p}\,(\mathrm{mod}\,N)) = \mathrm{ht}(\mathfrak{p})$$

for any prime ideal $\mathfrak{p}$ of R.

Note finally that from the definitions, we have

$$\dim(R) = \sup\{\mathrm{ht}(\mathfrak{p}) \,|\, \mathfrak{p} \in \mathrm{Spec}(R)\}$$

More generally, for any ideal $I \subseteq R$, we clearly have $\dim(R) \geq \dim(R/I)$.

Lemma 27

Let R be a ring and let $\mathfrak{p} \in \operatorname{Spec}(R)$.

Then $\operatorname{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$. Also, we have

$$\dim(R) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ a maximal ideal of } R\}.$$

Proof. Recall that the prime ideals of $R_{\mathfrak{p}}$ are in one to one correspondence with the prime ideals contained in $\mathfrak{p}$ by Lemma 8.

Furthermore this correspondence preserves inclusion.

The first equality follows directly from this.

For the second one, note that by definition, we have

$$\dim(R) \geq \sup\{\mathrm{ht}(\mathfrak{p}) \,|\, \mathfrak{p} \text{ a maximal ideal of } R\}$$

so we only have to establish the reverse inequality.

To establish this, let $\mathfrak{p}$ be a prime ideal, which is not maximal. Consider a chain of prime ideals

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n,$$

and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. We then have a chain

$$\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n.$$

Hence $\mathrm{ht}(\mathfrak{m}) > \mathrm{ht}(\mathfrak{p})$ and thus we clearly have

$$\begin{aligned}
&\sup\{\mathrm{ht}(\mathfrak{p}) \,|\, \mathfrak{p} \text{ a maximal ideal of } R\} \\
&\geq \sup\{\mathrm{ht}(\mathfrak{p}) \,|\, \mathfrak{p} \text{ a prime ideal of } R\} \\
&= \dim(R).
\end{aligned}$$

□

Note that Lemma 27 has in particular the following consequence.

Let R be a ring and let S be a multiplicative subset of R.

Let $\mathfrak{p}$ be a prime ideal of R_S and let $\lambda : R \to R_S$ be the natural ring homomorphism.

Then $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\lambda^{-1}(\mathfrak{p}))$.

If R is a ring and $I \subseteq R$ is an ideal, we define the *codimension* or *height* $\mathrm{ht}(I)$ of I as follows:

$$\mathrm{ht}(I) := \min\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(R),\, \mathfrak{p} \supseteq I\}.$$

(this generalises the definition of the height of a prime ideal given above).

From the definition, we see that if J is another ideal and $J \subseteq I$, then $\mathrm{ht}(J) \leq \mathrm{ht}(I)$.

If $\mathrm{ht}(I) < \infty$, there is a prime ideal $\mathfrak{p}$, which is minimal among all the prime ideals containing I, and such that $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(I)$.

This follows directly from the definitions.

The two next subsections contain some preliminary results (which are also of independent interest) that we shall need before we resume the study of dimension.

Transcendence bases

Let k be a field and let K be a field containing k.

If $S \subseteq K$ is a finite subset of K, we shall write $k(S)$ for the smallest subfield of K containing k and S.

By construction, $k(S)$ is isomorphic to the field of fractions of the k-algebra $k[S] \subseteq K$.

If $S = \{\alpha_1, \ldots, \alpha_h\}$ then we shall as usual use the shorthand $k(\alpha_1, \ldots, \alpha_h)$ for $k(\{\alpha_1, \ldots, \alpha_h\})$.

If $S_1, S_2 \subset K$ are two finite subsets, we have from the definitions that $k(S_1 \cup S_2) = k(S_1)(S_2)$.

Also, recall that if the elements of S are all algebraic (equivalently, integral) over k, then we actually have $k(S) = k[S]$.

If there is a finite subset S of K such that $K = k(S)$ we say that K is *finitely generated over k as a field*.

This is a weaker condition than *finitely generated as a k algebra* but by the previous paragraph it coincides with it if all the elements of S are algebraic over k.

We say that the set $S \subseteq K$ is a *finite transcendence basis* of K over k if

- S is finite;

- the elements of S are algebraically independent over k;

- K is algebraic (equivalently, integral) over the field $k(S)$.

It is easy to see that if K is finitely generated over k as a field, then K has a transcendence basis over k.

Proposition 0.35

Let K be a field and $k \subseteq K$ a subfield. Suppose that K is finitely generated over k as a field.

Let S and T be two finite transcendence bases of K over k.

Then $\#S = \#T$.

Proof. Omitted. See the notes. □

Let k be a subfield of a field K and suppose that K is finitely generated over k as a field.

In view of the last proposition, we may define the *transcendence degree* $\mathrm{tr}(K|k)$ of k over K as the cardinality of any transcendence basis of K over k.

As a basic example, we have $\mathrm{tr}(k(x_1, \ldots, x_n)|k) = n$ for any field k.

END OF LECTURE 12

The lemma of Artin-Rees and Krull's theorem

Let R be a ring.

A *ring grading* on R is the datum of a sequence $R_0, R_1, \ldots$ of additive subgroups of R, such that $R = \oplus_{i \geq 0} R_i$ and such that $R_i \cdot R_j \subseteq R_{i+j}$ for any $i, j \geq 0$.

One can see from the definition that R_0 is then a subring of R and that $\oplus_{i \geq i_0} R_i$ is an ideal of R for any $i_0 \geq 0$.

Each R_i naturally carries a structure of R_0-module.

Finally, the natural map $R_0 \to R/(\oplus_{i \geq 1} R_i)$ is an isomorphism of rings and we have natural isomorphism of R_0-modules $R_{i_0} \simeq (\oplus_{i \geq i_0} R_i)/(\oplus_{i \geq i_0 + 1} R_i)$ for any $i_0 \geq 0$.

If $r \in R$, we shall often write $[r]_i$ for the projection of r to R_i and we call it the *i-th graded component* of r.

For example, if k is a field, the ring $k[x]$ has a natural grading given by $(k[x])_i = \{a \cdot x^i \mid a \in k\}$.

Any ring carries a trivial grading, such that $R_0 = R$ and $R_i = 0$ for all $i \geq 0$.

Suppose that R is a graded ring.

Let M be an R-module.

A grading on M (relative to the grading on R) is the datum of a sequence $M_0, M_1, \ldots$ of additive subgroups of R, such that $M = \oplus_{i \geq 0} M_i$ and such that $R_i \cdot M_j \subseteq M_{i+j}$ for any $i, j \geq 0$.

In this situation, we say that M is a graded R-module (this is slight abuse of language because the reference to the grading of R is only implicit).

There is an obvious notion of homomorphism of graded R-modules.

Lemma 28

Let R be a graded ring with grading R_i $(i \geq 0)$.

The following are equivalent:

(i) *The ring R is noetherian.*

(ii) *The ring R_0 is noetherian and R is finitely generated as a R_0-algebra.*

Proof. The implication (ii)⇒(i) is a consequence of Hilbert's basis theorem and Lemma 17.

For the the implication (i)⇒(ii) see the notes. □

Let R be a ring and let M be an R-module.

A (descending) *filtration* $M_\bullet$ of M is a sequence of R-submodules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

of M.

If I is an ideal of R, then $M_\bullet$ is said to be a *I-filtration* if $IM_i \subset M_{i+1}$ for all $i \geq 0$.

A I-filtration $M_\bullet$ is said to be *stable* if $IM_i = M_{i+1}$ for all i larger than some fixed natural number.

Now suppose given a ring R, an ideal $I \subseteq R$, a R-module M and a I-filtration $M_\bullet$ on M.

Note that the direct sum of R-modules $R^\# := \oplus_{i \geq 0} I^i$ carries a natural structure of graded ring, with the grading given by the presentation $R^\# = \oplus_{i \geq 0} I^i$.

The ring $R^\#$ is often called the *blow-up algebra* associated with R and I (this terminology comes from algebraic geometry).

The direct sum $M^\# := \oplus_{i \geq 0} M_i$ of R-modules then carries a natural structure of graded $R^\#$-module.

Note that $R^\#$ is naturally a R-algebra, since there is an natural injective homomorphism of rings $R \to R^\#$, sending $r \in R$ to the corresponding element of degree 0.

Lemma 29

Let R be a ring and let $I \subseteq R$ be an ideal. Suppose that R is noetherian. Then the ring $R^{\#}$ associated with R and I is also noetherian.

Proof. Let $r_1, \ldots, r_k \in I$ be generators of I (this exists because R is noetherian).

There is a homomorphism of R-algebras $\phi : R[x_1, \ldots, x_k] \to R^{\#}$, given by the formula $P(x_1, \ldots, x_k) \mapsto P(r_1, \ldots, r_k)$.

Here $r_1, \ldots, r_k$ are viewed as elements of degree 1 in $R^{\#}$ and the coefficients of $P(x_1, \ldots, x_k)$ are viewed as elements of degree 0.

By construction, ϕ is surjective and hence $R^{\#}$ is also noetherian by the Hilbert basis theorem and Lemma 17. $\square$

Lemma 30

Let R be a ring. Let $I \subseteq R$ be an ideal. Let $M_\bullet$ be a I-filtration on M.

Suppose that M_j is finitely generated as a R-module for all $j \geq 0$.

Let $R^\#$ be the corresponding graded ring and let $M^\#$ be the corresponding graded $R^\#$-module.

The following are equivalent:

(i) *The $R^\#$-module $M^\#$ is finitely generated.*

(ii) *The filtration $M_\bullet$ is stable.*

Proof. Let $n \geq 0$ and consider the graded subgroup

$$M^{\#}_{(n)} := (\bigoplus_{j=0}^{n} M_j) \bigoplus (\bigoplus_{k=1}^{\infty} I^k M_n)$$

of $M^{\#}$.

Note that $M^{\#}_{(n)}$ is a sub-$R^{\#}$-module of $M^{\#}$ by construction.

Note also that each M_j with $j \in \{0, \ldots, n\}$ is finitely generated as a R-module by assumption and thus $M^{\#}_{(n)}$ is finitely generated as a $R^{\#}$-module (it is generated by $\bigoplus_{j=0}^{n} M_j$).

We have inclusions

$$M^{\#}_{(0)} \subseteq M^{\#}_{(1)} \subseteq M^{\#}_{(2)} \subseteq \ldots$$

and by construction we have $M^{\#} = \cup_{i=0}^{\infty} M^{\#}_{(i)}$.

Note that saying that the I-filtration $M_\bullet$ is stable is equivalent to saying that $M^{\#}_{(n_0+k)} = M^{\#}_{(n_0)}$ for all $k \geq 0$ and some $n_0 \geq 0$.

We claim that $M^{\#}_{(n_0+k)} = M^{\#}_{(n_0)}$ for all $k \geq 0$ and some $n_0 \geq 0$ iff $M^{\#}$ is finitely generated as a $R^{\#}$-module.

Indeed, if $M^{\#}$ is finitely generated as a $R^{\#}$-module, then $M^{\#}_{(n_0+k)} = M^{\#}_{(n_0)}$ for all $k \geq 0$ as soon as $M^{\#}_{(n_0)}$ contains a given finite set of generators for $M^{\#} = \cup_{i=0}^{\infty} M^{\#}_{(i)}$.

On the other hand, if $M^{\#}_{(n_0+k)} = M^{\#}_{(n_0)}$ for all $k \geq 0$ then $M^{\#} = M^{\#}_{(n_0)}$, and $M^{\#}$ is finitely generated since $M^{\#}_{(n_0)}$ is finitely generated. $\square$

Proposition 0.36 (lemma of Artin-Rees)

Let R be a noetherian ring. Let $I \subseteq R$ be an ideal.

Let M be a finitely generated R-module and let $M_\bullet$ be a stable I-filtration on M.

Let $N \subseteq M$ be a submodule.

Then the filtration $N \cap M_\bullet$ is a stable I-filtration of N.

Proof. By construction, there is a natural inclusion of $R^\#$-modules $N^\# \subseteq M^\#$.

By Lemma 30, the $R^\#$-module $M^\#$ is finitely generated.

The module $N^\#$ is thus also finitely generated by Lemma 29 and by Lemma 19.

Hence $N \cap M_\bullet$ is a stable I-filtration by Lemma 30. $\square$

Corollary 0.37

Let R be a noetherian ring. Let $I \subseteq R$ be an ideal and let M be a finitely generated R-module.

Let $N \subseteq M$ be a submodule.

Then there exists a natural number $n_0 \geq 0$ such that

$$I^n(I^{n_0} M \cap N) = I^{n_0+n} M \cap N.$$

for all $n \geq 0$.

Proof. Apply the lemma of Artin-Rees to the filtration $I^\bullet M$ of M. □

Corollary 0.38 (Krull's theorem)

Let R be a noetherian ring. Let $I \subseteq R$ be an ideal and let M be a finitely generated R-module.

Then we have

$$\cap_{n\geq 0} I^n M = \cup_{r\in 1+I} \ker(r_M)$$

where $r_M : M \to M$ is the map such that $r_M(m) = r \cdot m$ for all $m \in M$.

Proof. Let $N := \cap_{n\geq 0} I^n M$.

By Corollary 0.37, there exists a natural number $n_0 \geq 0$ such that

$$I(I^{n_0} M \cap N) = IN = I^{n_0+1} M \cap N = N$$

We deduce from Q4 of sheet 1 (the general form of Nakayama's lemma) that there exists $r \in R$ such that $r \in 1 + I$ and such that $rN = 0$.

Hence $N = \cap_{n\geq 0} I^n M \subseteq \cup_{r\in 1+I} \ker(r_M)$.

On the other hand, if $r \in 1 + I$, $y \in M$ and $ry = 0$, then $(1 + a)y = y + ay = 0$ for some $a \in I$ and so $y \in IM$.

Since $y + ay = 0$, we conclude that $y \in I^2M$. Continuing in this way, we conclude that $y \in N$. □

Corollary 0.39 (of Krull's theorem)

Let R be a noetherian domain. Let I be an ideal of R.

Then $\cap_{n \geq 0} I^n = 0$.

Proof. This is clear. □

Corollary 0.40 (of Krull's theorem)

Let R be a noetherian ring and let I be an ideal of R. Let M be a finitely generated R-module.

Suppose that I is contained in the Jacobson radical of R.

Then $\cap_{n\geq 0} I^n M = 0$.

Proof. If $r \in 1 + I$ then r is a unit.

Indeed, if r is not a unit, then r is contained in some maximal ideal $\mathfrak{m}$.

But then 1 is also contained in $\mathfrak{m}$, since $I \subseteq \mathfrak{m}$, which is a contradiction.

Hence $\ker(r_M) = 0$ and the result follows from Krull's theorem. □

Corollary 0.40 is especially useful when R is a local ring (in which case I is always contained in the Jacobson radical).

END OF LECTURE 13

Dimension theory of noetherian rings

We first examine the case of dimension 0.

We will call a ring *Artinian* if whenever we have a descending sequence of ideals

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$$

in R, there exists an $n \geq 1$ such that $I_{n+k} = I_n$ for all $k \geq 0$.

We then say that the sequence $I_\bullet$ *stabilises* (compare with Lemma 16).

Lemma 31

Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$. The following are equivalent:

(i) $\dim(R) = 0$;

(ii) $\mathfrak{m}$ *is the nilradical of* R;

(iii) $\mathfrak{m}^n = 0$ *for some* $n \geq 1$;

(iv) R *is Artinian.*

Proof.

(i)⇒(ii): If $\dim(R) = 0$ then every prime ideal of R coincides with $\mathfrak{m}$. Hence $\mathfrak{m}$ is the nilradical of R.

(ii)⇒(iii): This is clear.

(iii)⇒(iv): See the notes.

(iv)$\Rightarrow$(i): Suppose for contradiction that $\dim(R) \neq 0$.

Then there are two prime ideals $\mathfrak{p}_0, \mathfrak{p}_1$ of R such that $\mathfrak{p}_0 \supsetneq \mathfrak{p}_1$.

In particular, we have $\mathfrak{m} \supsetneq \mathfrak{p}_1$.

This implies that $\mathfrak{m}$ is not the nilradical of R.

On the other hand, since R is Artinian, we know that there is a natural number $n_0 \geq 0$ such that $\mathfrak{m}^{n_0} = \cap_{i=0}^{\infty} \mathfrak{m}^i$.

By Corollary 0.40, we have $\cap_{i=0}^{\infty} \mathfrak{m}^i = 0$ so we have $\mathfrak{m}^{n_0} = 0$.

In particular, every element of $\mathfrak{m}$ is nilpotent and $\mathfrak{m}$ is the nilradical of R.

This is a contradiction, so we cannot have $\dim(R) \neq 0$. $\square$

Theorem 0.41 (Krull's principal ideal theorem)

Let R be a noetherian ring.

Let $f \in R$ be an element which is not a unit.

Let $\mathfrak{p}$ be minimal among the prime ideals containing f.

Then we have $\mathrm{ht}(\mathfrak{p}) \leq 1$.

Proof. Note that the maximal ideal of $R_{\mathfrak{p}}$ is minimal among the prime ideals of $R_{\mathfrak{p}}$ containing $f/1 \in R_{\mathfrak{p}}$.

Furthermore, the height of $\mathfrak{p}$ is the same as the height of the maximal ideal of $R_{\mathfrak{p}}$.

Since $R_{\mathfrak{p}}$ is also noetherian, we may thus suppose that R is a local ring and that $\mathfrak{p}$ is a maximal ideal.

Let

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_{k_0}$$

be a chain of prime ideals starting with $\mathfrak{p}$.

We want to show that $k_0 \leq 1$.

We may suppose that $k_0 > 0$ (because if there is no chain as above with $k_0 > 0$ there is nothing to prove).

Write $\mathfrak{q} := \mathfrak{p}_1$. By assumption, we then have $f \notin \mathfrak{q}$.

Write $\lambda : R \to R_{\mathfrak{q}}$ for the natural map (sending r to $r/1$).

For $n \geq 1$, write $\overline{\lambda(\mathfrak{q}^n)}$ for the ideal of $R_{\mathfrak{q}}$ generated by $\lambda(\mathfrak{q}^n)$.

We know that $\overline{\lambda(\mathfrak{q}^n)}$ consists of the elements of the form r/t, where $r \in \mathfrak{q}^n$ and $t \in R \backslash \mathfrak{q}$ (see Lemma 8).

Also, it is easily checked that $\overline{\lambda(\mathfrak{q}^n)} = (\overline{\lambda(\mathfrak{q})})^n$.

Now consider the ideal $I_n := \lambda^{-1}(\overline{\lambda(\mathfrak{q}^n)})$ (this ideal is called the *n-th symbolic power of* $\mathfrak{q}$).

By construction, we have $I_n \supseteq \mathfrak{q}^n$.

Furthermore, we have $I_1 = \mathfrak{q}$ by Lemma 8.

The ideal I_n has the advantage over $\mathfrak{q}^n$ that if $fr \in I_n$ for some $r \in R$, then we must have $r \in I_n$, because

$$\lambda(fr)(1/f) = \lambda(r) \in \overline{\lambda(\mathfrak{q}^n)},$$

noting that $f \in R \backslash \mathfrak{q}$.

Now consider the ring $R/(f)$.

The ring $R/(f)$ is also local (because if $R/(f)$ had more than one maximal ideal, then so would R) and it is noetherian (by Lemma 17).

The ring $R/(f)$ has dimension 0, since its only maximal ideal (given by $\mathfrak{p} \pmod{(f)}$) is a minimal prime ideal of $R/(f)$ by construction.

Now we are given a descending sequence of ideals

$$I_1 \supseteq I_2 \supseteq I_3 \ldots \tag{6}$$

We conclude from Lemma 31 that the image of this sequence in $R/(f)$ must stabilise (note that the image of an ideal by a surjective homomorphism is an ideal).

In other words, there is an $n_0 \geq 1$ with the property that for any $n \geq n_0$, we have $I_n \subseteq I_{n+1} + (f)$.

Furthermore, in this situation, if $r \in I_n$, $t \in I_{n+1}$ and $r = t + hf$ for some $h \in R$, then we have $r - t \in I_n$, so that $h \in I_n$ (see above).

This means that we actually have $I_n \subseteq I_{n+1} + (f)I_n$, and in particular $I_n \subseteq I_{n+1} + \mathfrak{p}I_n$.

In particular, the natural map $I_{n+1}/\mathfrak{p}I_{n+1} \to I_n/\mathfrak{p}I_n$ is surjective.

By Nakayama's lemma, we conclude that $I_{n+1} \to I_n$ is surjective, so that $I_{n+1} = I_n$.

So the sequence (6) stabilises at n_0.

Now note that since $I_n \supseteq \mathfrak{q}^k$ for all $n \geq 1$, we have

$$\overline{\lambda(I_n)} = \overline{\lambda(\mathfrak{q}^n)} = (\overline{\lambda(\mathfrak{q})})^n.$$

Hence the descending sequence of ideals of $R_{\mathfrak{q}}$

$$\overline{\lambda(\mathfrak{q})} \supseteq (\overline{\lambda(\mathfrak{q})})^2 \supseteq (\overline{\lambda(\mathfrak{q})})^3 \supseteq \dots$$

also stabilises at n_0.

But now (this is the crucial step of the proof), Corollary 0.40 implies that

$$\cap_{i \geq 0} (\overline{\lambda(\mathfrak{q})})^i = 0,$$

so that we have $(\overline{\lambda(\mathfrak{q})})^{n_0} = 0$.

Since $\overline{\lambda(\mathfrak{q})}$ is the maximal ideal of $R_{\mathfrak{q}}$ (by Lemma 8), we conclude from Lemma 31 that $R_{\mathfrak{q}}$ has dimension 0.

In particular, we have $\mathrm{ht}(\mathfrak{q}) = 0$ (by Lemma 27).

In other words, $\mathfrak{q}$ cannot contain any prime ideal other than itself. Hence $k = 1$. $\square$

Corollary 0.42

Let R be a noetherian ring.

Let $f_1, \ldots, f_k \in R$.

Let $\mathfrak{p}$ be a prime ideal minimal among those containing $(f_1, \ldots, f_k)$.

Then $\mathrm{ht}(\mathfrak{p}) \leq k$.

Proof. By induction on k.

The case $k = 1$ is Krull's principal ideal theorem. We suppose that $k > 1$ and that the statement is true for $k - 1$ in place of k.

Just as at the beginning of the proof of Krull's principal ideal theorem, we may suppose that R is a local ring with maximal ideal $\mathfrak{p}$.

Let

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{\mathrm{ht}\mathfrak{p}}$$

be a chain of prime ideals beginning with $\mathfrak{p}$ and of length $\mathrm{ht}(\mathfrak{p})$.

Note that by maximality, there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{p}_1$, other than $\mathfrak{p}$ and $\mathfrak{p}_1$.

We may suppose that $\mathrm{ht}(\mathfrak{p}) > 0$, otherwise there is nothing to prove. Let $\mathfrak{q} := \mathfrak{p}_1$.

We claim that $\mathrm{ht}(\mathfrak{q}) \leq k - 1$.

We prove the claim.

By assumption, there exists an f_i, say f_1, such that $f_i \notin \mathfrak{q}$.

Since there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$ other than $\mathfrak{p}$ and $\mathfrak{q}$, we see that $\mathfrak{p}$ is minimal among the prime ideals containing $\mathfrak{q} + (f_1)$.

Hence the ring $R/(\mathfrak{q} + (f_1))$ has dimension 0.

We conclude from Lemma 31 (iii) that the image of all the f_i are nilpotent $R/(\mathfrak{q} + (f_1))$. In other words, for all $i \in \{2, \ldots, k\}$, there are elements $a_i \in R$, $b_i \in \mathfrak{q}$ and $n_i \geq 1$ such that

$$f_i^{n_i} = a_i f_1 + b_i.$$

Hence $(f_1, b_2, \ldots, b_k) = (f_1, f_2^{n_2}, f_3^{n_3}, \ldots, f_k^{n_k})$. Note that

$$\mathfrak{p} \supseteq (f_1, f_2^{n_2}, f_3^{n_3}, \ldots, f_k^{n_k})$$

and that $\mathfrak{p}$ is also minimal among all the prime ideals containing $(f_1, f_2^{n_2}, f_3^{n_3}, \ldots, f_k^{n_k}) = (f_1, b_2, \ldots, b_k)$, since

$$\mathfrak{v}((f_1, f_2^{n_2}, f_3^{n_3}, \ldots, f_k^{n_k})) = \mathfrak{v}((f_1, f_2, \ldots, f_k)).$$

Write $J := (b_2, \ldots, b_k)$. Note that $J \subseteq \mathfrak{q}$.

Since $\mathfrak{p}$ is minimal among all the prime ideals containing f_1 and J, we see that $\mathfrak{p} \pmod{J}$ is minimal among all the prime ideals of R/J containing $f_1 \pmod{J}$.

On the other hand, we have

$$\mathfrak{p} \pmod J \supsetneq \mathfrak{q} \pmod J$$

so that $\operatorname{ht}(\mathfrak{q} \pmod J) = 0$.

In other words, $\mathfrak{q}$ is minimal among all the prime ideals containing J.

Applying the inductive hypothesis, we see that $\operatorname{ht}(\mathfrak{q}) \leq k - 1$.

Finally, we see from the assumptions that $\operatorname{ht}(\mathfrak{p}) \leq \operatorname{ht}(\mathfrak{q}) + 1 \leq k$ and so the corollary is proven. $\square$

In particular, *in a noetherian ring, the height of any prime ideal is finite*.

Together with Lemma 27, this shows that the dimension of a noetherian local ring is finite.

It is not true however that any noetherian ring has finite dimension. For an example of such a ring, see Ex. 3 of chap. 11, p. 126 of AT.

Note also that Corollary 0.42 implies that $\mathrm{ht}((f_1, \ldots, f_k)) \leq k$.

If we have $\mathrm{ht}((f_1, \ldots, f_k)) = k$, then any minimal prime ideal associated with $(f_1, \ldots, f_k)$ has height k (because any such ideal has height $\geq k$ by assumption, and height $\leq k$ by Corollary 0.42).

Corollary 0.43

Let R be a noetherian ring. Let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots$$

be a descending chain of prime ideals of R.

Then there is $i_0 \geq 0$ such that $\mathfrak{p}_{i_0+i} = \mathfrak{p}_{i_0}$ for all $i \geq 0$.

Moreover, if $\mathfrak{p}_0$ is generated by c elements, we have $i_0 \leq c$.

The proof follows directly from Corollary 0.42 and the definition of the height.

Corollary 0.44

Let R be a noetherian ring. Let $\mathfrak{p}$ be a prime ideal of height c.

Suppose that $0 \leq k \leq c$ and that we have elements $t_1, \ldots, t_k \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k)) = k$.

Then there are elements $t_{k+1}, \ldots, t_c \in \mathfrak{p}$, such that $\mathrm{ht}(t_1, \ldots, t_c) = c$.

Proof. Skipped. By induction on k, using Proposition 0.13 (i). See the notes. □

END OF LECTURE 14

The dimension of polynomial rings

We now turn to the computation of the dimension of polynomial rings. The main result is

Theorem 0.45

Let R be a noetherian ring. Suppose that $\dim(R) < \infty$.

Then $\dim(R[x]) = \dim(R) + 1$.

Before we start with the proof, we prove a few intermediate results.

Lemma 32

Let K be a field and let $\mathfrak{p}$ be a non zero prime ideal of $K[x]$.

Then $\mathrm{ht}(\mathfrak{p}) = 1$. *In particular, we have* $\dim(K[x]) = 1$.

Proof. Exercise. This follows from the fact that non zero prime ideals of $K[x]$ are maximal and from the fact that the zero ideal in $K[x]$ is prime, since $K[x]$ is a domain. □

If R is a ring and $\mathfrak{a}$ is an ideal of R, we shall write $\mathfrak{a}[x]$ for the ideal generated by $\mathfrak{a}$ in $R[x]$.

The ideal $\mathfrak{a}[x]$ can easily be seen to consist of the polynomials with coefficients in $\mathfrak{a}$ (hence the notation).

If the ideal $\mathfrak{a}$ is also prime, then so is $\mathfrak{a}[x]$, since

$$R[x]/\mathfrak{a}[x] \simeq (R/\mathfrak{a})[x]$$

and $(R/\mathfrak{a})[x]$ is a domain, if $R/\mathfrak{a}$ is a domain.

The construction of the following Lemma already appears in Proposition 0.26.

Lemma 33

Let $\phi : R \to T$ be a ring homomorphism.

Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and let I be the ideal generated by $\phi(\mathfrak{p})$ in T.

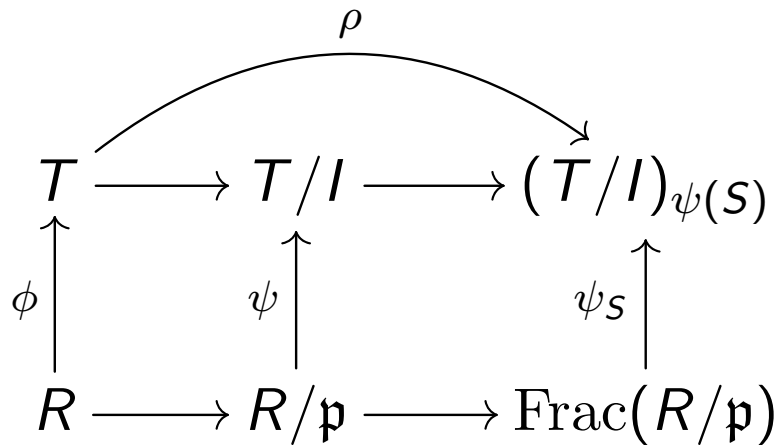
Write $\psi : R/\mathfrak{p} \to T/I$ for the ring homomorphism induced by ϕ and let $S := (R/\mathfrak{p})^*$.

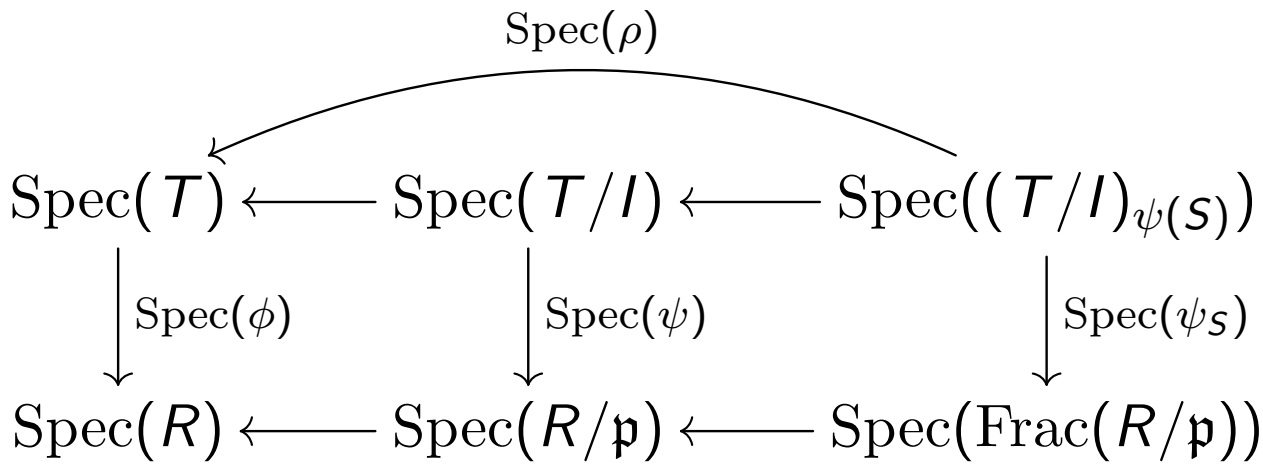
Write $\psi_S : \mathrm{Frac}(R/\mathfrak{p}) \to (T/I)_{\psi(S)}$ for the induced ring homomorphism.

Finally, write $\rho : T \to (T/I)_{\psi(S)}$ for the natural ring homomorphism.

Then $\mathrm{Spec}(\rho)(\mathrm{Spec}((T/I)_{\psi(S)})$ consists precisely of the prime ideals $\mathfrak{q}$ of T, such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

In diagrams:





The lemma is saying that the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$ is precisely the image of $\mathrm{Spec}(\rho)$.

The proof is straightforward (see proof of Proposition 0.26).

The previous lemma will be applied below in the situation where $T = R[x]$. In this situation, we have

$$(T/I)_{\psi(S)} = (R[x]/\mathfrak{p}[x])_{\psi(S)} \simeq (R/\mathfrak{p})[x]_{(R/\mathfrak{p})^*} = \mathrm{Frac}(R/\mathfrak{p})[x].$$

Here we used the fact that if A is a domain, we have a natural identification

$$(A[x])_{A^*} \simeq \mathrm{Frac}(A)[x]$$

(exercise).

Lemma 34

We keep the notation of Lemma 33.

Suppose that we have a chain of prime ideals

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_k$$

in T, such that $\phi^{-1}(\mathfrak{q}_i) = \mathfrak{p}$ for all $i \in \{0, \ldots, k\}$.

Then $k \leq \dim((T/I)_{\psi(S)})$.

Proof. Immediate from Lemma 33. □

Lemma 35

Let R be a ring and let N be the nilradical of R.

Then the nilradical of $R[x]$ is $N[x]$.

Proof. Any element of $N[x]$ is a polynomial with nilpotent coefficients and its thus clearly nilpotent (check).

On the other hand, let $P(x) = a_0 + a_1 x + \cdots + a_d x^d \in R[x]$ be an element of the nilradical of $R[x]$ (ie a nilpotent polynomial).

Suppose for contradiction that $P(x)$ has a coefficient a_i, which is not nilpotent.

Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be a prime ideal, such that $a_i \notin \mathfrak{p}$.

Then $P(x) \pmod{\mathfrak{p}} \in (R/\mathfrak{p})[x]$ is a non zero nilpotent polynomial.

This is contradiction, since $(R/\mathfrak{p})[x]$ is a domain. $\square$

Lemma 36

Let R be a noetherian ring and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the minimal prime ideals of R.

Then the minimal prime ideals of $R[x]$ are the ideals $\mathfrak{p}_1[x], \ldots, \mathfrak{p}_k[x]$.

More generally, if $\mathfrak{a}$ is an ideal of R and $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are the minimal prime ideals associated with $\mathfrak{a}$, then the ideals $\mathfrak{p}_1[x], \ldots, \mathfrak{p}_k[x]$ are the minimal prime ideals associated with $\mathfrak{a}[x]$.

Proof. We first prove the first statement. Note that we have $\bigcap_i \mathfrak{p}_i = \mathfrak{r}((0))$, because the nilradical $\mathfrak{r}((0))$ of R is decomposable by the Lasker-Noether theorem.

We deduce from this that $\bigcap_i \mathfrak{p}_i[x] = \mathfrak{r}((0))[x]$. Thus $\bigcap_i \mathfrak{p}_i[x]$ is a minimal primary decomposition of $\mathfrak{r}((0))[x]$.

In view of Lemma 35, this implies that the minimal prime ideals of $R[x]$ are precisely the ideals $\mathfrak{p}_1[x], \ldots, \mathfrak{p}_k[x]$ (use Theorem 0.15 and Lemma 15), which is what we wanted to prove.

For the second statement, apply the first statement to $\mathfrak{p} \pmod{\mathfrak{a}}$, noting that $(R/\mathfrak{a})[x] \simeq R[x]/\mathfrak{a}[x]$ (or provide a direct proof, similar to the proof for $\mathfrak{a} = (0)$). $\square$

Lemma 37

Let R be a noetherian ring and let $\mathfrak{a}$ be an ideal of R. Then $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{a}[x])$.

Proof. Suppose first that the lemma is proven if $\mathfrak{a}$ is a prime ideal.

We know that there is a minimal prime ideal $\mathfrak{p}$ associated with $\mathfrak{a}$, such that $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{a})$.

We conclude from this that $\mathrm{ht}(\mathfrak{a}[x]) \leq \mathrm{ht}(\mathfrak{p}[x]) = \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{a})$.

On the other hand there is a minimal prime ideal $\mathfrak{q}$ associated with $\mathfrak{a}[x]$ such that $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{a}[x])$.

By Lemma 36 we have $\mathfrak{q} = (\mathfrak{q} \cap R)[x]$ so that $\mathrm{ht}(\mathfrak{a}[x]) = \mathrm{ht}(\mathfrak{q} \cap R) \geq \mathrm{ht}(\mathfrak{a}[x] \cap R) = \mathrm{ht}(\mathfrak{a})$.

Hence $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{a}[x])$.

So we only need to prove the statement if $\mathfrak{a} = \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of R.

Let $c := \mathrm{ht}(\mathfrak{p})$ and let $a_1, \ldots, a_c \in \mathfrak{p}$ be such that $\mathrm{ht}((a_1, \ldots, a_c)) = c$, so that $\mathfrak{p}$ is a minimal prime ideal associated with $(a_1, \ldots, a_c)$. This exists by Corollary 0.44.

Let $J := (a_1, \ldots, a_c)$. By the previous lemma, $\mathfrak{p}[x]$ is a minimal prime ideal associated with $J[x]$.

We conclude from Corollary 0.42 that $\mathrm{ht}(\mathfrak{p}[x]) \leq c$ (since the elements $a_1, \ldots, a_c$ generate $J[x]$ in $R[x]$).

On the other hand, if

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \cdots \supsetneq \mathfrak{p}_c$$

is a descending of prime ideals in R, then

$$\mathfrak{p}[x] \supsetneq \mathfrak{p}_1[x] \supsetneq \mathfrak{p}_2 \cdots \supsetneq \mathfrak{p}_c[x]$$

is a descending chain of prime ideals in $R[x]$, so that $\mathrm{ht}(\mathfrak{p}[x]) \geq c$. Hence $\mathrm{ht}(\mathfrak{p}[x]) = c$. $\square$

Lemma 38

Let $\mathfrak{q}$ be a prime ideal of $R[x]$ and let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{a} \subseteq \mathfrak{q} \cap R$.

Suppose that $\mathfrak{q} \cap R$ is a minimal prime ideal associated with $\mathfrak{a}$.

Let $\mathfrak{q}' \subseteq \mathfrak{q}$ be a prime ideal of $R[x]$, which is a minimal prime ideal associated with $\mathfrak{a}[x]$.

Then $\mathfrak{q}' = (\mathfrak{q} \cap R)[x]$.

Proof. We have

$$\mathfrak{q}' \cap R \supseteq \mathfrak{a}[x] \cap R = \mathfrak{a}$$

and thus

$$(\mathfrak{q}' \cap R)[x] \supseteq \mathfrak{a}[x].$$

Hence

$$\mathfrak{q}' \supseteq (\mathfrak{q}' \cap R)[x] \supseteq \mathfrak{a}[x].$$

By minimality, we thus have $\mathfrak{q}' = (\mathfrak{q}' \cap R)[x]$.

On the other hand, we have $\mathfrak{q}' \subseteq \mathfrak{q}$, so that

$$\mathfrak{q}' = (\mathfrak{q}' \cap R)[x] \subseteq (\mathfrak{q} \cap R)[x].$$

Now by Lemma 36, we know that $(\mathfrak{q} \cap R)[x]$ is a minimal prime ideal associated with $\mathfrak{a}[x]$ and thus we must have $\mathfrak{q}' = (\mathfrak{q} \cap R)[x]$. □

Proposition 0.46

Let R be a noetherian ring and $\mathfrak{m}$ be a prime ideal of $R[x]$. Then

$$\operatorname{ht}(\mathfrak{m}) \leq 1 + \operatorname{ht}(\mathfrak{m} \cap R).$$

If $\mathfrak{m}$ is maximal, we even have

$$\operatorname{ht}(\mathfrak{m}) = 1 + \operatorname{ht}(\mathfrak{m} \cap R).$$

Proof. Let $\delta := \operatorname{ht}(\mathfrak{m} \cap R)$ and let $c := \operatorname{ht}(\mathfrak{m})$.

Note that since $(\mathfrak{m} \cap R)[x] \subseteq \mathfrak{m}$, we have $\delta \leq c$ by Lemma 37. Let $a_1, \ldots, a_c \in \mathfrak{m}$ be such that $\operatorname{ht}((a_1, \ldots, a_i)) = i$ for all $i \in \{1 \ldots, c\}$. This exists by Corollary 0.44.

Using Lemma 37 again, we may suppose that $a_1, \ldots, a_\delta \in \mathfrak{m} \cap R$.

In particular, $(\mathfrak{m} \cap R)[x]$ is a minimal prime ideal associated with $(a_1, \ldots, a_\delta)$.

We shall now inductively define a chain a of prime ideals

$$\mathfrak{m} = \mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_c$$

such that $\mathfrak{q}_i$ is a minimal prime ideal associated with $(a_1, \ldots, a_{c-i})$.

We let $\mathfrak{q}_0 := \mathfrak{m}$ and we suppose that $i > 0$ and that the ideals $\mathfrak{q}_0, \ldots, \ldots \mathfrak{q}_{i-1}$ are given.

We then let $\mathfrak{q}_i$ be a (arbitrary) minimal prime ideal associated with $(a_1, \ldots, a_{c-i})$, which is contained in $\mathfrak{q}_{i-1}$.

We have thus constructed our chain of prime ideals.

Note that we have by construction $\mathrm{ht}(\mathfrak{q}_i) = c - i$ (see after Corollary 0.42).

Now note the key fact that both $\mathfrak{q}_{c-\delta}$ and $(\mathfrak{m} \cap R)[x]$ are minimal prime ideals associated with $(a_1, \ldots, a_\delta)$.

Applying Lemma 38, we find that we actually have

$$\mathfrak{q}_{c-\delta} = (\mathfrak{m} \cap R)[x].$$

We thus see that for all $i \in \{0, \ldots, c - \delta\}$, we have

$$\mathfrak{m} \supseteq \mathfrak{q}_i \supseteq (\mathfrak{m} \cap R)[x]$$

and thus

$$\mathfrak{m} \cap R \supseteq \mathfrak{q}_i \cap \mathfrak{m} \supseteq \mathfrak{m} \cap R$$

so that $\mathfrak{q}_i \cap R = \mathfrak{m} \cap R$.

We now conclude from Lemma 34 and Lemma 32 that

$$c-\delta \leq \dim((R[x]/(\mathfrak{m}\cap R)[x])_{(R/(\mathfrak{m}\cap R))^*}) = \dim(\mathrm{Frac}(R/(\mathfrak{m}\cap R))[x]) \leq 1.$$

This proves the first statement.

For the second one, note that if $\mathfrak{m}$ is maximal then $\mathfrak{m} \neq (\mathfrak{m}\cap R)[x] = \mathfrak{q}_{c-\delta}$ (because $(\mathfrak{m}\cap R)[x]$ is not maximal), so that $c-\delta \geq 1$.

In particular, we then have that $c = \delta + 1$, as required. □

Proof of Theorem 0.45.

We first show that $\dim(R[x]) \geq \dim(R) + 1$.

For this, let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{\dim(R)}$$

be a chain of prime ideals of maximum length in R.

From this, we obtain as earlier a chain

$$\mathfrak{p}_0[x] \supsetneq \mathfrak{p}_1[x] \supsetneq \cdots \supsetneq \mathfrak{p}[x]_{\dim(R)}$$

in $R[x]$. Now $\mathfrak{p}_0[x]$ is not a maximal ideal, so there is a maximal ideal $\mathfrak{m}$ in $R[x]$ so that

$$\mathfrak{m} \supsetneq \mathfrak{p}_0[x] \supsetneq \mathfrak{p}_1[x] \supsetneq \cdots \supsetneq \mathfrak{p}[x]_{\dim(R)}$$

In particular, $\dim(R[x]) \geq \dim(R) + 1$.

We now show that $\dim(R[x]) \leq \dim(R) + 1$.

Let $\mathfrak{m}$ be a maximal ideal of $R[x]$ so that $\mathrm{ht}(\mathfrak{m}) = \dim(R[x])$.

This exists by Lemma 27. We then have $\mathrm{ht}(\mathfrak{m}) = 1 + \mathrm{ht}(\mathfrak{m} \cap R)$ by the last proposition.

We must then have $\mathrm{ht}(\mathfrak{m} \cap R) = \dim(R)$.

Indeed, suppose for contradiction that $\mathrm{ht}(\mathfrak{m} \cap R) < \dim(R)$.

Then there is there a maximal ideal $\mathfrak{p}$ in R, so that $\mathrm{ht}(\mathfrak{p}) > \mathrm{ht}(\mathfrak{m} \cap R)$. Let $\mathcal{N}$ be a maximal ideal of $R[x]$, which contains $\mathfrak{p}[x]$.

By maximality, we have $\mathcal{N} \cap R = \mathfrak{p}$, so that $\mathrm{ht}(\mathcal{N}) = 1 + \mathrm{ht}(\mathfrak{p}) > 1 + \mathrm{ht}(\mathfrak{m} \cap R) = \mathrm{ht}(\mathfrak{m})$, a contradiction.

So we conclude that $\mathrm{ht}(\mathfrak{m}) = \dim(R[x]) = \dim(R) + 1$, as required. $\square$

Remarks. Let R be a noetherian ring and let $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals of R.

We then obviously have

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{ht}(\mathfrak{q} \,(\mathrm{mod}\, \mathfrak{p})) \leq \mathrm{ht}(\mathfrak{q})$$

(where $\mathfrak{q} \,(\mathrm{mod}\, \mathfrak{p})$ is an ideal of $R/\mathfrak{p}$).

However it is <u>not</u> true that $\mathrm{ht}(\mathfrak{p}) + \mathrm{ht}(\mathfrak{q} \,(\mathrm{mod}\, \mathfrak{p})) = \mathrm{ht}(\mathfrak{q})$ in general.

One class of rings, where equality holds is the class of so called *catenary* domains.

One can show that finitely generated algebras over fields are catenary.

So equality will hold if R is a domain, which is finitely generated over a field (we will not prove this however).

Note that in the proof of Proposition 0.46, we showed that $\mathrm{ht}((\mathfrak{m} \cap R)[x]) + \mathrm{ht}(\mathfrak{m}/(\mathfrak{m} \cap R)[x]) = \mathrm{ht}(\mathfrak{m})$ (why?) and the fact that equality holds in this situation was crucial in the proof.

Corollary 0.47

Let R be a noetherian ring. Suppose that $\dim(R) < \infty$.

Then $\dim(R[x_1, \ldots, x_t]) = \dim(R) + t$.

Proof. This follows from Theorem 0.45 and Hilbert's basis theorem. □

Corollary 0.48

Let k be a field and let R be a finitely generated k-algebra.

Suppose that R is a domain and let $K := \mathrm{Frac}(R)$.

Then $\dim(R)$ and $\mathrm{tr}(K|k)$ are finite and $\dim(R) = \mathrm{tr}(K|k)$.

For the proof of the corollary, we shall need the

Lemma 39

Let R be a subring of a ring T. Suppose that T is integral over R. Then $\dim(T) = \dim(R)$.

Note that the lemma also holds if R or T has infinite dimension (in which case it says that the other ring also has infinite dimension).

Proof. (of the lemma) Suppose first that $\dim(R), \dim(T) < \infty$.

Let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{\dim(R)}$$

be a descending chain of prime ideals in R, which is of maximal length.

By Theorem 0.23, there is a prime ideal $\mathfrak{q}_{\dim(R)}$ in T such that $\mathfrak{q}_{\dim(R)} \cap R = \mathfrak{p}_{\dim(R)}$.

Also, by Q6 of sheet 2, there are prime ideals $\mathfrak{q}_i$ in T, such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ and such that

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(R)}.$$

Hence $\dim(T) \geq \dim(R)$.

Now, resetting terminology, let

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(T)}.$$

be a descending chain of prime ideals in T, which is of maximal length.

Then we have

$$\mathfrak{q}_0 \cap R \supsetneq \mathfrak{q}_1 \cap R \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(T)} \cap R.$$

by Q1 of sheet 3. Hence $\dim(T) \leq \dim(R)$ and thus $\dim(T) = \dim(R)$.

The argument in the situation where either $\dim(R) = \infty$ or $\dim(T) = \infty$ proceeds along the same lines and is left to the reader. $\square$

Proof of Corollary 0.48 . By Noether's normalisation lemma, there is for some $d \geq 0$ an injection of rings $k[x_1, \ldots, x_d] \hookrightarrow R$, which makes R into an integral $k[x_1, \ldots, x_d]$-algebra.

From the previous lemma and Corollary 0.47, we deduce that $\dim(R) = d$.

On the other hand, the fraction field $k(x_1, \ldots, x_d)$ of $k[x_1, \ldots, x_d]$ is naturally a subfield of K and since every element of R is integral over $k[x_1, \ldots, x_d]$, we see that every element of K is algebraic over $k(x_1, \ldots, x_d)$ (why?).

Hence

$$\mathrm{tr}(K|k) = \mathrm{tr}(k(x_1, \ldots, x_d)|k) = d = \dim(R).$$

□

END OF LECTURE 15

Dedekind rings

A *Dedekind domain* is a noetherian ring of dimension one, which is integrally closed.

Examples of Dedekind domains include $\mathbb{Z}$ and polynomial rings in one variable over a field.

We will see that in a Dedekind domain, every ideal can be written in unique fashion as a product of powers of distinct prime ideals.

This unique decomposability generalises to ideals the decomposability into irreducibles of an element that exists in a UFD (and in fact a Dedekind domain is a UFD iff it is a PID - see Sheet 4).

We will also see below that the integral closure of $\mathbb{Z}$ in a finite extension of $\mathbb{Q}$ is a Dedekind domain.

This last kind of ring is much studied in algebraic number theory.

We first note a couple of simple facts:

Lemma 40

Let R be a Dedekind domain.

(i) *All the non-zero prime ideals of R are maximal.*

(ii) *If $\mathfrak{q}_1, \mathfrak{q}_2$ are primary ideals and $\mathfrak{r}(\mathfrak{q}_1) \neq \mathfrak{r}(\mathfrak{q}_2)$ then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are coprime.*

Proof. Skipped. See the notes. The proof uses the next lemma. □

Lemma 41

Let R be a ring. Suppose that the ideals $\mathfrak{r}(I)$ and $\mathfrak{r}(J)$ of R are coprime.

Then I and J are coprime.

Proof. See the notes. □

Lemma 42

Let R be an integrally closed domain.

Then $R_{\mathfrak{p}}$ is also integrally closed for all $\mathfrak{p} \in \operatorname{Spec}(R)$.

Proof. Exercise. Use Lemma 23. □

Proposition 0.49

Let R be a noetherian local domain of dimension one with maximal ideal $\mathfrak{m}$.

The following conditions are equivalent:

(1) *R is integrally closed;*

(2) *$\mathfrak{m}$ is a principal ideal;*

(3) *for any non-zero ideal I of R, we have $I = \mathfrak{m}^n$ for a uniquely determined $n \geq 0$.*

Proof. Let K be the fraction field of R.

(1)⇒(2): Let $a \in \mathfrak{m} \backslash \{0\}$. Note that the ring $R/(a)$ is local with maximal ideal $\mathfrak{m} \pmod{(a)}$ and noetherian (see the beginning of the proof of Krull's principal ideal theorem for details).

Furthermore, we have $\mathrm{ht}(\mathfrak{m} \pmod{(a)}) = \dim(R/(a)) = 0$, because if there were a prime ideal properly contained in $\mathfrak{m} \pmod{(a)}$, this would lead to a descending chain $\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq (0)$ of prime ideals in R, which contradicts the assumption that $\mathrm{ht}(\mathfrak{m}) = 1$.

By Lemma 31, the ideal $\mathfrak{m} \pmod{(a)}$ is thus nilpotent. Let $n > 0$ be the minimal integer such that

$$(\mathfrak{m} \pmod{(a)})^n = (\mathfrak{m}^n \pmod{(a)}) = (0)$$

and let $b \in \mathfrak{m}^{n-1}$ be such that $b \pmod{(a)} \neq 0$.

Now let $x = a/b \in K$. We have $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$ so that $x^{-1}\mathfrak{m} \subseteq R$.

Furthermore, we have $x^{-1} \notin R$, for otherwise we would have $b = x^{-1} \cdot a \in (a)$, which is excluded by assumption.

We claim that we cannot have $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$.

Indeed, suppose that $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$.

Then x^{-1} induces a homomorphism of R-modules $\mathfrak{m} \to \mathfrak{m}$ (given by multiplication by x^{-1}) and such a homomorphism is annihilated by a monic polynomial $P(x)$ with coefficients in R by Proposition 0.19 (because $\mathfrak{m}$ is finitely generated, as R is noetherian).

We then have $P(x^{-1})(h)$ for any non zero element $h \in \mathfrak{m}$ and since R is a domain this implies that $P(x^{-1}) = 0$.

Since R is integrally closed, this implies that $x^{-1} \in R$, which is a contradiction.

Hence $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ and since R is local, we thus must have $x^{-1}\mathfrak{m} = R$. In other words, $x \in R$ and $\mathfrak{m} = (x)$.

(2)⇒(3): See the notes.

(3)⇒(1): See the notes. □

Corollary 0.50

The localisation of a Dedekind domain at a non zero prime ideal is a PID.

The proof is immediate.

Corollary 0.51

Let R be a Dedekind domain.

Then any primary ideal is equal to a power of its radical.

Proof. By localisation. See the notes. □

Proposition 0.52

Let R be a Dedekind domain. Let I be an ideal in R.

Then all the minimal primary decompositions of I are equal up to reindexing.

Proof. Again by localisation. See the notes. □

We conclude from Proposition 0.52 that

in a Dedekind domain, every ideal can be written in a unique way (up to reindexing) as a product of powers of distinct prime ideals.

The next three results require some knowledge of Galois Theory.

Proposition 0.53

Let R be an integrally closed domain and let K be its fraction field. Let $L|K$ be a finite separable extension. Then

(1) the fraction field of the integral closure of R in L is L;

(2) the integral closure of R in L is finite over R.

Proof. Omitted. See AT, Th. 5.17, p. 64. The proof of (1) is easy (prove it).

The proof of (2) exploits the fact that the so-called "trace form" associated with a finite separable extensions is non-degenerate. □

Corollary 0.54

Let R be Dedekind domain with fraction field K. Let L be a finite separable extension of K. Let T be the integral closure of R in L.

Then T is also a Dedekind domain.

Proof. The ring R is clearly a domain, and it is integrally closed by Lemma 22 and Proposition 0.53 (1).

Also, the ring R is of dimension 1 by Lemma 39.

Finally, by the Hilbert basis theorem, T is noetherian.

Indeed, T is finite, and in particular finitely generated over R, and R is noetherian by assumption. □

Proposition 0.55

Let R be an integrally closed domain and let K be its fraction field.

Let $L|K$ be a finite Galois extension of K.

Let T be the integral closure of R in L.

Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and let $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathrm{Spec}(T)$ be prime ideals of T such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R = \mathfrak{p}$.

Then there exists an element $\sigma \in \mathrm{Gal}(L|K)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.

Note that $\sigma(T) \subseteq T$ for all $\sigma \in \mathrm{Gal}(L|K)$ (why?).

In particular, each $\sigma \in \mathrm{Gal}(L|K)$ induces an automorphism $\sigma|_T : T \xrightarrow{\sim} T$ of R-algebras, with inverse $(\sigma^{-1})|_T$.

Proof. Suppose first that

$$\mathfrak{q}_2 \subseteq \bigcup_{\sigma \in \mathrm{Gal}(L|K)} \sigma(\mathfrak{q}_1).$$

In this situation, Proposition 0.13 (i) implies that $\mathfrak{q}_2 \subseteq \tau(\mathfrak{q}_1)$ for a particular $\tau \in \mathrm{Gal}(L|K)$.

According to Q1 of sheet 3, this is only possible if $\mathfrak{q}_2 = \tau(\mathfrak{q}_1)$ and hence we are done in this situation.

Now suppose that

$$\mathfrak{q}_2 \not\subseteq \bigcup_{\sigma \in \mathrm{Gal}(L|K)} \sigma(\mathfrak{q}_1).$$

In particular, there is an element $e \in \mathfrak{q}_2$ such that $e \notin \sigma(\mathfrak{q}_1)$ for all $\sigma \in \mathrm{Gal}(L|K)$, or in other words such that $\sigma(e) \notin \mathfrak{q}_1$ for all $\sigma \in \mathrm{Gal}(L|K)$.

Now consider that the element $f := \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(e)$ is invariant under $\mathrm{Gal}(L|K)$ by construction.

Hence f lies in $K \cap T$, since $L|K$ is a Galois extension.

Since R is integrally closed, we have $K \cap T = R$, so $f \in R$.

On the other hand, since $e \in \mathfrak{q}_2$ and $\mathfrak{q}_2$ is an ideal, we also have $f \in \mathfrak{q}_2$, so that $f \in R \cap \mathfrak{q}_2 = \mathfrak{p}$.

In particular, $f \in R \cap \mathfrak{q}_1 = \mathfrak{p}$.

Now since $\mathfrak{q}_1$ is a prime ideal, this implies that one of the elements $\sigma(e)$ (for some $\sigma \in \mathrm{Gal}(L|K)$) lies in $\mathfrak{q}_1$, which is a contradiction.

Hence we must have $\mathfrak{q}_2 \subseteq \bigcup_{\sigma \in \mathrm{Gal}(L|K)} \sigma(\mathfrak{q}_1)$ and we can conclude using the argument given above. $\square$

The following final lemma (and the complement that follows) plays a key role in Algebraic Number Theory.

Lemma 43

Let R be a Dedekind domain with fraction field K.

Let $L|K$ be a finite separable extension of K and let T be the integral closure of R in L (recall that T is also a Dedekind domain by Corollary 0.54).

Let $\mathfrak{p}$ be a non-zero prime ideal in R.

Let $\bar{\mathfrak{p}} = \mathfrak{p}T$ be the ideal generated by $\mathfrak{p}$ in T.

Let

$$\bar{\mathfrak{p}} = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_k^{n_k}$$

be the minimal primary decomposition of $\bar{\mathfrak{p}}$.

Then the $\mathfrak{q}_i$ are precisely the prime ideals $\mathfrak{q}$ of T which have the property that $\mathfrak{q} \cap R = \mathfrak{p}$.

Proof. We have already seen that $\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_k^{n_k} = \mathfrak{q}_1^{n_1} \cap \cdots \cap \mathfrak{q}_k^{n_k}$.

Hence $\mathfrak{q}_i \cap R \supseteq \mathfrak{p}$ and thus $\mathfrak{q}_i \cap R = \mathfrak{p}$, since $\mathfrak{p}$ is maximal.

Thus the $\mathfrak{q}_i$ are among the prime ideals $\mathfrak{q}$ of T, with the property that $\mathfrak{q} \cap R = \mathfrak{p}$.

Conversely, let $\mathfrak{q}$ be a prime ideal of T, such that $\mathfrak{q} \cap R = \mathfrak{p}$.

Then

$$\mathfrak{q} \supseteq \mathfrak{q}_1^{n_1} \cap \cdots \cap \mathfrak{q}_k^{n_k}$$

and thus by Proposition 0.13 (ii), we have $\mathfrak{q} \supseteq \mathfrak{q}_i^{n_i}$ for some i.

Since $\mathfrak{q}_i$ is the radical of $\mathfrak{q}_i^{n_i}$, we thus have $\mathfrak{q} \supseteq \mathfrak{q}_i$ and thus $\mathfrak{q} = \mathfrak{q}_i$ (again because $\mathfrak{q}_i$ is maximal). $\square$

Complement. We keep the notation of the last lemma.

If $F_2|F_1$ is a finite field extension, recall that one writes $[F_2 : F_1]$ for the dimension of F_2 as a F_1-vector space.

Write $f_i := [T/\mathfrak{q}_i : \mathrm{R}/\mathfrak{p}]$.

One can show that

$$\sum_i n_i f_i = [L : K].$$

See S. Lang, Algebraic Number Theory, I, par. 7, Prop. 21, p. 24 for a proof.

The integer n_i is called the *ramification degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$.

Finally, note that it follows from Proposition 0.52 and Proposition 0.55 that the integers n_i and f_i are independent of i if $L|K$ is a Galois extension (why?).

END OF LECTURE 16