Commutative Algebra. Lectures 1-16 (all lectures).

Damian RÖSSLER*

Hilary Term

PLEASE LET ME KNOW OF ANY MISTAKES OR TYPOS THAT YOU FIND IN THESE NOTES[1]

Contents

*Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom

[1]I am so very grateful to Yutong Dai, who carefully read the text and provided me with a long list of typos.

1 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 these notes.

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.

2 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.

In particular, we assume that the following notions/terminology is known:

ring, product of rings, subring, domain (or integral domain, or entire ring), field, homomorphism of rings, module over a ring, finitely generated module over a ring, ideal, ideal generated by a set, product of two ideals, intersection of a family of ideals, sum of a family of ideals, coprime ideals, submodule, intersection of family of submodules, sum of a family of submodules, submodule generated by a set, quotient module, direct sum of modules over a ring, homomorphisms of modules over a ring, prime ideal, maximal ideal, ring of polynomials over a ring, zero-divisor, unit, Chinese remainder theorem, Euclidean division, fraction field of a domain.

The basic reference for this course is the book

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

We shall refer to this book as "AT".

Note however that certain parts of section 8 and section 10 are not covered by this book.

If in doubt, all the terms (and the associated symbols, which are standard) in the list above are defined in the first chapter of AT.

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.

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-times) $= 0$.

The ring R is *local* if it has a single maximal ideal $\mathfrak{m}$. Note that in this case, every element of $R\backslash\mathfrak{m}$ is a unit (because otherwise, any such element would be contained in a non trivial maximal ideal of R, which would not coincide with $\mathfrak{m}$ - see Lemma 2.4 below).

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 is a ring, a *zero-divisor* of R is an element $r \in R$ such that there exists an element $r' \in R\backslash\{0\}$ such that $r \cdot r' = 0$. Note that 0 is always a zero-divisor of R.

A *domain* or (*integral domain*) is a ring R with the property that the set of zero-divisors of R consists only of 0.

A *Unique Factorisation Domain* (UFD) or *factorial ring* is a domain R, which has the following property. For any $r \in R\backslash\{0\}$, there is a sequence $r_1, \ldots, r_k \in R$ (for some $k \geq 1$), st

(1) all the r_i are irreducible;

(2) $(r) = (r_1 \cdots r_k)$;

(3) if $r'_1, \ldots, r'_{k'}$ is another sequence with properties (1) and (2), then $k = k'$ and there is a permutation $\sigma \in S_k$ st $(r_i) = (r'_{\sigma(i)})$ for all $i \in \{1, \ldots, k\}$.

If R, T are rings, then T is said to be a *R-algebra* if there is a homomorphism of rings $R \to T$. Note that this homomorphism is part of the datum of a R-algebra, so that strictly speaking, it is not T which should be called a R-algebra, but the homomorphism $R \to T$. Note also that a R-algebra T naturally carries a structure of R-module. 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 $R[x_1, \ldots, x_k] \to T$ (where $R[x_1, \ldots, x_k] = R$ if $k = 0$). Note the following elementary fact: if $R \to T$ (resp. $T \to W$) is a finitely generated R-algebra (resp. a finitely generated T-algebra), then the composed map $R \to W$ makes W into a finitely generated R-algebra (why?).

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

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

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

From the definitions, we see that $(I : J)$ is also an ideal and that $((0) : J) = \mathrm{Ann}(J)$. If $x, y \in R$, we shall often write $(I : x)$ for $(I : (x))$, $(x : I)$ for $((x), I)$ and $(x : y)$ for $((x) : (y))$. Note that if M is another ideal of R, we have $(I : M) \cap (J : M) = (I \cap J : M)$ (why?).

Let

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

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 2.1 (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 $\phi(r) = \prod_{i=1}^{k}(r \,(\mathrm{mod}\, I_i))$ 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 $i \neq j$, and 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 2.2 (Euclidean division)**.** *Let R be a ring. Let $P(x), T(x) \in R[x]$ and 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 $\deg(J(x)) < \deg(T(x))$ (here we set the degree of the zero polynomial to be $-\infty$).

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 $s = t$.

Note that if S is partially ordered by the relation $\leq$ and $T \subseteq S$ is a subset, then the relation $\leq$ restricts to a partial order on T.

Proposition 2.3 (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 (with the restriction of the relation $\leq$ to T), 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. □

A classical application of Zorn's lemma is the following.

Lemma 2.4. *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 $\cup_{J \in \mathcal{T}} J$ (verify that this is an ideal containing I; it is non trivial because otherwise we would have $1 \in J$ for some $J \in \mathcal{T}$). 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 $M \subseteq J$. In other words, M is a maximal ideal of R, which contains I. $\square$

END OF LECTURE 1

3 The nilradical and the Jacobson radical

Definition 3.1. *Let R be a ring. The nilradical of R is the set of nilpotent elements of R.*

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 3.2. *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 (verify that the assumptions of Zorn's lemma are verified). 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 $(x) + M$ strictly contains M and hence cannot belong to Σ (by the maximality property of M). Similarly, the ideal $(y) + M$ strictly contains M and hence cannot belong to Σ. 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 $m_3 \in M$. We thus see that $xy \notin M$, 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. $\square$

Corollary 3.3. *Let R be a ring. The nilradical of R is an ideal.*

Note that this corollary can also easily be proven directly (without using Proposition 3.2) (exercise).

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

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. Abusing language, we will sometimes write $\mathfrak{r}(R)$ for the nilradical of R. Again from the definitions and from Proposition 3.2, 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.

Notice the following elementary properties of the operator $\mathfrak{r}(\bullet)$. Let I, J be a ideals of R. Then we have $\mathfrak{r}(\mathfrak{r}(I)) = \mathfrak{r}(I)$ and we have $\mathfrak{r}(I \cap J) = \mathfrak{r}(I) \cap \mathfrak{r}(J)$ (why?).

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

Definition 3.4. *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 3.5 (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 $IM = M$ (ie every $m \in M$ is a finite sum of elements of the form $a \cdot n$, where $a \in I$ and $n \in M$). 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 (ie every set of generators for M has at least s elements). 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 $x_1, \ldots, x_{s-1}$. Here we set $x_0 := 0$ if $s = 1$. 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 (apply Lemma 2.4) and by assumption $a_s \in \mathfrak{m}$ so that we would have $1 \in \mathfrak{m}$, which is contradiction. Hence

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

If $s = 1$ then we see from (1) that $x_s = 0$. This is a contradiction, since $M \neq (0)$. Thus either $M \simeq (0)$ or $s > 1$. If $s > 1$ we again see from (1) that M has $s - 1$ generators, which is also a contradiction. Hence $M \simeq (0)$. $\square$

Corollary 3.6. *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 $x_1 \,(\mathrm{mod}\, \mathfrak{m}), \ldots, x_s \,(\mathrm{mod}\, \mathfrak{m}) \in M/\mathfrak{m}M$ 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 $M = M'$. $\square$

Corollary 3.7. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M, N be finitely generated R-modules and let $\phi : M \to N$ be a homomorphism of R-modules. Suppose that the induced homomorphism $M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Then ϕ is surjective.*

Proof. Let $x_1, \ldots, x_s$ be generators of M. By assumption, the elements $\phi(x_1) \,(\mathrm{mod}\, \mathfrak{m}), \ldots, \phi(x_s) \,(\mathrm{mod}\, \mathfrak{m})$ generate $N/\mathfrak{m}$. Hence the elements $\phi(x_1), \ldots, \phi(x_s)$ generate N by Corollary 3.6. In particular, ϕ is surjective. $\square$

Definition 3.8. *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.

We will study Jacobson rings in section 10 below. 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 (see Theorem 10.5 below). On the other hand, a local domain is never Jacobson unless it is a field (why?). 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

4 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 4.1. *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. Left to the reader. $\square$

An immediate consequence of Lemma 4.1 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 classical points of the variety (ie the simultaneous solutions of the polynomials defining the variety), whereas the other prime ideals correspond to the irreducible closed subvarieties of W.

From the definitions, we see that if R is a Jacobson ring, then the closed points are dense in any closed set of $\mathrm{Spec}(R)$. This is not true for a general ring.

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 $\mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$ (check that this is well-defined). 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. Notice also that if $\psi : T \to P$ is another ring homomorphism, then we have from the definition that $\mathrm{Spec}(\phi) \circ \mathrm{Spec}(\psi) = \mathrm{Spec}(\psi \circ \phi)$.

Lemma 4.2. *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 $V(\ker(\phi))$.*

Proof. To see that $\mathrm{Spec}(\phi)$ is injective, note that if $\mathfrak{p} \in \mathrm{Spec}(T)$, then $\mathfrak{p} = \phi(\phi^{-1}(\mathfrak{p}))$, since ϕ is surjective, so distinct elements of $\mathrm{Spec}(T)$ have distinct images in $\mathrm{Spec}(R)$.

For the second statement, note first that the image of $\mathrm{Spec}(\phi)$ is clearly contained in $V(\ker(\phi))$. On the other hand if $\mathfrak{p}$ is a prime ideal containing $\ker(\phi)$ (ie $\mathfrak{p} \in V(\ker(\phi))$), then $\phi(\mathfrak{p})$ is a prime ideal of T and $\phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$. Indeed $\phi(\mathfrak{p})$ is an ideal of T since ϕ is surjective. Furthermore, we clearly have $\phi^{-1}(\phi(\mathfrak{p})) \supseteq \mathfrak{p}$ and if $r \in \phi^{-1}(\phi(\mathfrak{p}))$ then there exists $r' \in \mathfrak{p}$ such that $\phi(r) = \phi(r')$, so that $\phi(r - r') = 0$. Since $\mathfrak{p}$ contains the kernel of ϕ, we thus see that $r \in \mathfrak{p}$. In other words $\phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$. Finally, $\phi(\mathfrak{p})$ is a prime ideal of T. Indeed, suppose that $x, y \in T$ and $xy \in \phi(\mathfrak{p})$. Let $x', y' \in R$ such that $\phi(x') = x$ and $\phi(y') = y$. Then $x'y' \in \phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$ and so either $x' \in \mathfrak{p}$ or $y' \in \mathfrak{p}$, since $\mathfrak{p}$ is prime. Hence either $x \in \phi(\mathfrak{p})$ or $y' \in \phi(\mathfrak{p})$. All in all, we have shown that $\mathrm{Spec}(\phi(\mathfrak{p})) = \mathfrak{p}$ for any $\mathfrak{p} \in V(\ker(\phi))$, as required. □

We shall see after Corollary 8.11 below that $\mathrm{Spec}(\phi)$ is actually a homeomorphism onto its image (exercise: prove this directly).

Lemma-Definition 4.3. *Let $f \in R$. The set*

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

is open in $\mathrm{Spec}(R)$. The open sets of $\mathrm{Spec}(R)$ of the form D_f form a basis for the Zariski topology of $\mathrm{Spec}(R)$. Furthermore, the topology of $\mathrm{Spec}(R)$ is quasi-compact.

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

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

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 Lemma 4.1, 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 for the Zariski topology of $\mathrm{Spec}(R)$, 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 by Lemma 4.1 and the proof of the first statement of the present lemma, 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. □

Lemma 4.4. *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. "⇒": Suppose that for all prime ideal $\mathfrak{p}$ of R, we have $\mathfrak{p} \supseteq \mathfrak{a}$ iff $\mathfrak{p} \supseteq \mathfrak{b}$. Then we have $\mathfrak{r}(\mathfrak{a}) = \mathfrak{r}(\mathfrak{b})$ by Proposition 3.2 (see before Definition 3.4).

"⇐": This is again a consequence of Proposition 3.2. □

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 $\mathfrak{a}, \mathfrak{b}$ are radical ideals then $\mathfrak{a} \subseteq \mathfrak{b}$ if and only if $V(\mathfrak{a}) \supseteq V(\mathfrak{b})$.

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.

We conclude from Lemma 4.2, Lemma 4.4 and Lemma 4.1 that if $q : R \to R/\mathfrak{r}((0))$ is the quotient map, then $\mathrm{Spec}(q)$ is bijective (and thus a homeomorphism - see after Lemma 4.2). So the Zariski topology "does not see the nilradical".

Remark 4.5. 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

5 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.

Consider the set $R \times S$ (cartesian product). 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

(verify) and we define $S^{-1}R$ to be $(R \times S)/\sim$, 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

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

This is well-defined (verify). We also define a map $\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R$ by the rule

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

Again this is well-defined. One checks that these two maps provide $S^{-1}R$ with the structure of a commutative unitary ring, whose identity element is $1/1$. Here $+$ give the addition in the ring and $\cdot$ gives the multiplication. 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 5.1 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. 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 $b/t = 0/1$.

Note also that if $0 \in S$, then $S^{-1}R$ is the zero ring (ie $1 = 0$ in $S^{-1}R$. This simply follows from the fact that in this case $0/1$ is a unit in $S^{-1}R$. More generally, the definition shows that $S^{-1}R$ is the zero ring iff for all $r \in R$, there is an $s \in S$ st $sr = 0$.

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. Here $+$ give the addition in the ring and $\cdot$ gives the scalar multiplication. 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 also use the less cumbersome notation R_S for $S^{-1}R$ and M_S for $S^{-1}M$. 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 5.1. *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. Define the map $\lambda : R_S \to R'$ by the formula $\lambda(a/s) = \phi(a)(\phi(s))^{-1}$ for all $a \in R$ and $s \in S$. We show that λ is well-defined. Suppose that $(a, s) \sim (b, t)$. Then

$$\lambda(b/t) = \phi(b)(\phi(t))^{-1}$$

and we have $u(ta - sb) = 0$ for some $u \in S$. Thus $\phi(u)(\phi(t)\phi(a) - \phi(s)\phi(b)) = 0$ and since $\phi(u)$ is a unit in R', we have $\phi(t)\phi(a) - \phi(s)\phi(b) = 0$. Thus $\phi(t)\phi(a) = \phi(s)\phi(b)$ and

$$\lambda(a/s) = \phi(a)(\phi(s))^{-1} = \phi(b)(\phi(t))^{-1} = \lambda(b/t).$$

Thus λ is well-defined. We skip the straightforward verification that λ is a ring homomorphism. We have thus proven that there is a ring homomorphism $\phi_S : R_S \to R'$ such that $\phi_S(r/1) = \phi(r)$ for all $r \in R$ (namely λ). We now prove unicity. Suppose that $\phi'_S : R_S \to R'$ is another ring homomorphism such that $\phi'_S(r/1) = \phi(r)$ for all $r \in R$. Then for any $r \in R$ and $t \in S$, we have

$$\phi'_S(r/t) = \phi'_S((r/1)(t/1)^{-1}) = \phi'_S(r/1)\phi'_S(t/1)^{-1} = \phi_S(r)\phi_S(t)^{-1} = \phi_S(r/t)$$

and thus ϕ'_S coincides with ϕ_S (and in particular with λ). $\square$

There is a similar result for modules:

Lemma 5.2. *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 $[s]_M : M \to M$ 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 $r \in R$.*

Keeping the notation of the lemma, note that if $r/s \in R_S$, we necessarily have $(r/s)(m) = [s]_M^{-1}(rm)$, where $[s]_M^{-1}$ is the inverse of the map $[s]_M$.

Proof. Left to the reader. $\square$

We also record the following important fact.

Lemma 5.3. *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. Consider the R-algebra $T := R[x]/(fx - 1)$. Note that T is a finitely generated R-algebra by definition. Let $\phi : R[x] \to R_S$ by the homomorphism of R-algebras such that $\phi(x) = 1/f$. Note that $\phi(fx - 1) = 0$ and hence ϕ induces a homomorphism of R-algebras $\psi : T \to R_S$. Now since the image of f in T is invertible by construction, there is by Lemma 5.1 a unique homomorphism of R-algebras $\lambda : R_S \to T$. We have $\psi \circ \lambda = \mathrm{Id}_T$ by unicity and hence λ is injective. On the other hand λ is surjective, since the image of λ contains $1/(f \pmod{(fx-1)}) = x \pmod{(fx-1)}$, which generates R as an R-algebra. Thus λ is bijective, and hence an isomorphism of R-algebras. $\square$

In view of Lemma 5.2, 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 $\phi_S(n/1) = \phi(n)/1$ 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 5.4. *Let R be a ring and let $S \subseteq R$ be a multiplicative subset. Let*

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

be an exact complex of R-modules. Then the sequence

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

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 $d_{i-1,S}(p/(us)) = m/s$. This concludes the proof. $\square$

Lemma 5.5. *Let $\phi : R \to T$ be a ring homomorphism. Let $S \subseteq R$ be a multiplicative subset. By Lemma-Definition 5.1 there is a unique homomorphism of rings $\phi' : R_S \to T_{\phi(S)}$ such that $\phi'(r/1) = \phi(r)/1$. We may thus view $T_{\phi(S)}$ (resp. T) as a R_S-module (resp. as a R-module). There is then a unique isomorphism of R_S-modules $\mu : T_S \simeq T_{\phi(S)}$ such that $\mu(a/1) = a/1$ for all $a \in T$ and we have $\mu \circ \phi_S = \phi'$.*

Proof. Define $\mu(a/s) := a/\phi(s)$ for any $a \in T$ and $s \in S$. This is well-defined. Indeed, suppose that $a/s = b/t$. Then there is $u \in S$ such that $\phi(u)(\phi(t)a - \phi(s)b) = 0$, ie $\phi(u)\phi(t)a = \phi(u)\phi(s)b$. We thus see that $a/\phi(s) = b/\phi(t)$, which shows that μ is well-defined. From the definitions, we see that μ is a map of R_S-modules. We also see from the definition that μ is surjective. To see that μ is injective, suppose that $\mu(a/s) = 0/1$ for some $a \in T$ and $s \in S$. Then there is a $u \in \phi(S)$ such that $ua = 0$. Hence $a/1 = 0$ in T_S and thus $a/s = 0$. Thus μ is bijective. The identity $\mu \circ \phi_S = \phi'$ follows from the fact that μ, ϕ_S and ϕ' are homomorphisms of R_S-modules and from the fact that $\mu \circ \phi_S(1) = \phi'(1/1)$. $\square$

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 $R_{R\backslash\mathfrak{p}}$ and 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 $\phi_{R\backslash\mathfrak{p}} : M_\mathfrak{p} \to N_\mathfrak{p}$.

If $\phi : U \to R$ is a homomorphism of rings and $\mathfrak{p}$ is a prime ideal of R, then ϕ naturally induces a homomorphism of rings $U_{\phi^{-1}(\mathfrak{p})} \to R_\mathfrak{p}$, since $\phi(U\backslash\phi^{-1}(\mathfrak{p})) \subseteq R\backslash\mathfrak{p}$. This homomorphism is sometimes also denoted $\phi_\mathfrak{p}$.

Lemma 5.6. *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 (which is a homomorphism of R-modules). Furthermore, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is then the ideal generated by $\lambda(\mathfrak{p})$ in R_S.*

Note that in view of Lemma 5.5, if we localise R at S when R is viewed as a R-module or as a ring, we get the same R_S-module.

Proof. We first prove that if $\mathfrak{p}$ is any ideal of R, then $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S. For this, notice that by definition $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ consists of all the element $a/s \in R_S$, where $a \in \mathfrak{p}$ and $s \in S$. Hence $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is an ideal of R_S, which contains $\lambda(\mathfrak{p})$. Furthermore, since $a/s = (a/1)(1/s)$, any element a/s as above is contained in the ideal generated by $\lambda(\mathfrak{p})$ in R_S. Hence $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S.

To prove the lemma, we thus only have to show the following

(i) If $\mathfrak{q}$ is a non trivial ideal of R_S then $\lambda^{-1}(\mathfrak{q}) \cap S = \emptyset$.

(ii) If $\mathfrak{q}$ is an ideal of R_S, the ideal generated by $\lambda(\lambda^{-1}(\mathfrak{q}))$ in R_S is $\mathfrak{q}$.

(iii) If $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$, then $\lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)) = \mathfrak{p}$.

(iv) If $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$ then $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is a prime ideal of R_S.

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

A more general form of statement (v) was left to the reader after Lemma 4.1 so we skip the proof of (v).

We prove (i). If $\lambda^{-1}(\mathfrak{q}) \cap S \neq \emptyset$ then (by definition) there exists $s \in \lambda^{-1}(\mathfrak{q})$ such that $s \in S$. But then $\lambda(s) = s/1 \in \mathfrak{q}$ and $s/1$ is a unit, so that $\mathfrak{q}$ is trivial. This proves (i).

To prove (ii), notice first that $\lambda(\lambda^{-1}(\mathfrak{q})) \subseteq \mathfrak{q}$. Furthermore, if $a/s \in \mathfrak{q}$ then as before $a/1 = (a/s)(s/1)$ also lies in $\mathfrak{q}$ and hence $a \in \lambda(\lambda^{-1}(\mathfrak{q}))$. Since $a/s = (a/1)(1/s)$ we thus see that a/s lies in the ideal generated by $\lambda(\lambda^{-1}(\mathfrak{q}))$. Since a/s was arbitrary, $\mathfrak{q}$ is thus the ideal generated by $\lambda(\lambda^{-1}(\mathfrak{q}))$.

To prove (iii) note that since $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S, we clearly have $\lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)) \supseteq \mathfrak{p}$. Now suppose that $a \in \lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S))$. Then by definition $a/1 = b/s$ for some $b \in \mathfrak{p}$ and some $s \in S$. Again by definition, this means that for some $t \in S$, we have $t(sa - b) = 0$, ie $tsa = tb$. Since $tb \in \mathfrak{p}$ and $ts \notin \mathfrak{p}$ (by assumption), we deduce from the fact that $\mathfrak{p}$ is prime that $a \in \mathfrak{p}$, as required.

To prove (iv), consider the exact sequence of R-modules

$$0 \to \mathfrak{p} \to R \xrightarrow{q} R/\mathfrak{p} \to 0$$

where q is the quotient map. Applying Lemma 5.4, we see that the sequence of R_S-modules

$$0 \to \mathfrak{p}_S \to R_S \xrightarrow{q_S} (R/\mathfrak{p})_S \to 0$$

is also exact. Furthermore, by Lemma 5.5, we see that $(R/\mathfrak{p})_S$ is isomorphic as a R_S-module with the ring $(R/\mathfrak{p})_{q(S)}$ and that we have an isomorphism of rings $R_S/\mathfrak{p}_S \simeq (R/\mathfrak{p})_{q(S)}$. Now since $S \cap \mathfrak{p} = \emptyset$, we see that $0 \notin q(S)$. Since $R/\mathfrak{p}$ is a domain by assumption, we deduce that $(R/\mathfrak{p})_{q(S)}$ is also a domain (see beginning of this section). We conclude that $\mathfrak{p}_S$ is a prime ideal. □

Note the following rewording of part of Lemma 5.6: $\mathrm{Spec}(\lambda)(\mathrm{Spec}(R_S))$ consists of the prime ideals in $\mathrm{Spec}(R)$, which do not meet S. In particular, in the notation of Lemma-Definition 4.3,

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

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

Still keeping the notation of Lemma 5.6, we also note the following. If $\mathfrak{q} \in \mathrm{Spec}(R_S)$ then λ induces a natural homomorphism of rings $R_{\lambda^{-1}(\mathfrak{q})} \to (R_S)_{\mathfrak{q}}$ (see before Lemma 5.6). This homomorphism is an isomorphism. We leave the proof of this statement as an exercise.

Second proof of Proposition 3.2 using localisations. Let R be a ring. Let $r \in R$ be an element, which is not nilpotent. To prove Proposition 3.2, we need to show that there is a prime ideal $\mathfrak{p}$ of R such that $r \notin \mathfrak{p}$. Let $S := \{1, r, r^2, \dots\}$ be the multiplicative set generated by r. The ring R_S is not the zero ring because $r/1 \neq 0/1$ (because r is not nilpotent). Let $\mathfrak{q}$ be a prime ideal of R_S (this exists by Lemma 2.4). By lemma 5.6, the ideal $\mathfrak{q}$ corresponds to a prime ideal $\mathfrak{p}$ of R such that $r \notin \mathfrak{p}$ so it has the required properties.

Lemma 5.7. *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 Lemma 5.6 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 Lemma 5.6, we have $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$. $\square$

Lemma 5.8. *Let R be a ring. Let*

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

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

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

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

Proof. "$\Rightarrow$": By Lemma 5.4.

"$\Leftarrow$": Suppose that the complex (4) is not exact. Then $\ker(d_{i+1})/\mathrm{Im}(d_i) \neq 0$ for some $i \in \mathbb{Z}$. By Lemma 5.4, 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.

Now 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 $\mathrm{Ann}(a)$ (this exists by Lemma 2.4). 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. Thus the complex (5) is not exact. $\square$

END OF LECTURE 4

6 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.

The main result is Theorem 6.7 below.

Let R be a ring.

Proposition 6.1. (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. (i) By induction on k. The case $k = 1$ holds tautologically. Suppose for contradiction that the conclusion does not hold. By the inductive hypothesis, we see that for each $i \in \{1, \dots, k\}$, we have $I \not\subseteq \cup_{j \neq i} \mathfrak{p}_j$. In other words, there are elements $x_1, \dots, x_k \in I$ such that for each $i \in \{1, \dots, k\}$ we have $x_i \in \mathfrak{p}_i$ and $x_i \notin \mathfrak{p}_j$ if $j \neq i$. Now consider the element

$$y := \sum_{i=1}^{k} x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k$$

where we set $x_0 = x_{k+1} = 1$. Note that for each $i \in \{1, \dots, k\}$ we have $x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_j$ for all $j \neq i$. Now let $i \in \{1, \dots, k\}$ be such that $y \in \mathfrak{p}_i$. Then $y - x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_i$ and thus

$$x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_i.$$

Now, since $\mathfrak{p}_i$ is prime, one of $x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_k$ must lie in $\mathfrak{p}_i$, which is a contradiction.

(ii) We first prove the first statement. Suppose that the conclusion does not hold. Then for each $i \in \{1, \dots, k\}$, there is an element $x_i \in I_i$ such that $x_i \notin \mathfrak{p}$. But $x_1 x_2 \cdots x_k \in \cap_{i=1}^{k} I_i \subseteq \mathfrak{p}$ and since $\mathfrak{p}$ is prime, one of the x_i must lie in $\mathfrak{p}$, which is a contradiction.

The second statement follows from the first, since $\cap_{i=1}^{k} I_i \subseteq I_{i_0}$. □

Note. The proof of Proposition 6.1 shows that in (i), the condition that the ideals $\mathfrak{p}_i$ are prime is superfluous if $k \leq 2$.

Definition 6.2. *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 6.3. *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 $x^{ln} \in I$ and $y^{nk} \in I$ for some $l, k > 1$. Hence either x or y lies in $\mathfrak{r}(I)$. □

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

Proof. (suggested by Hanming Liu; see also Q3 of Sheet 1). From the assumptions, we see that the nilradical $\mathfrak{r}(R/J)$ of R/J is maximal. Hence R/J is a local ring, because any maximal ideal of R/J contains $\mathfrak{r}(R/J)$ by Proposition 3.2 and hence must coincide with it. Hence any element of R/J is either a unit or is nilpotent. In particular, all the zero divisors of R/J are nilpotent, in particular J is primary.

Here is another proof, which does not use Proposition 3.2. Let $x, y \in R$ and suppose that $xy \in J$ and that $x, y \notin J$. Since $xy \in \mathfrak{r}(J)$ and since $\mathfrak{r}(J)$ is prime, we have either $x \in \mathfrak{r}(J)$ or $y \in \mathfrak{r}(J)$. Suppose

without restriction of generality that $y \in \mathfrak{r}(J)$. Then $y^n \in J$ for some $n > 1$. Suppose for contradiction that $x \notin \mathfrak{r}(J)$. Then there exists $x' \in R$ such that $xx' - 1 \in \mathfrak{r}(J)$ by the maximality of $\mathfrak{r}(J)$. In other words, there is $l > 0$ such that

$$(xx' - 1)^l = (-1)^l + \sum_{i=1}^{l} \binom{l}{i} (-1)^{l-i} (xx')^i \in J.$$

Then we have

$$y(-1)^l + \sum_{i=1}^{l} \binom{l}{i} (-1)^{l-i} (yx) x^{i-1} (x')^i \in J$$

and since $\sum_{i=1}^{l} \binom{l}{i} (-1)^{l-i} (yx) x^{i-1} (x')^i \in J$ we conclude that $y \in J$, a contradiction. So we must have $x \in \mathfrak{r}(J)$. All in all, we have $x, y \in \mathfrak{r}(J)$, which is what we wanted to prove. $\square$

From the previous Lemma, we see that powers of maximal ideals are primary ideals.

Lemma 6.5. *Let $\mathfrak{p}$ be a prime ideal and let I be a $\mathfrak{p}$-primary ideal. Let $x \in R$.*

(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 6.6. *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, $x, y \in \mathfrak{r}(\mathfrak{q}_i) = \mathfrak{r}(\mathfrak{q}_j) = \mathfrak{p} = \mathfrak{r}(\mathfrak{q})$. In other words, $\mathfrak{q}$ is primary. $\square$

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 Lemma 6.6 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 in section 7 below 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 6.7. *Let I be a decomposable ideal. Let $\mathfrak{q}_1 \dots, \mathfrak{q}_k$ 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 $\{\mathfrak{p}_i\}_{i\in\{1,\dots,k\}}$;

- 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 6.5, 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 $i_0 \in \{1, \dots, k\}$ by Proposition 6.1.

Conversely, note that for any $i_0 \in \{1, \dots, k\}$, 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. □

As a consequence of Theorem 6.7, we can associate with any decomposable ideal I in R a uniquely defined set of prime ideals. These prime ideals are said to be *associated* with I. Note that the intersection of these prime ideals is the ideal $\mathfrak{r}(I)$. Another consequence is that any radical decomposable ideal has a minimal primary decomposition by prime ideals (so that in this case, the associated primes are the elements of the minimal primary decomposition itself). Furthermore, any two minimal primary decompositions by prime ideals of a radical ideal coincide.

Remark. One can show that any minimal primary decomposition of a radical ideal consists only of prime ideals (without requiring a priori that the primary decomposition consist of prime ideals, as in the previous paragraph). This follows from the '2nd uniqueness theorem'. See AT, p. 54, Cor. 4.11. In particular, a decomposable radical ideal has a unique primary decomposition. We do not prove this in these notes however.

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 $\{(p_1), \dots, (p_k)\}$.

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 $\{(x), (x, y)\}$. To see that we indeed have $(x^2, xy) = (x) \cap (x, y)^2$ note that by construction, the ideal $(x, y)^2$ consists of the polynomials of the form $x^2P(x, y) + xyQ(x, y) + y^2T(x, y)$. Thus $(x) \cap (x, y)^2$ consists of the polynomials $x^2P(x, y) +$

$xyQ(x,y) + y^2T(x,y)$ such that $T(x,y)$ is divisible by x. Hence $(x) \cap (x,y)^2 \subseteq (x^2, xy)$ and clearly we also have $(x^2, xy) \subseteq (x) \cap (x,y)^2$ so that $(x^2, xy) = (x) \cap (x,y)^2$. To see that the decomposition is primary, note that $\mathbb{C}[x,y]/(x) \simeq \mathbb{C}[y]$ and $\mathbb{C}[x,y]/(x,y) \simeq \mathbb{C}$. Thus (x) is prime and (hence primary) and (x,y) is maximal, so that $(x,y)^2$ is primary by Lemma 6.4.

Lemma 6.8. *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 6.7, 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 6.1. We conclude that $\mathfrak{p}_0 \supsetneq \mathfrak{p}$, which contradicts the minimality of $\mathfrak{p}_0$. Thus $\mathcal{S}_{\min} = \mathcal{I}_{\min}$. □

The elements of $\mathcal{S}_{\min}$ are called the *isolated* or *minimal* prime ideals associated with I whereas the elements of $\mathcal{S} \backslash \mathcal{S}_{\min}$ are called the *embedded* prime ideals associated with I. This terminology is justified by algebraic geometry. According to the last lemma, the isolated prime ideals associated with I are precisely the prime ideals, which are minimal among all the prime ideals containing I.

In the second example given before Lemma 6.8, the set $\mathcal{S}_{\min}$ consists only of (x).

Note also the following important facts:

- if I is a decomposable radical ideal, then all the associated primes of I (which coincide with the elements of the unique minimal primary decomposition - see above) are isolated. This simply follows from the fact that I has a minimal primary decomposition by prime ideals.

- if I is a decomposable ideal, there are only finitely many prime ideals, which contain I and are minimal among all the prime ideals containing I. These prime ideals are also the isolated ideals associated with I.

We also record the following lemma, which makes no assumption of decomposability.

Lemma 6.9. *Let R be a ring. Let $I \subseteq R$ be an ideal. Then there are prime ideals, which are minimal among all the prime ideals containing I. Furthermore, if $\mathfrak{p} \supseteq I$ is a prime ideal, then $\mathfrak{p}$ contains such a prime ideal.*

Proof. Exercise. Use (and generalise) Q7 of sheet 1. □

END OF LECTURE 6

7 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 7.1. *The ring R is noetherian iff whenever $I_1 \subseteq I_2 \subseteq \dots$ is an ascending sequence of ideals, 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. "$\Rightarrow$". Suppose first that R is noetherian. Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending sequence of ideals. 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.

"$\Leftarrow$". Conversely, suppose that whenever $I_1 \subseteq I_2 \subseteq \dots$ is an ascending sequence of ideals, there exists a $k \geq 1$ such that $I_k = I_{k+i} = \cup_{t=1}^{\infty} I_t$ for all $i \geq 0$. Let $J \subseteq R$ be an ideal. We need to show that J is finitely generated. For contradiction, suppose that J is not finitely generated. Define a sequence $r_1, r_2 \dots \in J$ by the following inductive procedure. Let $r_1 \in J$ be arbitrary. Suppose that $r_1, \dots, r_i \in J$ is given and let $r_{i+1} \in J \backslash (r_1, \dots, r_i)$. Note that $J \backslash (r_1, \dots, r_i) \neq \emptyset$ for otherwise J would be finitely generated. We then have an ascending sequence

$$(r_1) \subsetneq (r_1, r_2) \subsetneq (r_1, r_2, r_3) \subsetneq \dots$$

which contradicts our assumptions. So J is finitely generated. $\square$

Lemma 7.2. *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. $\square$

Lemma 7.3. *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 5.6, 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. $\square$

Lemma 7.4. *Let R be a noetherian ring. Let M be a finitely generated R-module. Then any submodule of M is also finitely generated.*

Proof. By assumption there is a surjective map of R-modules $q : R^n \to M$ for some $n \geq 0$. To prove that a submodule $N \subseteq M$ is finitely generated, it is sufficient to prove that $q^{-1}(N)$ is finitely generated. Hence we may assume that $M = R^n$. We now prove the statement by induction on n. The case $n = 1$ is verified by assumption. Let $\phi : R^n \to R$ be the projection on the first factor. Let $N \subseteq R^n$ be a submodule. We then have an exact sequence

$$0 \to N \cap R^{n-1} \to N \to \phi(N) \to 0$$

where R^{n-1} is viewed as a submodule of R^n via the map $(r_1, \dots, r_{n-1}) \mapsto (r_1, \dots, r_{n-1}, 0)$. Now $\phi(N)$ is finitely generated since $\phi(N)$ is an ideal in R and $N \cap R^{n-1}$ is finitely generated by the inductive hypothesis. Let $a_1, \dots, a_k \in N \cap R^{n-1}$ be generators of $N \cap R^{n-1}$ and let $b_1, \dots, b_l \in \phi(N)$ be generators of $\phi(N)$. Let $b_1', \dots, b_l' \in R^n$ be such that $\phi(b_i') = b_i$ for all $i \in \{1, \dots, l\}$. Then the set $\{a_1, \dots, a_k, b_1', \dots, b_l'\}$ generates N (verify). $\square$

Lemma 7.5. *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 theorem is one of the main justifications for the introduction of the noetherian condition.

Theorem 7.6 (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 $f_i(x) = a_i x^{n_i} +$ (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 $f(x) = ax^m +$ (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 $< n$. We have then expressed the polynomial $f(x)$ as a sum of a polynomial of degree $< n$ and an element of I'. In other words, we have shown that $f(x)$ lies in the R-submodule $M \cap I + I'$ of $R[x]$, where M is the R-submodule of $R[x]$, generated by $1, x, x^2, \ldots, x^{n-1}$.

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 see that 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 7.4. 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). □

Some history. The German mathematician Paul Gordan, who was active at the beginning of the 20th century, was the first to ask explicitly (to my knowledge) whether Theorem 7.6 is true and considered this to be a central question of a then very popular subject, called Invariant Theory (which we don't have the time to describe here). As the name of the theorem suggests, David Hilbert found the above simple proof. Paul Gordan had presumably tried to tackle the problem directly, by devising an algorithm that would provide a finite set of generators for an ideal given by an infinite set of generators and did not think of applying the abstract methods, which are used in Hilbert's proof (which is the above proof). The proof of Hilbert's basis theorem is one of the starting points of modern commutative algebra. Paul Gordan is said to have quipped on seeing Hilbert's proof that "Das is nicht Mathematik, das ist Theologie!" (This is not mathematics, this is theology!). There are nowadays more "effective" proofs of Hilbert's basis theorem, using so-called Groebner bases.

From Theorem 7.6, we deduce that $R[x_1, \ldots, x_k]$ is noetherian for any $k \geq 0$. From this and Lemma 7.2, we deduce that every finitely generated algebra over a noetherian ring is noetherian.

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 7.7 (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 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 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 $b, d \in \{1, \ldots, k\}$, 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}. Since every element of T can be written as an R-linear combination of products of some r_a ($a \in \{1, \ldots, k\}$, we see using the two formulae above 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 (see after Theorem 7.6) 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 7.4. In particular S is a finitely generated S_0-algebra, and since S_0 is finitely generated over R, so is S. $\square$

Finally, we consider primary decompositions in noetherian rings.

Proposition 7.8 (Lasker-Noether)**.** *Let R be a noetherian ring. Then every ideal of R is decomposable.*

Proof. If I is an ideal of R, we shall say that 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 $I = I_2$.

Claim. Let $J \subseteq R$ be an ideal. Then there are irreducible ideals $J_1, \ldots, J_k$ such that $J = \cap_{i=1}^{k} J_k$.

We prove the claim. Let us say that an ideal is *decomposable by irreducible ideals* (short: dic) if it is a finite intersection of irreducible ideals. Suppose that J is not dic (otherwise we are done). In particular, J is not irreducible and thus there are ideals M and N such that $M \cap N = J$ and such that $J \subsetneq M$ and $J \subsetneq N$. Since J is not dic, we see that either N or M are not dic. Suppose without restriction of generality that M is not dic. Repeating the same reasoning for M and continuing we obtain a sequence of non dic ideals $J \subsetneq M \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots$ This contradicts Lemma 7.1. Thus J is dic.

Claim. An irreducible ideal is primary.

We prove the claim. Let J be an irreducible ideal and suppose that J is not primary. Then there is an element $x \in R/J$, which is a zero divisor and is not nilpotent. Let $q : R \to R/J$ be the quotient map.

Consider the ascending sequence

$$\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \mathrm{Ann}(x^3) \subseteq \dots$$

This sequence must stop by Lemma 7.1 and Lemma 7.2. So let us suppose that

$$\mathrm{Ann}(x^k) = \mathrm{Ann}(x^{k+1}) = \mathrm{Ann}(x^{k+2}) = \dots$$

for some $k \geq 1$. Now consider the ideal $(x^k) \cap \mathrm{Ann}(x^k)$. If $\lambda x^k \in (x^k) \cap \mathrm{Ann}(x^k)$ for some $\lambda \in R/J$ then we have by definition $\lambda x^{2k} = 0$ and hence $\lambda \in \mathrm{Ann}(x^{2k})$. Since $\mathrm{Ann}(x^{2k}) = \mathrm{Ann}(x^k)$ we then have $\lambda x^k = 0$. Thus $(x^k) \cap \mathrm{Ann}(x^k) = (0)$. On the other hand, note that $(x^k) \neq (0)$ and $\mathrm{Ann}(x^k) \neq 0$ by construction. Thus we have $J = q^{-1}((x^k)) \cap q^{-1}(\mathrm{Ann}(x^k))$ and $q^{-1}((x^k)) \neq J$, $q^{-1}(\mathrm{Ann}(x^k))) \neq J$, a contradiction. Thus J is primary.

The conjunction of both claims obviously proves the Proposition, so we are done. □

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 6.7, a consequence of Proposition 7.8 is that there is a unique set $\{\mathfrak{q}_1 \dots, \mathfrak{q}_k\}$ of distinct prime ideals in R such that

- $I = \cap_{i=1}^k \mathfrak{q}_i$;

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

Furthermore, the set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_k\}$ is precisely the set of prime ideals, which are minimal among 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.

In particular, if $\mathfrak{p}_1, \dots, \mathfrak{p}_l$ is the set of minimal prime ideal of R, then there is a natural injective homomorphism of rings

$$R/\mathfrak{r}((0)) \hookrightarrow \prod_{i=1}^{l} R/\mathfrak{p}_i.$$

END OF LECTURE 7

8 Integral extensions

The notion of integral extension of rings is a generalisation of the notion of algebraic extension of fields. We shall see below that an extension of fields is integral iff it is algebraic.

Let B be a ring and let $A \subseteq B$ be a subring. Let $b \in B$. We shall say that b is *integral* over A if there is a monic polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in A[x]$ such that

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

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 (why?) 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

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

and that we have

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

(why?).

Proposition 8.1. *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. By assumption, there is a surjective homomorphism of R-modules $\lambda : R^n \to M$ for some $n \geq 0$. Let $b_1, \ldots, b_n$ be the natural basis of R^n. For each b_i, choose an element $v_i \in R^n$ such that $\lambda(v_i) = \phi(\lambda(b_i))$. Define a homomorphism of R-modules $\widetilde{\phi} : R^n \to R^n$ by the formula $\widetilde{\phi}(b_i) = v_i$. By construction, we have $\lambda \circ \widetilde{\phi} = \phi \circ \lambda$ and thus we have $\lambda \circ \widetilde{\phi}^{\circ n} = \phi^{\circ n} \circ \lambda$ for all $n \geq 0$. Hence it is sufficient to find a monic polynomial $Q(x) \in R[x]$ such that $Q(\widetilde{\phi}) = 0$. Hence we might assume that $M = R^n$.

The homomorphism ϕ is now described by a $n \times n$-matrix $C \in \mathrm{Mat}_{n\times n}(R)$. We need to find a monic polynomial $Q(x) \in R[x]$ such that $Q(C) = 0$.

Let R' be the subring of R generated by the coefficients of C over the prime ring of R. There is by construction a surjective homomorphism of rings $h : \mathbb{Z}[x_{11}, x_{21}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}] \to R'$. Let $D \in \mathrm{Mat}_{n\times n}(\mathbb{Z}[x_{11}, x_{21}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}])$ be a matrix, whose image by h is C. If we can exhibit a monic polynomial $T(x) \in (\mathbb{Z}[x_{11}, x_{21}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}])[x]$ such that $T(D) = 0$ then the monic polynomial $Q(x)$, whose coefficients are the images of the coefficients of $T(x)$ under h, will have the property that $Q(C) = 0$. So we may assume that $R = \mathbb{Z}[x_{11}, x_{21}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}]$.

Let K be the fraction field of R. The natural homomorphism of rings $R \to K$ is then injective, since $R = \mathbb{Z}[x_{11}, x_{21}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}]$ is a domain. Hence we may view R as a subring of K. By the Cayley-Hamilton theorem, the polynomial $Q(x) = \det(x \cdot \mathrm{Id}_{n\times n} - C) \in K[x]$ is monic and it has the property that $Q(C) = 0$, when C is viewed as an element of $\mathrm{Mat}_{n\times n}(K)$. Since $Q(x)$ is a polynomial in the coefficients of C, it has coefficients in R. It thus has the required properties. $\square$

Proposition 8.2. *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 8.1, 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. □

The following lemma and its proof is a generalisation of the tower law (see the part B course on Galois Theory or the part A course on Rings and Modules).

Lemma 8.3. *Let $\phi : R \to T$ be a homomorphism 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 8.4 (of Proposition 8.2)**.** *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 8.2 (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, $A[b_1, b_2, b_3] = A[b_1][b_2][b_3]$ is finitely generated as a $A[b_1, b_2]$-module etc. Hence by Lemma 8.3, $A[b_1, \ldots, b_k]$ is finitely generated as a A-module. □

Corollary 8.5 (of Corollary 8.4 and Proposition 8.2)**.** *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 8.4. Hence $b + c$ and bc are integral over A by Proposition 8.2 (ii). □

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 8.2 and Corollary 8.4 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 8.5. 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 8.6. *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 $B' = A[b_0, \ldots, b_{n-1}]$. Then c is integral over B' and so $B'[c]$ is finitely generated as a B'-module by Proposition 8.2 (i). Hence $B'[c]$ is finitely generated as a A-module by Corollary 8.4 and Lemma 8.3. Hence c is integral over A by Proposition 8.2 (ii). □

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

We first prove the unbracketed statement. So suppose that B is integral over A. The ring homomorphism $A_S \to B_S$ arises from Lemma-Definition 5.1. It is injective by Lemma 5.4 and Lemma 5.5 (injectivity can also be established directly).

Proof. Let $b/s \in B_S$, where $b \in B$ and $s \in S$. By assumption we have

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

for some $a_i \in A$. Thus

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + (a_{n-2}/s^2)(b/s)^{n-2} + \cdots + a_0/s^n = (1/s^n)(b^n + a_{n-1}b^{n-1} + \cdots + a_0) = 0/1.$$

In particular, b/s is integral over A_S.

We now prove the bracketed statement. Suppose that $a_1, \ldots, a_k$ are generators for B as a A-module. Then $a_1/1, \ldots, a_k/1 \in B_S$ are generators of B_S as an A_S-module so B_S is also finite over A_S. $\square$

END OF LECTURE 8

Theorem 8.8 (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 8.8, we shall need the following lemma.

I am grateful to Tobia Beccari for having suggested a simplification of its proof.

Lemma 8.9. *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. (of Lemma 8.9). "$\Leftarrow$": 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. By assumption, D is integral over C so there is a polynomial $P(t) = t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_0 \in C[t]$ such that $P(1/c) = 0$. 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 8.9:

Corollary 8.10 (of lemma 8.9)**.** *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 of 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 8.9. $\square$

Proof. (of Theorem 8.8) 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 by Lemma 5.5, $B_{\mathfrak{p}}$ is isomorphic to the localisation of B at $\mathfrak{p}$, when B is viewed as an A-module. By Lemma-Definition 5.1, 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 $\lambda_B\circ\phi=\phi_{\mathfrak{p}}\circ\lambda_A$ (check) and thus we 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 5.7, $\mathfrak{p}$ 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 2.4). Note that the ring $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$ by Lemma 8.7. Thus Corollary 8.10 implies that $\phi_{\mathfrak{p}}^{-1}(\mathfrak{q})$ 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 8.11. *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:

$$\begin{array}{ccc}A & \xrightarrow{\phi} & B\\ \downarrow{\scriptstyle q_\mu} & \searrow^{\mu} & \downarrow{\scriptstyle q_{\mathfrak{a}}}\\ A/\ker(\mu) & \xrightarrow{\psi} & B/\mathfrak{a}\end{array}$$

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 8.8, we thus have $\mathrm{Spec}(\psi)(\mathrm{Spec}(B/\mathfrak{a}))=\mathrm{Spec}(A/\ker(\mu))$. Furthermore, by Lemma 4.2, 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. $\square$

Note that the previous corollary shows in particular (although this is easier to prove) that if $\phi:A\to B$ is surjective, then $\mathrm{Spec}(\phi)$ is a closed map. In particular, since $\mathrm{Spec}(\phi)$ is injective and continuous in that case (by Lemma 4.2), it is a homeomorphism onto its image.

Proposition 8.12. *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 (ie for any $\mathfrak{p}\in\mathrm{Spec}(A)$, the set $\mathrm{Spec}(\phi)^{-1}(\{\mathfrak{p}\})$ is finite).*

Proof. Let $q:A\to A/\ker(\phi)$ be the quotient map. The map $\mathrm{Spec}(q)$ has finite fibres by Lemma 4.2 (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 4.2) 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 $\lambda_{B/\bar{\mathfrak{p}}}$ (see Lemma 5.5). 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 $\mathfrak{q} \in \mathrm{Spec}(B/\bar{\mathfrak{p}})$ then $\psi^{-1}(\mathfrak{q}) = (0)$ iff $\mathfrak{q} \cap \psi(S) = \emptyset$. In particular, 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 8.8 anyway).

Now, since B is finite over A, $B/\bar{\mathfrak{p}}$ is also finite over $A/\mathfrak{p}$ and further, applying Lemma 8.7, 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 8.9. 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

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 9.1 (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*

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

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

The idea of the proof is as follows. It is easy to see that there is an injective homomorphism of algebras $K[y_1, \dots, y_t] \to R$ so that R is algebraic over $K[y_1, \dots, y_t]$. The proof of the normalisation lemma basically considers such a homomorphism and tweaks it, using properties of polynomials, so that R becomes integral over $K[y_1, \dots, y_t]$.

Proof. We will only prove this result in the situation where K is infinite. For a proof in the situation where K is finite, see H. Matsumura, Commutative Algebra, 2nd ed., Benjamin 1980 (14.G).

Let $r_1, \dots, r_n \in R$ 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 $k \in \{1, \dots, n\}$ such that for all $i \in \{1, \dots, k\}$, r_i is not algebraic over $K[r_1, \dots, r_{i-1}]$ (where we set $K[r_1, \dots, r_{i-1}] = K$ if $i = 1$) and such that r_{k+i} is algebraic over $K[r_1, \dots, r_k]$ for all $i \in \{1, \dots, n-k\}$ (where we set $\{1, \dots, n-k\} = \emptyset$ if $k = n$).

Indeed, we may assume that not all the elements of $\{r_1, \dots, r_n\}$ are algebraic over K, for then they would all be integral over K (since K is a field) and we could then set $t = 0$ in the theorem by Corollary 8.4. To find a suitable renumbering, choose one generator $r_{i_1} \in \{r_1, \dots, r_k\}$, which is not algebraic over K and then look for a second generator $r_{i_2} \in \{r_1, \dots, r_k\}$, which is not algebraic over $K[r_{i_1}]$. If this does not exist then renumber the remaining generators in an arbitrary way. Otherwise, let $r_{i_2} \in \{r_1, \dots, r_k\}$ be such a generator and look for a generator r_{i_3}, which is not algebraic over $K[r_{i_1}, r_{i_2}]$. Keep going in this way until all the remaining generators are algebraic over the K-algebra generated by the previous ones, and renumber the remaining generators in an arbitrary way.

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 $K[r_1, \dots, r_{n-1}]$. Let $P_1(x) \in K[r_1, \dots, r_{n-1}][x]$ be a non zero polynomial (not necessarily monic) such that $P_1(r_n) = 0$. Since $K[r_1, \dots, r_{n-1}]$ is the image of the polynomial ring $K[x_1, \dots, x_{n-1}]$ by the homomorphism of K-algebras sending x_i to r_i, there is a non zero polynomial

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

such that $P(r_1, \dots, r_n) = 0$. Let $F(x_1, \dots, x_n)$ be the sum of the monomials of degree $d := \deg(P)$ which appear in P (so that in particular $\deg(P - F) < d$). Choose $\lambda_1, \dots, \lambda_{n-1} \in K$ so that $F(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$. To see why the λ_i exist, note that since F is a homogenous polynomial, the polynomial $F(x_1, \dots, x_{n-1}, 1)$ is a sum of homogenous polynomials of distinct degrees and thus is not the zero polynomial. Hence

$F(x_1, \ldots, x_{n-1}, 1)$ must be non-zero for some specific values of $x_1, \ldots, x_{n-1}$, because a non-zero polynomial with coefficients in an infinite field cannot evaluate to 0 for all the values of its variables (why? - exercise).

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

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

for some polynomials $F_1, \ldots, F_d$ in the u_i. To see why these equalities hold, note that if $J(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is a monomial of degree δ, then

$$J(u_1 + \lambda_1 r_n, u_2 + \lambda_2 r_n, \ldots, u_{n-1} + \lambda_{n-1} r_n, r_n) = J(\lambda_1, \ldots, \lambda_{n-1}, 1) r_n^\delta + (\text{polynomial in } r_n \text{ of lower degree})$$

and apply this remark to the monomials of maximal degree appearing in $P(x_1, \ldots, x_k)$.

Thus

$$r_n^d + (F(\lambda_1, \ldots, \lambda_{n-1}, 1))^{-1} F_1(u_1, \ldots, u_{n-1}) r_n^{d-1} + \cdots + (F(\lambda_1, \ldots, \lambda_{n-1}, 1))^{-1} F_d(u_1, \ldots, u_{n-1}) = 0$$

and we see that r_n is integral over $K[u_1, \ldots, u_{n-1}]$. Now, by the inductive hypothesis, there exists an injective homomorphism of K-algebras

$$K[y_1, \ldots, y_t] \to K[u_1, \ldots, u_{n-1}]$$

for some $t \geq 0$, such that $K[u_1, \ldots, u_{n-1}]$ is integral over $K[y_1, \ldots, y_t]$. Hence

$$R = K[r_1, \ldots, r_n] = K[u_1, \ldots, u_{n-1}][r_n]$$

is integral over $K[y_1, \ldots, y_t]$ by Lemma 8.6. □

Noether's normalisation lemma has the following fundamental corollary.

Corollary 9.2 (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 8.8, 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.

To see this, suppose $t \geq 1$ and note first that the ring $K[y_1, \ldots, y_t]$ has the prime ideal (0) since it is a domain. Also, the element y_1 is not a unit and it is thus contained in a maximal ideal (use Lemma 2.4), which is not equal to (0), since $y_1 \neq 0$. Hence $K[y_1, \ldots, y_t]$ has at least two prime ideals (in fact it has infinitely many but we don't need this here).

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 8.5). □

END OF LECTURE 10

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

Corollary 9.3. *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 9.2, $K[x_1, \ldots, x_t]/I$ 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 (obtained by composing the isomorphism with the quotient map $K[x_1, \ldots, x_t] \to K[x_1, \ldots, x_t]/I$). 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 9.4. *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 $S = \{1, f, f^2, \ldots\}$. Since f is not nilpotent, we have $f^k \cdot f \neq 0$ for all $k \geq 0$ (setting $f^k = 1$ if $k = 0$) 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 2.4). Since R_S is a finitely generated K-algebra (see Lemma 5.3), the quotient $R_S/\mathfrak{q}$ is also finitely generated over K. Thus, by Corollary 9.2, 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 (since $R_S/\mathfrak{q}$ is integral over K, being finite over K - see after Corollary 8.5) and thus $\mathrm{Im}(\phi)$ is a field by Lemma 8.9. 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 9.5 (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*

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

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 9.4), there exists a maximal ideal $\mathfrak{m}$ in R, such that $\mathfrak{m} \supseteq I$ and $Q \notin \mathfrak{m}$. By Corollary 9.3, 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 9.3, we see that $Q(a_1, \ldots, a_t) \neq 0$. This is a contradiction, so $Q \in \mathfrak{r}(I)$. □

10 Jacobson rings

In this section, we collect more consequences of the weak Nullstellensatz and we show that the property of being a Jacobson ring is a very stable property. See Theorem 10.5 below. We also give an alternative proof of the weak Nullstellensatz, based of the theorem of Artin-Tate 7.7, which does not depend on Noether's normalisation lemma. This shows in particular that the proof of Theorem 10.5 below can be made independent of Noether's normalisation lemma. In the situation where the ring is noetherian, it can even be made independent of the more difficult results of the theory of integral extensions (like Theorem 8.8).

New proof of the weak Nullstellensatz (Corollary 9.2).

For this, we shall need the following lemma.

Lemma 10.1. *Let K be a field. Let $t \geq 1$ and let $P(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$ be a non-zero polynomial. Then there exists a non zero prime ideal in $K[x_1, \ldots, x_t]$, which does not contain $P(x_1, \ldots, x_t)$.*

Proof. (of Lemma 10.1). Let $L := K(x_1, \ldots, x_{t-1})$ be the quotient field of $K[x_1, \ldots, x_{t-1}]$ (where we set $L := K$ if $t = 1$). Let $\iota : K[x_1, \ldots, x_t] = K[x_1, \ldots, x_{t-1}][x_t] \to L[x_t]$ be the natural injective map. If we can find a prime ideal $\mathfrak{p}$ in $L[x_t]$ such that $\iota(P) \notin \mathfrak{p}$, then the prime ideal $\iota^{-1}(\mathfrak{p})$ will not contain P, so we may assume that $t = 1$.

Let us write $x_t = x_1 = x$ so that $K[x_1, \ldots, x_t] = K[x]$. We may assume without restriction of generality that $P(x)$ is monic (why?). We may also assume that $P(x)$ is not constant (otherwise, any maximal ideal of $K[x]$ will do).

Let $P = P_1^{n_1} \ldots P_k^{n_k}$ be the decomposition of P into irreducible factors, where all the P_i are monic (and irreducible). Let Q be an irreducible factor of $1 + P$. Then the ideal (Q) does not contain P because otherwise there would be polynomials $R_1, R_2 \in K[x]$ such that $QR_1 = 1 + P$ and $QR_2 = P$, so that

$Q(R_1 - R_2) = 1$, which is impossible, since Q is not constant. Since Q is irreducible, the ideal (Q) is prime and therefore the ideal (Q) satisfies the requirements of the lemma. $\square$

Now to the proof of the weak Nullstellensatz. Let K be a field and let R be a finitely generated K-algebra. Suppose that R is a field. We want to show that R is finite over K. Let $r_1, \dots, r_k$ be generators of R over K. Suppose that the r_i are numbered in such a way that the elements $r_1, \dots, r_l$ are algebraically independent over K for some $l \in \{0, \dots k\}$ (in particular, the set $r_1, \dots, r_l$ might be empty) and so that r_{k+i} is algebraic over $K(r_1, \dots, r_l)$ for all $i \in \{1, \dots k-l\}$. Recall that to say that the generators $r_1, \dots, r_l$ are algebraically independent means that the homomorphism of K-algebras from $K[x_1, \dots, x_l]$ to R, which sends x_i to r_i for all $i \in \{1, \dots, l\}$, is injective. This renumbering can be carried out as in the proof of Noether's normalisation lemma. We may assume that $l \geq 1$, for otherwise R is a finite field extension of K (since R would be then an integral and finitely generated K-algebra) and there is nothing to prove. Since R is a field, the quotient field $L \simeq K(x_1, \dots, x_l)$ of $K[x_1, \dots, x_l] \simeq K[r_1, \dots, r_l]$ can be viewed as a subfield of R (ie, the subfield $K(r_1, \dots, r_l)$). Now note that R is generated by $r_{l+1}, \dots, r_k$ as an L-algebra and that the r_{l+i} ($i \in \{1, \dots, k-l\}$) are algebraic over L, since they are algebraic over $K(r_1, \dots, r_l)$. Since L is a field, the r_{l+i} are actually integral over L and hence R is a finite field extension of L. We deduce from the Theorem of Artin-Tate 7.7 that L is finitely generated over K. In particular, $K(x_1, \dots, x_l) \simeq L$ is finitely generated as a $K[x_1, \dots, x_l]$-algebra. Let $P_1(x)/Q_1(x), \dots, P_a(x)/Q_a(x)$ be generators of $K(x_1, \dots, x_l)$ as a $K[x_1, \dots, x_l]$-algebra. Let $Q(x) := \prod_{i=1}^{a} Q_i(x)$ and let $S := \{1, Q(x), Q^2(x), \dots\}$. Since $K[x_1, \dots, x_l]$ is a domain, the localised ring $K[x_1, \dots, x_l]_S$ can be viewed as a subring of $K(x_1, \dots, x_l)$. Furthermore, since every element of $K(x_1, \dots, x_l)$ can now be written as a quotient $R(x)/Q^b(x)$ for some $b \geq 0$, we see that $K[x_1, \dots, x_l]_S = K(x_1, \dots, x_l)$. Since $K(x_1, \dots, x_l)$ has only one prime ideal, namely the zero ideal, we conclude from Lemma 5.6 that every non zero prime ideal of $K[x_1, \dots, x_l]$ contains $Q(x)$. This contradicts Lemma 10.1. We conclude that $l = 0$, so that R is finite over K. $\square$

The Jacobson property enters the proof of Theorem 10.5 via the following lemma.

Lemma 10.2. *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 5.6 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 (why?). $\square$

Corollary 10.3. *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.*

Proof. Let $K \subseteq T$ be the fraction field of R. Note that by Corollary 9.2, T is a finite extension of K. Let $t_1, \dots, t_k \in T$ be generators of T as a R-algebra. Let

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

be a monic polynomial with coefficients in K, which annihilates t_i (this exists since T is integral over K). Let $b := \prod_{i=1}^{k} \prod_{j=1}^{d_i} b_{i,d_i-j}$. Let $S := \{1, b, b^2, \dots\}$. Then there is a natural injective homomorphism of

R-algebras from R_S into K, because R is a domain (check) and 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. Lemma 8.9 now implies that R_S is a field. Finally, Lemma 10.2 implies that R is a field.

Second proof of Corollary 10.3 in the noetherian situation. Suppose that R is noetherian. Let $K \subseteq T$ be the fraction field of R. By Corollary 9.2, T is a finite extension of K. Then K is finitely generated over R by Theorem 7.7. But then K has the form $R_{S'}$ for a multiplicative set S' generated by an element of R (which can be taken to be the product of the denominators of a finite set of generators of K over R - we leave the details to the reader). Hence R is a field by Lemma 10.2. □

Corollary 10.4. *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 $R/\psi^{-1}(\mathfrak{m})$. Also, $R/\psi^{-1}(\mathfrak{m})$ is a Jacobson ring, since it is the quotient of a Jacobson ring. Thus Corollary 10.3 implies the result. □

Theorem 10.5. *A finitely generated algebra over a Jacobson ring is Jacobson.*

Proof. The beginning of the proof is similar to the proof of Corollary 9.4.

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 $k \geq 0$ (setting $f^k = 1$ if $k = 0$) and thus the localisation T_S is not the zero ring. Let $\mathfrak{q}$ be a maximal ideal of T_S (this exists by Lemma 2.4). Since T_S is a finitely generated R-algebra (see Lemma 5.3), 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. From Corollary 10.4, we deduce that $\ker(\phi)$ is a maximal ideal and that $T_S/\mathfrak{q}$ 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 8.9. 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

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 11.1. *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 $\operatorname{ht}(\mathfrak{p}) > \operatorname{ht}(\mathfrak{q})$, provided $\operatorname{ht}(\mathfrak{p}) < \infty$.

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

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

for any prime ideal $\mathfrak{p}$ of R (where $\mathfrak{p} \,(\operatorname{mod} N)$ is the image of $\mathfrak{p}$ in R/N).

Note finally that from the definitions, we have

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

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

Lemma 11.2. *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*

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

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 5.6. Furthermore this correspondence preserves inclusion. The first equality follows directly from this. For the second one, note that by definition, we have

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

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

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

□

Note that Lemma 11.2 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 $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\lambda^{-1}(\mathfrak{p}))$ (use the second remark after Lemma 5.6).

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:

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

(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 next two subsections contain some preliminary results (which are also of independent interest) that we shall need before we resume the study of dimension in subsection 11.3 below.

11.1 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 $k[S] \subseteq K$ (recall that $k[S]$ is the smallest k-subalgebra of K containing k and S). 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 $k(S_1 \cup S_2) = k(S_1)(S_2)$ (this follows from the definitions).

Also, recall that if the elements of S are all algebraic (equivalently, integral) over k, then we actually have $k(S) = k[S]$. To see this, note that we only have to verify this in the situation where $S = \{s\}$ in view of the compatibility mentioned in the previous paragraph. Now notice that if an element $s \in K$ is algebraic over k, then we have a homomorphism of k-algebras $k[t] \to K$, which sends t to s. Since the image of this homomorphism is a domain and s is algebraic, the kernel of this homomorphism is a non zero prime ideal of $k[t]$, which is thus maximal (why?). Hence $k[s]$ is actually field (all this should be familiar from Rings and Modules and/or the Galois Theory course). Finally note that if all the elements of S are algebraic over k then $k(S)$ is a finite extension of k. This follows from Corollary 8.4 and Proposition 8.2.

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. To obtain such a basis, start with a finite set S such that $K = k(S)$. Take a subset $S' \subseteq S$, which is algebraically independent and has maximal cardinality among such subsets (note that S' might be empty). Then each of the elements of $S \backslash S'$ is by construction algebraic over $k(S')$ and thus K is algebraic over $k(S')$. This subset will be a transcendence basis of K over k.

Proposition 11.3. *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. For convenience, write $S := \{\gamma_1, \ldots, \gamma_n\}$ and $T := \{\rho_1, \ldots, \rho_m\}$, where $n = \#S$ and $m = \#T$.

We shall prove that $m = n$ by induction on $\min(m, n)$. The statement is true if $\min(m, n) = 0$ (so that either S or T is empty), for in that case K is algebraic over k and then both S and T must be empty.

We may assume without restriction of generality that $S \cap T = \emptyset$. To see this, suppose that $S \cap T = U$ and that $U \neq \emptyset$. Then $S \backslash U$ and $T \backslash U$ are transcendence bases for K over $k(U)$. We have

$$\min(\#(S \backslash U), \#(T \backslash U)) = \min(m, n) - \#U$$

and thus by induction, we have $\#(S \backslash U) = \#(T \backslash U)$ so that $\#S = n = \#T = m$.

We also contend that m or n is minimal among the cardinalities of all possible transcendence bases of K over k. To see this, suppose that $m \leq n$ (say) so that $m = \min(m, n)$. Suppose that $m = \#T$ is not minimal. Choose a transcendence basis T' of K over k such that $\#T' < m$ and such that $\#T'$ is minimal. We have $\min(\#T, \#T') < \min(m, n)$ and so by induction we have $\#T' = \#T = m$, which a contradiction. Hence m is minimal.

We now start the proof. Suppose without restriction of generality that m is minimal among the cardinalities of all possible transcendence bases of K over k (swap S and T if necessary).

By assumption there is a non zero polynomial $P(x_0, \ldots, x_m) \in k[x_0, \ldots, x_m]$, such that

$$P(\gamma_1, \rho_1, \ldots, \rho_m) = 0$$

(to obtain this polynomial, start with a non zero polynomial with coefficients in $k(\rho_1, \ldots, \rho_m) \simeq \mathrm{Frac}(k[x_1, \ldots, x_m])$, which annihilates γ_1, and clear denominators). We suppose that $P(x_0, \ldots, x_m)$ has minimal degree among all non zero polynomials with this property.

By assumption, $P(x_0, \ldots, x_m)$ contains monomials with positive powers of x_k for some $k \geq 1$ (otherwise γ_1 is algebraic over k). Renumbering, we may suppose that this variable is x_1.

We may thus write

$$P(x_0, \ldots, x_m) = \sum_j P_j(x_0, x_2, \ldots, x_m) x_1^j$$

where $P_j(x_0, x_2, \ldots, x_m) \in k[x_0, x_2, \ldots, x_m]$. Since $P(x_0, \ldots, x_m)$ is a non constant polynomial in the variable x_1, we know that $P_{j_0}(x_0, x_2, \ldots, x_m) \neq 0$ for some $j_0 > 0$. Also, we cannot have $P_{j_0}(\gamma_1, \rho_2, \ldots, \rho_m) = 0$, because that would violate the assumption that the degree of $P(x_0, \ldots, x_m)$ is minimal.

Thus, since $P(\gamma_1, \rho_1, \ldots, \rho_m) = \sum_j P_j(\gamma_1, \rho_2, \ldots, \rho_m) \rho_1^j = 0$, we see that ρ_1 is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$. Hence $k(\gamma_1, \rho_1, \rho_2, \ldots, \rho_m)$ is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$ and thus K is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$ (again use Corollary 8.4 and Proposition 8.2). Since m is minimal, we conclude that $\{\gamma_1, \rho_2, \ldots, \rho_m\}$ is a

transcendence basis of K. In particular $\{\gamma_2, \ldots, \gamma_n\}$ and $\{\rho_2, \ldots, \rho_m\}$ are transcendence bases of K over $k(\gamma_1)$. By induction, we thus have $m - 1 = n - 1$, ie $m = n$ and the proof is complete. $\square$

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

11.2 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 $R = \oplus_{i \geq 0} R_i$ (where $\oplus$ refers to an internal direct sum of additive subgroups) and such that $R_i \cdot R_j \subseteq R_{i+j}$ for any $i, j \geq 0$ (ie if $r \in R_i$ and $t \in R_j$ then $rt \in R_{i+j}$). 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 $i_0 \geq 0$ (why?).

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 M, such that $M = \oplus_{i \geq 0} M_i$ (where $\oplus$ refers to an internal direct sum) and such that $R_i \cdot M_j \subseteq M_{i+j}$ for any $i, j \geq 0$ (ie if $r \in R_i$ and $t \in M_j$ then $rt \in M_{i+j}$). 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 11.4. *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 7.2.

We prove the implication (i)⇒(ii). The ring R_0 is noetherian since it is a quotient of a noetherian ring (by Lemma 7.2).

To show that R is finitely generated as a R_0-module, let $a_1, \ldots, a_k$ be generators of $\oplus_{i>0} R_i$ viewed as an ideal of R (this exists, since R is noetherian). We claim that the graded components of $a_1, \ldots, a_k$ generate R as a R_0-algebra (more concretely: the elements $[a_1]_1, [a_1]_2 \ldots, [a_2]_1, [a_2]_2, \ldots$ generate R as a R_0-algebra). This will prove the lemma, since each a_i only has finitely many graded components.

We shall prove by induction on $i \geq 0$ that R_i lies inside the sub-R_0-algebra generated by the graded components of $a_1, \ldots, a_k$. Since R is generated by all the R_i, this will prove the claim. For $i = 0$, there is nothing to prove. So suppose that $i > 0$ and that the subgroups $R_0, \ldots, R_{i-1}$ lie inside the sub-R_0-algebra generated by the graded components of $a_1, \ldots, a_k$.

Let $r \in R_i$. By assumption, there are elements $t_1, \ldots, t_k \in R$ such that $r = t_1 a_1 + \cdots + t_k a_k$. We deduce that

$$r = [r]_i = \sum_{j=1}^{k} \sum_{u=1}^{i} [t_j]_{i-u} [a_j]_u$$

Now, in this sum, we have $[t_j]_{i-u} \in R_0 \oplus R_1 \oplus \cdots \oplus R_{i-1}$ and thus $[t_j]_{i-u}$ lies in the sub-R_0-algebra generated by the graded components of $a_1, \ldots, a_k$ by the inductive hypothesis. Thus r lies in this sub-R_0-algebra also, which proves the claim and the lemma. □

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

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

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 $R^\# := \oplus_{i \geq 0} I^i$ (where $I^0 = R$) carries a natural structure of graded ring, with the grading given by the presentation $R^\# = \oplus_{i \geq 0} I^i$ (if $\alpha \in I^i$ and $\beta \in I^j$, then the product of α and β in $R^\#$ is given by the product of α and β in R, viewed as an element of I^{i+j}). 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 (if $\alpha \in I^i$ and $\beta \in M_j$, then the multiplication of β by α in $M^\#$ is given by the multiplication of β by α in M, viewed as an element of M_{i+j}, in which it lies since $M_\bullet$ is a I-filtration). 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. The corresponding R-module structure on $M^\#$ is then simply $M^\# = \oplus_{i \geq 0} M_i$ viewed as a direct sum of R-modules.

Lemma 11.5. *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 rings $\phi : R[x_1, \ldots, x_k] \to R^\#$, 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 (so that ϕ is a homomorphism of R-algebras). By construction, ϕ is surjective and hence $R^\#$ is also noetherian by the Hilbert basis theorem and Lemma 7.2. □

Note that in this context there is a slight inaccuracy in AT, p. 107, before Lemma 10.8.

Lemma 11.6. *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 11.7 (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 11.6, the $R^{\#}$-module $M^{\#}$ is finitely generated. The module $N^{\#}$ is thus also finitely generated by Lemma 11.5 and by Lemma 7.4. Hence $N \cap M_\bullet$ is a stable I-filtration by Lemma 11.6. $\square$

Corollary 11.8. *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. $\square$

Corollary 11.9 (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 11.8, 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 $y \in I^2 M$. Continuing in this way, we conclude that $y \in N$. $\square$

Corollary 11.10 (of Krull's theorem)**.** *Let R be a noetherian domain. Let I be a proper ideal of R. Then $\cap_{n\geq 0} I^n = 0$.*

Proof. This is clear. □

Corollary 11.11 (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 (a similar reasoning was made during the proof of Nakayama's lemma). 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 11.11 is especially useful when R is a local ring (in which case I is always contained in the Jacobson radical if $I \neq R$).

END OF LECTURE 13

11.3 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 7.1).

Lemma 11.12. *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 follows from Lemma 7.5.

(iii)⇒(iv): Let

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$$

be a descending sequence of ideals in R. Let $k \geq 0$ be the minimal natural number such that the sequence

$$\mathfrak{m}^k I_1 \supseteq \mathfrak{m}^k I_2 \supseteq \mathfrak{m}^k I_3 \supseteq \dots$$

stabilises. The number k exists since $\mathfrak{m}^k = 0$ for some $k \geq 0$ by (iii). Suppose for contradiction that $k > 0$. Let $n_0 \geq 1$ be such that $\mathfrak{m}^k I_n = \mathfrak{m}^k I_{n_0}$ for all $n \geq n_0$. Consider the descending sequence

$$\mathfrak{m}^{k-1} I_1 \supseteq \mathfrak{m}^{k-1} I_2 \supseteq \mathfrak{m}^{k-1} I_3 \supseteq \dots$$

By construction we have $\mathfrak{m}^{k-1}I_n \supseteq \mathfrak{m}^k I_{n_0}$ for all $n \geq 1$. There are thus natural inclusions

$$\mathfrak{m}^{k-1}I_1/\mathfrak{m}^k I_{n_0} \supseteq \mathfrak{m}^{k-1}I_2/\mathfrak{m}^k I_{n_0} \supseteq \mathfrak{m}^{k-1}I_3/\mathfrak{m}^k I_{n_0} \supseteq \dots$$

and furthermore, for all $n \geq n_0$, we have $\mathfrak{m}(\mathfrak{m}^{k-1}I_n/\mathfrak{m}^k I_{n_0}) = 0$. Hence $\mathfrak{m}^{k-1}I_n/\mathfrak{m}^k I_{n_0}$ has a natural structure of $R/\mathfrak{m}$-module if $n \geq n_0$. In particular, the sequence

$$\mathfrak{m}^{k-1}I_{n_0}/\mathfrak{m}^k I_{n_0} \supseteq \mathfrak{m}^{k-1}I_{n_0+1}/\mathfrak{m}^k I_{n_0} \supseteq \mathfrak{m}^{k-1}I_{n_0+2}/\mathfrak{m}^k I_{n_0} \supseteq \dots$$

is a decreasing sequence of $R/\mathfrak{m}$-modules. Also, all these $R/\mathfrak{m}$-modules are finitely generated because R is a noetherian ring. Since $R/\mathfrak{m}$ is a field, one thus obtains a decreasing sequence of finite-dimensional vector spaces and such a sequence must stabilise. Let $n_{00} \geq n_0$ be such that $\mathfrak{m}^{k-1}I_n/\mathfrak{m}^k I_{n_0} = \mathfrak{m}^{k-1}I_{n_{00}}/\mathfrak{m}^k I_{n_0}$ for all $n \geq n_{00}$. Then we have by construction $\mathfrak{m}^{k-1}I_n = \mathfrak{m}^{k-1}I_{n_{00}}$ for all $n \geq n_{00}$. In particular, the sequence $\mathfrak{m}^{k-1}I_n$ also stabilises. This contradicts the minimality of k so we must have $k = 0$, ie the sequence $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ stabilises.

(iv)⇒(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 (since the nilradical is contained in $\mathfrak{p}_1$ by Proposition 3.2). 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 11.11, 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 $\dim(R) \neq 0$. □

Theorem 11.13 (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 $f/1 \in R_{\mathfrak{p}}$ (use Lemma 5.6 and Lemma 5.7). Furthermore, the height of $\mathfrak{p}$ is the same as the height of the maximal ideal of $R_{\mathfrak{p}}$ (again, use Lemma 5.6 and Lemma 5.7). Since $R_{\mathfrak{p}}$ is also noetherian by Lemma 7.3, we may thus suppose that R is a local ring and that $\mathfrak{p}$ is a maximal ideal.

Let

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \dots \supsetneq \mathfrak{p}_{k_0}$$

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 5.6). 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 5.6. 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 7.2). 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

$$I_1 \supseteq I_2 \supseteq I_3 \dots \tag{6}$$

We conclude from Lemma 11.12 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 Corollary 3.7 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 11.11 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 5.6), we conclude from Lemma 11.12 that $R_\mathfrak{q}$ has dimension 0. In particular, we have $\mathrm{ht}(\mathfrak{q}) = 0$ (by Lemma 11.2). In other words, $\mathfrak{q}$ cannot contain any prime ideal other than itself. Hence $k = 1$. □

Lemma 11.14. *Let R be a noetherian ring. Let $\mathfrak{p}, \mathfrak{p}'$ be prime ideals of R and suppose that $\mathfrak{p} \subsetneq \mathfrak{p}'$. There exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{p} \subseteq \mathfrak{q} \subsetneq \mathfrak{p}'$ with the following property: if $\mathfrak{q}'$ is a prime ideal such that $\mathfrak{q} \subseteq \mathfrak{q}' \subseteq \mathfrak{p}$, then either $\mathfrak{q}' = \mathfrak{q}$ or $\mathfrak{q}' = \mathfrak{p}$.*

Proof. Suppose that the conclusion does not hold. Let $\mathfrak{q}_1$ be any prime ideal such that $\mathfrak{p} \subseteq \mathfrak{q}_1 \subsetneq \mathfrak{p}$ (we might eg take $\mathfrak{q}_1 = \mathfrak{p}$). By assumption, there exists a prime ideal $\mathfrak{q}_2$ such that $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \mathfrak{p}$. Applying the assumption again to $\mathfrak{q}_2$, we obtain a prime ideal $\mathfrak{q}_3$ such that $\mathfrak{q}_2 \subsetneq \mathfrak{q}_3 \subsetneq \mathfrak{p}$. Continuing in this way we obtain an ascending sequence of ideals

$$\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \mathfrak{q}_3 \subsetneq \dots$$

However, this sequence must stop since R is noetherian. This is a contradiction, so one of the $\mathfrak{q}_i$ must have the property mentioned in the lemma. □

Corollary 11.15. *Let R be a noetherian ring. Let $f_1, \dots, f_k \in R$. Let $\mathfrak{p}$ be a prime ideal minimal among those containing $(f_1, \dots, f_k)$. 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

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \dots \supsetneq \mathfrak{p}_{\mathrm{ht}\mathfrak{p}} \quad (*)$$

be a (possibly infinite) chain of prime ideals beginning with $\mathfrak{p}$ and of length $\mathrm{ht}(\mathfrak{p})$. We also assume that there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{p}_1$, other than $\mathfrak{p}$ and $\mathfrak{p}_1$. Note that this last condition is automatically

satisfied if $\mathrm{ht}(\mathfrak{p}) < \infty$, because the chain then has maximal (finite) length). If $\mathrm{ht}(\mathfrak{p}) = \infty$ we can create a chain satisfying this condition using 11.14.

We want to show that that $\mathrm{ht}(\mathfrak{p}) \leq k$. We may suppose that $\mathrm{ht}(\mathfrak{p}) > 0$, otherwise there is nothing to prove. Let $\mathfrak{q} := \mathfrak{p}_1$. We claim that $\mathrm{ht}(\mathfrak{q}) \leq k-1$ (so that in particular, we cannot have $\mathrm{ht}(\mathfrak{p}) = \infty$).

We prove the claim. From the assumptions, there is an f_i such that $f_i \notin \mathfrak{q}$ (otherwise $\mathfrak{p}$ is not minimal among the prime ideals containing $(f_1, \ldots, f_k)$). Up to renumbering, we may assume that $f_1 \notin \mathfrak{q}$. 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 11.12 (iii) that the image of all the f_i are nilpotent in $R/(\mathfrak{q}, f_1)$. In other words there are elements $b_i \in \mathfrak{q}, a_i \in R$ and integers $n_i \geq 2$ such that

$$f_i^{n_i} = a_i f_1 + b_i.$$

Note that

$$\mathfrak{p} \supseteq (f_1, f_2^{n_2}, f_3^{n_3}, \ldots, f_k^{n_k}) = (f_1, b_2, \ldots, b_k)$$

and that $\mathfrak{p}$ is also minimal among all the prime ideals containing $(f_1, b_2, \ldots, b_k)$, since

$$\mathfrak{r}((f_1, f_2^{n_2}, f_3^{n_3}, \ldots, f_k^{n_k})) = \mathfrak{r}((f_1, f_2, \ldots, f_k)).$$

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 $f_1 \pmod J$. Hence $\mathrm{ht}(\mathfrak{p} \pmod J) \leq 1$ by Krull's principal ideal theorem. On the other hand, we have

$$\mathfrak{p} \pmod J \supsetneq \mathfrak{q} \pmod J$$

(since $J \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ and $\mathfrak{q} \subsetneq \mathfrak{p}$) so that $\mathrm{ht}(\mathfrak{p} \pmod J) = 1$ and $\mathrm{ht}(\mathfrak{q} \pmod J) = 0$. In particular, $\mathfrak{q}$ is minimal among all the prime ideals containing J. Applying the inductive hypothesis, we see that $\mathrm{ht}(\mathfrak{q}) \leq k-1$. In particular, the chain $(*)$ is finite.

Finally, we see from the assumptions that $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q}) + 1 \leq k$ and so the corollary is proven. □

In particular, *in a noetherian ring, the height of any prime ideal is finite.* Together with Lemma 11.2, 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 a noetherian ring of infinite dimension, see Ex. 3 of chap. 11, p. 126 of AT.

Note also that Corollary 11.15 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 11.15).

Corollary 11.16. *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 11.15 and the definition of the height.

Corollary 11.17. *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 $\mathrm{ht}(t_1, \ldots, t_c) = c$.*

Note that the assumptions imply that we have $k \leq c$. Here we set $(t_1, \ldots, t_k) = (0)$ (resp. $(t_1, \ldots, t_c) = 0$) if $k = 0$ (resp. if $c = 0$). Note also that if $\mathrm{ht}(t_1, \ldots, t_c) = c$ then $\mathfrak{p}$ is a minimal prime ideal associated with the ideal $(t_1, \ldots, t_c)$. Indeed, if there were a prime ideal $\mathfrak{q}$ such that $\mathfrak{q} \subsetneq \mathfrak{p}$ and $\mathfrak{q} \supseteq (t_1, \ldots, t_c)$, then we would have $\mathrm{ht}(\mathfrak{p}) = c > \mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(t_1, \ldots, t_c) = c$, which is a contradiction.

Proof. If $c = 0$ then $\mathfrak{p}$ is a minimal prime ideal of R and then $\mathrm{ht}((0)) = c = 0$ so there is nothing to prove. So we suppose that $c > 0$. We may obviously assume that $k < c$.

By induction on $k < c$, it is sufficient to construct an element $t \in \mathfrak{p}$ so that $\mathrm{ht}((t_1, \ldots, t_k, t)) = k + 1$. Since by Corollary 11.15, we have $\mathrm{ht}((t_1, \ldots, t_k, t)) \leq k+1$ for any $t \in R$, we actually only have to find an element $t \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k, t)) > k$. Suppose for contradiction that such an element does not exist. Since $\mathrm{ht}((t_1, \ldots, t_k, t)) \geq k$ for any $t \in R$, this implies that $\mathrm{ht}((t_1, \ldots, t_k, t)) = k$ for all $t \in \mathfrak{p}$. In particular, for any $t \in \mathfrak{p}$, there is a prime ideal $\mathfrak{q}$, which contains $(t_1, \ldots, t_k, t)$ and which has height k; now $\mathfrak{q}$ contains a minimal prime ideal $\mathfrak{q}_1$ associated with $(t_1, \ldots, t_k)$ by Lemma 6.9 and we have $\mathrm{ht}(\mathfrak{q}_1) \geq k$ by assumption; hence we must have $\mathfrak{q} = \mathfrak{q}_1$, so that $\mathfrak{q}$ is a minimal prime ideal associated with $(t_1, \ldots, t_k)$, which has height k. We conclude that for all $t \in \mathfrak{p}$, t is contained in a minimal prime ideal of height k associated with $(t_1, \ldots, t_k)$. In other words, $\mathfrak{p}$ is contained in the union of the minimal prime ideals of height k associated with $(t_1, \ldots, t_k)$. By Proposition 6.1 (1), we conclude that $\mathfrak{p}$ is contained in, and hence equal to, one of these minimal prime ideals. Since $\mathrm{ht}(\mathfrak{p}) = c > k$, this contradicts Corollary 11.15. □

END OF LECTURE 14

11.4 The dimension of polynomial rings

We now turn to the computation of the dimension of polynomial rings. The main result is

Theorem 11.18. *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 11.19. *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 8.12.

Lemma 11.20. *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 $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Proof. We have a commutative diagram of rings

$$\begin{array}{ccccc} & & \overset{\rho}{\frown} & & \\ T & \longrightarrow & T/I & \longrightarrow & (T/I)_{\psi(S)} \\ \uparrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \psi_S} \\ R & \longrightarrow & R/\mathfrak{p} & \longrightarrow & \mathrm{Frac}(R/\mathfrak{p}) \end{array}$$

leading to a commutative diagram of spectra

$$\begin{array}{ccccc} & & \overset{\mathrm{Spec}(\rho)}{\frown} & & \\ \mathrm{Spec}(T) & \longleftarrow & \mathrm{Spec}(T/I) & \longleftarrow & \mathrm{Spec}((T/I)_{\psi(S)}) \\ \downarrow{\scriptstyle \mathrm{Spec}(\phi)} & & \downarrow{\scriptstyle \mathrm{Spec}(\psi)} & & \downarrow{\scriptstyle \mathrm{Spec}(\psi_S)} \\ \mathrm{Spec}(R) & \longleftarrow & \mathrm{Spec}(R/\mathfrak{p}) & \longleftarrow & \mathrm{Spec}(\mathrm{Frac}(R/\mathfrak{p})) \end{array}$$

The lemma is saying that the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$ is precisely the image of $\mathrm{Spec}(\rho)$.

Note first that $\mathrm{Spec}(\mathrm{Frac}(R/\mathfrak{p}))$ consists of one point, since $\mathrm{Frac}(R/\mathfrak{p})$ is a field. The image of $\mathrm{Spec}(\mathrm{Frac}(R/\mathfrak{p}))$ in $\mathrm{Spec}(R/\mathfrak{p})$ is the ideal $(0) \subseteq R/\mathfrak{p}$ and the preimage of the ideal $(0) \subseteq R/\mathfrak{p}$ in R is $\mathfrak{p}$. Thus the image of $\mathrm{Spec}(\rho)$ is contained in the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$, since the diagram is commutative.

Now suppose that $\mathfrak{q} \in \mathrm{Spec}(T)$ and that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ (ie $\mathfrak{q}$ lies inside the fibre of $\mathrm{Spec}(\phi)$ above $\mathfrak{p}$).

Then $\mathfrak{q} \supseteq I$ and there is thus an ideal $\mathfrak{q}' \in \mathrm{Spec}(T/I)$, such that $\mathfrak{q}$ is the image of $\mathfrak{q}'$ in $\mathrm{Spec}(T)$. On the other hand, we know that $\psi^{-1}(\mathfrak{q}')$ is the 0 ideal, since $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ and the diagram of rings is commutative. In other words, we have $\mathfrak{q}' \cap \psi(S) = \emptyset$. We conclude from Lemma 5.6 that $\mathfrak{q}'$ lies in the image of the map $\mathrm{Spec}((T/I)_{\psi(S)}) \to \mathrm{Spec}(T/I)$.

This concludes the proof of the lemma. $\square$

Note that the correspondence between

- prime ideals $\mathfrak{q}$ such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$

and

- prime ideals of $(T/I)_{\psi(S)}$

described by the lemma respects the inclusion relation in both directions (ie an inclusion of prime ideals holds on one side iff it holds on the other side). (why?)

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 11.21. *We keep the notation of Lemma 11.20. 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. This is an immediate consequence of Lemma 11.20 and the following remark. □

Lemma 11.22. *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 is 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 $\mathfrak{p} \in \mathrm{Spec}(R)$ 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. □

Lemma 11.23. *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 $\mathfrak{r}((0))[x]$ (use Proposition 6.1 (ii)). In view of Lemma 11.22, 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 6.7 and Lemma 6.8), which is what we wanted to prove.

For the second statement, apply the first statement to $\mathfrak{p}_i \pmod{\mathfrak{a}}$, noting that $(R/\mathfrak{a})[x] \simeq R[x]/\mathfrak{a}[x]$ (or provide a direct proof, similar to the proof for $\mathfrak{a} = (0)$). □

Lemma 11.24. *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 11.23 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 $c := \operatorname{ht}(\mathfrak{p})$ and let $a_1, \dots, a_c \in \mathfrak{p}$ be such that $\operatorname{ht}((a_1, \dots, a_c)) = c$, so that $\mathfrak{p}$ is a minimal prime ideal associated with $(a_1, \dots, a_c)$. This exists by Corollary 11.17. Let $J := (a_1, \dots, a_c)$. By the previous lemma, $\mathfrak{p}[x]$ is a minimal prime ideal associated with $J[x]$. We conclude from Corollary 11.15 that $\operatorname{ht}(\mathfrak{p}[x]) \leq c$ (since the elements $a_1, \dots, a_c$ 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 chain 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 $\operatorname{ht}(\mathfrak{p}[x]) \geq c$. Hence $\operatorname{ht}(\mathfrak{p}[x]) = c$. □

Lemma 11.25. *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 11.23, 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 11.26. *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 11.24. Let $a_1, \dots, a_c \in \mathfrak{m}$ be such that $\operatorname{ht}((a_1, \dots, a_i)) = i$ for all $i \in \{1, \dots, c\}$. This exists by Corollary 11.17 (or rather, its proof). Using Lemma 11.24 again, we may suppose that $a_1, \dots, a_\delta \in \mathfrak{m} \cap R$. In particular, $(\mathfrak{m} \cap R)[x]$ is a minimal prime ideal associated with $(a_1, \dots, a_\delta)$.

We shall now inductively define a chain 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 $\mathfrak{q}_{i-1}$. This exists by Lemma 6.9 and so we have constructed our chain of prime ideals.

Note that we have by construction $\mathrm{ht}(\mathfrak{q}_i) = c - i$ (see after Corollary 11.15).

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 11.25, 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

$$\mathfrak{m} \cap R \supseteq \mathfrak{q}_i \cap R \supseteq \mathfrak{m} \cap R$$

so that $\mathfrak{q}_i \cap R = \mathfrak{m} \cap R$. We now conclude from Lemma 11.21 and Lemma 11.19 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. $\square$

Proof of Theorem 11.18.

Let $\mathfrak{m}$ be a maximal ideal of $R[x]$ so that $\mathrm{ht}(\mathfrak{m}) = \dim(R[x])$. This exists by Lemma 11.2. 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 a maximal ideal $\mathfrak{p}$ in R, so that $\mathrm{ht}(\mathfrak{p}) > \mathrm{ht}(\mathfrak{m} \cap R)$. Let $\mathfrak{n}$ be a maximal ideal of $R[x]$, which contains $\mathfrak{p}[x]$. By maximality, we have $\mathfrak{n} \cap R = \mathfrak{p}$, so that $\mathrm{ht}(\mathfrak{n}) = 1 + \mathrm{ht}(\mathfrak{p}) > 1 + \mathrm{ht}(\mathfrak{m} \cap R) = \mathrm{ht}(\mathfrak{m})$, 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 11.26, 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 11.27. *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 11.18 and Hilbert's basis theorem. □

Corollary 11.28. *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 11.29. *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. 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 8.8, there is a prime ideal $\mathfrak{q}_{\dim(R)}$ in T such that $\mathfrak{q}_{\dim(R)} \cap R = \mathfrak{p}_{\dim(R)}$ and 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. □

Proof of Corollary 11.28. 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 11.27, 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

12 Dedekind rings [NOT EXAMINABLE]

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, which are domains and are integrally closed. 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 12.1. *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.*

Note that the lemma, together with the Chinese remainder theorem, shows that if $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ are primary ideals with distinct radicals in a Dedekind domain, we have

$$\bigcap_i \mathfrak{q}_i = \prod_i \mathfrak{q}_i.$$

Proof. (of Lemma 12.1). (i) If $\mathfrak{p}$ is a non-zero prime ideal, then we have the chain $\mathfrak{p} \supsetneq (0)$ of prime ideals (note that (0) is a prime ideal since R is a domain). This chain is of maximal length, since R is of dimension one. Now let $\mathfrak{m} \supseteq \mathfrak{p}$ be a maximal ideal containing $\mathfrak{p}$. We must have $\mathfrak{m} = \mathfrak{p}$, otherwise

$$\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq (0)$$

would be a chain of prime ideals of length 2, which is impossible by the above.

(ii) Since $\mathfrak{r}(\mathfrak{q}_1) \neq \mathfrak{r}(\mathfrak{q}_2)$, the ideals $\mathfrak{r}(\mathfrak{q}_1)$ and $\mathfrak{r}(\mathfrak{q}_2)$ are coprime, since they are prime, and hence maximal by (i). Thus the conclusion follows from Lemma 12.2 below. □

Lemma 12.2. *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. Note that we have $\mathfrak{r}(I+J) \subseteq \mathfrak{r}(\mathfrak{r}(I) + \mathfrak{r}(J))$, since $I + J \subseteq \mathfrak{r}(I) + \mathfrak{r}(J)$. On the other hand, we also have $\mathfrak{r}(I) + \mathfrak{r}(J) \subseteq \mathfrak{r}(I+J)$, and thus we have $\mathfrak{r}(\mathfrak{r}(I) + \mathfrak{r}(J)) \subseteq \mathfrak{r}(\mathfrak{r}(I+J)) = \mathfrak{r}(I+J)$. So we have $\mathfrak{r}(I+J) = \mathfrak{r}(\mathfrak{r}(I) + \mathfrak{r}(J))$ (this equality holds without any assumptions on the ideals $\mathfrak{r}(I)$ and $\mathfrak{r}(J)$). In our situation, we have $\mathfrak{r}(I) + \mathfrak{r}(J) = (1)$, so that $\mathfrak{r}(I+J) = (1)$. In particular, $1 \in I + J$, so that $I + J = (1)$, as required. □

Lemma 12.3. *Let R be an integrally closed domain. Then $R_\mathfrak{p}$ is also integrally closed for all $\mathfrak{p} \in \mathrm{Spec}(R)$.*

Proof. Exercise. Use Lemma 8.7. □

Proposition 12.4. *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 11.12, 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 8.1 (because $\mathfrak{m}$ is finitely generated, as R is noetherian). We then have $P(x^{-1})(h) = 0$ 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): We first prove that I is a power of $\mathfrak{m}$. We may suppose without restriction of generality that $I \neq R$ (otherwise $I = \mathfrak{m}^0$). Suppose for contradiction that I is not a power of $\mathfrak{m}$. Let $b \in R$ be such that $\mathfrak{m} = (b)$. The ring R/I is Artinian (reason as at the beginning of the proof of the implication (1)⇒(2)) and thus the ideal $\mathfrak{m} \pmod{I}$ is nilpotent. Let $n > 0$ be the largest integer such that $I \subsetneq \mathfrak{m}^n$. This exists by assumption and because some power of $\mathfrak{m}$ is contained in I, since $\mathfrak{m} \pmod{I}$ is nilpotent. Let $a \in I$ be an element such that $a \notin \mathfrak{m}^{n+1}$ (this exists by construction). By construction, we may write $a = tb^n$ for some $t \in R$. We cannot have $t \in \mathfrak{m}$ because otherwise we would have $a \in \mathfrak{m}^{n+1}$, which is excluded. Hence t is a unit of R (since R is local) and thus $\mathfrak{m}^n = (t^{-1}a) = (a) \subseteq I$. This is a contradiction, so we must have $I = \mathfrak{m}^n$ for some $n > 0$.

Secondly, n is uniquely determined. Indeed, suppose that $(b^{n_1}) = (b^{n_2})$ for $n_1 \leq n_2$. Then there is a $u \in R$ such that $b^{n_1} = b^{n_2}u$. Since R is a domain, $b^{n_2-n_1}u = 1$, so b is a unit if $n_2 \neq n_1$. Since b is not a unit, we thus have $n_1 = n_2$.

(3)⇒(1): The R-module $\mathfrak{m}/\mathfrak{m}^2$ is not zero (if it were zero, the ideal $\mathfrak{m}$ would be zero by Corollary 3.6, which is not possible, since R has dimension 1). So we may choose an element $x \in \mathfrak{m} \backslash \mathfrak{m}^2$. By assumption (x) is equal to some power of $\mathfrak{m}$, which must be 1 by construction. Hence $\mathfrak{m} = (x)$. We conclude that R is a PID and thus a UFD. We saw in the solution to Q4 of sheet 2 that any UFD is integrally closed and thus R is integrally closed. □

Corollary 12.5. *The localisation of a Dedekind domain at a non zero prime ideal is a PID.*

The proof is immediate.

Corollary 12.6. *Let R be a Dedekind domain. Then any primary ideal is equal to a power of its radical.*

Proof. Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{a}$ be a $\mathfrak{p}$-primary ideal. Let $\lambda : R \to R_\mathfrak{p}$ be the natural homomorphism from R to its localisation at $\mathfrak{p}$. Let $\mathfrak{m} = \mathfrak{p}_\mathfrak{p}$ be the maximal ideal of $R_\mathfrak{p}$ (recall that this is also the ideal generated by $\lambda(\mathfrak{p})$).

We claim that $\lambda^{-1}(\mathfrak{a}_\mathfrak{p}) = \mathfrak{a}$. Indeed, consider the exact sequence

$$0 \to \mathfrak{a} \to \lambda^{-1}(\mathfrak{a}_\mathfrak{p}) \to \lambda^{-1}(\mathfrak{a}_\mathfrak{p})/\mathfrak{a} \to 0.$$

The localisation at $\mathfrak{p}$ of this sequence is

$$0 \to \mathfrak{a}_\mathfrak{p} \to (\lambda^{-1}(\mathfrak{a}_\mathfrak{p}))_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} \to (\lambda^{-1}(\mathfrak{a}_\mathfrak{p}))_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} = 0 \to 0$$

By Lemma 5.4, there is a natural isomorphism of $R_\mathfrak{p}$-modules

$$(\lambda^{-1}(\mathfrak{a}_\mathfrak{p})/\mathfrak{a})_\mathfrak{p} = (\lambda^{-1}(\mathfrak{a}_\mathfrak{p}))_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} = 0.$$

Now note that $\mathfrak{r}(\mathfrak{a}) = \mathfrak{p}$ by assumption and that for any element $a \in R\backslash\mathfrak{p}$, we have $(a, \mathfrak{p}) = (1)$, since $\mathfrak{p}$ is maximal by Lemma 12.1 (i). Hence, by Lemma 12.2, we have $(a, \mathfrak{a}) = (1)$ if $a \in R\backslash\mathfrak{p}$ and in that case the image of a in $R/\mathfrak{a}$ is a unit. Since $\lambda^{-1}(\mathfrak{a}_\mathfrak{p})/\mathfrak{a}$ is naturally an $R/\mathfrak{a}$-module, we conclude that $(\lambda^{-1}(\mathfrak{a}_\mathfrak{p})/\mathfrak{a})_\mathfrak{p} = \lambda^{-1}(\mathfrak{a}_\mathfrak{p})/\mathfrak{a}$ and we thus see that $\lambda^{-1}(\mathfrak{a}_\mathfrak{p})/\mathfrak{a} = 0$. In other words, $\lambda^{-1}(\mathfrak{a}_\mathfrak{p}) = \mathfrak{a}$, and the claim is proved.

Now notice that by Proposition 12.4 (3), we have $\mathfrak{a}_\mathfrak{p} = \mathfrak{m}^k = \mathfrak{p}_\mathfrak{p}^k$ for some $k \geq 1$. Also we have $\mathfrak{p}^k = \lambda^{-1}(\mathfrak{p}_\mathfrak{p}^k)$, since $\mathfrak{p}^k$ is also $\mathfrak{p}$-primary by Lemma 6.4. We conclude that

$$\mathfrak{a} = \lambda^{-1}(\mathfrak{a}_\mathfrak{p}) = \lambda^{-1}(\mathfrak{p}_\mathfrak{p}^k) = \mathfrak{p}^k$$

as required. □

Proposition 12.7. *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.*

Note that I has primary decompositions by the Lasker-Noether theorem, since R is noetherian.

Proof. Let $\bigcap_{i=1}^n \mathfrak{a}_i = I$ be a minimal primary decomposition of I. By Corollary 12.6, we have $\mathfrak{a}_i = \mathfrak{p}_i^{n_i}$ for some distinct prime ideals $\mathfrak{p}_i$ and some integers $n_i \geq 1$. Furthermore, we have

$$\bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i$$

(see after Lemma 12.1). We thus have to show that if $I = \prod_{j=1}^m \mathfrak{q}_j^{m_j}$ is another representation of I as a product of powers of distinct prime ideals, then we have $n = m$ and there is some bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ and $n_i = m_{\sigma(i)}$ for all $i \in \{1, \ldots, n\}$. So suppose that

$$\prod_{j=1}^m \mathfrak{q}_j^{m_j} = \prod_{i=1}^n \mathfrak{p}_i^{n_i} \quad (*)$$

where the $\mathfrak{q}_i$ (resp. the $\mathfrak{p}_i$) are distinct prime ideals. It will be sufficient to show that if some prime ideal appears with some multiplicity on the left of $(*)$ then it will appear with the same multiplicity on the right of $(*)$. So consider eg $\mathfrak{q}_1$. Localising $(*)$ at $\mathfrak{q}_1$, we obtain

$$\prod_{j=1}^m (\mathfrak{q}_{j,\mathfrak{q}_1})^{m_j} = \prod_{i=1}^n (\mathfrak{p}_{i,\mathfrak{q}_1})^{n_i}$$

Now note that if $\mathfrak{q}_j \neq \mathfrak{q}_1$, we have $\mathfrak{q}_{j,\mathfrak{q}_1} = (1) = R_{\mathfrak{q}_1}$, because $\mathfrak{q}_j \not\subseteq \mathfrak{q}_1$ (since $\mathfrak{q}_j$ is maximal). Similarly, if $\mathfrak{p}_i \neq \mathfrak{q}_1$, we have $\mathfrak{p}_{i,\mathfrak{q}_1} = (1)$. Hence we obtain the equality

$$(\mathfrak{q}_{1,\mathfrak{q}_1})^{m_1} = (\mathfrak{p}_{i_1,\mathfrak{q}_1})^{n_{i_1}}$$

for some $i_1 \in \{1, \ldots, n\}$ such that $\mathfrak{p}_{i_1} = \mathfrak{q}_1$. On the other hand $\mathfrak{q}_{1,\mathfrak{q}_1} = \mathfrak{p}_{i_1,\mathfrak{q}_1}$ is the maximal ideal of $R_{\mathfrak{q}_1}$ and every ideal in $R_{\mathfrak{q}_1}$ is a uniquely determined power of this maximal ideal by Proposition 12.4 (3). Hence $m_1 = n_{i_1}$. This concludes the proof. □

We conclude from Proposition 12.7 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 12.8. *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. □

Remark. The previous proposition is also true if R is a domain, which is finitely generated over a field (without the requirement that R is integrally closed) and $L|K$ is any finite extension of fields (in particular one could take $L = K$). This is a theorem of E. Noether. See D. Eisenbud, Commutative Algebra with a view toward algebraic geometry, par. 13.3, Cor. 13.13, p. 297. Note that if R is domain, it is in general difficult to show that the integral closure of R in its own fraction field is finite over R.

Corollary 12.9. *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 T is clearly a domain, and it is integrally closed by Lemma 8.6 and Proposition 12.8 (1). Also, the ring T is of dimension 1 by Lemma 11.29. 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 12.10. *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 6.1 (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. □

The following lemma (and the complement that follows) plays a key role in Algebraic Number Theory.

Lemma 12.11. *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 12.9). 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 6.1 (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). □

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 12.7 and Proposition 12.10 that the integers n_i and f_i are independent of i if $L|K$ is a Galois extension (why?).

END OF LECTURE 16

Exercise sheet 1. Prerequisites: sections 1-5. Week 4.

Part A

Q1. Let R be a ring. Show that the Jacobson radical of R coincides with the set $\{x \in R \mid 1 - xy \text{ is a unit for all } y \in R\}$.

Part B

Solution. Suppose x lies in the Jacobson radical of R. Suppose for contradiction that $1 - xy$ is not a unit for some $y \in R$. Let $\mathfrak{m}$ be a maximal ideal containing $1 - xy$. We know that $xy \in \mathfrak{m}$ since $x \in \mathfrak{m}$ and thus we conclude that $1 \in \mathfrak{m}$, a contradiction.

Suppose now that $x \in R$ and that $1 - xy$ is a unit for all $y \in R$. Suppose for contradiction that there is a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$. Then $x \pmod{\mathfrak{m}}$ is a unit in $R/\mathfrak{m}$ and hence there is a $y \in R$ such that $xy \pmod{\mathfrak{m}} = 1 \pmod{\mathfrak{m}}$. In other words, $1 - xy \in \mathfrak{m}$ and so $1 - xy$ is not a unit.

Q2. Let R be a ring.

(i) Show that if $P(x) = a_0 + a_1 x + \cdots + a_k x^k \in R[x]$ is a unit of $R[x]$ then a_0 is a unit of R and a_i is nilpotent for all $i \geq 1$.

(ii) Show that the Jacobson radical and the nilradical of $R[x]$ coincide.

Solution.

(i) Let $Q(x) = b_0 + \cdots + b_t x^t \in R[x]$ be an inverse of $P(x)$. Then $P(0)Q(0) = a_0 b_0 = 1$ so that a_0 and b_0 are units. Let $\mathfrak{p}$ be a prime ideal. Let $j \geq 0$ be the largest integer so that $a_j \pmod{\mathfrak{p}} \neq 0$ and let $l \geq 0$ be the largest integer so that $b_l \pmod{\mathfrak{p}} \neq 0$. If $j > 0$ we have $a_j b_l = 0 \pmod{\mathfrak{p}}$ (since $P(x)Q(x) = 1$), which is not possible because $R/\mathfrak{p}$ is a domain. Hence $j = 0$ and in particular $a_i \in \mathfrak{p}$ for all $i > 0$. Since $\mathfrak{p}$ was arbitrary, we see that a_i lies in the nilradical of R for all $i > 0$.

(ii): We only have to show that any element of the Jacobson radical if $R[x]$ is nilpotent. So let $P(x) \in a_0 + a_1 x + \cdots + a_k x^k \in R[x]$ be an element of the Jacobson radical. By Q1, we know that for any $T(x) \in R[x]$, the element $1 - P(x)T(x)$ is a unit. In particular,

$$1 + xP(x) = 1 + a_0 x + a_1 x^2 + \cdots + a_k x^{k+1}$$

is a unit. By (i), a_i is thus nilpotent for all $i > 0$. In particular $a_0 + a_1 x + \cdots + a_k x^k$ is nilpotent (since the radical of a ring is an ideal).

Q3. Let R be a ring and let $N \subseteq R$ be its nilradical. Show that the following are equivalent:

(i) R has exactly one prime ideal.

(ii) Every element of R is either a unit or is nilpotent.

(iii) R/N is a field.

Solution. (i)⇒(ii): Let $\mathfrak{p}$ be the unique prime ideal. Suppose that $r \in R$ is not a unit. Then r is a contained in a maximal ideal, which must coincide with $\mathfrak{p}$. Since $\mathfrak{p}$ is the only prime ideal, the ideal $\mathfrak{p}$ is the nilradical N of R and hence r is nilpotent.

(ii)⇒(iii): Suppose that R/N is not a field. Then either R/N is the zero ring or there is an element $x \in (R/N)^*$, which is not a unit. If R/N is the zero ring, then every element of R is nilpotent (and in fact R is the zero ring). If there is an element $x \in (R/N)^*$, let $x_1 \in R$ be a preimage of x. Then x_1 is not a unit and is not nilpotent. So we have proven the contraposition of (ii)⇒(iii).

(iii)⇒(i): We prove the contraposition. If R has more than one prime ideal then R/N has a non zero prime ideal (since any prime ideal contains N). But this contradicts the fact that R/N is a field.

Q4. Let R be a ring and let $I \subseteq R$ be an ideal. Let $S := \{1 + r \,|\, r \in I\}$.

(i) Show that S is a multiplicative set.

(ii) Show that the ideal generated by the image of I in R_S is contained in the Jacobson radical of R_S.

(iii) Prove the following generalisation of Nakayama's lemma:

Lemma. *Let M be a finitely generated R-module and suppose that $IM = M$. Then there exists $r \in R$, such that $r - 1 \in I$ and such $rM = 0$.*

Solution. (i): This is clear.

(ii): The ideal I_S generated generated by I in R_S consists of the elements a/b such that $a \in I$ and $b \in S$. By Q1, we thus only have to show that if a/b is such that $a \in I$ and $b \in S$, then $1 - (a/b)(c/d)$ is a unit for all $c \in R$ and $d \in S$. Now $1/b$ and $1/d$ are units of R_S, hence we only have to show that $bd - ac$ is a unit for a, b, c, d as in the previous sentence. Now $bd = (1 + b_1)(1 + d_1) = 1 + b_1 + d_1 + b_1 d_1$ for some $b_1, d_1 \in I$, and thus $bd - ac = 1 + b_1 + d_1 + b_1 d_1 - ac$. Since $b_1 + d_1 + b_1 d_1 - ac \in I$ we see that $bd - ac = 1 + b_1 + d_1 + b_1 d_1 - ac \in S$ and hence is a unit of R_S.

(iii) If $IM = M$ we clearly have $I_S M_S = M_S$. Hence by (ii) and the form of Nakayama's lemma proven in the course, we have $M_S = 0$. Now $m_1, \ldots, m_k$ be generators of M. Since M is the kernel of the natural map $M \to M_S$ (since $M_S = 0$), there is an element $s_i \in S$ such that $s_i m_i = 0$ for all i (see the beginning of section 5). Let $s = \prod_i s_i$. Then s annihilates all the m_i and hence M. By construction, $s - 1 \in I$ so we are done.

Q5. Let R be a ring and let M be a finitely generated R-module. Let $\phi : M \to M$ be a surjective homomorphism of R-modules. Prove that ϕ is injective, and is thus an automorphism. [Hint: use ϕ to construct a structure of $R[x]$-module on M and use the previous question.]

Solution. View M as an $R[x]$-module by setting $P(x) \cdot m = P(\phi)(m)$. We have $(x)M = M$ by construction and hence by Q4 (iii), there is a polynomial $Q(x) \in R[x]$ such that $Q(x) - 1 \in (x)$ and $Q(x)M = 0$. Let $m_0 \in \ker(\phi)$. Then $Q(x)(m_0) = m_0$ and hence $m_0 = 0$. Thus ϕ is injective.

Q6. Let R be a ring. Let $\mathcal{S}$ be the subset of the set of ideals of R defined as follows: an ideal I is in $\mathcal{S}$ iff all the elements of I are zero-divisors. Show that $\mathcal{S}$ has maximal elements (for the relation of inclusion) and that every maximal element is a prime ideal. Show that the set of zero divisors of R is a union of prime ideals.

Solution. If $\mathcal{T}$ is a totally ordered subset of $\mathcal{S}$, then the union of its elements is an ideal, and it clearly consists of zero divisors. So every totally ordered subset of $\mathcal{T}$ has upper bounds and thus by Zorn's lemma, the ordered set $\mathcal{T}$ has maximal elements. Note that we may refine this reasoning as follows. Let $I \in \mathcal{S}$. Consider the subset $\mathcal{S}_I$ of $\mathcal{S}$, which consists of ideals containing I. By a completely similar reasoning, the subset $\mathcal{S}_I$ has maximal elements for the relation of inclusion. We contend that if $J \in \mathcal{S}_I$ is a maximal element, then it is also maximal in $\mathcal{S}$. Indeed, suppose that $J' \supseteq J$ for some ideal $J' \in \mathcal{S}$. Then $J' \in \mathcal{S}_I$ and hence $J' = J$. Now note that

$$\{\text{zero-divisors of } R\} = \cup_{r \in R,\, r \text{ a zero-div.}}(r) \subseteq \cup_{r \in R,\, r \text{ a zero-div.}} J(r)$$

where $J(r)$ a maximal element of $\mathcal{S}$ containing the ideal (r). Since $J(r)$ also consists of zero-divisors, we

conclude that

$$\{\text{zero-divisors of } R\} = \cup_{r\in R,\, r \text{ a zero-div.}} J(r)$$

Hence we only have to prove that the maximal elements of $\mathcal{S}$ are prime ideals.

Let I be a maximal element of $\mathcal{S}$. Let $x, y \in R\backslash I$ and suppose for contradiction that $xy \in I$. Then we have

$$((x) + I)((y) + I) \subseteq I$$

By maximality of I, there are elements $a \in (x)+I$ and $b \in (y)+I$, which are not zero divisors. Hence $ab \in I$ so that ab is a zero divisor, which is contradiction (note that the set of non zero divisors is a multiplicative set). So we must have $x \in I$ or $y \in I$, so I is prime.

Part C

Q7. (optional) Let R be a ring. Consider the inclusion relation on the set $\mathrm{Spec}(R)$. Show that there are minimal elements in $\mathrm{Spec}(R)$.

Solution. Let $\mathcal{T}$ be a totally ordered subset of $\mathrm{Spec}(R)$ for the relation $\supseteq$. Note that the maximal elements for the relation $\supseteq$ are the minimal elements for the inclusion relation (which is $\subseteq$). Let $I := \cap_{\mathfrak{p}\in\mathcal{T}}$. Then I is an ideal. We claim that I is prime.

To see this, let $x, y \in R$ and suppose for contradiction that $x, y \in R\backslash I$ and that $xy \in I$. By assumption there are prime ideals $\mathfrak{p}_x, \mathfrak{p}_y \in \mathcal{T}$ such that $x \notin \mathfrak{p}_x$ and $y \notin \mathfrak{p}_y$. Suppose without restriction of generality that $\mathfrak{p}_x \supseteq \mathfrak{p}_y$ (recall that $\mathcal{T}$ is totally ordered). We have $xy \in \mathfrak{p}_y$ and thus either x or y lies in $\mathfrak{p}_y$. This contradicts the fact that $x, y \notin \mathfrak{p}_y$. The ideal I thus lies in $\mathrm{Spec}(R)$ and it is a lower bound for $\mathcal{T}$. We may thus apply Zorn's lemma to conclude that there are minimal elements in $\mathrm{Spec}(R)$.

Exercise sheet 2. Prerequisites: sections 1-8. Week 6

Part A

Q1. Consider the ideals $\mathfrak{p}_1 := (x, y)$, $\mathfrak{p}_2 := (x, z)$ and $\mathfrak{m} := (x, y, z)$ of $K[x, y, z]$, where K is a field. Show that $\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a minimal primary decomposition of $\mathfrak{p}_1 \cdot \mathfrak{p}_2$. Determine the isolated and the embedded prime ideals of $\mathfrak{p}_1 \cdot \mathfrak{p}_2$.

Solution. For future reference, note that we have

$$\mathfrak{m}^2 = ((x) + (y) + (z))^2 = (x^2, y^2, z^2, xy, xz, yz)$$

and

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 = ((x) + (y))((x) + (z)) = (x^2, xz, yx, yz).$$

We have $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2$ and we also clearly have $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{m}^2$ since $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathfrak{m}$. Thus we have $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$. Note that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime since the rings $K[x, y, z]/\mathfrak{p}_1 \simeq K[z]$ and $K[x, y, z]/\mathfrak{p}_2 \simeq K[y]$ are domains. Note also that $\mathfrak{m}$ is a maximal ideal, since $K[x, y, z]/\mathfrak{m} \simeq K$ is a field. Thus $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}^2$ are primary (see after Lemma 6.4 for the latter). The radicals of the ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}^2$ are $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}$ (see again Lemma 6.4 for the latter). These three ideals are distinct. Finally, we have $\mathfrak{p}_1 \not\supseteq \mathfrak{p}_2 \cap \mathfrak{m}^2$ (because $z^2 \notin \mathfrak{p}_1$ but $z^2 \in \mathfrak{p}_2 \cap \mathfrak{m}^2$), $\mathfrak{p}_2 \not\supseteq \mathfrak{p}_1 \cap \mathfrak{m}^2$ (because $y^2 \notin \mathfrak{p}_2$ but $y^2 \in \mathfrak{p}_1 \cap \mathfrak{m}^2$) and $\mathfrak{m}^2 \not\supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2$ (because $x \notin \mathfrak{m}^2$ but $x \in \mathfrak{p}_2 \cap \mathfrak{p}_2$). Hence if $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ then this decomposition is indeed primary and minimal. Thus we only have to show that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$. From the above, we have to show that

$$(x, y) \cap (x, z) \cap (x^2, y^2, z^2, xy, xz, yz) \subseteq (x^2, xz, yx, yz)$$

Now note that we have $P(x, y, z) \in (x, y)$ iff $P(0, 0, z) = 0$ (because a polynomial lies in (x, y) iff it has no monomial containing only the variable z). Similarly, we have $P(x, y, z) \in (x, z)$ iff $P(0, y, 0) = 0$. Thus we have $P(x, y, z) \in (x, y) \cap (x, z)$ iff $P(0, y, 0) = P(0, 0, z) = 0$.

Now an element $Q(x, y, z)$ of $(x^2, y^2, z^2, xy, xz, yz)$ has the form

$$Q(x, y, z) = P_1(x, y, z)x^2 + P_2(x, y, z)y^2 + P_3(x, y, z)z^2 + P_4(x, y, z)xy + P_5(x, y, z)xz + P_6(x, y, z)yz.$$

and $Q(x, y, z)$ will thus lie in $(x, y) \cap (x, z)$ iff

$$Q(0, y, 0) = Q(0, 0, z) = P_2(0, y, 0) = P_3(0, 0, z) = 0.$$

In other words, the element $Q(x, y, z) \in (x^2, y^2, z^2, xy, xz, yz) = \mathfrak{m}^2$ will lie in $(x, y) \cap (x, z)$ iff $P_2(x, y, z) \in (x, z)$ and $P_3(x, y, z) \in (x, y)$. Consequently, if $Q(x, y, z) \in \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ then

$$Q(x, y, z) \in (x^2)+(x, z)(y^2)+(x, y)(z^2)+(xy)+(xz)+(yz) = (x^2, xy^2, zy^2, xz^2, yz^2, xy, xz, yz) = (x^2, xy, xz, yz) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

as required.

The prime ideals associated with the decomposition are $\mathfrak{p}_1 = \mathfrak{r}(\mathfrak{p}_1)$, $\mathfrak{p}_2 = \mathfrak{r}(\mathfrak{p}_2)$ and $\mathfrak{m} = \mathfrak{r}(\mathfrak{m}^2)$. The ideal $\mathfrak{m}$ contains $\mathfrak{p}_1$ and $\mathfrak{p}_2$ and there are no other inclusions between the prime ideals. So $\mathfrak{m}$ is an embedded ideal and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are isolated ideals.

Part B

Q2. Let K be a field. Show that the ideal $(x^2, xy, y^2) \subseteq K[x, y]$ is a primary ideal, which is not irreducible.

Solution. We first show that (x^2, xy, y^2) is primary. This simply follows from the fact that (x, y) is maximal ideal and from the fact that $(x^2, xy, y^2) = (x, y)^2$ (see after Lemma 6.4).

Now note that $(x^2, xy, y^2) = (x^2, y) \cap (x, y^2)$. Indeed, we clearly have $(x^2, xy, y^2) \subseteq (x^2, y) \cap (x, y^2)$. On the other hand, if $P(x, y) \in (x^2, y)$ then $P(x, y)$ has the form $P_1(x, y)x^2 + P_2(x, y)y$. Since $P_1(x, y)x^2$ is already in (x^2, xy, y^2), we thus only have to show that a polynomial of the form $P_2(x, y)y$, which lies in (x, y^2), necessarily lies in (x^2, xy, y^2). A polynomial in (x, y^2) is of the form $Q_1(x, y)y^2 + Q_2(x, y)x$. Now if we have $P_2(x, y)y = Q_1(x, y)y^2 + Q_2(x, y)x$ then $Q_2(x, y)$ is divisible by y and hence $Q_2(x, y)x = Q_2'(x, y)xy$ for some polynomial $Q_2'(x, y)$ so that $P_2(x, y)y \in (y^2, xy) \subseteq (x^2, xy, y^2)$, as required.

Q3. Let R be a noetherian ring and let T be a finitely generated R-algebra. Let G be a finite subgroup of the group of automorphisms of T as a R-algebra. Let T^G be the fixed point set of G (ie the subset of T, which is fixed by all the elements of G).

- Show that T is integral over T^G.

- Show that T^G is a subring of T, which contains the image of R and that T^G is finitely generated over R.

Solution. It is clear from the definitions that T^G is a subring which contains the image of R. Let $t \in T$. Then t satisfies the polynomial equation

$$\prod_{g \in G} (t - g(t)) = 0$$

The polynomial $M_t(x) := \prod_{g \in G}(x - g(t))$ has coefficients in T^G, because the coefficients are symmetric functions in the $g(t)$, which are invariant under G. Hence t is integral over T^G. Since t was arbitrary, T is integral over T^G. Since T is also finitely generated as a T^G-algebra (because it is finitely generated as a R-algebra), we thus see that T is finite over T^G (see after Lemma 6.6). Hence T^G is finitely generated over R by the Theorem of Artin-Tate.

Q4. Show that $\mathbb{Z}$ is integrally closed and that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

Solution. We first prove that $\mathbb{Z}$ is integrally closed. Let $p/q \in \mathbb{Q}$, where p and q are coprime integers, and let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be a monic polynomial. Suppose that $P(p/q) = 0$. Then we have

$$q^n P(p/q) = p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_0 q^n = 0.$$

Since $a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_0 q^n$ is divisible by q and p^n is coprime to q, this implies that $q = \pm 1$, so $p/q \in \mathbb{Z}$.

To prove that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$, note first that $\mathbb{Z}[i]$ is part of the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$. Indeed we have $(a + ib)^2 - 2a(a + ib) + a^2 + b^2 = 0$ for any $a, b \in \mathbb{Z}$. So we only have to prove that $\mathbb{Z}[i]$ is integrally closed in $\mathbb{Q}(i)$ (see Lemma 8.6). Note furthermore that $\mathbb{Q}(i)$ is the fraction field of $\mathbb{Z}[i]$. To see this, write let $r + it \in \mathbb{Q}(i)$, where $r, t \in \mathbb{Q}$ (any element of $\mathbb{Q}(i)$ can be written in this form because $\mathbb{Q}(i) \simeq \mathbb{Q}[x]/(x^2 + 1)$). Let $r = p/q$ and $t = u/v$. We then have $r + it = (vp + uqi)/(vq)$, which is a fraction of elements of $\mathbb{Z}[i]$, proving our claim. Finally, recall that we know from Rings and Modules that $\mathbb{Z}[i]$ is a Euclidean domain, where the Euclidean function is given by the norm (the norm of $c + id$ is $c^2 + d^2$ if $c + id \in \mathbb{Z}[i]$). In particular, $\mathbb{Z}[i]$ is a PID and every ideal in $\mathbb{Z}[i]$ is generated by an element of smallest norm.

To prove that $\mathbb{Z}[i]$ is integrally closed in $\mathbb{Q}(i)$, we may now proceed as for $\mathbb{Z}$. Let

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[i](x)$$

and let $r+it = B/A$, where $A, B \in \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, it is factorial and we may thus assume that $(A, B) = \mathbb{Z}[i]$. We can now write as before

$$A^n P(B/A) = B^n + a_{n-1}B^{n-1}A + a_{n-2}B^{n-2}A^2 + \cdots + a_0 A^n = 0.$$

Since $a_{n-1}B^{n-1}A + a_{n-2}B^{n-2}A^2 + \cdots + a_0 A^n$ is divisible by A and B^n is coprime to A, this implies that A is a unit, so $B/A \in \mathbb{Z}[i]$.

Note that the proof above actually shows that any UFD (Unique Factorisation Domain) is integrally closed.

Q5. Let S be a ring and let $R \subseteq S$ be a subring of S. Suppose that R is integrally closed in S. Let $P(x) \in R[x]$ and suppose that $P(x) = Q(x)J(x)$, where $Q(x), J(x) \in S[x]$ and $Q(x)$ and $J(x)$ are monic. Show that $Q(x), J(x) \in R[x]$. Use this to give a new proof of the fact that if $T(x) \in \mathbb{Z}[x]$ and $T(x) = T_1(x)T_2(x)$, where $T_1(x), T_2(x) \in \mathbb{Q}[x]$ are monic polynomials, then $T_1(x), T_2(x) \in \mathbb{Z}[x]$.

Solution. We first prove the

Lemma. Let A be a ring and let $U(x) \in A[x]$ be a non zero monic polynomial. Then there exists a ring B containing A, which is integral over A and such that

$$U(x) = \prod_{i=1}^{\deg(U)} (x - b_i)$$

for some $b_i \in B$, where we set $\prod_{i=1}^{\deg(U)}(x-b_i) = 1$ if $\deg(U) = 0$.

Proof of the lemma. By induction on the degree $d = \deg(U)$ of $U(x)$. If $d = 0, 1$, there is nothing to prove. So suppose that $d > 1$ and that the result holds for any smaller value of d. The ring $C := A[y]/(U(y))$ is integral over A by Proposition 8.2. The element y of C satisfies the equation $U(y) = 0$ by construction. By Euclidean division (see Preamble), we thus have $U(x) = (x-y)Z(x)$ for some $Z(x) \in C[x]$. Since $Z(x)$ has degree $< d$, we may apply the inductive hypothesis and we obtain a ring B, which contains C and where $Z(x)$ splits. The polynomial $U(x)$ also splits in B, so we are done. □

We now apply the lemma to $Q(x)$ and $J(x)$ successively and we obtain a ring B, which contains S, such that B is integral over S and such that

$$Q(x) = \prod_{i=1}^{\deg(Q)} (x - b_i)$$

and

$$J(x) = \prod_{i=1}^{\deg(J)} (x - c_i)$$

where $b_i, c_i \in B$. Now we have $P(b_i) = P(c_i) = 0$ by construction, so the b_i and c_i are actually integral over R. Since the integral closure of R in B is a subring, we conclude that the coefficients of $Q(x)$ and $J(x)$ are integral over R (and in S, by assumption). But since R is integrally closed in S, this means that these coefficients lie in R.

Note that we did not actually use the fact that B was integral over S in the proof.

Q6. Let R be a subring of a ring T and suppose that T is integral over R. Let $\mathfrak{p}$ be prime ideal of R and let $\mathfrak{q}$ be a prime ideal of T. Suppose that $\mathfrak{q} \cap R = \mathfrak{p}$. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_k$ be primes ideal of R and suppose that $\mathfrak{p}_1 = \mathfrak{p}$. Show that there are prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_k$ of T such that $\mathfrak{q}_1 = \mathfrak{q}$ and such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $i \in \{1, \ldots, k\}$.

Solution. By induction on k, we only need to treat the case $k = 2$. Consider the extension of rings $R/\mathfrak{p} \subseteq T/\mathfrak{q}$. This is also an integral extension. Furthermore, there is a unique prime ideal $\mathfrak{p}_2'$ in $R/\mathfrak{p}$, which corresponds to $\mathfrak{p}_2$ via the quotient map. By Theorem 8.8, there is a prime ideal $\mathfrak{q}_2'$ in $T/\mathfrak{q}$, which is such that $\mathfrak{q}_2' \cap R/\mathfrak{p} = \mathfrak{p}_2'$. The prime ideal $\mathfrak{q}_2$ corresponding to $\mathfrak{q}_2'$ via the quotient map has the required properties.

Q7. Let R be a ring. Let $\mathcal{S}$ be the set of ideals in R, which are not finitely generated.

(i) Let I be maximal element of $\mathcal{S}$ (with respect to the relation of inclusion). Show that I is prime.

(ii) Suppose that all the prime ideals of R are finitely generated. Prove that R is noetherian.

[Hint: exploit the fact that R/I is noetherian.]

Solution.

(i): Let $x, y \notin I$ and suppose for contradiction that $xy \in I$. Let $I_x := (x) + I$ and $I_y = (y) + I$. Write $J := I_x \cdot I_y$. By assumption I_x, I_y and hence J are finitely generated, and we have $J \subseteq I$. Consider the image $I \pmod J$ of I in the R/I_y-module I_x/J. Note that I_x/J is finitely generated as a R/I_y-module since I_x is finitely generated as a R-module. Note also that the ring R/I_y is noetherian, since every ideal of R/I_y is the image of either the zero ideal or of an ideal of R strictly containing I. Hence $I \pmod J$ is also finitely generated as a R/I_y-module by Lemma 7.4. Let $m_1, \ldots, m_k$ be preimages in I of a finite set of generators of $I \pmod J$ as a R/I_y-module and let $y_1, \ldots, y_l$ be generators of J. Then $m_1, \ldots, m_k, y_1, \ldots, y_l$ is a finite set of generators of I, which is a contradiction.

(ii): If $\mathcal{T}$ is a totally ordered subset of $\mathcal{S}$ then the ideal $J := \cup_{H \in \mathcal{S}} H$ also lies in $\mathcal{S}$ (because if J were finitely generated then a finite set of generators of J would lie in one of the ideals in $\mathcal{T}$, and thus generate it, which is a contradiction). The ideal J is an upper bound for $\mathcal{T}$ and thus we may apply Zorn's lemma to conclude that there are maximal elements in $\mathcal{S}$, if $\mathcal{S}$ is not empty. By definition, $\mathcal{S}$ is empty iff R is noetherian. Hence, by (i), if R is not noetherian, there is a prime ideal, which is not finitely generated. The contraposition of this implication gives (i).

Part C

Q8. (optional). Let R be a ring. Let $\mathcal{S}$ be the set of non-principal ideals in R. Let I be a maximal element of $\mathcal{S}$. Prove that I is a prime ideal.

Solution.

Let $x, y \notin I$ and suppose for contradiction that $xy \in I$. Let $I_x := (x) + I$. By assumption, we have $I_x = (g_x)$ for some $g_x \in R$. Let $\phi : R \to I_x$ be the surjection of R-modules given by the formula $\phi(r) = rg_x$. We then have $I \subseteq \phi^{-1}(I)$.

Suppose first that $I = \phi^{-1}(I)$. In other words, for all $r \in R$, we have $rg_x \in I$ iff $r \in I$. This contradicts the fact that $yg_x \in I$. So we conclude that $I \subsetneq \phi^{-1}(I)$. From the definition of I, we then see that $\phi^{-1}(I)$ is a principal ideal of R, and hence so is $I = \phi(\phi^{-1}(I))$. This is a contradiction, so we cannot have $xy \in I$ if $x, y \notin I$. In other words, I is prime.

Exercise sheet 3. Prerequisites: sections 1-10. Week 8

Part A

Q1. Let R be a subring of a ring T. Suppose that T is integral over R. Let $\mathfrak{p}$ be a prime ideal of R and let $\mathfrak{q}_1, \mathfrak{q}_2$ be prime ideals of T such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R = \mathfrak{p}$ and $\mathfrak{q}_1 \neq \mathfrak{q}_2$. Show that we have $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2 \not\subseteq \mathfrak{q}_1$.

Solution. By symmetry, we only have to show that $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$. Suppose for contradiction that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$. The ring $R/\mathfrak{p}$ is can be viewed as a subring of $T/\mathfrak{q}_1$ and by assumption we have $\mathfrak{q}_2 \pmod{\mathfrak{q}_1} \cap R/\mathfrak{p} = (0)$. We may thus assume wrog that R and T to be domains and that $\mathfrak{q}_1$ and $\mathfrak{p}$ are zero ideals. Now let $e \in \mathfrak{q}_2 \backslash \{0\}$ and let $P(x) \in R[x]$ be a non zero monic polynomial such that $P(e) = 0$. Since T is a domain, we may assume that the constant coefficient of $P(x)$ is non zero (otherwise replace $P(x)$ by $P(x)/x^k$ for a suitable $k \geq 1$). But then $P(0)$ is a linear combination of positive powers of e (since $P(e) = 0$), so $P(0) \in R \cap \mathfrak{q}_2 = (0)$. This is a contradiction, since $P(0) \neq 0$.

Part B

Q2. Let R be a ring. Show that the two following conditions are equivalent:

(i) R is a Jacobson ring.

(ii) If $\mathfrak{p} \in \mathrm{Spec}(R)$ and $R/\mathfrak{p}$ contains an element b such that $(R/\mathfrak{p})[b^{-1}]$ is a field, then $R/\mathfrak{p}$ is a field.

Here we write $(R/\mathfrak{p})[b^{-1}]$ for the localisation of $R/\mathfrak{p}$ at the multiplicative subset $1, b, b^2, \ldots$.

Solution.

(i) $\Rightarrow$ (ii) : If R is a Jacobson, then so is $R/\mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$. Hence (ii) follows from Lemma 10.2.

(ii) $\Rightarrow$ (i) : Note first that R is a Jacobson ring iff any prime ideal of R is the intersection of the maximal ideals containing it (this is straightforward). Now suppose that R is not Jacobson. Then there is a prime ideal $\mathfrak{p}$ of R and an element $e \notin \mathfrak{p}$ such that e is in the Jacobson radical of $\mathfrak{p}$. In other words, $e \pmod{\mathfrak{p}} \neq 0$ and $e \pmod{\mathfrak{p}}$ lies in the Jacobson radical of $R/\mathfrak{p}$. Now let $\mathfrak{q}$ be an ideal maximal among the prime ideals of $R/\mathfrak{p}$, which do not contain $e \pmod{\mathfrak{p}}$. The ideal $\mathfrak{q}$ is prime, because it corresponds to a maximal ideal of $(R/\mathfrak{p})[(e \pmod{\mathfrak{p}})^{-1}]$ by Lemma 5.6, and it is not maximal, since $e \pmod{\mathfrak{p}}$ lies in the intersection of all the maximal ideals of $R/\mathfrak{p}$. The ring $(R/\mathfrak{p})/\mathfrak{q}$ has by construction the property that any of its non zero prime ideals contains $(e \pmod{\mathfrak{p}}) \pmod{\mathfrak{q}}$. In particular, the ring $((R/\mathfrak{p})/\mathfrak{q})[((e \pmod{\mathfrak{p}}) \pmod{\mathfrak{q}})^{-1}]$ is a field, because it is a domain and its only prime ideal is the zero ideal. On other hand, $((R/\mathfrak{p})/\mathfrak{q})$ is a not field, since $\mathfrak{q}$ is not maximal. Now if we let $q : R \to R/\mathfrak{p}$ be the quotient map, we have $((R/\mathfrak{p})/\mathfrak{q}) \simeq R/q^{-1}(\mathfrak{q})$ and thus this contradicts (ii). We have thus proven the contraposition of the implication (ii) $\Rightarrow$ (i).

Q3. Let k be field and let R be a finitely generated algebra over k. Show that the two following conditions are equivalent:

(i) $\mathrm{Spec}(R)$ is finite.

(ii) R is finite over k.

Solution. (i) $\Rightarrow$ (ii) : Suppose that $\mathrm{Spec}(R)$ is finite. By Noether's normalisation lemma, there is an injection $k[x_1, \ldots, x_d] \to R$, which makes R into a finite $k[x_1, \ldots, x_d]$-algebra. Since the corresponding map of spectra $\mathrm{Spec}(R) \to \mathrm{Spec}(k[x_1, \ldots, x_d])$ is surjective by Theorem 8.8, this implies that $\mathrm{Spec}(k[x_1, \ldots, x_d])$ is finite. In particular, $k[x_1, \ldots, x_d]$ has only finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$. Since $k[x_1, \ldots, x_d]$

is a Jacobson ring by Theorem 10.5, we have $\cap_i \mathfrak{m}_i = \mathfrak{r}((0)) = 0$ and so we may deduce from the Chinese remainder theorem that $k[x_1, \ldots, x_d] \simeq \oplus_i R/\mathfrak{m}_i$. Since $k[x_1, \ldots, x_d]$ is a domain, this implies that $t = 1$. In particular, $k[x_1, \ldots, x_d]$ is field, which is only possible if $d = 0$ (otherwise, x_1 is a non unit). Hence R is finite over k.

(ii) $\Rightarrow$ (i) : This follows from Proposition 8.12.

Q4. Let k be an algebraically closed field. Let $P_1, \ldots, P_d \in k[x_1, \ldots, x_d]$. Suppose that the set

$$\{(y_1, \ldots, y_d) \in k^d \,|\, P_i(y_1, \ldots, y_d) = 0 \, \forall i \in \{1, \ldots, d\}\}$$

is finite. Show that

$$\mathrm{Spec}(k[x_1, \ldots, x_d]/(P_1, \ldots, P_d))$$

is finite.

Solution. From Corollary 9.5 and Corollary 9.3, we deduce that $\mathfrak{r}((P_1, \ldots, P_d))$ is the intersection of finitely many maximal ideals of $k[x_1, \ldots, x_d]$, say $\mathfrak{m}_1, \ldots \mathfrak{m}_t$. From the Chinese remainder theorem, we deduce that

$$k[x_1, \ldots, x_d]/\mathfrak{r}((P_1, \ldots, P_d)) \simeq \prod_i k[x_1, \ldots, x_d]/\mathfrak{m}_i \simeq \prod_i k,$$

In particular, $\mathrm{Spec}(k[x_1, \ldots, x_d]/\mathfrak{r}((P_1, \ldots, P_d)))$ is finite. Now we have

$$\mathrm{Spec}(k[x_1, \ldots, x_d]/\mathfrak{r}((P_1, \ldots, P_d))) \simeq \mathrm{Spec}(k[x_1, \ldots, x_d]/(P_1, \ldots, P_d))$$

(see the remark after Lemma 4.4) so the conclusion follows.

Q5. Let R be a ring and let R_0 be the prime ring of R (see the preamble of the notes for the definition). Suppose that R is a finitely generated R_0-algebra. Suppose also that R is a field. Prove that R is a finite field.

Solution. Since R_0 is contained in a field, it is a domain and so R_0 is either a finite field or it is isomorphic to $\mathbb{Z}$. Suppose first that R_0 is a finite field. Then R is a finite field extension of a finite field by the weak Nullstellensatz and hence R is a finite field. Now suppose that $R \simeq \mathbb{Z}$. Then R contains the fraction field $\mathbb{Q}$ of $\mathbb{Z}$ and R is a finitely generated $\mathbb{Q}$-algebra, which is a field. By the weak Nullstellensatz again, we conclude that R is a finite field extension of $\mathbb{Q}$. From Corollary 10.3, we deduce that $\mathbb{Z} \simeq \mathbb{Q}$ (note that $\mathbb{Z}$ is a Jacobson ring), which is a contradiction. So R_0 must be a finite field and so R is a finite field.

Q6. Let k be a field and let $\mathfrak{m}$ be a maximal ideal of $k[x_1, \ldots, x_d]$. Show that there are polynomials $P_1(x_1), P_2(x_1, x_2), P_3(x_1, x_2, x_3), \ldots, P_d(x_1, \ldots, x_d)$ such that $\mathfrak{m} = (P_1, \ldots, P_d)$.

Solution. By induction on $d \geq 1$. If $d = 1$ then this follows from the fact that $k[x_1]$ is a PID. We suppose that the statement holds for $d - 1$. Let $K = k[x_1, \ldots, x_d]/\mathfrak{m}$. By the weak Nullstellensatz, this is a finite field extension of k. Let $\phi : k[x_1, \ldots, x_d] \to K$ be the natural surjective homomorphism of k-algebras. Let $L = \phi(k[x_1, \ldots, x_{d-1}])$. This is a domain and by Lemma 8.9, L is a field, since it contains k and is contained inside an integral extension of k. Let $\psi : k[x_1, \ldots, x_{d-1}] \to L$ be the surjective homomorphism of k-algebras arising by restricting ϕ. The map ψ induces a surjective homomorphism of k-algebras

$$\Psi : k[x_1, \ldots, x_d] \simeq (k[x_1, \ldots, x_{d-1}])[x_d] \to L[x_d]$$

and there is a surjective homomorphism of L-algebras

$$\Lambda : L[x_d] \to K,$$

which sends x_d to $\phi(x_d)$. By construction, we have $\phi = \Lambda \circ \Psi$. In particular, we have $\mathfrak{m} := \Psi^{-1}(\Lambda^{-1}(0))$. Since $L[x_d]$ is a PID and $\phi(x_d)$ is algebraic over k, we have $\Lambda^{-1}(0) = (P(x_d))$ for some non zero polynomial $P(x_d) \in L[x_d]$. Now let $P_d(x_1, \ldots, x_d) \in (k[x_1, \ldots, x_{d-1}])[x_d]$ be a preimage by Ψ of $P(x_d)$.

We claim that $\mathfrak{m} = (\ker(\Psi), P_d)$. To see this, note that $\Psi((\ker(\Psi), P_d)) = (P(x_d))$ and so we have $(\ker(\Psi), P_d) \subseteq \mathfrak{m}$. On the other hand, if $e \in \mathfrak{m}$ then $\Psi(e) \in (P(x_d))$ and thus there is an element $e' \in (P_d)$ such that $\Psi(e) = \Psi(e')$ (since Ψ is surjective). In particular, we have $e - e' \in \ker(\Psi)$, so that $e \in (\ker(\Psi), P_d)$.

Now by the inductive assumption, $\ker(\Psi)$ is generated by polynomials

$$P_1(x_1), P_2(x_1, x_2), P_3(x_1, x_2, x_3), \ldots, P_{d-1}(x_1, \ldots, x_{d-1})$$

and so $\mathfrak{m}$ is generated by $P_1(x_1), P_2(x_1, x_2), P_3(x_1, x_2, x_3), \ldots, P_d(x_1, \ldots, x_d)$.

Part C

Q7. (optional) Let R be a domain. Show $R[x]$ is integrally closed if R is integrally closed.

Here are some hints for this exercise. Let K be the fraction field of R.

(i) Show first that it suffices to show that $R[x]$ is integrally closed in $K[x]$ (ie that the integral closure of $R[x]$ in $K[x]$ is $R[x]$).

(ii) Consider $Q(x) \in K[x]$ and suppose that $Q(x)$ is integral over $R[x]$. Show that $Q(x) + x^t$ satisfies an integral equation with coefficients in $R[x]$, whose constant coefficient is a monic polynomial, if t is sufficiently large.

(iii) Conclude.

Solution.

Suppose that R is integrally closed in its fraction field K. The fraction field of $R[x]$ is $K(x) = \mathrm{Frac}(K[x])$. Let $Q(x) \in K(x)$ and suppose that $Q(x)$ is integral over $R[x]$. Then $Q(x)$ is in particular integral over $K[x]$ and we saw that in the solution of Q4 that $K[x]$ is integrally closed, since it is a PID. So we deduce that $Q(x) \in K[x]$.

Now let

$$Q^n + P_{n-1}Q^{n-1} + \cdots + P_0 = 0$$

be a non trivial integral equation for Q over $R[x]$ (so that $P_i \in R[x]$ and $n \geq 1$). Let t be a natural number, which is strictly larger than the degrees of all the P_i and of Q. Let $T = Q - x^t$. The polynomial T is monic by construction and we have

$$(T + x^t)^n + P_{n-1}(T + x^t)^{n-1} + \cdots + P_0 = 0$$

so that T satisfies an integral equation of the type

$$T^n + H_{n-1}T^{n-1} + \cdots + H_0 = 0$$

where

$$H_0 = P_0 + x^t P_1 + x^{2t} P_2 + \cdots + x^{tn}.$$

Now note that H_0 is a monic polynomial, because $tn > ti + \deg(P_i)$ for all $i \in \{0, \ldots, n-1\}$. Finally, note that in view of the penultimate equation, we have

$$T(T^{n-1} + H_{n-1}T^{n-2} + \cdots + H_1) = -H_0$$

and by Q5 of sheet 2, we have $T \in R[x]$ (because $H_0 \in R[x]$ and H_0 and T are monic). Since $x^t \in R[x]$ we see that we also have $Q \in R[x]$, which is what was to be proven.

Exercise sheet 4. Prerequisites: all lectures. W1 of Trinity Term

Part A

Q1. Let R be a noetherian domain. Let $\mathfrak{m}$ be a maximal ideal in R. Let $r \in R\backslash\{0\}$ and suppose that (r) is a $\mathfrak{m}$-primary ideal. Show that $\mathrm{ht}((r)) = 1$.

Solution. By assumption, the nilradical of (r) is $\mathfrak{m}$. Since the nilradical is the intersection of all the prime ideals containing (r), we see that every prime ideal containing (r) also contains $\mathfrak{m}$. On the other hand, a prime ideal containing $\mathfrak{m}$ must be equal to $\mathfrak{m}$. We conclude that $\mathfrak{m}$ is the only prime ideal containing (r). In particular, $\mathfrak{m}$ is minimal among the prime ideals containing (r) and thus $\mathrm{ht}((r)) = \mathrm{ht}(\mathfrak{m}) \leq 1$ by Krull's principal ideal theorem. On the other hand, $\mathrm{ht}(\mathfrak{m}) = 1$, since we have the chain $\mathfrak{m} \supsetneq (0)$ (note that R is a domain).

Part B

Q2. Let A, B be integral domains and suppose that $A \subseteq B$. Suppose that A is integrally closed and that B is integral over A. Let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

be a descending chain of prime ideals in A. Let $k \in \{0, \ldots, n-1\}$ and let

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_k$$

be a descending chain of prime ideals in B, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \in \{0, \ldots, k\}$. Then there is a descending chain of prime ideals

$$\mathfrak{q}_k \supsetneq \mathfrak{q}_{k+1} \supsetneq \cdots \supsetneq \mathfrak{q}_n$$

such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \in \{k+1, \ldots, n\}$. This is the "going-down theorem". See AT, Th. 5.16, p. 64. Let L (resp. K) be the fraction field of B (resp. A). Prove the going-down theorem when L is a (finite) Galois extension of K.

Solution. One immediately reduces the question to $n = 1$ and $k = 0$. Let $\bar{A}$ be the integral closure of A in L. Note that by assumption we have $B \subseteq \bar{A}$ and that $\bar{A}$ is integral over B (since it is integral over A). Let $\mathfrak{q}_0'$ be a prime ideal of $\bar{A}$ such that $\mathfrak{q}_0' \cap B = \mathfrak{q}_0$ (this exists by the (part of the) going-up theorem). Let $\mathfrak{a}$ be a prime ideal of $\bar{A}$ such that $\mathfrak{a} \cap A = \mathfrak{p}_1$ (again this exists by the going-up theorem). According to Q6 of sheet 2, there is a prime ideal $\mathfrak{b}$ in $\bar{A}$ such that $\mathfrak{b} \supsetneq \mathfrak{a}$ and such that $\mathfrak{b} \cap A = \mathfrak{p}_0$. According to Proposition 12.10, there is an element $\sigma \in \mathrm{Gal}(L|K)$ such that $\sigma(\mathfrak{b}) = \mathfrak{q}_0'$. We have $\sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1$ and $\sigma(\mathfrak{a}) \subsetneq \sigma(\mathfrak{b}) = \mathfrak{q}_0'$. Hence $\sigma(\mathfrak{a}) \cap B \subseteq \mathfrak{q}_0' \cap B = \mathfrak{q}_0$ and $(\sigma(\mathfrak{a}) \cap B) \cap A = \sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1$. Furthermore, we have $\sigma(\mathfrak{a}) \cap B \subsetneq \mathfrak{q}_0$ because $\sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1 \subsetneq \mathfrak{q}_0 \cap A = \mathfrak{p}_0$. So we may set $\mathfrak{q}_1 := \sigma(\mathfrak{a}) \cap B$.

Q3. Let R be an integrally closed domain. Let $K := \mathrm{Frac}(R)$. Let $L|K$ be an algebraic field extension. Show that an element $e \in L$ is integral over R iff the minimal polynomial of e over K has coefficients in R.

Solution. Let $P(x) \in K[x]$ be the minimal polynomial of e. If $P(x) \in R[x]$ then e is integral over R by the definition of integrality. On other hand, suppose that e is integral over R and let $Q(x) \in R[x]$ be a monic polynomial such that $Q(e) = 0$. Then $P(x)$ divides $Q(x)$ by the definition of the minimal polynomial and $P(x) \in R[x]$ by Q5 of sheet 2.

Q4. Let R be a PID. Suppose that $2 = 1 + 1$ is a unit in R. Let $c_1, \ldots, c_t \in R$ be distinct irreducible elements and let $c := c_1 \cdots c_t$. Show that the ring $R[x]/(x^2 - c)$ is a Dedekind domain. Use this to show that $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ is a Dedekind domain.

Solution. Let $K := \mathrm{Frac}(R)$. Notice first that c is not a square in K.

Indeed, suppose for contradiction that there is an element $e \in K$ such that $e^2 = c$. Write $e = f/g$, with $f, g \in R$ and f and g coprime. We then have $f^2/g^2 = c$ and hence $f^2 = g^2 c$. In particular, c_1 divides f and thus c_1^2 divides $g^2 c$. Since $(f, g) = 1$, we deduce that c_1^2 divides c, which contradicts our assumptions.

We deduce that the polynomial $x^2 - c$ is irreducible over K, since it has no roots in K. Let $L := K[y]/(y^2 - c)$. Note that L is a field, since $y^2 - c$ is irreducible. Now let $\phi : R[x] \to L$ be the homomorphism of R-algebras, which sends x to $y \,(\mathrm{mod}\,(y^2 - c))$. We have $\phi(Q(x)) = Q(y) = 0$ iff $x^2 - c$ divides $Q(x)$ in $K[x]$. On the other hand, if $x^2 - c$ divides $Q(x)$ in $K[x]$, then $x^2 - c$ divides $Q(x)$ in $R[x]$ by the unicity statement in the Euclidean algorithm (see preamble). Hence $\ker(\phi) = (x^2 - c)$. We thus see that $R[x]/(x^2 - c)$ can be identified with the sub-R-algebra of L generated by y. Under this identification, the elements of $R[x]/(x^2 - c)$ correspond to the elements of the form $\lambda + \mu y$, with $\lambda, \mu \in R$, whereas the elements of K can all be written as $\lambda + \mu y$, with $\lambda, \mu \in K$.

We claim that that L is the fraction field of $R[x]/(x^2 - c)$. Note first that the fraction field of $R[x]/(x^2 - c)$ naturally embeds in L, since L is field containing $R[x]/(x^2 - c)$. To prove the claim, we only have to show that every element of L can be written as a fraction in L of elements of $R[x]/(x^2 - c)$. This simply follows from the fact that if $f, g, h, j \in R$ and $f/g + (h/j)y \in L$, then

$$f/g + (h/j)y = \frac{fj + hgy}{gj}.$$

Now to prove that $R[x]/(x^2 - c)$ is a Dedekind domain, we have to show that it is noetherian, that is has dimension 1 and that it is integrally closed. The ring $R[x]/(x^2 - c)$ is clearly noetherian (by the Hilbert basis theorem and Lemma 7.2). Also, the ring $R[x]/(x^2 - c)$ is integral over R by construction and R has dimension one by Lemma 11.19. We deduce from Lemma 11.29 that $R[x]/(x^2 - c)$ also has dimension 1. To show that $R[x]/(x^2 - c)$ is integrally closed, we have to show that the integral closure of $R[x]/(x^2 - c)$ in L is $R[x]/(x^2 - c)$. The integral closure of $R[x]/(x^2 - c)$ in L is also the integral closure of R in L by Lemma 8.6 (since $R[x]/(x^2 - c)$ consists of elements, which are integral over R). Furthermore, by Q3 an element $\lambda + \mu y \in L$ is integral iff its minimal polynomial $P(t) \in K[t]$ has coefficients in R. Thus we have to show that if $\lambda + \mu y \in L$ has a minimal polynomial $P(t) \in R[t]$ then $\lambda, \mu \in R$. We prove this statement.

If $\mu = 0$ then $\lambda + \mu y \in R$ and thus the minimal polynomial of $\lambda + \mu y$ is $t - \lambda$. So the statement certainly holds in this situation.

If $\mu \neq 0$, we note that the polynomial

$$(t - (\lambda + \mu y))(t - (\lambda - \mu y)) = t^2 - 2\lambda + \lambda^2 - \mu^2 y^2 = t^2 - 2\lambda + \lambda^2 - c\mu^2$$

annihilates $\lambda + \mu y$ and has coefficients in K. It must thus coincide with the minimal polynomial $P(t)$ of $\lambda + \mu y$, since we know that $\deg(P(t)) > 1$.

Thus we have to show that if $-2\lambda \in R$ and $\lambda^2 - c\mu^2 \in R$, then $\lambda, \mu \in R$. So suppose that $-2\lambda \in R$ and $\lambda^2 - c\mu^2 \in R$. We have $\lambda \in R$, since -2 is a unit in R by assumption. Hence $c\mu^2 \in R$. We claim that $\mu \in R$. Indeed, let $\mu = f/g$, where $f, g \in R$ and f and g are coprime. Then $cf^2 = g^2 r$ for some $r \in R$. Let $i \in \{1, \ldots, t\}$ and suppose first that c_i divides g. Then c_i^2 divides rg^2 and since c_i appears with multiplicity one in c by assumption, we thus see that c_i divides f, which is a contradiction (because $(f, g) = 1$). Hence c_i does not divide g and thus c_i divides r. Since all the c_i are distinct, we thus see that c divides r and thus $(f/g)^2 = r/c =: d \in R$. Hence $f^2 = g^2 d$. Since f and g are coprime, we see that f^2 divides d and hence $d/f^2 \in R$. Since $g^2(d/f^2) = 1$, we conclude that g is a unit and hence $\mu = f/g \in R$.

To see that $\mathbb{R}[x,y]/(x^2+y^2-1)$ is a Dedekind domain, note that $\mathbb{R}[x,y]/(x^2+y^2-1) \simeq (\mathbb{R}[x])[y]/(y^2-(1-x^2))$ and apply the first statement of the question with $R = \mathbb{R}[x]$ and $c = 1-x^2 = (1-x)(1+x)$.

Q5. Let R be a PID. Suppose that $2 = 1+1$ is invertible in R. Let $c_1, c_2 \in R$ be two distinct irreducible elements and let $c := c_1 \cdot c_2$. Show that the decomposition of the ideal (c) in $R[x]/(x^2-c)$ into a product of prime ideals is $(c) = (x, c_1)^2 \cdot (x, c_2)^2$ (noting that $R[x]/(x^2-c)$ is a Dedekind domain by Q4).

Solution. Note first that (x, c_i) $(i = 1, 2)$ is indeed a prime ideal of $R[x]/(x^2-c)$, because

$$(R[x]/(x^2-c))/(x, c_i) = R[x]/(x^2-c, x, c_i) = R/(-c, c_i) = R/(c_i),$$

which is a domain, since c_i is irreducible.

We only have to show that $(c_i) = (x, c_i)^2$.

We first show that $(c_i) \subseteq (x, c_i)^2$. For this, note that $c_i^2 \in (x, c_i)^2$ by definition and

$$(x - c_i)(x + c_i) = x^2 - c_i^2 = c - c_i^2 = c_i(c_j - c_i) \in (x, c_i)^2,$$

where $j = 1$ if $i = 2$ and $j = 2$ if $i = 1$. But $\gcd_R(c_i^2, c_i(c_j - c_i)) = c_i$ (because $c_j - c_i$ is coprime to c_i in R, since c_j is irreducible and distinct from c_i), and in particular $c_i \in (x, c_i)^2$, so that $(c_i) \subseteq (x, c_i)^2$.

To show that $(c_i) \supseteq (x, c_i)^2$, we only have to show that $(x, c_i)^2 \pmod{(c_i)} = ((x, c_i) \pmod{(c_i)})^2 = 0$ in $(R[x]/(x^2-c))/(c_i)$. Now we have $(R[x]/(x^2-c))/(c_i) = R[x]/(x^2-c, c_i) = (R/(c_i))[x]/x^2$. The image $(x, c_i) \pmod{(c_i)}$ of (x, c_i) in $(R/(c_i))[x]/x^2$ is generated by x, so that $((x, c_i) \pmod{(c_i)})^2 = 0$.

Q6. Let R be a ring (not necessarily noetherian). Suppose that $\dim(R) < \infty$.

Show that $\dim(R[x]) \leq 1 + 2\dim(R)$.

Solution. Let

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \mathfrak{q}_2 \supsetneq \cdots \supsetneq \mathfrak{q}_d$$

be a descending chain of prime ideals in $R[x]$, where $d \geq 0$. By restriction, we obtain a descending chain of prime ideals

$$\mathfrak{q}_0 \cap R \supseteq \mathfrak{q}_1 \cap R \supseteq \mathfrak{q}_2 \cap R \supseteq \cdots \supseteq \mathfrak{q}_d \cap R \quad (*)$$

(possibly with repetitions) in R. For each $i \in \{0, \ldots, d\}$, let $\rho(i) \geq 0$ be the largest integer k such that $\mathfrak{q}_i \cap R = \mathfrak{q}_{i+1} \cap R = \cdots = \mathfrak{q}_{i+k} \cap R$. By Lemma 11.21 (and the remark before it) and Lemma 11.19 we have $\rho(i) \leq 1$ for all $i \in \{0, \ldots, d\}$. Now let

$$\mathfrak{q}_{i_0} \cap R = \mathfrak{q}_0 \cap R \supsetneq \mathfrak{q}_{i_1} \cap R \supsetneq \cdots \supsetneq \mathfrak{q}_{i_\delta} \cap R$$

be an enumeration of all the prime ideals appearing in the chain $(*)$, in decreasing order of inclusion. We have

$$d + 1 = (1 + \rho(i_0)) + (1 + \rho(i_1)) + \cdots + (1 + \rho(i_\delta)) \leq 2(\delta + 1)$$

so that $d \leq 2\delta + 1$. Now we have $\delta \leq \dim(R)$ and the required inequality follows.

Q7. Let R be a Dedekind domain. Let $\mathfrak{a}$ be a non zero ideal in R. Show that every ideal in $R/\mathfrak{a}$ is principal. Show that every ideal in a Dedekind domain can be generated by two elements.

Solution. We first prove the first statement. Since R is a Dedekind domain, we have a primary decomposition

$$\mathfrak{a} = \bigcap_{i=1}^{k} \mathfrak{p}_i^{m_i}$$

for some prime ideals $\mathfrak{p}_i$. Using Lemma 12.2 and the Chinese remainder theorem, we see that we have

$$R/\mathfrak{a} \simeq \bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{m_i}$$

Now an ideal I of $\bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{m_i}$ is of the form $\bigoplus_{i=1}^{k} I_i$, where I_i is an ideal of $R/\mathfrak{p}_i^{m_i}$. This follows from the fact that if $e \in I$ and $e = \oplus_{i=1}^{k} e_i$ then $e_i = e \cdot (0, \ldots, 1, \ldots, 0) \in I$, where 1 appears in the i-th place in the expression $(0, \ldots, 1, \ldots, 0)$. Hence, if we can find generators $g_i \in I_i$ for I_i in $R/\mathfrak{p}_i^{m_i}$, then $(g_1, \ldots, g_k)$ will be a generator of I. We proceed to show that any ideal in $R/\mathfrak{p}_i^{m_i}$ can be generated by one element. Consider the exact sequence

$$0 \to \mathfrak{p}_i^{m_i} \to R \to R/\mathfrak{p}_i^{m_i} \to 0$$

Localising this sequence at $R \backslash \mathfrak{p}_i$, we get the sequence of $R_{\mathfrak{p}}$-modules

$$0 \to (\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i} \to R_{\mathfrak{p}_i} \to (R/\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i} \to 0$$

Now the $R_{\mathfrak{p}}$-submodule $(\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i}$ of $R_{\mathfrak{p}}$ is the ideal generated by the image of $\mathfrak{p}_i^{m_i}$ in $R_{\mathfrak{p}}$ (see the beginning of the proof of Lemma 5.6). If we let $\mathfrak{m}$ be the maximal ideal of $R_{\mathfrak{p}}$, this is also $\mathfrak{m}^{m_i}$. On the other hand, $\mathfrak{p}_i$ is contained in the nilradical of $\mathfrak{p}_i^{m_i}$ and since $\mathfrak{p}_i$ is maximal (by Lemma 12.1) it coincides with the radical of $\mathfrak{p}_i^{m_i}$. Hence $R/\mathfrak{p}_i^{m_i}$ has only one maximal ideal, namely $\mathfrak{p}_i \pmod{\mathfrak{p}_i^{m_i}}$. Since the image of $R \backslash \mathfrak{p}_i$ in $R/\mathfrak{p}_i^{m_i}$ lies outside $\mathfrak{p}_i \pmod{\mathfrak{p}_i^{m_i}}$, we see that this image consists of units. Hence $(R/\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i} \simeq R/\mathfrak{p}_i^{m_i}$. All in all, there is thus an isomorphism

$$R_{\mathfrak{p}_i}/\mathfrak{m}^{m_i} \simeq R/\mathfrak{p}_i^{m_i}.$$

Now by Proposition 12.4, every ideal in $R_{\mathfrak{p}_i}/\mathfrak{m}^{m_i}$ is principal, and so we have proven the first statement.

For the second one, let $e \in \mathfrak{a}$ be any non-zero element. Then the ideal $\mathfrak{a} \pmod{(e)} \subseteq R/(e)$ is generated by one element, say g. Let $g' \in R$ be a preimage of g. Then $\mathfrak{a} = (e, g')$.

Q8. Let A (resp. B) be a noetherian local ring with maximal ideal $\mathfrak{m}_A$ (resp. $\mathfrak{m}_B$). Let $\phi : A \to B$ be a ring homomorphism and suppose that $\phi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$ (such a homomorphism is said to be 'local').

Suppose that

(1) B is finite over A via ϕ;

(2) the map $\mathfrak{m}_A \to \mathfrak{m}_B/\mathfrak{m}_B^2$ induced by ϕ is surjective;

(3) the map $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ induced by ϕ is bijective.

Prove that ϕ is surjective. [Hint: use Nakayama's lemma twice].

Solution. By Corollary 3.6, the image of of $\mathfrak{m}_A$ in $\mathfrak{m}_B$ generates $\mathfrak{m}_B$ as a B-module. In other words, $\phi(\mathfrak{m}_A)B = \mathfrak{m}_B$. On the other hand, since B is finitely generated as a A-module, the homomorphism ϕ is surjective iff the induced map $A/\mathfrak{m}_A \to B/\phi(\mathfrak{m}_A)B$ is surjective, again by Corollary 3.6. Now $B/\phi(\mathfrak{m}_A)B = B/\mathfrak{m}_B$ by the above and by (3) the map $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is surjective. The conclusion follows.

Part C

Q9. (optional) Let R be a Dedekind domain. Show that R is a PID iff it is a UFD.

Solution. See https://planetmath.org/pidandufdareequivalentinadedekinddomain