Commutative Algebra

Lectured by C. Brookes

Michaelmas Term 2013

Last updated: Fri 20th Aug, 2021

Please let me know of any corrections: glt1000@cam.ac.uk

Course description

The aim of the course is to give an introduction to the theory of commutative Noetherian rings and modules, a theory that is an essential ingredient in algebraic geometry, algebraic number theory and representation theory.

Topics I hope to fit in will be the theory of ideals for Noetherian and Artinian rings; localisations and completions; integral closure, valuation rings and Dedekind rings; dimension theory; projective and injective modules, resolutions, Koszul complex, (co)homology, derivations and Kaehler differentials.

There will be four example sheets.

Desirable Previous Knowledge

It will be assumed that you have attended a first course on ring theory, eg IB Groups, Rings and Modules. Experience of other algebraic courses such as II Representation Theory, Galois Theory or Number Fields will be helpful but not necessary.

Books

1. M.F. Atiyah and I.G. Macdonald, Introduction to commutative algebra, Addison-Wesley, 1969.

2. N. Bourbaki, Commutative algebra, Elements of Mathematics, Springer, 1989.

3. H. Matsumura, Commutative ring theory, Cambridge Studies 8, Cambridge University Press, 1989.

4. M.Reid, Undergraduate Commutative Algebra, LMS student texts 29, Cambridge University Press, 1995.

5. R.Y. Sharp, Steps in commutative algebra, LMS Student Texts 19, Cambridge University Press, 1990.

The basic text is Atiyah and Macdonald but it doesn't go into much detail and many results are left to the exercises. Sharp fills in some of the detail but neither book goes far enough. Matsumura covers the additional homological material but is a bit tough as an introduction. Reid's book is a companion to one on algebraic geometry and that influences his choice of topics and examples. Bourbaki is encyclopaedic.

Lecture 1

0. Introduction

David Hilbert: 1888-1893, a series of papers on invariant theory

k a field

$k[X_1, \ldots, X_n]$ a polynomial ring

Σ_n, the symmetric group on $\{1, \ldots, n\}$

Σ_n acts on $k[X_1, \ldots, X_n]$ by permuting variables.

The set of invariants $\{f \in k[X_1, \ldots, X_n] : g(f) = f \text{ for all } g \in \Sigma_n\}$ forms a ring S.

The elementary symmetic functions: $f_1(X_1, \ldots, X_n) = X_1 + \cdots + X_n$, $f_2(X_1, \ldots, X_n) = \sum_{i<j} X_i X_j$, $\ldots$, $f_n(X_1, \ldots, X_n) = X_1 X_2 \cdots X_n$.

In fact, S is generated as a ring by these f_i, and $S \cong k[f_1, \ldots, f_n]$ – polynomial ring, i.e. no algebraic dependence.

Hilbert showed that S is finitely generated, and lots of other groups as well. Along the way he proved four long theorems:

1. Basis Theorem
2. Nullstellensatz ('zeros theorem')
3. polynomial nature of the Hilbert function
4. Syzygy theorem

Emmy Noether (1921) abstracted from Hilbert's work the fundamental property that made the Basis Theorem work.

A (commutative) ring R is **Noetherian** if every ideal of R is finitely generated. (There are equivalent definitions.)

Noether developed the theory of ideals for Noetherian rings – e.g., there is a primary decomposition which generalises factorisation into primes in number theory.

Link between commutative algebra and algebraic geometry

Fundamental theorem of algebra: a polynomial $f \in \mathbb{C}[X]$ is determined up to scalar multiples by its zeros up to multiplicity.

Given $f \in \mathbb{C}[X_1, \ldots, X_n]$ there is a polynomial function $f : \mathbb{C}^n \to \mathbb{C}$, $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$.

Thus we get polynomial functions on affine n-space.

Given $I \subset \mathbb{C}[X_1, \ldots, X_n]$, define

$$Z(I) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

– the set of common zeros. Such a subset of $\mathbb{C}^n$ is an **algebraic set**.

Note that we can replace I by the ideal generated by I without changing $Z(I)$.

For a subset $\mathcal{S} \subset \mathbb{C}^n$, define

$$I(\mathcal{S}) = \big\{ f \in \mathbb{C}[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in \mathcal{S} \big\}$$

This is an ideal of $\mathbb{C}[X_1, \ldots, X_n]$. Moreover, it is **radical**, i.e. if $f^r \in I(\mathcal{S})$ for some $r \geqslant 1$, then $f \in I(\mathcal{S})$.

Nullstellensatz is really a family of theorems, but one way of looking at it is that there is a $1-1$ correspondence

$$\begin{array}{rcl} \big\{\text{radical ideals in } \mathbb{C}[X_1, \ldots, X_n]\big\} & \longleftrightarrow & \big\{\text{algebraic subsets of } \mathbb{C}^n\big\} \\ I & \longrightarrow & Z(I) \\ I(\mathcal{S}) & \longleftarrow & \mathcal{S} \end{array}$$

In particular, the maximal ideals of $\mathbb{C}[X_1, \ldots, X_n]$ correspond to points in $\mathbb{C}^n$.

Remark. There is a topology on $\mathbb{C}^n$ under which the closed sets are the algebraic sets – called the **Zariski topology**.

Basis Theorem. If R is Noetherian then $R[X]$ is Noetherian.

Corollary. If k is a field then $k[X_1, \ldots, X_n]$ is Noetherian.

Quite a large section of the course is about dimension. There are (at least) three ways of defining dimension.

1. The maximal length of chains of prime ideals.
2. In the geometric context, we look at growth rates. (This is the context of the Hilbert function.)
3. Transcendence degree of the field of quotients (of an integral domain).

In the commutative context, these all give the same answer.

In fact, there is a fourth way using homological algebra, which for 'nice' Noetherian rings give the same answer again.

Most of the theory is from 1920-1950.

Lecture 2

1. Noetherian rings: definitions, ideal structure

Throughout, R is a commutative ring with a 1.

Lemma 1.1. Let M be a left R-module. The following are equivalent.

1. Every submodule is finitely generated.
2. The ascending chain condition (ACC): there is no strictly ascending chain of submodules.
3. Every non-empty set of submodules of M contains at least one maximal member.

Proof.

(1) $\Rightarrow$ (2). Suppose $M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \ldots$.

Let $N = \bigcup M_j$. This is a submodule of M. Assuming (1), then N is finitely generated, and a finite generating set lies in some M_j. So $N = M_j$, contradicting strict ascent.

(2) $\Rightarrow$ (3). Suppose ACC.

Let $M_1 \in \mathcal{S}$. If it is a maximal member, then we're done. If not, then choose M_2 which is bigger. Etc. By ACC, this process stops.

(3) $\Rightarrow$ (1). Suppose (3).

Let N be a submodule of M. Let $\mathcal{S}$ be the set of all finitely-generated submodules of N. Then $\mathcal{S}$ is non-empty, since it contains the zero submodule. So $\mathcal{S}$ contains a maximal member, say L.

Check that $L = N$, and so N is finitely generated. □

Definition 1.2. A module satisfying these conditions is **Noetherian**.

Lemma 1.3. Let N be a submodule of M. Then M is Noetherian $\iff$ N and M/N are Noetherian.

Proof. ($\Rightarrow$). Exercise.

($\Leftarrow$). Suppose that N and M/N are Noetherian, and that $L_1 \leqslant L_2 \leqslant \ldots$ is an ascending chain of submodules of M.

Set $Q_i/N = (L + N)/N$ and $N_i = L_i \cap N$. By ACC, there are r, s such that $Q_i/N = Q_r/N$ for $i \geqslant r$, and $N_i = N_s$ for $i \geqslant s$. Set $k = \max(r, s)$.

Claim. $L_i = L_k$ for $i \geqslant k$. (Check this.) □

Lemma 1.4. Suppose that $M = M_1 + \ldots + M_n$ (not necessarily direct). Then M is Noetherian $\iff$ each M_i is Noetherian.

Proof. ($\Rightarrow$). Clear.

($\Leftarrow$). If each M_i is Noetherian then $M_1 \oplus \ldots \oplus M_n$ is Noetherian, and so M is Noetherian since it is an image of $M_1 \oplus \ldots \oplus M_n$ under the canonical map $M_1 \oplus \ldots \oplus M_n \to$

$M_1 + \ldots + M_n$. □

Definition 1.5. A ring R is Noetherian if it is Noetherian as a (left) R-module.

Remark. The submodules of R as an R-module are its ideals.

So ACC for modules $\longleftrightarrow$ ACC for ideals.

Lemma 1.6. Let R be a Noetherian ring. Then any finitely-generated R-module is Noetherian.

Proof. Suppose $M = Rm_1 + \ldots + Rm_n$. We have surjective R-module maps

$$\begin{aligned} R &\to Rm_i \\ r &\mapsto rm_i \end{aligned}$$

R is Noetherian and so Rm_i is. Hence M is Noetherian by Lemma 1.4. □

Theorem 1.7 (Basis theorem). Let R be a Noetherian ring. Then $R[X]$ is Noetherian.

Proof. We prove that every ideal of $R[X]$ is finitely generated.

Let I be an ideal. Define $I(n)$ to be the set of polynomials in I of degree $\leqslant n$. Then $0 \in I(n)$ and so $I(n)$ is non-empty.

We have $I(0) \subseteq I(1) \subseteq \ldots$

Let $R(n)$ be the set of all leading coefficients of elements of $I(n)$ – i.e., the coefficients of X^n.

Check that each $R(n)$ is an ideal of R, and that $R(0) \leqslant R(1) \leqslant \ldots$. Then ACC in R yields that $\bigcup R(n) = R(N)$ for some N.

We know that each of $R(0), \ldots, R(N)$ is finitely generated – say that $R(j)$ is generated by $a_{j1}, \ldots, a_{jk_j}$, and that these are the leading coefficients of $f_{j1}, \ldots, f_{jk_j}$ in $I(j)$.

Claim. The set $\left\{f_{jk} : j \leqslant N, 1 \leqslant k \leqslant k_j\right\}$ generates I. (Check this.) □

Remark. In practice, one uses **Gröbner bases** for ideals – they are generating sets with added properties that make algorithms efficient.

Examples.

1. Fields are Noetherian.
2. Principal ideal domains – e.g., $k[X]$, $\mathbb{Z}$ – are Noetherian.
3. $\{q \in \mathbb{Q} : q$ is of the form m/n with $m, n \in \mathbb{Z}$ and $p \nmid n\}$ for a fixed prime p.

   This is an example of a **localisation** of $\mathbb{Z}$.

   All localisations of Noetherian rings are Noetherian.
4. $k[X_1, X_2, \ldots]$ is *not* Noetherian: $(X_1) \subsetneq (X_1, X_2) \subsetneq \ldots$
5. $k[X_1, \ldots, X_n]$ is Noetherian – corollary of the Basis theorem.

   $\mathbb{Z}[X_1, \ldots, X_n]$ is Noetherian. So any finitely-generated ring is Noetherian, since

such a ring is an image of some $\mathbb{Z}[X_1, \ldots, X_n]$.

6. $k[[X]]$, the ring of formal power series, is Noetherian.

   In general, we have the following.

Theorem 1.8. R Noetherian $\implies$ $R[[X]]$ Noetherian.

Exercise. Prove this by an argument analogous to that for the Basis theorem, but by using 'trailing coefficients'.

Lecture 3 Alternatively, use Cohen's theorem.

Theorem 1.9 (Cohen). If every prime ideal is finitely generated then R is Noetherian.

Proof. Suppose that R is not Noetherian, and so there exist ideals that are not finitely generated. By Zorn's lemma there is a maximal member I of the family of non-finitely-generated ideals.

(Recall that to apply Zorn's lemma one needs to check the family is non-empty and that an ascending chain of non-finitely-generated ideals has union which is non-finitely generated.)

Claim. I is prime. (And hence we're getting a contradiction if we're assuming all primes to be finitely generated.)

Proof. Suppose not, so that there exist $a, b \notin I$ with $ab \in I$.

Then $I + Ra$ is an ideal strictly containing I. The maximality of I ensures that $I + Ra$ is finitely generated, by $i_1 + r_1 a, \ldots, i_n + r_n a$, say.

Let $J = \{s \in R : sa \in I\} \geqslant I + Rb \gneq I$. So by maximality of I, we know that J is finitely generated.

We prove that $I = Ri_1 + \ldots + Ri_n + Ja$, a finitely-generated ideal, a contradiction.

Take $t \in I \leqslant I + Ra$. So $t = u_1(i_1 + r_1 a) + \ldots + u_n(i_n + r_n a)$ for some $u_i \in R$.

So $u_1 r_1 + \ldots + u_n r_n \in J$, and so it is of the required form. □

To use Cohen's theorem, we apply the following.

Lemma 1.10. Let P be a prime ideal of $R[[X]]$, and θ be the map $\theta : R[[X]] \to R$ sending $X \mapsto 0$.

Then P is a finitely-generated ideal of $R[[X]]$ if and only if $\theta(P)$ is a finitely-generated ideal of R.

Proof. Clearly if P is finitely generated then $\theta(P)$ is.

Conversely, suppose that $\theta(P) = Ra_1 + \ldots + Ra_n$.

If $X \in P$ then P is generated by $a_1, \ldots, a_n$ and X.

Suppose $X \notin P$. Let $f_1, \ldots, f_n$ be power series with constant terms $a_1, \ldots, a_n$. Take

$g \in P$, say $g = b + \ldots$, with b the constant term.

Then $b = \sum b_i a_i$. So $g - \sum b_i f_i = g_1 X$ for some power serise g_1. Note $g_1 X \in P$.

But P is prime and $X \notin P$, so $g_1 \in P$. So similarly, $g_1 = \sum c_i f_i + g_2 X$ with $g_2 \in P$.

Continuing, we get $h_1, \ldots, h_n \in R[[X]]$ with $h_i = b_i + c_i X + \ldots$, satisfying $g = h_1 f_1 + \ldots + h_n f_n$. □

For the next bit, assume that R is commutative, but not necessarily Noetherian.

1.11. The set $N(R)$ of all nilpotent elements of R is an ideal, and $R/N(R)$ has no non-zero nilpotent elements. □

Proof. If $x \in N(R)$ then $x^n = 0$ for some n, and so $(rx)^n = 0$. Thus $rx \in N(R)$.

If $x, y \in N(R)$ then $x^n = 0$ and $y^m = 0$ for some n, m. Then $(x+y)^{m+n} = 0$. So $x + y \in N(R)$.

If $s \in R/N(R)$ and we have $s = x + N(R)$ then $s^n = x^n + N(R)$. If $s^n = N(R)$ then $x^n \in N(R)$, so $x^{nm} = 0$ for some M. So $x \in N(R)$ and thus $s = N(R)$. □

Definition 1.12. This ideal is the **nilradical** of R.

Theorem 1.13 (Krull). $N(R)$ is the intersection of all the prime ideals of R.

Proof. Let $I = \bigcap_{P \text{ prime}} P$.

If $x \in R$ is nilpotent then $x^n = 0 \in P$ for any prime P. So $x \in P$. Hence $N(R) \leqslant I$.

Now suppose that x is not nilpotent. Set $\mathcal{S}$ to be the set of all ideals J such that for $n > 0$ we have $x^n \notin J$.

Then $\mathcal{S}$ is non-empty, as $(0) \in \mathcal{S}$. We can apply Zorn's lemma to get a maximal member J_1 of $\mathcal{S}$. (If R is Noetherian then we don't have to think about Zorn.)

Claim. J_1 is prime.

Proof. Suppose $yz \in J_1$ with $y, z \notin J_1$. So the ideals $J_1 + Ry$ and $J_1 + Rz$ strictly contain J_1 and hence for some n we have $x^n \in J_1 + Ry$ and $x^n \in J_1 + Rz$. Then $x^{2n} \in J_1 + Ryz$, and so $yz \notin J_1$. ⨳

Definition 1.14. The **radical** $\sqrt{I}$ of an ideal I is defined by $\sqrt{I}/I = N(R/I)$.

An ideal is **radical** if $I = \sqrt{I}$.

Note that $\sqrt{I}$ is radical, and $\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ \text{containing } I}} P$.

Definition 1.15. The **Jacobson radical** $J(R)$ of R is the intersection of the maximal ideals of R.

Lemma 1.16 (Nakayama). If M is a finitely-generated R-module with $MJ = M$ (where $J = J(R)$), then $M = 0$.

Proof. M is a non-zero finitely-generated R-module, so Zorn (or the Noetherian property, if R is Noetherian) yields maximal (proper) submodules.

Take M_1 maximal in M. Thus M/M_1 is an irreducible (or simple) R-module. Take a generator of M/M_1, say $M_1 + m$. Then $M/M_1 \cong R/I$ with I a maximal ideal of R.

(E.g., the map $R \to M/M_1$ sending $r \mapsto rm + M_1$ is an R-module homomorphism, with kernel necessarily a maximal ideal.)

But, by definition, $J \leqslant I$. So $MJ \leqslant M_1 \lneq M$. So if $M \neq 0$ then $MJ \lneq M$. □

Lecture 4

For a commutative ring,, we have

$$N(R) = \bigcap_{P \text{ prime}} P \leqslant J(R) = \bigcap_{P \text{ maximal}} P$$

These need not be equal. For example, $R = \{\frac{m}{n} \in \mathbb{Q} : \text{fixed prime } p \nmid n\}$. This has a unique maximal ideal $P = \{\frac{m}{n} \in \mathbb{Q} : p \mid m, p \nmid n\}$. But it is an integral domain, so has no non-zero nilpotent elements, so $N(R) = (0)$ and $J(R) = P$.

However, for rings of the form $R = k[X_1, \ldots, X_n]/I$ with k algebraically closed and I any ideal, we do have $N(R) = J(R)$. This is the context of the Nullstellensatz. There are 'weak' and 'strong' versions. Below is the proof due to Artin and Tate.

Lemma 1.17. Let $R \leqslant S \leqslant T$ be commutative rings. Suppose that R is Noetherian and T is generated as a ring by R and finitely many elements $t_1, \ldots, t_n$. Suppose that T is a finitely-generated S-module. Then S is generated as a ring by R and finitely many elements.

Proof. Let T be generated by $x_1, \ldots, x_m \in T$ as an S-module, so $T = Sx_1 + \ldots + Sx_m$. Then

$$t_i = \sum s_{ij} x_j \text{ for some } s_{ij} \in S \tag{1}$$

$$x_i x_j = \sum s_{ijk} x_k \text{ for some } s_{ijk} \in S \tag{2}$$

Let S_0 be the ring generated by R, the s_{ij}, and the s_{ijk}. Thus $R \leqslant S_0 \leqslant S$.

Any element of T is a 'polynomial' in the t_i with coefficients in R. In (1) and (2), we see that each element is a linear combination of the x_j with coefficients in S_0. Thus T is a finitely-generated S_0-module. But S_0 is Noetherian, being generated as a ring by R and finitely many elements. T is a Noetherian S_0-module, and S is an S_0-submodule of T and hence is finitely generated as an S_0-module. But S_0 is generated by R and finitely many elements, so S is generated by R and finitely many elements. □

Lemma 1.18. Let k be a field, and R a finitely-generated k-algebra. If R is itself a field, then it is an algebraic extension of k.

Proof. Suppose that R is generated by k and $x_1, \ldots, x_n$, and is a field. If R is not algebraic over k then we can reorder $x_1, \ldots, x_n$ so that $x_1, \ldots, x_m$ are algebraically independent (i.e., the ring generated by k and $x_1, \ldots, x_m \cong$ the polynomial algebra $k[X_1, \ldots, X_m]$), and $x_{m+1}, \ldots, x_n$ are algebraic over the field $F = k(x_1, \ldots, x_m)$ (the field of fractions of $k[X_1, \ldots, X_m]$).

Hence R is a finite algebraic extension of F, and hence a finitely-generated F-module. (R contains a copy of F since R is a field.)

Apply 1.17 for $k \leqslant F \leqslant R$. It follows that F is a finitely-generated k-algebra generated by k and $q_1, \ldots, q_t$, say, with each $q_i = f_i/g_i$, with $f_i, g_i \in k[X_1, \ldots, X_m]$, $g_i \neq 0$.

There exists a polynomial h which is prime to each of the g_i (such as $g_1 \ldots g_t + 1$), and the element $1/h$ cannot be in the ring generated by k and $q_1, \ldots, q_t$. ⫻

Hence R is algebraic over k. □

Theorem 1.19 (Weak Nullstellensatz). Let k be a field, and S be a finitely-generated k-algebra. Let P be a maximal ideal of S. Then S/P is a finite algebraic extension of k. In particular, if k is algebraically closed, then $S/P \cong k$.

Proof. Apply 1.18 to $R = S/P$, a field.

Theorem 1.20 (Strong Nullstellensatz). Let k be an algebraically closed field, and S be a finitely-generated k-algebra. Let P be a prime ideal. Then $P = \bigcap\{\text{maximal ideals containing } P\}$.

Furthermore, any radical ideal is the intersection of the maximal ideals containing it.

Proof. Let $s \in S \setminus P$. Let $\overline{s}$ be the image os s in S/P. Now, $R = S/P$ is an integral domain (as P is prime), and is finitely generated as a k-algebra, say by $r_1, \ldots, r_n$. Invert $\overline{s}$ to get $T = \langle R, \overline{s}^{-1} \rangle \leqslant$ fraction field of S/P.

Take a maximal ideal Q of T. By 1.19, the weak Nullstellensatz, we have $T/Q \cong k$, and so $Q \cap R$ contains elements $r_i - \lambda_i$ for some $\lambda_i \in k$. Hence $Q \cap R$ is a maximal ideal of R, not containing $\overline{s}$. Thus there exists a maximal ideal of S containing P but not s.

Thus $\bigcap\{\text{maximal ideals containing } P\} = P$. □

Lemma 1.21. If R is Noetherian then every ideal I contains a power of its radical $\sqrt{I}$. In particular, $N(R)$ is nilpotent – i.e., $N(R)^m = 0$ for some m.

Proof. Suppose $x_1, \ldots, x_m$ generate $\sqrt{I}$ (as an ideal). So $x_i^{n_i} \in I$ for some n_i (for each I).

Let $n = \sum(n_i - 1) + 1$. Then $(\sqrt{I})^n$ is generated by products $x_1^{r_1} \ldots x_m^{r_m}$ with $\sum r_i = n$. We must have some $r_i \geqslant n_i$. Hence all products lie in R.

Lemma 1.22. If R is Noetherian then a radical ideal is the intersection of finitely many prime ideals.

Lecture 5

Proof. Suppose not, and take I to be a maximal member of the set of radical ideals not of this form.

Claim. I is prime (yielding a contradiction).

Proof. Suppose not. Then there are ideals J_1, J_2 with $J_1 \supsetneqq I$ and $J_2 \supsetneqq I$, but $J_1 J_2 \leqslant I$.

So, maximality of I gives that $\sqrt{J_1} = Q_1 \cap \ldots \cap Q_s$ and $\sqrt{J_2} = Q_1' \cap \ldots \cap Q_t'$, with Q_i, Q_j' prime.

Set $J = Q_1 \cap \ldots \cap Q_s \cap Q'_1 \cap \ldots \cap Q'_t = \sqrt{J_1} \cap \sqrt{J_2}$.

So $J^{m_1} \leqslant J_1$ and $J^{m_2} \leqslant J_2$ for some m_1, m_2, and hence $J^{m_1+m_2} \leqslant J_1 J_2 \leqslant I$.

But I is radical and so $J \leqslant I$. But all $Q_i, Q'_j \geqslant I$ and so $J \geqslant I$.

Hence $J = I$. ⫻ □

Now suppose $\sqrt{I} = P_1 \cap \ldots \cap P_m$. We may remove any prime which contains one of the others. So we may assume that $P_i \not\leqslant P_j$ for $i \neq j$.

If P is prime with $\sqrt{I} \leqslant P$ then $P_1 \ldots P_m \leqslant \bigcap P_i = \sqrt{I} \leqslant P$, and so some $P_i \leqslant P$.

Definition 1.23. The **minimal primes** P over an ideal I of a Noetherian ring are such that if P' is prime with $I \leqslant P' \leqslant P$, then $P' = P$.

Observe that the P_i above are minimal primes. We can show

1.24. Let I be an ideal of a Noetherian ring. Then $\sqrt{I}$ is the intersection of the minimal primes over I, and I contains a finite product of the minimal primes over I.

Proof. Each (minimal) prime over I contains $\sqrt{I}$. So the primes minimal over I are exactly those minimal over $\sqrt{I}$.

The above discussion shows that $\sqrt{I}$ is the intersection of these. Thus their product lies in $\sqrt{I}$, and (1.21) yields the final statement.

Definition 1.25. Let M be a finitely-generated R-module M, where R is Noetherian. A prime ideal P is an **associated prime** of M if it is the annihilator of an element of M.

(Recall that the annihilator of m is $\mathrm{Ann}(m) = \{r \in R : rm = 0\}$.)

Define $\mathrm{Ass}(M) = \big\{P : P \text{ prime}, P = \mathrm{Ann}(m) \text{ for some } m \in M\big\}$.

E.g., $\mathrm{Ass}(R/P) = \{P\}$ for P prime.

Definition 1.26 A submodule N of M is **P-primary** (or just **primary**) if $\mathrm{Ass}(M/N) = \{P\}$ for a prime ideal P.

An ideal is **P-primary** if I is P-primary as a submodule of R.

Lemma 1.27. If $\mathrm{Ann}(M) = P$ for a prime ideal P then $P \in \mathrm{Ass}(M)$.

Proof. Let $m_1, \ldots, m_k$ generate M and $I_j = \mathrm{Ann}(m_j)$.

Then the product $\prod I_j$ annihilates each m_j, and so $\prod I_j \leqslant \mathrm{Ann}(M) = P$.

So $I_j = P$ for some J, and so $P \in \mathrm{Ass}(M)$. □

In fact, we can always be sure that $\mathrm{Ass}(M)$ is non-empty.

Lemma 1.28. Let Q be maximal among all annihilators of non-zero elements.

Then Q is a prime ideal and so $Q \in \mathrm{Ass}(M)$.

Proof. Let $Q = \mathrm{Ann}(m)$ and $r_1, r_2 \in Q$ with $r_2 \notin Q$. We show that $r_1 \in Q$.

Now, $r_1 r_2 \in Q$ implies that $r_1 r_2 m = 0$. So $r_1 \in \mathrm{Ann}(r_2 m)$. And $r_2 \notin q$ implies that $r_2 m \neq 0$.

But $Q \leqslant \mathrm{Ann}(r_2 m)$. Hence Q and r_1 lie in $\mathrm{Ann}(r_2 m)$, and so maximality of Q among annhilators forces $r_1 \in Q$. □

Lemma 1.29. For a finitely-generated non-zero R-module M with R Noetherian, there is a chain of submodules

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_t = M$$

with $M_i/M_{i-1} \cong R/P_i$ for some prime ideal P_i.

Proof. By 1.28, there is a non-zero $m_1 \in M$ with $\mathrm{Ann}(m_1)$ being prime, say P_1.

Set $M_1 = Rm_1$. Thus $M_1 \cong R/P_1$.

Now repeat for M/M_1 to find $M_2/M_1 \cong R/P_2$ for some prime P_2.

Repeat. The Noetherian property of M forces the process to terminate. □

Lemma 1.30. If $N \subset M$, then $\mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$.

Proof. Suppose $P = \mathrm{Ann}(m)$ for some $m \in M$. P is prime.

Let $M_1 = Rm \cong R/P$. For any non-zero $m_1 \in M_1$, we have $\mathrm{Ann}(m_1) = P$ since P is prime.

If $M_1 \cap N \neq 0$ then there exists $m_1 \in M_1 \cap N$ with $\mathrm{Ann}(m_1) = P$ and so $P \in \mathrm{Ass}(N)$.

If $M_1 \cap N = 0$ then the image of M_1 in M/N is isomorphic to R/P. Thus $P \in \mathrm{Ass}(M/N)$. □

1.31. $\mathrm{Ass}(M)$ is finite for any finitely-generated R-module (where R is Noetherian).

Proof. We use 1.30 inductively on the chain in 1.29, recalling that $\mathrm{Ass}(R/P_i) = \{P_i\}$.

So $\mathrm{Ass}(M) \subset \{P_1, \ldots, P_t\}$. □

Lecture 6

Proposition 1.32. Each minimal prime over an ideal I is an associated prime.

Proof. By (1.24), there is a prodict of minimal primes over I (possibly with repetition) contained in I, say $P_1^{s_1} \ldots P_n^{s_n} \leqslant I$ with $P_i \neq P_j$ if $i \neq j$.

Consider $J = \mathrm{Ann}\left(P_2^{s_2} \ldots P_n^{s_n} + I/I\right)$. Certainly, $J \geqslant P_1^{s_1}$. Also, $J P_s^{s_2} \ldots P_n^{s_n} \leqslant I \leqslant P_1$, and since P_1 is prime (and not equal to $P_2, \ldots, P_n$) we have $J \leqslant P_1$.

Let $M = \mathrm{Ann}\left(P_2^{s_2} \ldots P_n^{s_n} + I/I\right)$. By (1.29), there is a chain of submodules in M, say $0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$, such that each factor $\cong R/Q_j$ for some prime ideal Q_j.

But $P_1^{s_1}$ annihilates M, and hence each M_j/M_{j-1}, and the primeness of of Q_j ensures $P_1 \leqslant Q_j$ for each j.

Not all of the $Q_j \gneqq P_1$ since $\prod Q_j \leqslant J \leqslant P_1$, and hence some $Q_j \leqslant P_1$.

Pick the least j such that $Q_j = P_1$, and then $\prod_{k<j} Q_k \nleq P_1$.

Take $x \in M_j \setminus M_{j-1}$. If $j = 1$ then $\mathrm{Ann}(x) = P_1$ and so $P_1 \subset \mathrm{Ass}(R/I)$.

If $j > 1$ then take $r \in \left(\prod_{k<j} Q_k \right) \setminus P_1$. Note that $r(sx) = 0$ for any $s \in P_1 = Q_j$. So $s(rx) = 0$ and so $P_1 \leqslant \mathrm{Ann}(rx)$.

However $rx \notin M_{j-1}$ since $M_j/M_{j-1} \cong R/Q_j = R/P_1$.

So $\mathrm{Ann}(rx) = P_1$, and we have shown that $P_1 \in \mathrm{Ass}(M) \subset \mathrm{Ass}(R/I)$. □

Example. The converse is false. Here is an example where there is $P \in \mathrm{Ass}(R/I)$ with P not minimal over I.

Let $R = k[X, Y]$, and take $P = (x, y) > Q = (X)$, and $I = PQ = (X^2, XY)$.

Then $\mathrm{Ass}(R/I) = \{P, Q\}$. But Q is the only minimal prime over I.

In practice, $\mathrm{Ass}\, M$ is of more practical use than primary decomposition.

Primary decomposition

Let M be a finitely-generated R-module where R is Noetherian, and let $N \leqslant M$.

Then there exist $N_1, \ldots, N_t$ with $N = N_1 \cap \ldots \cap N_t$, and with $\mathrm{Ass}(M/N_i) = \{P_i\}$ for some *distinct* $P_1, \ldots, P_t$.

Recall. Such an N_i is a P_i-primary submodule of M.

Remark. In the above example, I is not Q-primary despite $\sqrt{I} = Q$. But $I = Q \cap P^2$ is a primary decomposition.

An alternative definition of a primary ideal I is that:

(a) I is proper

(b) If $ab \in I$ but $a \notin I$ then $b^n \in I$ for some n.

2. Localisation

As always, R is a commutative ring with a 1.

Let S be a **multiplicatively closed** subset of R. (I.e., S is closed under multiplication, and by convention we have $1 \in S$.)

Define a relation $\equiv$ on $R \times S$ by:

$$(r_1, s_1) \equiv (r_2, s_2) \iff (r_1 s_2 - r_2 s_1)x = 0 \text{ for some } x \in S$$

This is reflexive, symmetric and transitive.

Transitivity: suppose that $(r_1, s_1) \equiv (r_2, s_2)$ and $(r_2, s_2) \equiv (r_3, s_3)$. Then there exist $x, y \in S$ with $(r_1 s_2 - r_2 s_1)x = 0$ and $(r_2 s_3 - r_3 s_2)y = 0$.

Then $(r_1 s_3 - r_3 s_1)s_2 xy = 0$, and S is multiplicatively closed and so $s_2 xy \in S$.

Thus $\equiv$ is an equivalence relation.

Denote the equivalence class of (r, s) by r/s, and the set of equivalence classes by $S^{-1}R$.

$S^{-1}R$ can be made into a ring, with addition $r_1/s_1 + r_2/s_2 = (r_1 s_2 + r_2 s_1)/s_1 s_2$ and multiplication $(r_1/s_1)(r_2/s_2) = (r_1 r_2)/(s_1 s_2)$.

We have a ring homomorphism $\theta : R \to S^{-1}R$ given by $r \mapsto r/1$.

$S^{-1}R$ has a universal property, as follows.

Exercise 2.1. Let $\varphi : R \to T$ be a ring homomorphism with $\varphi(s)$ a unit in T for all $s \in S$.

Then there exists a unique ring homomorphism $\alpha : S^{-1}R \to T$ with $\varphi = \alpha \circ \theta$.

Examples.

1. Fraction fields of an integral domain R. Put $S = R \setminus \{0\}$.
2. $S^{-1}R$ is the zero ring if and only if $0 \in S$.
3. If I is an ideal of R then we can set $S = 1 + I = \{1 + x : x \in I\}$.
4. If P is a prime ideal of R, set $S = R \setminus P$. Write R_P for $S^{-1}R$ in this case.

   The process of passing from R to R_P is called **localisation**.

   The elements r/s with $r \in P$ form an ideal of R_P. This is a unique maximal ideal in R_P. For if r/s is such that $r \notin P$ then $r \in S$, and so has an inverse in R_P.

Definition 2.2. A ring with a unique maximal ideal is called **local**.

Remark. Some authors require a local ring to be Noetherian.

Examples.

1. Take $R = \mathbb{Z}$, and $P = (p)$ for p prime is a prime ideal.

Then $R_P = \left\{ \frac{m}{n} : p \nmid n \right\} \subset \mathbb{Q}$.

2. Take $R = k[X_1, \ldots, X_n]$ and $P = (X_1 - a_1, \ldots, X_n - a_n)$.

   R_P is a subring of $k(X_1, \ldots, X_n)$ of rational functions defined at $(a_1, \ldots, a_n) \in k^n$, and the unique maximal ideal consists of those functions which are zero at $(a_1, \ldots, a_n)$.

Lecture 7

Modules

Given an R-module M, define a relation $\equiv$ on $M \times S$, with respect to a multiplicatively closed set $S \subset R$, by:

$$(m_1, s_1) \equiv (m_2, s_2) \iff x(m_1 s_2 - m_2 s_1) = 0 \text{ for some } x \in S$$

This is an equivalence relation (check this). Denote the equivalence class of (m, s) by m/s, and the set of equivalence classes by $S^{-1}M$.

$S^{-1}M$ is an $S^{-1}R$-module, via

$$m_1/s_1 + m_2/s_2 = (s_2 m_1 + s_1 m_2)/s_1 s_2$$

$$(r_1/s_1)(m_2/s_2) = r_1 m_2 / s_1 s_2$$

Write M_P in the case where $S = R \setminus P$ for a prime ideal P.

If $\theta : M_1 \to M_2$ is an R-module map, then $S^{-1}\theta : S^{-1}M_1 \to S^{-1}M_2$ is an $S^{-1}R$-module map, defined by $S^{-1}\theta : m_1/s \mapsto \theta(m_1)/s$.

And if $\varphi : M_2 \to M_3$ then $S^{-1}(\varphi \circ \theta) = S^{-1}\varphi \circ S^{-1}\theta$.

A sequence of R-modules

$$M_0 \to M_1 \to M_2 \to \cdots \xrightarrow{\theta} M_i \xrightarrow{\varphi} \cdots \to M_t$$

is **exact** at M_i if $\operatorname{im}\theta = \ker\varphi$.

A **short exact sequence** is of the form

$$0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0$$

with exactness at M_1, M, M_2. So θ is injective, φ is surjective, and $\operatorname{im}\theta = \ker\varphi$.

Lemma 2.3. If M_1, M, M_2 are R-modules and $M \xrightarrow{\theta} M \xrightarrow{\varphi} M_2$ is exact at M, then

$$S^{-1}M \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}M_2$$

is exact at $S^{-1}M$.

Proof. Since $\ker\varphi = \operatorname{im}\theta$ we have $\varphi \circ \theta = 0$.

So $S^{-1}\varphi \circ S^{-1}\theta = S^{-1}(\varphi \circ \theta) = S^{-1}0 = 0$ and hence $\operatorname{im} S^{-1}\theta \subset \ker S^{-1}\varphi$.

Now suppose that $m/s \in \ker S^{-1}\varphi \subset S^{-1}M$. So $\varphi(m)/s = 0$ in $S^{-1}M_2$, and there is $t \in S$ with $t\varphi(m) = 0$ in M_2.

But $t\varphi(m) = \varphi(tm)$ since φ is an R-module map. So $tm \in \ker\varphi = \operatorname{im}\theta$, and $tm = \theta(m_1)$ for some $m_1 \in M_1$.

Hence, in $S^{-1}M$ we have $m/s = \theta(m)/ts = S^{-1}\theta(m_1/ts) \in \operatorname{im} S^{-1}\theta$.

Thus $\ker S^{-1}\varphi = \operatorname{im} S^{-1}\theta$. □

Lemma 2.4. Let N be a submodule of M. Then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Proof. Apply Lemma 2.3 to the short exact sequence $0 \to N \xrightarrow{\theta} M \xrightarrow{\varphi} M/N \to 0$ to get that

$$0 \to S^{-1}N \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}(M/N) \to 0$$

is a short exact sequence.

Note that $S^{-1}\theta$ is an embedding and $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$. □

If R is a ring with multiplicatively closed subset S, and I is an ideal in R, then $S^{-1}I$ is an ideal in $S^{-1}R$.

Lemma 2.5.

1. Every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.
2. The prime ideals of $S^{-1}R$ are in 1-1 correspondence with the prime ideals of R that do not meet S.

Proof.

1. Let J be an ideal of $S^{-1}R$. Let $r/s \in J$, so then $r/1 \in J$.

   Let $I = \{r \in R : r/1 \in J\}$. Then $r \in I$. Clearly $J \subset S^{-1}I$. $If r \in I$ then $r/1 \in J$, and hence $r/s \in J$. So $S^{-1}I = J$.

2. Let Q be a prime in $S^{-1}R$. Then set $P = \{r \in R : r/1 \in Q\}$.

   P is prime: if $xy \in P$ then $xy/1 \in Q$, and so either $x/1$ or $y/1$ is in Q, and so $x \in P$ or $y \in P$.

   P does not meet S. If $r \in S \cap P$ then $r/1 \in Q$ and $1/r \in Q$, so $1 \in Q$, ⨳

   Conversely, if $r/s, x/y \in S^{-1}P$ then $rx/sy \in S^{-1}P$. So $z(rx) \in P$ for some $z \in S$. So $rx \in P$ since P is prime and $z \notin P$ (since $z \in S$). So $r \in P$ or $x \in P$. And so $r/s \in S^{-1}P$ or $x/y \in S^{-1}P$.

Lemma 2.6. If R is Noetherian then $S^{-1}R$ is Noetherian.

Proof. Any chain of ideals in $S^{-1}R$ if of the form $J_1 \leqslant J_2 \leqslant \ldots$.

Consider $I_k = \{r \in R : r/1 \in J_k\}$. Then $I_1 \leqslant I_2 \leqslant \ldots$.

This must terminate since R is Noetherian. So $I_t = I_{t+1} = \ldots$, for some t.

Then $J_t = J_{t+1} = \ldots$ since $J_k = S^{-1}I_k$ for each k. □

Definition 2.7. A property $\mathcal{P}$ of a ring R (or an R-module M) is **local** if R (or M) has property $\mathcal{P} \iff R_P$ (or M_P) has property $\mathcal{P}$ for each prime ideal P of R.

Lemma 2.8. The following are equivalent:

(i) $M = 0$.

(ii) $M_P = 0$ for all prime ideals P of R.

(ii) $M_Q = 0$ for all prime ideals Q of R.

Proof. It's clear that (i) $\implies$ (ii) $\implies$ (iii).

Suppose (iii) holds, but that $M \neq 0$. Take $0 \neq m \in M$. The annihilator of m is a proper ideal of R. It is therefore contained in a maximal ideal by Zorn's lemma.

Consider $m/1 \in M_Q$. By assumption, $M_Q = 0$, so $m/1 = 0$. So $sm = 0$ for some $s \in S$, where $S = R \setminus Q$. This is a contradiction, since Q contains the annihilator of m. □

Lemma 2.9. Let $\varphi : M \to N$ be an R-module map. The following are equivalent:

(i) φ is injective.

(ii) $\varphi_P : M_P \to N_P$ is injective for all prime ideals P of R.

(iii) $\varphi_Q : M_Q \to N_Q$ is injective for all maximal ideals Q of R.

Proof. Exercise. □

Lecture 8

Lemma 2.10. Let P be a prime ideal of R and S be a multiplicatively closed subset of R with $S \cap P = \emptyset$. By 2.5, $S^{-1}P$ is a prime ideal of $S^{-1}R$.

Then $(S^{-1}R)_{S^{-1}P} \cong R_P$.

In particular, if Q is a prime ideal of R with $P \leqslant Q$, then $(R_Q)_{P_Q} \cong R_P$, by taking $S = R \setminus Q$.

Proof. We have ring homomorphisms $\theta_1 : R \to S^{-1}R$ and $\theta_2 : S^{-1}R \to (S^{-1}R)_{S^{-1}P}$.

Let $\varphi = \theta_2 \circ \theta_1$. Then φ is a ring homomorphism $R \to (S^{-1}R)_{S^{-1}P}$ with $\varphi(s)$ a unit for all $s \in S' = R \setminus P$.

So we can apply our universal property to give a unique ring homomorphism α

$$\begin{array}{ccc} R & \xrightarrow{\theta_P} & R_P \\ & \overset{\varphi}{\searrow} & \downarrow \alpha \\ & & (S^{-1}R)_{S^{-1}P} \end{array}$$

Now, α is surjective since all elements of $(S^{-1}R)_{S^{-1}P}$ are of the form $\varphi(r)\varphi(s')^{-1}$ for some $r \in R$, $s' \in S'$.

And α is injective. Suppose $r/' \in \ker \alpha \leqslant R_P$ with $s' \in S'$. Then $r/1 \in \ker \alpha$ and hence $r \in \ker \alpha$.

But if $\varphi(r) = 0$ then $(r/1)(x/y) = 0$ in $S^{-1}R$ for some $x/y \notin S^{-1}P$, and so $srx = 0$ for some $s \in S$, $x \notin P$. But $S \cap P = \emptyset$ and so $sx \notin P$ and we have $y \in S'$ such that $ry = 0$.

Hence $r/s' \in R_P$ is zero in R_P. □

3. Dimension

As always, R is a commutative ring with a 1.

Definition 3.1. The **spectrum** of R, denoted $\mathrm{Spec}(R)$, is $\{P : P \text{ a prime ideal of } R\}$.

Definition 3.2. The **length** of a chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \ldots \subsetneq P_n$$

is n. (Note: the numbering starts at 0.)

Definition 3.3. The **(Krull) dimension** of R, denoted $\dim R$, is

$$\sup\{n : \text{ there is a chain of prime ideals of length } n\}$$

if this exists, and is ∞ otherwise.

Definition 3.4. The **height** of $P \in \mathrm{Spec}(R)$, denoted $\mathrm{ht}(P)$, is

$$\sup\{n : \text{ there is a chain of prime ideals } P_0 \subsetneq \ldots \subsetneq P_n = P\}$$

Note. The 1-1 correspondence between primes with empty intersection with $R \setminus P$ and the prime of R_P shows that $\mathrm{ht}(P) = \dim R_P$.

Examples.

1. An Artinian ring (see example sheet 1) has dimension 0, since all prime ideals are maximal (exercise).

   Conversely, any Noetherian ring of dimension 0 is Artinian (exercise).

2. $\dim \mathbb{Z} = 1$. A chain of maximal length is of the form $(0) \subsetneq (p)$ where p is prime.

   $\dim k[X] = 1$, where k is a field.

   There are both examples of **Dedekind domains** (integrally closed domains of dimension 1 – see next chapter).

3. $\dim k[X_1, \ldots, X_n] \geqslant n$ since we have a chain of prime ideals

   $$0 \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$$

   In fact, $\dim k[X_1, \ldots, X_n] = n$ when k is a field. To prove this, we need to prove some results about the relationship between chains of prime ideals in subrings and chains in the whole ring under some condition relating the subring to the larger ring. First, though, observe the following.

Lemma 3.5. The height 1 primes of $k[X_1, \ldots, X_n]$ are precisely those of the form (f) where f is irreducible.

Proof. See question 3 on the example sheet.

(Height 1 primes in a unique factorisation domain are the principal ideals generated by an irreducible.) □

Definition 3.6. Let $R \subset S$ be rings. Then $x \in S$ is **integral over** R if is satisfies some monic polynomial with coefficients in R.

For example, the elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$ are precisely the elements of $\mathbb{Z}$.

Lemma 3.7. The following are equivalent:

(i) $x \in S$ is integral over R.

(ii) The ring $R[x]$ (the subring generated by R and x) is a finitely-generated R-module.

(iii) $R[x]$ is contained in a subring T of S with T being a finitely-generated R-module.

Remark. Some authors say that S is **finite over** R is S is a finitely-generated R-module, and a k-algebra R is of **finite type** if it is finitely generated as a k-algebra.

Proof of 3.7.

(i) $\Rightarrow$ (ii). If x satisfies $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$, then $x^{n-1}, \ldots, x, 1$ generate $R[x]$ as an R-module.

(ii) $\Rightarrow$ (iii). Trivial.

(iii) $\Rightarrow$ (i). Consider multiplication by x in the ring T, and take $y_1, \ldots, y_n$ to be R-module generators for T.

Then $xy_i = \sum_j r_{ij}y_j$ for each i, so $\sum_j (x\delta_{ij} - r_{ij})y_j = 0$.

Multiply on the left by the adjugate of the matrix $A_{ij} = (x\delta_{ij} - r_{ij})$, and dedice that $(\det A)y = 0$ for all y.

But 1 is an R-linear combination of the y_j, and so $\det A = 0$. But $\det A$ is of the form $x^n + r_{n-1}x^{n-1} + \ldots + r_0$. □

Remark. This proof is reminiscent of one proof often used for Nakayama's lemma.

Lecture 9

Lemma 3.8. If $x_1, \ldots, x_m \in S$ are integral over R, then $R[x_1, \ldots, x_m]$, the subring of S generated by R and $x_1, \ldots, x_m$ is a finitely-generated R-module.

Proof. Easy induction on m. □

Lemma 3.9. The set $T \subset S$ of elements integral over R forms a subring of S.

Proof. Clearly every element of R is integral over R. If $x, y \in T$ then by 3.8, $R[x, y]$ is a finitely-generated R-module.

So by 3.7(iii), we have that $x \pm y$ and xy are integral over R. □

Definitions 3.10.

T is the **integral closure** of R in S.

If $T = R$ then R is **integrally closed in** S.

If $T = S$ then S is **integral over** R.

If R is an integral domain then we just say that R is **integrally closed** if it is integrally closed in its field of fractions.

Examples.

$\mathbb{Z}$ is integrally closed.

$k[X_1, \ldots, X_n]$ is integrally closed.

In an algebraic number field K with $|K : \mathbb{Q}| < \infty$, the integral closure of $\mathbb{Z}$ in K is the ring of integers in K.

Lemma 3.11. If $R \subset T \subset S$ are rings with T integral over R, and S integral over T, then S is integral over R.

Proof. Exercise. □

Lemma 3.12. Let $R \subset T$ be rings with T integral over R.

(i) If J is an ideal of T then T/J is integral over $R/(J \cap R)$ (identifying $R/(J \cap R)$ with $(R + J)/J$, a subring of T/J).

(ii) If S is a multiplicatively closed subset of R, then $S^{-1}T$ is integral over $S^{-1}R$.

Proof.

(i) If $x \in T$ then $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$ for some $r_i \in R$.

Modulo J (writing $\bar{}$ for images in T/J), we have a monic equation

$$\bar{x}^n + \bar{r}_{n-1}\bar{x}^{n-1} + \ldots + \bar{r}_0 = \bar{0}$$

in T/J with $\bar{r}_i \in (R + J)/J$.

(ii) Suppose $x/s \in S^{-1}T$. Then x satisfies a monic polynomial equation as in (i).

So $(x/s)^n + (r_{n-1}/s)(x/s)^{n-1} + \ldots + (r_0/s^n) = 0$ in $S^{-1}T$.

So x/s is integral over $S^{-1}R$. □

Lemma 3.13. Suppose $R \subset T$ are integral domains with T integral over R.

Then T is a field if and only if R is a field.

Proof. Suppose that R is a field. Let $t \in T$ be non-zero, and choose a monic equation of least degree of the form $t^n + r_{n-1}t^{n-1} + \ldots + r_0 = 0$, with $r_i \in R$.

T is an integral domain, and so $r_0 \neq 0$ – otherwise we have $t(t^{n-1} + \ldots + r_1) = 0$, and then $t^{n-1} + \ldots + r_1 = 0$, contradicting the minimality of degree.

So t has a inverse, namely $-r_0^{-1}(t^{n-1} + \ldots + r_1) \in T$. So T is a field.

Conversely, suppose that T is a field. Let $x \in R$ be non-zero. Then x has inverse x^{-1} in T.

So x^{-1} satisfies a monic equation $x^{-m} + r'_{m-1}x^{-m+1} + \ldots + r'_0 = 0$.

Rearrange for a formula for x^{-1}, and note that it is in R. Thus R is a field. □

Lemma 3.14. Let $R \subset T$ be rings with T integral over R. Let Q be a prime ideal of T and set $P = R \cap Q$.

Then Q is maximal if and only if P is maximal.

Proof. By 3.12(i), T/Q is integral over R/P, and since P and Q are prime, we have that T/Q and R/P are integral domains.

So 3.13 implies that T/Q is a field $\iff$ R/P is a field.

So Q is maximal $\iff$ P is maximal. □

Theorem 3.15 (Incomparability theorem). Let $R \subset T$ be rings with T integral over R. Let $Q \leqslant Q_1$ be prime ideals of T.

Suppose that $Q \cap R = P = Q_1 \cap R$. Then $Q = Q_1$.

Proof. Apply 3.12(ii) with $S = R \setminus P$. We have T_P integral over R_P (with abuse of notation: $T_P = S^{-1}T$).

From Chapter 2 we have that there is a prime $S^{-1}P$ in R_P which is the unique maximal ideal of R_P, and that there are $S^{-1}Q$ and $S^{-1}Q_1$ in T_P which are also prime and $S^{-1}Q \cap S^{-1}R = S^{-1}P = S^{-1}Q_1 \cap S^{-1}R$.

By 3.14, $S^{-1}Q$ and $S^{-1}Q_1$ are maximal, since $S^{-1}P$ is. But $S^{-1}Q \leqslant S^{-1}Q_1$ and so $S^{-1}Q = S^{-1}Q_1$.

But the 1-1 correspondence between prime ideals of $S^{-1}T$ and those of T that do not meet S tells us that $Q = Q_1$. □

Theorem 3.16 (Lying Over Theorem). Let $R \subset T$ be rings with T integral over R. Let P be a prime ideal of R.

Then there is a prime ideal Q of T with $Q \cap R = P$. (I.e., Q 'lies over' P.)

Proof. By 3.12(ii), T_P is integral over R_P with $S = R \setminus P$.

Take a maximal ideal of T_P. It must be of the form $S^{-1}Q$ for some ideal Q of T, which is necessarily prime (because primality is preserved under the 1-1 correspondence).

Then $S^{-1}Q \cap S^{-1}R$ is maximal by 3.14. But $R_P = S^{-1}P$ has a unique maximal ideal, namely $S^{-1}P$, and so $S^{-1}Q \cap S^{-1}R = S^{-1}P$.

Therefore, $Q \cap R = P$. □

Lecture 10

We next have two theorems due to Cohen and Seidelberg (1946) that allow us to move from chains of prime ideals in R to chains of prime ideals in T, where $R \subset T$ are rings with T integral over R. However, the second one requires stronger conditions.

Theorem 3.17 (Going Up Theorem). Let $R \subset T$ be rings with T integral over R. Let $P_1 \leqslant \ldots \leqslant P_n$ be a chain of prime ideals of R, and $Q_1 \leqslant \ldots \leqslant Q_m$, with $m < n$, be a chain of prime ideals of T with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant m$.

Then the chain of Q's extends to a chain $Q_1 \leqslant \ldots \leqslant Q_n$ with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant n$.

Theorem 3.18 (Going Down Theorem). Let $R \subset T$ be integral domains, with R integrally closed, and T integral over R.

Let $P_1 \geqslant \ldots \geqslant P_n$ be a chain of prime ideals of R, and $Q_1 \geqslant \ldots \geqslant Q_m$, with $m < n$, be a chain of prime ideals of T with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant m$.

Then the chain of Q's extends to a chain $Q_1 \geqslant \ldots \geqslant Q_n$ with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant m$.

One major application of these is in the context of finitely-generated k-algebras T assume T is an integral domain). Noether normalisation yields $R \subset T$ with T integral over R and R isomorphic to a polynomial algebra, hence integrally closed.

Proof of Going Up. By induction, it's enough to consider the case $n = 2$, $m = 1$.

Write $\overline{R}$ for R/P_1 and $\overline{T} = T/Q_1$. Then $\overline{R} \hookrightarrow \overline{T}$ with $\overline{T}$ integral over $\overline{R}$ (using $Q_1 \cap R = P_1$), using 3.12(ii).

By the Lying Over Theorem, there is a prime $\overline{Q}_2$ of $\overline{T}$ such that $\overline{Q}_2 \cap \overline{R} = \overline{P}_2$.

Lifting back gives a prime ideal Q_2 of T with $Q_2 \geqslant Q_1$ and $Q_2 \cap R = P_2$. □

Corollary 3.19 (Corollary of Going Up). Let $R \subset T$, with T integral over R. Then $\dim R = \dim T$.

Proof. Take a chain $Q_0 \subsetneq Q_1 \subsetneq \ldots \subsetneq Q_n$ of primes in T. Intersecting with R gives a (strict) chain $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n$ of primes in R with $Q_i \cap R = P_i$. Thus $\dim R \geqslant \dim T$.

Conversely, suppose $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n$ is a chain of primes in R. There is a prime Q_0 lying over P_0 by (3.16), and Going Up (3.17) gives a (strict) chain $Q_0 \leqslant Q_1 \leqslant \ldots \leqslant Q_n$ with $Q_i \cap R = P_i$. So $\dim R \leqslant \dim T$. □

Corollary 3.20 (Corollary of Going Down). Let $R \subset T$ be integral domains with R integrally closed and T integral over R. Let Q be a prime of T.

Then $\mathrm{ht}(Q \cap R) = \mathrm{ht}(R)$.

Proof. Take a chain $Q_0 \subsetneq Q_1 \subsetneq \ldots Q_n = Q$ in $\mathrm{Spec}(T)$. As above, there is a chain $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n = Q \cap R$ with $Q_i \cap R = P_i$. So $\mathrm{ht}(Q \cap R) \geqslant \mathrm{ht}(Q)$.

Conversely, if $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n = Q \cap R$, then Going Down (3.18) yields $Q_0 \subsetneq Q_1 \subsetneq \ldots Q_n = Q$ with $Q_i \cap R = P_i$. So $\mathrm{ht}(Q \cap R) \leqslant \mathrm{ht}(Q)$. □

The proof of the Going Down Theorem requires a couple of lemmas and a bit of knowledge of field theory (Galois Theory).

Definition 3.21. If I is an ideal of R, and $R \subset T$, then $x \in T$ is **integral over** I if x satisfies a monic equation $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$ with $r_i \in I$. The **integral closure of** I **in** T is the set of such x.

Lemma 3.22. Let $R \subset T$ be rings with T integral over R. Let I be an ideal of R.

Then the integral closure of I in T is the radical $\sqrt{TI}$ (observe that TI is an ideal of T) and is thus closed under addition and multiplication.

In particular, if $R = T$, then the integral closure of I in R is $\sqrt{I}$.

Proof. If x is integral over I. Then the definition in 3.21 implies that $x^n \in TI$ and thus $x \in \sqrt{TI}$.

Conversely, if $x \in \sqrt{TI}$ then $x^n = \sum_{i=1}^{k} t_i r_i$ for some $r_i \in I$, $t_i \in T$. But each t_i is integral over R, and so (3.8) shows that $M = R[t_1, \ldots, t_n]$ is a finitely-generated R-module. Also, $x^n R[t_1, \ldots, t_n] \subset IM$.

Let $y_1, \ldots, y_s$ be a generating set of M as an R-module. Then we have $x^n y_j = \sum_\ell r_{j\ell} y_\ell$ with $r_{j\ell} \in I$.

As in the proof of (3.7), we get $\sum_\ell (x^n \delta_{j\ell} - r_{j\ell}) y_\ell = 0$, and we deduce that x^n satisfies a monic equation $(x^n)^s + \ldots + r'_0 = 0$, namely $\det A = 0$. Note that all but the top coefficient are in I. Thus x is integral over I. □

Lecture 11

Lemma 3.23. Let $R \subset T$ be integral domains, with R integrally closed, and let $x \in T$ be integral over an ideal I in R.

Then x is algebraic over the field of fractions K of R, and its minimal polynomial over K, say

$$X^n + r_{n-1} X^{n-1} + \ldots + r_0 \qquad (*)$$

has its coefficients $r_{n-1}, \ldots, r_0$ in $\sqrt{I}$.

Proof. Certainly x is algebraic over K (from the integrality of x over R).

Claim. The coefficients r_i in $(*)$ are integral over I.

Proof. Take an extension field L of K containing all of the conjugates $x_1, \ldots, x_n$ of x – e.g., a splitting field of $(*)$.

There is[1] a K-automorphism of L sending x to x_i and so if $x^m + r'_{m-1} x^{m-1} + \ldots + r'_0 = 0$ with $r'_i \in I$, then $x_i^m + r'_{m-1} x_i^{m-1} + \ldots + r'_0 = 0$.

Thus each x_i is integral over I, and each in particular lies in the integral cosure T_1 of R in L.

Then (3.12) implies that a polynomial in the x_i with coefficients in $\mathbb{Z}$ will also be integral over I. But the coefficients of the minimal polynomial of x over K are of this form by the usual theory linking coefficients to roots of polynomials. So we have established the claim.

Thus the r_i are in R since R is integrally closed, and by (3.22) with $T = R$, we have the $r_i \in \sqrt{I}$, since they lie in the integral closure of I in R. □

Proof of 3.18 (Going Down Theorem). By induction, it's enough to look at the case $n = 2$, $m = 1$.

So we have $P_1 \supsetneq P_2$, and Q_1 with $Q_1 \cap R = P_1$. We want to find Q_2 with $Q_1 \supsetneqq Q_2$ and $Q_2 \cap R = P_2$.

[1] See, for example, Proposition 10.2 in *Galois Theory* by Stewart.

Let $S_2 = R \setminus P_2$ and $S_1 = T \setminus Q_1$, and set $S = S_1 S_2 = \{rt : r \in S_1, t \in S_2\}$. Then S is multiplicatively closed and contains both S_1 and S_2.

For now, assume that $TP_2 \cap S = \emptyset$.

TP_2 is an ideal of T, and so $S^{-1}(TP_2)$ is an ideal of $S^{-1}T$, which is proper by our assumption that $TP_2 \cap S = \emptyset$. Hence TP_2 lies in a maximal ideal of $S^{-1}T$, which is necessarily of the form $S^{-1}Q_2$ for some prime ideal Q_2 of T with $Q_2 \cap S = \emptyset$ and $TP_2 \leqslant Q_2$ (since $S^{-1}(TP_2) \leqslant S^{-1}Q_2$).

Hence $P_2 \leqslant TP_2 \cap R \leqslant Q_2 \cap R$ and since $Q_2 \cap S = \emptyset$ and $S_2 = R \setminus P_2 \subset S$ we have $P_2 = Q_2 \cap R$.

Similarly, $S_1 = T \setminus Q_1 \subset S$ and $Q_2 \leqslant Q_1$, as desired.

It remains to prove our assumption that $TP_2 \cap S = \emptyset$.

Take $x \in TP_2 \cap S$. By (3.22) with $I = P_2$, we find x is in the integral closure of P_2 in T. So by (3.22) it is algebraic over the field of fractions K of R and its minimal polynomial $X^n + r_{n-1}X^{n-1} + \ldots + r_0$ over K has coefficients in P_2 (since $\sqrt{P_2} = P_2$ as P_2 is prime).

But $x \in S$ and so x is of the form rt with $r \in S_2$ and $t \in S_1$, so $t = x/r$ has minimal polynomial $X^n + \frac{r_{n-1}}{r}X^{n-1} + \ldots + \frac{r_0}{r^n}$ over K, and these coefficients are in R (using (3.23) with $I = R$), since $t \in T$ is integral over R.

Write these coefficients as r_i' $(i = 0, \ldots, n-1)$. But $r_i \in P_2$ and $r \notin P_2$, so $r_i' \in P_2$. So, by definition, t is integral over P_2, and so by (3.22), we find t is in $\sqrt{TP_2}$. This is a contradiction, since $t \in S_1 = T \setminus Q_1$ and $TP_2 \subset Q_1$, and hence $\sqrt{TP_2} \subset Q_1$. □

We now concentrate on finitely-generated k-algebras – some authors call these affine algebras.

Theorem 3.24. Let T be a finitely-generated k-algebra, which is an integral domain with fraction field L.

Then $\dim(T) = \text{tr.deg}(L)$, where $\text{tr.deg}(L)$ is the transcendence degree of L (over k).

What is transcendence degree?

Say that $x_1, \ldots, x_n$ be **algebraically independent** over a field k if the map $k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$ given by $X_i \mapsto x_i$ is an isomorphism, and thus $k[x_1, \ldots, x_n]$ may be regarded as a polynomial algebra.

As in linear algebra, one wants to consider maximal algebraically independent sets – they all have the same cardinality. Such a set is a **transcendence basis** of L over k, and that the **transcendence degree** is the cardinality.

linearly independent set	$\longleftrightarrow$	algebraically independent set
span $\langle S \rangle$	$\longleftrightarrow$	algebraic closure of S
spanning set	$\longleftrightarrow$	S whose algebraic closure is L

(where the 'algebraic closure of S' is the set of elements in L which are algebraically dependent over the field generated by k and S).

Example. Let $L = k(X_1, \ldots, X_n)$ be the fraction field of $k[X_1, \ldots, X_n]$, and f be an irreducible in $k[X_1, \ldots, X_n]$, and K be the fraction field of $k[X_1, \ldots, X_n]/(f)$.

Then $\mathrm{tr.deg}_k(L) = n$ and $\mathrm{tr.deg}_k(K) = n - 1$, since K is an algebraic extension of $k(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ where X_i appears in some term in f.

The key result in proving the theorem is:

Lemma 3.25 (Noether's Normalisation Lemma). Let T be a finitely-generated k-algebra. Then T is integral over some subring $R = k[X_1, \ldots, X_n]$ with $X_1, \ldots, X_n$ algebraically independent.

Lecture 12

Proof. Let $T = k[a_1, \ldots, a_n]$. The proof is by induction on n, the number of generators.

Let r be the maximum number of algebraically independent elements. Observe that we may assume $r \geqslant 1$, as otherwise T is a finite-dimensional vector space.

There is nothing to do if $a_1, \ldots, a_n$ are algebraically independent. So renumber the a_i so that $a_1, \ldots, a_r$ are algebraically independent, and $a_{r+1}, \ldots, a_n$ are algebraically dependent on $a_1, \ldots, a_r$.

Take non-zero $f \in k[X_1, \ldots, X_r, X_n]$ with $f(a_1, \ldots, a_r, a_n) = 0$. Then $f(X_1, \ldots, X_r, X_n)$ is a sum of terms $\lambda_{\underline{\ell}} X_1^{\ell_1} \ldots X_r^{\ell_r} X_n^{\ell_n}$ where $\underline{\ell} = (\ell_1, \ldots, \ell_r, \ell_n)$ an $(r+1)$-tuple.

Claim. There are positive integers $m_1, \ldots, m_r$ such that $\varphi : \underline{\ell} \mapsto m_1\ell_1 + \ldots + m_r\ell_r + \ell_n$ is 1-1 for those $\underline{\ell}$ with $\lambda_{\underline{\ell}} \neq 0$.

Proof of claim. There are finitely many possibilities for differences $\underline{d} = \underline{\ell} - \underline{\ell}'$ with $\lambda_{\underline{\ell}} \neq 0 \neq \underline{\ell}'$.

Write $\underline{d} = (d_1, \ldots, d_r, d_n)$ and consider the finitely many non-zero $(d_1, \ldots, d_r) \in \mathbb{Z}^r$ obtained.

Vectors in $\mathbb{Q}^r$ orthogonal to one of these lie in finitely many $(r-1)$-dimensional subspaces. Put $(q_1, \ldots, q_r) \in \mathbb{Q}^r$ with each $q_i > 0$ so that $\sum q_i d_i \neq 0$ for all of the finitely many nonzero $(d_1, \ldots, d_r)$.

Multiply by a positive integer to get $(m_1, \ldots, m_r)$ with $m_i \in \mathbb{Z}_{>0}$ so that $\left|\sum m_i d_i\right| > |d_n|$ for all of the finitely many differences $\underline{d}$ with $(d_1, \ldots, d_r) \neq 0$.

Thus if $\varphi(\underline{\ell}) = \varphi(\underline{\ell}')$ then $d_1 = \ldots = d_r = 0$, and so $\ell_n = \ell_n'$ and so $\underline{\ell} = \underline{\ell}'$.

Now, for these $m_1, \ldots, m_r$, set $g(X_1, \ldots, X_r, X_n) = f(X_1 + X_n^{m_1}, \ldots, X_r + X_n^{m_r}, X_n)$.

This is a sum $\displaystyle\sum_{\underline{\ell}:\lambda_{\underline{\ell}} \neq 0} \lambda_{\underline{\ell}} (X_1 + X_n^{m_1})^{\ell_1} \ldots (X_r + X_n^{m_r})^{\ell_r} X_n^{\ell_n}$.

Different terms have different powers of X_n, and so there will be a single term with the highest power of X_n. As a polynomial in X_n, the leading coefficient is therefore one of the $\lambda_{\underline{\ell}}$ and is therefore in k.

Put $b_i = a_i - a_n^{m_i}$ for $1 \leqslant i \leqslant r$, and $h(X_n) = g(b_1, \ldots, b_r, X_n)$.

This has leading coefficient in k and all coefficients are in $k[b_1, \ldots, b_r]$. Moreover,

$h(a_n) = g(b_1, \ldots, b_r, a_n) = f(a_1, \ldots, a_r, a_n) = 0.$

Dividing through by the leading coefficients shows tht a_n is integral over $k[b_1, \ldots, b_r]$. So for each i with $1 \leqslant i \leqslant r$, we have that $a_i = b_i + a_n^{m_i}$ is also integral over $k[b_1, \ldots, b_r]$.

Hence T is integral over $k[b_1, \ldots, b_r, a_{r+1}, \ldots, a_{n-1}]$, and we may apply the inductive hypothesis to this subring with fewer generators. □

We'll now use Noether's Normalisation Lemma to prove (3.24).

Proof of 3.24. Let T be a finitely-generated k-algebra. Apply (3.25) to get $x_1, \ldots, x_r$ algebraically independent with T integral over $k[x_1, \ldots, x_r]$ ($\cong$ a polynomial algebra).

By (3.19), $\dim T = \dim k[x_1, \ldots, x_r]$. Thus any finitely-generated k-algebra has dimension equal to that of a polynomial algebra with r variables, with tr.deg(fraction field of T) $= r$.

So we need to show that $\dim k[x_1, \ldots, x_r] = r$.

Recall from the earlier example that $\dim k[x_1, \ldots, x_r] \geqslant r$.

We prove equality by induction on r. If $r = 0$, done, so assume $r \geqslant 1$.

Take $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_s$, a chain of prime ideals. We may assume that $P_0 = 0$, and since P_1 contains (f), for some irreducible f (since $k[x_1, \ldots, x_r]$ is a UFD – sheet 1, question 3), we may assume $P_1 = (f)$.

But tr.deg $\big($ff.$k[x_1, \ldots, x_r]/(f)\big) = r - 1$. So $\dim k[x_1, \ldots, x_r]/(f) = \dim k[Y_1, \ldots, Y_{r-1}]$ for some polynomial algebra with $r - 1$ variables, and this is $r - 1$ by induction.

But $P_1 = (f)$, and $P_1/P_1 \subsetneq P_2/P_1 \subsetneq \ldots \subsetneq P_s/P_1$ is a chain of length $s - 1$, so $s - 1 \leqslant r - 1$. And so $s \leqslant r$. Thus $\dim k[x_1, \ldots, x_r] = r$. □

Corollary 3.26. Let Q be a prime ideal of T, a finitely-generated k-algebra which is an integral domain, with $\dim T = n$.

Then $\mathrm{ht}(Q) + \dim(T/Q) = n$.

Proof. Let $m = \mathrm{ht}(Q)$ and take a prime chain $Q_0 \subsetneq Q_1 \subsetneq \ldots \subsetneq Q_m = Q$.

By Noether Normalisation (3.25), there is a subalgebra $R \cong$ polynomial algebra, with T integral over R. By (3.19), $\dim T = \dim R$, and by (3.24), $n = \dim R = \mathrm{tr.deg}\, R =$ number of variables in this polynomial algebra.

Write $P_i = Q_i \cap R$. Observe that $\mathrm{ht}(Q_1) = 1$, as otherwise we could find a longer chain.

So, by (3.20) (Corollary of Going Down), since R is integrally closed (as it is a polynomial algebra), we have $\mathrm{ht}(P_1) = 1$.

So $P_1 = (f)$, with f irreducible, as R is a UFD. And so tr.deg(ff.R/P_1) $= n - 1$. Hence $\dim R/P_1 = n - 1$ by (3.24).

Now we want to apply induction to the prime Q/Q_1 in T/Q_1.

First, $\mathrm{ht}(Q/Q_1) = m-1$. Second, $\dim(T/Q_1) = \dim(R/P_1) = n-1$, since R/P_1 embeds in T/Q_1 as $(R+Q_1)/Q_1$, and T/Q_1 is integral over it. And third, $\dim((T/Q_1)/(Q/Q_1)) = \dim(T/Q)$.

So induction gives $(m-1) + \dim(T/Q) = n-1$, and hence $\mathrm{ht}(Q) + \dim(T/Q) = n$. □

Lecture 13

Remarks.

1. If $k = \mathbb{C}$ then the maximal ideals of $k[x_1, \ldots, x_r]$ are of the form $P = (X_1 - a_1, \ldots, X_r - a_r)$ by the Nullstellensatz, and so they correspond to the points of $\mathbb{C}^r$.

   But T/TP is finite dimensional over $\mathbb{C}$ since T is a finitely-generated $k[x_1, \ldots, x_r]$-module (integrality of T over R).

   So T/TP is Artinian and hence only has finitely many primes, which are all maximal. They correspond to the maximal ideals of T lying over P.

   Thus there is a map

   $$f : \{\text{maximal ideal of } T\} \longrightarrow \{\text{maximal ideals of } k[x_1, \ldots, x_r]\} \cong \mathbb{C}$$

   given by $Q \mapsto P$, with each fibre $f^{-1}(P)$ being non-empty and finite.

2. In fact, if T is a finitely-generated k-algebra which is an integral domain, then its integral closure T_1 in its fraction field L is a finitely-generated T-module (and hence Noetherian). Take $k = \mathbb{C}$.

   $$g : \{\text{maximal ideals of } T_1\} \longrightarrow \{\text{maximal ideals of } T\}$$

   The fibres $g^{-1}(Q)$ are finite and non-empty (for curves, normal variety ≡ non-singular).

Lemma 3.27. *R a Noetherian integral domain, integrally closed. K the fraction field of R.*

Let L be a finite degree separable field extension of K. Let T_1 be the integral closure of R in L. Then T_1 is finitely generated as an R-module.

Corollary. If $R = \mathbb{Z}$, then the integral closure of $\mathbb{Z}$ in an algebraic number field L is a finitely-generated $\mathbb{Z}$-module.

Sketch proof of 3.27. This uses the trace function $\mathrm{Tr}_{L/K}(x) = -|L : K(x)|$, the next-to-top coefficient in the minimal polynomial of x over K, for any finite degree field extension L of K.

Equivalently, if L is Galois over K, then $\mathrm{Tr}_{L/K}(x) = \sum_{g \in \mathrm{Gal}(L/K)} g(x)$, a sum of conjugates but potentially with repetitions (and hence getting a multiple of the relevant coefficient of the minimal polynomial).

Quote. E.g., in Reid. If L is separable, then

$$L \times L \to K, \quad (x, y) \mapsto \mathrm{Tr}(xy)$$

is a *non-degenerate* symmetric bilinear form.

Pick a K-vector space basis of L, say $y_1, \ldots, y_n$. By multiplying by suitable elements of K, we may assume that $y_i \in T_1$.

(If the minimal polynomial of y_i is $X^m + \frac{r_{m-1}}{s_{m-1}}X^{m-1} + \ldots + \frac{r_0}{s_0}$ with $\frac{r_i}{s_i} \in K$, then the minimal polynomial of $y_i / \prod s_j$ has coefficients in R.)

Since $\mathrm{Tr}(xy)$ yields a non-degenerate symmetric bilinear form, there is a basis $x_1, \ldots, x_n$ such that $\mathrm{Tr}(x_i y_j) = \delta_{ij}$.

Let $z \in T_1$. Then $z = \sum \lambda_i x_i$ with $\lambda \in K$. So $\mathrm{Tr}(zy_j) = \mathrm{Tr}(\sum \lambda_i x_i y_j) = \sum \lambda_i \delta_{ij} = \lambda_j$.

But z and y_j are in T_1, and hence zy_j is in T_1. By (3.23) (with $I = R$), the coefficients of the minimal polynomial of zy_j lie in R (using that R is integrally closed), and so $\mathrm{Tr}(zy_j) \in R$.

So $\lambda_j \in R$ for each j. Hence $T_1 \leqslant \sum Rx_i$, which is a Noetherian module, and so T_1 is a finitely-generated R-module. □

Krull's principal ideal theorem (1931) tells us about minimal primes over principal ideals.

Theorem 3.28 (Krull's principal ideal theorem). Let R be a Noetherian ring, and $a \in R$ a non-unit. Let P be a minimal prime over (a).

Then $\mathrm{ht}(P) \leqslant 1$.

This provides the inductive step for:

Theorem 3.29 (Generalised principal ideal theorem). Let R be a Noetherian ring, and I a proper ideal generated by n elements.

Then $\mathrm{ht}(P) \leqslant n$, for any minimal prime P over I.

Corollary 3.30.

(a) Each prime of a Noetherian ring has finite height.

(b) Every Noetherian local ring R has finite dimension $\leqslant$ the minimum number of generators of the unique maximal ideal P, which equals the dimension of P/P^2 as a vector space over R/P.

Proof of 3.30 from 3.29.

(a) Any prime ideal is minimal over itself and is finitely generated.

(b) For a local ring, $\dim R = \mathrm{ht}\, P$, where P is the unique maximal ideal. Apply (a) to get that $\dim R$ is finite.

By (3.29), $\mathrm{ht}\, P \leqslant$ minimum number of generators of P.

The final equality follows from Nakayama.

Claim: P is generated by $x_1, \ldots, x_n \iff P/P^2$ is generated by $\overline{x_1}, \ldots, \overline{x_n}$, where $^- : P \to P/P^2$.

($\Rightarrow$). Clear.

($\Leftarrow$). Suppose $\overline{x_1}, \ldots, \overline{x_n}$ generate P/P^2. Consider $I = (x_1, \ldots, x_n) \leqslant P$. Clearly $I + P^2 = P$ and so $P(P/I) = P/I$. Nakayama implies $P/I = 0$. □

Corollary 3.31. A Noetherian ring satisfies the descending chain condition (DCC) on prime ideals.

Proof. If we have a strictly descending chain $P \gneq \dots$ of prime ideals, then the chain can have length at most $\mathrm{ht}(P)$. Use (3.30)(a). □

Lecture 14

Definition 3.32. A **regular** local ring is one where $\dim R = \dim P/P^2$ (the R/P-vector space dimension), where P is the unique maximal ideal.

In fact, regular local rings are integral domains. In geometry, they correspond to localisations at *non-singular* points.

In Corollary (3.30), which said that the dimension of a Noetherian local ring is $\leqslant$ the minimum number of generators of the maximal ideal P, the inequality can be strengthened for Noetherian local domains, to say that the dimension of the ring = the minimum number of generators of some ideal I with $\sqrt{I} = P$.

Proof of 3.28 (Principal Ideal Theorem). Let P be a minimal prime over (a), where $a \in R$ is a non-unit. First localise at P to get R_P which has a unique maximal ideal $P_P = S^{-1}P$, where $S = R \setminus P$.

We observe that $S^{-1}P$ is a minimal prime over $S^{-1}(a)$. (This follows from the correspondence between ideal in R and in the localisation R_P.)

So we may assume that R is local with unique maximal ideal P.

Suppose $\mathrm{ht}\, P \geq 1$ and so there is a chain of primes $Q' \lneq Q \lneq P$.

Consider $R/(a)$. This has unique maximal ideal $P/(a)$. Moreover, it is also a minimal prime. So it is the only prime. So $N(R/(a)) = P/(a)$ is nilpotent. So $P^n \leqslant (a)$ for some n.

In the chain $R \gneq P \gneq P^2 \geq P^3 \gneq \dots$, each factor is a finite-dimensional R/P-vector space and hence Artinian. So R/P^n and hence $R/(a)$ is Artinian.

Now consider $I_n = \{r \in R : r/1 \in S^{-1}Q^n$, where $S = R \setminus Q$.

Clearly $Q = I_1 \geqslant I_2 \geqslant \dots$, and hence $(I_1 + (a))/(a) \geqslant (I_2 + (a))/(a) \geqslant \dots$ is a descending chain in $R/(a)$ which necessarily terminates: $I_m + (a) = I_{m+1} + (a)$ for some m.

Next we show that $Q = I_1 \geqslant I_2 \geqslant \dots$ terminates.

Let $r \in I_m$. Then $r = t + xa$ for some $t \in I_{m+1}$ and $x \in R$. So $xa = r - t \in I_m$. But $a \notin Q$, since P is the minimal prime over (a).

$Q = I_1 \geqslant I_m \geqslant Q^m$. So $x \in I_m$ since we have $S^{-1}R \geqslant S^{-1}Q \geqslant \dots \geqslant S^{-1}Q_m$, and if $x/1 \notin S^{-1}Q^m$ then $xa/1 \notin S^{-1}Q^m$.

So $I_m = I_{m+1} + I_m a$. Hence $I_m/I_{m+1} = P(I_m/I_{m+1})$ since $a \in P$. Nakayama implies that $I_m/I_{m+1} = 0$, and thus $I_m = I_{m+1}$.

Now, $(S^{-1}Q)^m = S^{-1}(Q^m) = S^{-1}I_m$ and $(S^{-1}Q^{m+1}) = S^{-1}(Q^{m+1}) = S^{-1}I_{m+1}$. So $(S^{-1}Q)^m = (S^{-1}Q)^{m+1}$.

Nakayama for the maximal ideal $S^{-1}Q$ of R_Q gives that $(S^{-1}Q)^m = 0$ in R_Q. The correspondence between primes under localisation gives $S^{-1}Q'$ is a prime $\leqslant S^{-1}Q$, contradiction. □

Proof of 3.29 (Generalised Ideal Theorem). We have R Noetherian, $I \lneq R$ generated by n elements. We are aiming to show that $\operatorname{ht} P \leqslant n$ for each minimal prime P over I.

We use induction on n. The case $n = 1$ is (3.28), the Principal Ideal Theorem. So assume $n > 1$.

We may assume by passing to R_P that R is local with unique maximal ideal P.

Pick any prime Q maximal subject to $Q \lneq P$, and thus P is the only prime strictly containing Q.

We show that $\operatorname{ht} Q \leqslant n-1$. It's enough to do this for all such Q as we then deduce that $\operatorname{ht} P \leqslant n$.

Since P is maximal over I, we have $Q \gneq I$. By assumption, there are generators $a_1, \ldots, a_n$ for I, and we may assume that $a_n \notin Q$. Now, P is the only prime containing $Q + (a_n)$, so as in the proof of (3.28) we have that $R/(Q + (a_n))$ is Artinian, and note that the maximal ideal of an Artinian local ring is nilpotent.

So there is m such that $a_i^m \in Q + (a_n)$ for all $1 \leqslant i \leqslant n-1$. So $a_i^m - x_i + r_i a_n$ for some $x_i \in Q$ and $r_i \in R$.

Any prime of R which contains $x_1, \ldots, x_{n-1}$ and a_n contains $a_1, \ldots, a_n$. Note that $(x_1, \ldots, x_{n-1}) \subset Q$ since $x_i \in Q$.

Claim. $\overline{Q}$ is a minimal prime of $\overline{R}$, where $\overline{R} = R/(x_1, \ldots, x_{n-1})$. (Write $^-$ for images in $\overline{R}$.)

Proof of claim. The unique maximal ideal $\overline{P}$ of $\overline{R}$ is a minimal prime over $\overline{(a_n)}$.

Apply the Principal Ideal Theorem to $\overline{P}$. So $\operatorname{ht} \overline{P} \leqslant 1$ and thus $\overline{Q}$ must be of height 0. Thus $\overline{Q}$ is a minimal prime of $\overline{R}$.

From the claim, we can apply the inductive hypothesis to Q to get $\operatorname{ht} Q \leqslant n-1$. □

We consider filtrations by powers of ideals I. That is, $R > I \geqslant I^2 \geqslant I^3 \geqslant \ldots$.

This is an example of a more general situation where one filters a ring R by R_i satisfying $R_i R_j \leqslant R_{i+j}$. Here, $R_j = I^j$. We will form the graded ring $\operatorname{gr}(R) = \bigoplus_{i \in \mathbb{N}} R_i/R_{i-1}$.

Lecture 15

Filtrations

Definition 3.33. A **($\mathbb{Z}$-)filtered ring** R is one whose additive group is filtered by subgroups

$$\ldots \subset R_{-1} \subset R_0 \subset R_1 \subset R_2 \subset \ldots$$

with R_i additive subgroups such that $1 \in R_0$ and $R_i R_j \subset R_{i+j}$ for $i, j \in \mathbb{Z}$.

We have that $\bigcup R_i$ is a subring and $\bigcap R_i$ is an ideal of $\bigcup R_i$. We shall assume, as is usual, that $\bigcup R_i = R$ ('exhaustive') and $\bigcap R_i = \{0\}$ ('separated').

For $i < 0$, R_i are ideals of R_0.

Examples.

1. The I-adic filtration. Take I an ideal of R, and define $R_i = I^{-i}$ for $i < 0$, and $R_i = R$ for $i \geqslant 0$.

2. R a k-algebra generated by $x_1, \ldots, x_n$. Define $R_i = 0$ for $i < 0$, and $R_0 = k.1$, and $R_i =$ the subspace spanned by polynomial expressions in the x_j of total degree $\leqslant i$.

Definition 3.34. The **associated graded ring** is $\mathrm{gr}(R) = \bigoplus R_i/R_{i-1}$ as an additive group with multiplication $(r + R_{i-1})(s + R_{j-1}) = rs + R_{i+j-1}$ for $r \in R_i$, $s \in R_j$.

Notation. Often books refer to the **symbol** of $r \in R_i/R_{i-1}$, namely $\sigma(r) = r + R_{i-1}$.

Definition 3.35. A **($\mathbb{Z}$-)graded ring** is a ring S with additive subgroups S_i such that $S = \bigoplus S_i$, with $S_i S_j \subset S_{i+j}$ for $i, j \in \mathbb{Z}$.

S_i is the $i^{\mathbf{th}}$ **homogeneous component**.

S_0 is a subring, and the S_i are S_0-modules.

A **graded ideal** I is of the form $I = \bigoplus I_i$ with $I_i \subset S_i$.

Note. For such an I, if it is finitely generated then it can be generated by a finite set of homogenous elements.

Definition 3.36. Let R be a filtered ring with filtration $\{R_i\}$, and let M be an R-module.

Then M is a **filtered R-module** if there is a compatible filtration $\{M_i\}$ of M consisting of additive subgroups such that $R_i M_j \subset M_{i+j}$.

Definition 3.37. The **associated graded module** of a filtered R-module is $\mathrm{gr}(M) = \bigoplus M_i/M_{i-i}$ as additive groups.

It is a graded $\mathrm{gr}(R)$-module, via $(r + R_{i-1})(m + M_{j-1}) = rm + M_{i-j-1}$.

If $S = \bigoplus S_i$ is a graded ring, then a **graded S-module** V is of the form $\bigoplus V_j$ with $S_i V_j \subset V_{i+j}$.

Given a filtered R-module M with filtration $\{M_i\}$ and N an R-submodule of M, there are induced filtrations $\{N \cap M_i\}$ of N, and $\{(N + M_i)/N\}$ of M/N.

The inclusion $N \subset M$ allows the definition $\varphi_i : (N \cap M_i)/(N \cap M_{i-1}) \to M_i/M_{i-1}$.

Putting these together gives a map of additive groups $\varphi : \bigoplus (N \cap M_i)/(N \cap M_{i-1}) \to \bigoplus M_i/M_{i-1}$, i.e. $\mathrm{gr}(N) \to \mathrm{gr}(M)$. This is a $\mathrm{gr}(R)$-module homomorphism.

Consider $(N + M_i)/N \cong M_i/(N \cap M_i)$.

Factor in induced filtration in quotient: $\Big((N + M_i)/N\Big)/\Big((N + M_{i-1})/N\Big) \cong M_i/\Big(M_{i-1} + (N \cap M_i)\Big)$.

There is a canonical map $M_i/M_{i-1} \to M_i/\Big(M_{i-1} + (N \cap M_i)\Big)$.

Which yields: $\pi_i : M_i/M_{i-1} \to \Big((N + M_i)/N\Big)/\Big((N + M_{i-1})/N\Big)$.

Putting these together gives $\pi \operatorname{gr}(M) \to \operatorname{gr}(M/N)$. Check that this is a $\operatorname{gr}(R)$-module homomorphism.

That bit went too fast for me in the lectures, so I might have copied things down incorrectly... I'll check later.

Lemma 3.38. If $N \leqslant M$, a filtered R-module, then

$$0 \longrightarrow \operatorname{gr}(N) \xrightarrow{\varphi} \operatorname{gr}(M) \xrightarrow{\pi} \operatorname{gr}(M/N) \longrightarrow 0$$

is exact when N and M/N are endowed with the filtrations induced by that of M.

Proof. $\ker \pi_i = \Big(M_{i-1} + (N + M_i)\Big)/M_{i-1} \cong (N \cap M_i)/(N \cap M_{i-1})$.

So we have that

$$0 \longrightarrow (N \cap M_i)/(N \cap M_{i-1}) \xrightarrow{\varphi_i} M_i/M_{i-1} \xrightarrow{\pi_i} \Big((N+M_i)/N\Big)/\Big((N+M_{i-1})/N\Big) \longrightarrow 0$$

is exact. Put these together. □

Definition 3.39. Let R be a filtered ring, with filtration $\{R_i\}$.

The **Rees ring** E of the filtration is the subring $\bigoplus_{i \in \mathbb{Z}} R_i T^i$ of the Laurent polynomial ring $R[T, T^{-1}]$.

Since $R_i R_j \subset R_{i+j}$, we have that E is a graded ring. The homogenous components are $R_i T^i$ of degree i.

Observe that

(a) $E/(T) \cong \operatorname{gr}(R)$, where (T) is the ideal generated by T.

(b) $E/(1-T) \cong R$, since $(1-T)$ is the kernel of the map $E \to R$ given by $\sum r_i T^i \mapsto \sum r_i$.

Thus, if E is Noetherian then R and $\operatorname{gr}(R)$ are Noetherian.

Example. R Noetherian, the I-adic filtration, $R_j = I^{-j}$ for $j > 0$.

So I is finitely generated by $x_1, \ldots, x_n$, say. Then $E = \bigoplus R_i T^i$ is generated as a ring by R_0, T and $x_1 T^{-1}, \ldots, x_n T^{-1}$.

So E is a ring image of $R[Z_0, Z_1, \ldots, Z_n]$, and so E is Noetherian.

Definition 3.40. The **associated Rees module** $\operatorname{Re}(M) = \bigoplus T^i M_i$ for a filtered R-module M.

It is an E-module via $(\sum r_j T^j)(T^i m_i) = \sum T^{i+j}(r_j m_i)$.

For $N \subset M$, given the induced filtrations, (3.38) implies that $\operatorname{Re}(M/N) = \operatorname{Re}(M)/\operatorname{Re}(N)$.

Definition 3.41. A filtration of M is **good** if $\mathrm{Re}(M)$ is a finitely-generated E-module.

Lemma 3.42. Let $N \subset M$, with $\{M_i\}$ a good filtration. If E is Noetherian then the induced filtrations of N and M/N are also good.

Proof. $\mathrm{Re}(N)$ is an E-submodule of $\mathrm{Re}(M)$. But $\mathrm{Re}(M)$ is a finitely-generated E-module and hence is Noetherian. So $\mathrm{Re}(N)$ is finitely generated.

$\mathrm{Re}(M/N) \cong \mathrm{Re}(M)/\mathrm{Re}(N)$ is also finitely generated.

So the induced filtrations of N and M/N are both good. □

If a filtration is good, then $\mathrm{Re}(M)$, as a finitely-generated E-module, is generated by a finite set of homogeneous elements $T^{k_1}m_{k_1}, \ldots, T^{k_n}m_{k_n}$, say with $m_{k_i} \in M$. So the i^{th} homogeneous component $T^iM_i = R_{i-k_1}T^{i-k_1}(T_{k_1}m_{k_1}) + \ldots + R_{i-k_n}T^{i-k_n}(T_{k_n}m_{k_n})$, and so $M_i = R_{i-k_1}m_{k_1} + \ldots + R_{i-k_n}m_{k_n}$ for these $m_{k_i} \in M$.

Example. For a finitely-generated R-module M with R Noetherian, $M_i = I^{-i}M$ for $i < 0$. Take $N \leqslant M$. We deduce from Lemma 3.42 that the induced filtration $\{N \cap I^{-i}M\}$ is a good filtration of M.

So there is a generating set $n_{k_1}, \ldots, n_{k_n}$ of N, negative integers k_i, with $n_{k_i} \in N \cap I^{-k_i}M$ and $N_nI^{-i}M = I^{-i+k_1}n_{k_1} + \ldots + I^{-i+k_n}n_{k_n}$.

So for $i \leqslant \min\{k_i\} = k$, $N \cap I^{-i}M = I^{-i+k}(M \cap I^{-k}M)$, for $i \leqslant k \leqslant 0$.

Set $a = -i$, $c = -k$.

Theorem 3.43 (Artin-Rees Lemma, 1956). Let R be Noetherian. Given $N \leqslant M$, finitely-generated R-modules,and I an ideal of R. Then there exists $c \geqslant 0$ such that $N \cap I^aM = I^{a-c}(N \cap I^cM)$ for $a \geqslant c$.

Proof. Above example.

Back to dimension

Suppose R is a finitely-generated k-algebra, which is an integral domain, and I an ideal. Form the I-adic filtration and its Rees ring E. Then E is a finitely-generated k-algebra which is an integral domain.

The principal ideal theorem implies that the minimal primes over the ideal $(1-T)$ and (T) inside E are of height 1, and Lemma 3.26 (catenary property) with $R \cong E/(1-T)$ and $\mathrm{gr}(R) \cong E/(T)$ gives $\dim E = 1 + \dim(E/(T)) = 1 + \dim(E/(1-T))$.

Thus $\dim R = \dim \mathrm{gr}(R)$.

So it is useful to consider dimensions of graded rings. We'll consider positively-graded rings $S = \bigoplus_{i=0}^{\infty} S_i$, and finitely-generated graded S-module $V = \bigoplus_{i=0}^{\infty} V_i$.

Remark. This all applies to negatively-graded rings as arising from I-adic filtrations – once one has formed the graded ring, one can renumber to change the indexing to be positive.

Suppose S is Noetherian, generated by S_0 and homogenous elements $x_1, \ldots, x_m$ of degree

$k_1, \ldots, k_m$. Let λ be an additive function, taking integral values on finitely-generated S_0-modules. I.e., if $0 \to U_1 \to U_2 \to U_3 \to 0$ is a short exact sequence of S_0-modules, then $\lambda(U_1) + \lambda(U_3) = \lambda(U_2)$.

Examples.

(a) E.g., if S_0 is a field k, then $\lambda = k$-vector space.

(b) More generally, if S_0 is local Artinian with maximal ideal P, then each finitely-generated S_0-module U has a chain of submodules $U \geqslant U_1 \geqslant \ldots \geqslant U_s = 0$, with each factor $\cong S_0/P$. Then number of terms in the chain is the **composition length** of U.

Exercise. Check that this is independent of the choice of chain.

We can take λ to be composition length.

Definition 3.44. The Poincaré series of V is the power series $P(V,t) = \sum \lambda(V_i)t^i \in \mathbb{Z}[[t]]$.

Theorem 3.45 (Hilbert, Serre). $P(V,t)$ is a rational function in t of the form $\dfrac{f(t)}{\prod_{i=1}^{m}(1-t^{k_i})}$, where $f(t) \in \mathbb{Z}[[t]]$, and k_i = degree of generators.

Proof. By induction on the number of generators.

$m = 0$. Then $S = S_0$, and V is a finitely-generated S_0-module. So $V_i = 0$ for large enough i. Then $P(V,t)$ is clearly a polynomial.

$m > 0$. Assume true for $m-1$ generators. Multiplication by x_m: $V_i \xrightarrow{x_m} V_{i+k_m}$, and so we can get an exact sequence $0 \to K_i \to V_i \xrightarrow{x_m} V_{i+k_m} \to L_{i+k_m} \to 0$ – $(*)$, where K_i is the kernel and V_{i+k_m} is the cokernel of $V_i \xrightarrow{x_m} V_{i+k_m}$.

Let $K = \bigoplus K_i$, $L = \bigoplus L_i$. K is a graded submodule of $V = \bigoplus V_i$, and hence a finitely-generated S-module. L is a quotient.

Both K and $L \cong V/x_mV$ are annihilated by x_m, and so are $S_0[x_1, \ldots, x_{m-1}]$-modules. Apply λ to $(*)$, obtaining $\lambda(K_i) - \lambda(V_i) + \lambda(V_{i+k_m}) - \lambda(L_{i+k_m})$.

Multiply by t^{i+k_m} and sum up: $t^{k_m}P(K,t) - t^{k_m}P(V,t) + P(V,t) - P(L,t) = g(t)$, where $g(t) \in \mathbb{Z}[t]$ is the polynomial arising from the first two terms.

Applying the inductive hypothesis to $P(K,t)$ and $P(L,t)$ gives the required result. □

Corollary 3.46. If each $k_1, \ldots, k_n$ is 1, then for large enough i, we have $\lambda(V_i) = \varphi(i)$, where $\varphi(t) \in \mathbb{Q}[t]$ of degree $d-1$, where the pole of $P(V,t)$ at $t = 1$ has order d.

Moreover, $\sum_{j=0}^{i} \lambda(V_j) = \chi(i)$, where $\chi(t) \in \mathbb{Q}[t]$ of degree d.

Definition 3.47. $\varphi(t)$ is the **Hilbert polynomial**, and $\chi(t)$ is the **Samuel polynomial**.

Lecture 17

Proof of 3.47. $P(V,t) = \frac{f(t)}{(1-t)^d}$ for some d with $f(1) \neq 0$, $f(t) \in \mathbb{Z}[t]$.

Since $(1-t)^{-1} = 1+t+t^2+\ldots$, repeated differentiation gives $(1-t)^{-d} = \sum \binom{d+i-1}{d-1} t^i$.

If $f(t) = a_0 + a_1 t + \ldots + a_s t^s$, say, then

$$\lambda(V_i) = a_0 \binom{d+i-1}{d-1} + a_1 \binom{d+i-2}{d-1} + \ldots + a_s \binom{d+i-s-1}{d-1} \qquad (\dagger)$$

setting $\binom{r}{d-1} = 0$ for $r < d-1$.

The right hand side of (†) can be rearranged to give $\varphi(i)$ for a polynomial $\varphi(t) \in \mathbb{Q}[t]$, valid for $d+i-s-1 \geqslant d-1$.

$$\varphi(t) = \frac{f(1)}{(d-1)!} t^{d-1} + \text{lower order terms}$$

So the degree of $\varphi(t)$ is $d-1$ since $f(1) \neq 0$.

Using (†) we can produce an expression for $\sum_{j=0}^{i} \lambda(V_j)$.

The formula $\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}$ yields $\sum_{j=0}^{i} \binom{d+j-1}{d-1} = \binom{d+i}{d}$.

And so

$$\sum_{j=0}^{i} \lambda(V_j) = a_0 \binom{d+i}{d} + a_1 \binom{d+i-1}{d} + \ldots + \binom{d+i-s}{d}$$

For $i > s$, this is equal to $\chi(i)$ for $\chi(t) \in \mathbb{Q}[t]$ of degree d. □

Now if we return to R a finitely-generated k-algebra, negatively filtered – e.g., I-adic filtration for some ideal I.

Let M be a finitely-generated R-module with good (negative) filtration $\{M_i\}$. Form $V = \operatorname{gr} M$ and $S = \operatorname{gr} R$, and renumber so that S is positively graded.

We can apply our Hilbert-Serre analysis of dimensions using, e.g., $\lambda = k$-vector space dimension.

By (3.46), there is the Samuel polynomial $\chi(t) \in \mathbb{Q}[t]$, where for large enough i,

$$\chi(i) = \sum_{j=i}^{0} \dim_k(M_j/M_{j-1}) = \dim_k(M_0/M_{-i}) \quad \text{for } i < 0$$

Remark. In fact, the degree is independent of which good filtration of M we pick (for a particular filtration of R).

Definition 3.48. $d(M) =$ degree of $\chi(t)$.

Theorem 3.49. For a finitely-generated k-algebra R that is an integral domain,

$$\dim R = \operatorname{tr.deg}_k(\text{f.field of } R) = d(R)$$

using the P-adic filtration for *any* maximal ideal P in R.

Remark. Note that this implies that $d(R)$ is independent of the choice of P.

Proof of 3.49 (rather sketchy). We've established the first equality in (3.24), and we've seen that $\dim R = \dim \operatorname{gr} R$ with respect to the P-adic filtration.

So it remains to show that for finitely-generated graded k-algebras S, we have $\dim S = d(S)$. Prove this by induction on dimension.

S is a finite-dimensional k-vector space $\iff \dim S = d(S) = 0$.

The induction step comes from considering S/xS, where x is a homogeneous element which is not a zero-divisor.

The princpal ideal theorem (3.28) and catenary property (3.24) imply that $\dim(S/xS) = \dim S - 1$.

Also observe from the proof of the Hilbert-Serre theorem (3.45), replacing x_m by x, then $K = 0$ since x is not a zero-divisor, and we deduce from the the equation involving $g(t)$ that $d(L) = d(M) - 1$ where $L = S/xS$ and $M = S$.

So $d(S/xS) = d(S) - 1$.

Apply the inductive hypothesis to S/xS to get that $\dim S = d(S)$ in general. □

Example. $R = k[X_1, \ldots, X_n]$, a polynomial algebra.

The number of monomials of (total) degree n is $\binom{n+m-1}{m-1}$ for all $n \geqslant 0$.

Thus the Hilbert polynomial $\varphi(t) = \frac{1}{(m-1)!}(t+m-1)\ldots(t+1)$, a polynomial of degree $m-1$.

Exercise. $d(M) = \max\{d(M_1), d(M_2)\}$, where $0 \to M_1 \to M \to M_2 \to 0$ is a short exact sequence.

Theorem (unproved here). R Noetherian local ring that is an integral domain, then with respect to the P-adic filtration for a maximal ideal P, we have $d(R) = \dim R =$ least number of generators of some ideal I such that $\sqrt{I} = P$.

Lecture 18

4. Valuation rings and Dedekind domains

Definition 4.1. An integral domain A with field of fractions K is a **valuation ring** of K if for each non-zero $x \in K$ either $x \in A$ or $x^{-1} \in A$ (or both).

E.g., $K = \mathbb{Q}$, $A = \mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at a prime ideal (p), $p \neq 0$.

Lemma 4.2. Let A be a valuation ring with fraction field K. Then

(i) A is a local ring.

(ii) If $A \subset B \subset K$ then B is a valuation ring.

(iii) A is integrally closed.

Proof.

(i) Let P be the set of non-units in A. Thus $x \in P$ if and only if $x = 0$ or $x^{-1} \notin A$. We see that P is an ideal:

(a) If $a \in A$ and $x \in P$, then $ax \in P$. Since otherwise $(ax)^{-1} \in A$ and so $x^{-1} = a(ax)^{-1} \in A$.

(b) If $x, y \in P$ then $x + y \in P$. Either $xy^{-1} \in A$ or $x^{-1}y \in A$. If $xy^{-1} \in A$ then $x + y = (1 + xy^{-1})y$, which is of the form ay and so is in P, using (a). Similarly if $x^{-1}y \in A$.

(ii) This is clear.

(iii) Let $x \in K$ be integral over A. So $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ for some $a_i \in A$.

Suppose $x \notin A$. Then $x = -(a_{n-1} + a_{n-2}x^{-1} + \ldots + a_0 x^{-n+1})$, and this lies in A since x^{-1} does. ⨻ □.

The reason for the terminology 'valuation ring' is that we may associate a **non-Archimedean valuation**, $v : K^\times \to \Gamma$, where Γ is a (well-chosen) ordered abelian group. (I.e., every pair of elements satisfies $\gamma_1 \leqslant \gamma_2$ or $\gamma_2 \leqslant \gamma_1$, and we only get both if $\gamma_1 = \gamma_2$. It respects the addition: $\gamma_1 \leqslant \gamma_2$ implies $\gamma + \gamma_1 \leqslant \gamma + \gamma_2$.)

The valuation v satisfies:

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x + y) \geqslant \min\{v(x), v(y)\}$ – the **ultrametric inequality**

so that $A = \{x \in K : x = 0 \text{ or } v(x) \geqslant 0\}$, and, given such a v, A is a valuation ring.

Definition 4.3. If $\Gamma \cong \mathbb{Z}$ we say that A is a **discrete valuation ring**.

Examples.

1. E.g., $v_p : \mathbb{Q}^\times \to \mathbb{Z}$, $p^n a/b \mapsto n$, where a, b are coprime. This is a p-adic valuation on $\mathbb{Q}$ with discrete valuation ring $\mathbb{Z}_{(p)}$.

2. $v_f : k(X)^\times \to \mathbb{Z}$, $f^n g/h \mapsto n$, where f is an irreducible polynomial in $k[X]$, and $g, h \in k[X]$ coprime to f. This has discrete valuation ring $k[X]_{(f)}$, the localisation

of $k[X]$ at the prime ideal (f).

Recipe for valuation rings

Given R, an integral domain with field of fractions K. Take an algebraically closed field F.

Consider pairs (R', φ') where R' is a subring of K, and $\varphi' : R' \to F$ is a ring homomorphism. Partially order these pairs: $(R_1, \varphi_1) \leqslant (R_2, \varphi_2) \iff R_1 \leqslant R_2$ and $\varphi_2|_{R_1} = \varphi_1$.

An ascending chain of such pairs has an upper bound (R_0, φ_0) such that $R_0 = \bigcup$(subrings appearing in the pairs in the chain), and φ_0 restricted to these subrings is the corresponding φ_i.

Apply Zorn's Lemma – these is a maximal such pair, say (A, θ).

Claim. Such an A is a valuation ring.

Step 1. A is a local ring with $\ker\theta = P$, the unique maximal ideal.

Proof. $\theta(A)$ is a subring of F, a field, and so is an integral domain. So $P = \ker\theta$ is a prime ideal.

Extend θ to a ring homomorphism $\varphi : A_P \to F$, $a/s \mapsto \theta(a)/\theta(s)$, where $S = A \setminus P$.

Maximality of the pair (A, θ) ensures that $A = A_P \leqslant K$. Hence A is a local ring with maximal ideal P.

Take non-zero $x \in K$. We must show that either $x \in A$ or $x^{-1} \in A$. I.e., either $A[x]$ or $A[x^{-1}]$ is equal to A.

Step 2. First we show that either $PA[x] \lneq A[x]$ or $PA[x^{-1}] \lneq A[x^{-1}]$.

Proof. Suppose $PA[x] = A[x]$ and $PA[x^{-1}] = A[x^{-1}]$.

So $1 \in PA[x]$, say $1 = a_m x^m + \ldots + a_0$, with $a_i \in P$ – (eqn1)

And $1 \in PA[x^{-1}]$, say $1 = b_n x^{-n} + \ldots + b_0$, with $a_i \in P$ – (eqn2)

Pick m, n minimal and assume (wlog) that $m \geqslant n$. Multiply (eqn2) by x^n to get $(1 - b_0)x^n = b_n + \ldots + b_1 x^{n-1}$ – (eqn3).

But $b_0 \in P$ and $1 - b_0 \notin P$, and so $1 - b_0$ is a unit.

So (eqn3) gives $x^n = c_n + \ldots + c_1 x^{n-1}$ with $c_i \in P$, and so $x^m = c_n x^{m-n} + \ldots c)1x^{m-1}$.

Substituting in (eqn1) gives an equation contradicting the minimality of n.

Step 3. We may assume that $I = PA[x] \lneq A[x]$. Let $B = A[x]$.

We show that $B = A$ and hence $x \in A$.

Proof. Let Q be a maximal ideal of B containing I. Then $Q \cap A = P$ since $Q \cap A \lneq A$ and P is in it.

Regard A/P as a subring of B/Q. Both are fields, say k, k_1.

Then $k_1 = k[\overline{x}]$, where $\overline{x}$ is the image of x in B/Q. Thus k_1 is an algebraic extension of k.

But θ induces a map $\overline{\theta} : k = A/P \to F$, and this extends to a map $\overline{\varphi} : k_1 \to F$, since F algebraically closed.

$\overline{\varphi}$ lifts back to a map $B \to F$, and the maximality of the pair (A, θ) ensures that $A = B$.

Lecture 19

Theorem 4.4. Let R be an integral domain with fraction field K. Then the integral closure T of R in K is the intersection of all the valuation rings of K containing R.

E.g., $\mathbb{Z} = \bigcap_{p \text{ prime}} \mathbb{Z}_{(p)}$.

Proof. Let A be a valuation ring containing R. But A is integrally closed by (4.2) and hence $T \subset A$.

Conversely, if $x \notin T$ then $x \notin R[x^{-1}] = R_1$. So x^{-1} is not a unit of R_1 and is therefore contained in a maximal ideal P_1 of R_1.

Let F be the algebraic closure of the field R_1/P_1. The canonical map $\varphi : R_1 \to R_1/P_1 \subset F$ restricts to give a map $R \to F$. So in our recipe for valuation rings, by Zorn there is a maximal pair (A, θ) with A being a valuation ring.

Since θ extends φ, we have $\theta(x^{-1}) = \varphi(x^{-1}) = 0$. So $x \notin A$.

Discrete Valuation Rings

A valuation ring A with fraction field K is local (by (4.2)(i)) and integrally closed (by (4.2)(iii)). Say the unique maximal ideal is P.

If we have a (surjective) discrete valuation $v : K\times \to \mathbb{Z}$, so that

$$A = \{x \in K : x = 0 \text{ or } v(x) \geqslant 0\}$$
$$P = \{x \in K : x = 0 \text{ or } v(x) \geqslant 1\}$$

If $v(a) = v(b)$, then $v(ab^{-1}) = 0$, so ab^{-1} is a unit in A. So $(a) = (b)$.

If I is a non-zero ideal of A, then there is a least K such that $v(a) = k$ for some $a \in I$. So I contains every b with $v(b) \geqslant k$, since $b = a(b/a)$ and $v(b/a) \geqslant 0$, so $b/a \in A$ and hence $b \in (a)$.

Hence $I = I_k = \{x \in A : v(x) \geqslant k\}$.

Thus there is only one chain of ideals $P = I_1 \supsetneq I_2 \supsetneq \ldots$, and therefore A is Noetherian.

Thus P is the only non-zero prime, and so $\dim A = 1$.

Lemma 4.5. Let A be a Noetherian local integral domain of dimension 1. Set $k = A/P$ wehere P is the unique maximal ideal. The following are equivalent:

1. A is a discrete valuation ring

2. A is integrally closed

3. P is principal

4. $\dim_k P/P_2 = 1$

5. Every non-zero ideal $\neq A$ is a power of P

6. There exists $x \in P$ such that every non-zero ideal $\neq A$ is of the form (x^k) for some $k \geqslant 1$.

Proof.

1⇒2. See (4.2)(iii).

2⇒3. Let $a \in P$ be non-zero. Then $\dim A = 1$ and A is local. P is the only minimal prime over (a), and we know that $P^n \leqslant (a)$ for some n.

Pick n minimal, so $P^{n-1} \not\leqslant (a)$, and we may pick $b \in P^{n-1}$ with $b \notin (a)$. Set $x = a/b$.

Claim. $P = (x)$.

Note that $x^{-1} \notin A$ since $b \notin (a)$ and the integrally closed property of A, x^{-1} is not integral over A.

If $x^{-1}P \leqslant P$ then P would be an $A[x^{-1}]$-module, finitely generated as an A-module. Any $A[x^{-1}] - \textit{submodule}$ will also be finitely generated as an A-module (since A is Noetherian). But any non-zero cyclic $A[x^{-1}]$-submodule of $A[x^{-1}]$ is isomorphic to $A[x^{-1}]$ and this gives a contradiction as $A[x^{-1}]$ is not a finitely-generated A-module (since x^{-1} is not integral).

So $x^{-1}P \not\leqslant P$. Thus $x^{-1}P \leqslant A$ by construction, and so $x^{-1}P = A$. Hence $P = (x)$.

3⇒4. P principal $\implies$ P/P^2 principal $\implies$ $\dim_k P/P^2 \leqslant 1$. And $P \neq P^2$ by Nakayama.

4⇒5. If I is an ideal of A ($I \neq 0, A$), then $P^n \leqslant I$ (as in 2 ⇒ 3). But $\dim_k P/P^2 = 1$, so P is principal (application of Nakayama).

Say $P = (x)$. There exists r such that $I \leqslant P^r$, $I \not\leqslant P^{r-1}$, and hence there is $y \in I$ such that $y = ax^r$ with $y \notin P^{r-1}$.

So $a \notin P$ and hence a is a unit of A. So $x^r \in I$ and $P^r \leqslant I$. So $I = P^r$.

5⇒6. By Nakayama, $P \neq P^2$. Take $x \in P \setminus P^2$. But then $P = (x)$. Every ideal I is of the form P^r for some r. So $I = (x^r)$.

6⇒1. From 6, $P = (x^r)$ for some r. But P is prime and so $r = 1$, so $P = (x)$.

By Nakayama, $P^k \neq P^{k+1}$ for any k.

Claim. A is a valuation ring.

If $y \in K$, $y \notin A$, then consider $\{x \in A : xy \in A\}$. This is an ideal of A, and so equals (x^k) for some k. So $yx^k \in A \setminus P$ (otherwise $yx^k \in P = (x)$, and $yx^{k-1} \in A$ and $x^{k-1} \in (x^k)$ ⨳).

Thus yx^k is a unit of A and we deduce that y^{-1} is in A.

If $a \in A$ then $(a) = (x^k)$ for exactly one value of k. Define $v(a) = k$. Extend to

$K^\times$ by $v(ab^{-1}) = v(a) - v(b)$.

Check. This gives a well-defined discrete valuation $v : K^\times \to \mathbb{Z}$.

Lecture 20

Dedekind domains

Definition 4.6. An integrally closed Noetherian integral domain of dimension 1 is called a **Dedekind domain**.

Examples.

1. Integral closure of $\mathbb{Z}$ in a finite field extension of $\mathbb{Q}$.
2. Co-ordinate rings of normal (smooth) curves.

Remark. Since R is integrally closed, then $S^{-1}R$ will be integrally closed for any multiplicatively closed subset S. In particular, R_Q will be integrally closed for any maximal ideal Q, and so R_Q is a DVR (discrete valuation ring), using (4.5).

Lemma 4.7. In a Dedekind domain, every ideal I with $\sqrt{I} = Q$, a maximal ideal, is a power of Q.

Proof. Let I be such that $\sqrt{I} = Q$, maximal. Then $S^{-1}I$ is a non-zero ideal of R_Q, where $S = R \setminus Q$.

By (4.5) applied to the DVR R_Q, we have $S^{-1}I = (S^{-1}Q)^r = S^{-1}(Q^r)$ for some r.

The bijective correspondence between ideal that don't meet S and the ideals of the localisation gives that $I = Q^r$. □

Theorem 4.8 (Dedekind). In a Dedekind domain R, every non-zero ideal I has a unique factorisation as a product of prime (maximal) ideals.

Proof. Given a non-zero ideal I, R/I has only finitely many primes, all of which are maximal, and it is Artinian.

Since $\dim R = 1$, R/I is a direct product of Artinian rings (example sheet 1), thus $I = \bigcap I_j$, with $\sqrt{I_j} = Q_j$. But by (4.7), $I_j = Q_j^{m_j}$ for some m_j. Thus $I = \bigcap Q_j^{m_j}$.

But for coprime ideals, products are the same as intersections (a lemma proved by induction on the number of ideals – see example sheet). So $I = \prod Q_j^{m_j}$.

Uniqueness. The Q_j appearing are the maximal primes over I. In any other similar expression for I, the same Q's must appear, and the powers must be the same because the powers are unique as in (4.5). □

Definition 4.9. Given an integral domain R with fraction field K, an R-submodule M of K is a **fractional ideal** of R if $xM \subset R$ for some non-zero x in R.

Remarks.

1. Every finitely-generated R-submodule M of K is a fractional ideal.
2. In a Dedekind domain, the fractional ideals form a group under multiplication – the **class group**.

5. Tensor products, homology and cohomology

Let L, M, N be R-modules.

Definition 5.1. A function $\varphi : M \times N \to L$ is R-bilinear if:

(i) $\varphi(r_1 m_1 + r_2 m_2, n) = r_1\varphi(m_1, n) + r_2\varphi(m_2, n)$

(ii) $\varphi(m, r_1 n_1 + r_2 n_2) = r_1\varphi(m, n_1) + r_2\varphi(m, n_2)$

The idea of tensor products is to reduce the discussion of multilinear maps to a discussion of linear maps.

If $\varphi : M \times N \to T$ is bilinear and $\theta : T \to L$ is linear then the composition is bilinear. Thus composition with φ gives a well-defined function φ^* from $\{R$-module maps $T \to L\}$ to $\{$bilinear maps $M \times N \to L\}$.

φ is **universal** if φ^* is a 1-1 correspondence for all L.

Lemma 5.2.

(i) Given M, N, there is an R-module T and a universal map $M \times N \to T$

(ii) Given two such maps $\varphi_1 : M \times N \to T_1$ and $\varphi_2 : M \times N \to T_2$, there is a unique isomorphism $\beta : T_1 \to T_2$ with $\beta \circ \varphi_1 = \varphi_2$.

Proof.

(i) Let F be the free module on generators $e_{(m,n)}$ indexed by pairs $(m, n) \in M \times N$. Let X be the R-submodule generated by all elements of the forms

$$e_{(r_1 m_1 + r_2 m_2, n)} - r_1 e_{(m_1, n)} - r_2 e_{(m_2, n)}$$
$$e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m, n_1)} - r_2 e_{(m, n_2)}$$

Set $T = F/X$ and write $m \otimes n$ for the image of the basis element $e_{(m,n)}$ in T.

And define $\varphi : M \times N \to T$ by $(m, n) \mapsto m \otimes n$.

Note: T is generated by the $m \otimes n$ and φ is bilinear.

Any map $\alpha : M \times N \to L$ extends to a map $\overline{\alpha} : F \to L$, $e_{(m,n)} \mapsto \alpha(m, n)$.

If α is bilinear then $\overline{\alpha}$ vanishes on X, and we have an induced map $\alpha' : T \to L$ with $\alpha'(m \otimes n) = \alpha(m, n)$. And α' is uniquely defined by this.

(ii) Exercise. It follows from universality. □

Definition 5.3. T is written $M \otimes_R N$, the **tensor product** of M and N over R. (We often drop the subscript R if it is clear what ring we are using.)

Warning. Not all elements of $M \otimes N$ are of the form $m \otimes n$. A general element is $\sum(m_i \otimes n_i)$.

E.g., if R is a field k and M, N are k-vector space of dimensions s, t respectively, then $M \otimes_k N$ is a k-vector space of dimension st.

Lemma 5.4. There are unique isomorphisms:

1. $M \otimes N \to N \otimes M$ given by $m \otimes n \mapsto n \otimes m$ (extending linearly)

2. $M \otimes (N \otimes L) \to (M \otimes N) \otimes L$ given by $m \otimes (n \otimes \ell) \mapsto (m \otimes n) \otimes \ell$

3. $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L)$ given by $(m \oplus n) \otimes \ell \mapsto (m \otimes \ell) \oplus (n \otimes \ell)$

4. $R \otimes M \to M$ given by $r \otimes m \mapsto rm$

Proof. Exercise.

Lecture 21

Restriction of scalars. If $\varphi : R \to T$ is a ring homomorphism and N is a T-module, it may be regarded as an R-module via $rm = \varphi(r)m$.

Thus T itself may be regarded as an R-module.

Extension of scalars. Given an R-module M, we can form $T \otimes_R M$. This can be viewed as a T-module via $t_1(t_2 \otimes m) = t_1 t_2 \otimes m$.

Example. In localisation, we had a map $R \to S^{-1}R$. Given an R-module M and the multiplicatively closed set S, there is a unique isomorphism $S^{-1}R \otimes_R M \to S^{-1}M$.

The map $S^{-1}R \times M \to S^{-1}M$ is R-bilinear, and universality yields an R-module map $S^{-1}R \otimes M \to S^{-1}M$.

Check that this is an isomorphism.

Definition 5.5. Given R-module maps $\theta : M_1 \to M_2$ and $\varphi : N_1 \to N_2$, the **tensor product** of θ and φ is

$$\theta \otimes \varphi : M_1 \otimes N_1 \to M_2 \otimes N_2, \quad m_1 \otimes n_1 \mapsto \theta(m_1) \otimes \varphi(n_1)$$

Note: the map $M_1 \times N_1 \to M_2 \otimes N_2$, $(m_1, n_1) \mapsto \theta(m_1) \otimes \varphi(m_1)$ is bilinear and so universality yields $\theta \otimes \varphi : M_1 \otimes N_1 \to M_2 \otimes N_2$.

Lemma 5.6. Given R-modules M, N, L, we have $\mathrm{Hom}(M \otimes N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, L))$.

Proof. Given a blinear map $\varphi : M \times N \to L$, we have $\theta : M \to \mathrm{Hom}(N, L)$, under which m is mapped to $\theta_m : N \to L$, $n \mapsto \varphi(m, n)$.

Conversely, given $\theta : M \to \mathrm{Hom}(N, L)$, we have a bilinear $M \times N \to L$, $(m, n) \mapsto \theta(m)(n)$.

Thus there is an isomorphism

$$\{\text{bilinear maps } M \times N \to L\} \longleftrightarrow \{\text{linear maps } M \to \mathrm{Hom}(N, L)\}$$

But the LHS corresponds to the linear maps $M \otimes N \to L$. □

Definition 5.7. Given $\varphi_1 : R \to T_1$ and $\varphi_2 : R \to T_2$ (the T_i are R-algebras), the tensor product of the two R-algebras is $T_1 \otimes_R T_2$, defined as an R-module.

$T_1 \otimes T_2$ can be endowed with a product: $(t_1 \otimes t_2)(t_1' \otimes t_2') = t_1 t_1' \otimes t_2 t_2'$.

Check that $(T_1 \otimes T_2) \times (T_1 \otimes T_2) \to T_1 \otimes T_2$ is well-defined, and that $1 \otimes 1$ is the multiplicative identity.

Check that $R \to T_1 \otimes T_2$, $r \mapsto \varphi_1(r) \otimes 1$ is a ring homomorphism. Note this equals $1 \otimes \varphi_2(r)$.

Examples.

1. k a field, then $k[X]$ is a k-algebra. We have $k[X_1] \otimes_k k[X_2] \cong k[X_1, X_1]$.
2. $\mathbb{Q}[X]/(x^2+1) \otimes_Q \mathbb{C} \cong \mathbb{C}[X]/(X^2+1)$.
3. $k[X_1]/(f(X_1)) \otimes_k k[X_2]/(g(X_2)) \cong k[X_1, X_2]/(f(X_1), g(X_2))$.

Lemma 5.8. If $M_1 \to M \to M_2 \to 0$ is an exact sequence and N is an R-module, then

$$M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$$

$$N \otimes M_1 \to N \otimes M \to N \otimes M_2 \to 0$$

are exact.

Remark. These are *not* short exact sequences. Given a short exact sequence, applying $-\otimes N$ does not necessarily preserve injectivity of the left-hand map.

For example, $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(2) \to 0$.

If we take $N = \mathbb{Z}/(2)$, then $\mathbb{Z} \otimes N \cong \mathbb{Z}/(2)$ and $\mathbb{Z}/(2) \otimes \mathbb{Z}/(2) \otimes \mathbb{Z}/(2)$.

So we get $\mathbb{Z}/(2) \to \mathbb{Z}/(2) \to \mathbb{Z}/(2) \to 0$, with the left-hand map here being the zero map – not injective.

Thus exactness is not preserved.

Definition 5.9. N is a **flat** R-module if given any short exact sequence

$$0 \to M_1 \to M \to M_2 \to 0$$

the sequence

$$0 \to M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$$

is exact.

Examples.

1. R itself is a flat R-module.
2. R^n is a flat R-module (the free module on n generators).
3. If $R = \mathbb{Z}$ then $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

   In fact, any torsion-free abelian group is a flat $\mathbb{Z}$-module.

Homology concerns measuring the failure of flatness.

If we consider $\mathrm{Hom}(-, N)$, we have an analogous situation, only things are now contravariant rather than covariant.

Lemma 5.10.

(i) The sequence

$$M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \to 0 \qquad (*)$$

is exact if and only if

$$0 \to \mathrm{Hom}(M_2, N) \xrightarrow{\overline{\varphi}} \mathrm{Hom}(M, N) \xrightarrow{\overline{\theta}} \mathrm{Hom}(M_1, N) \qquad (**)$$

is exact for all N.

(ii) $0 \to M_1 \to M \to M_2$ is exact iff

$$0 \to \mathrm{Hom}(N, M_1) \to \mathrm{Hom}(N, M) \to \mathrm{Hom}(N, M_2)$$

Lecture 22

is exact for all N.

Proof.

(i) Suppose $0 \to \mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M_1, N)$ is exact for all N.

Since $\mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M, N)$ is injective for all N, the map $M \to M_2$ is surjective. So we have exactness at M_2 in $(*)$.

We need to check exactness at M.

First, $\mathrm{im}\,\theta \leqslant \ker\varphi$. Take $N = M_2$, and $f : M_2 \to M_2$ the identity map.

Then $\overline{\theta} \circ \overline{\varphi}(f) = 0$, so $f \circ \varphi \circ \theta = 0$ and so $\varphi \circ \theta = 0$.

Finally, take $N = M/\mathrm{im}\,\theta$ and $\pi : M \to N$ projection. Then $\pi \in \ker\overline{\theta}$ and hence there exists $\psi \in \mathrm{Hom}(M_2, N)$ such that $\pi = \overline{\varphi}(\psi)$.

So $\mathrm{im}\,\theta = \ker\pi \supset \ker\varphi$. Hence $\ker\varphi = \mathrm{im}\,\theta$.

Rest of proof: exercise. □.

We now prove (5.8), using (5.6) and (5.10).

Proof of 5.8. Given the exact sequence $M_1 \to M \to M_2 \to 0$, tensoring with N gives $M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$.

Let P be any R-module. The sequence

$$0 \to \mathrm{Hom}(M_2, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M_1, \mathrm{Hom}(N, P))$$

is exact by (5.10). Hence

$$0 \to \mathrm{Hom}(M_2 \otimes N, P) \to \mathrm{Hom}(M \otimes N, P) \to \mathrm{Hom}(M_1 \otimes N, P)$$

is exact for any P, using (5.6).

So (5.10) again gives that

$$M_1 \otimes N \to M \otimes N \to M_2 \otimes \to 0$$

is exact. □

Observe that given a short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, the sequence

$$0 \to \mathrm{Hom}(M_1, N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M_2, N) \to 0$$

is not necessarily exact.

Definition 5.11. A module P is **projective** if whenever we have a surjective $M \twoheadrightarrow P$ and a map $P \to M_2$ then we can complete the diagram with a map $P \to M$.

I.e., this commutes:

$$\begin{array}{ccccc} & & & & P \\ & & \swarrow & & \downarrow \\ M & \twoheadrightarrow & M_2 & \to & 0 \end{array}$$

Similarly, we define an **injective** module E as being able to complete diagrams of the form

$$\begin{array}{ccccc} 0 & \to & M_1 & \to & M \\ & & \downarrow & \swarrow & \\ & & E & & \end{array}$$

Examples.

1. Free modules are projective.
2. If R is an integral domain with fraction field K, then K is an injective R-module. E.g., $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Lemma 5.12. For an R-module P, the following are equivalent.

1. P is projective.
2. For every short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, the induced sequence $0 \to \mathrm{Hom}(P, M_1) \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M_2) \to 0$ is exact.
3. If $\varepsilon : M \twoheadrightarrow P$ is surjective then there exists a map $\beta : P \to M$ such that $\varepsilon \circ \beta =$ identity.
4. P is a direct summand in every module of which it is a quotient.
5. P is a direct summand of a free module.

Proof.

$1 \Rightarrow 2$. This follows from the definition of projective.

$2 \Rightarrow 3$. Choose an exact sequence $0 \to \ker \varepsilon \to M \xrightarrow{\varepsilon} P \to 0$.

The induced sequence $0 \to \mathrm{Hom}(P, \ker \varepsilon), \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, P) \to 0$ is exact, and so there exists $\beta : P \to M$ such that $\varepsilon \circ \beta =$ identity.

$3 \Rightarrow 4$. Let $P \cong M/M_1$, a quotient of M. So we have $0 \to M_1 \to M \to M \xrightarrow{\alpha} P \to 0$ is a short exact sequence.

By 3, there is $\beta : P \to M$ such that $\alpha \circ \beta =$ identity. Therefore P is a direct summand of M.

$4 \Rightarrow 5$. P is a quotient of a free module. Take a generating set X for P, form the free module with basis $\{e_x\}$, indexed by X, and map basis elements $e_x \mapsto x$ for $x \in X$.

$5 \Rightarrow 1$. By 5, $F = P \oplus Q$. Since free modules are projective and we have good behaviour under $\oplus$, so P is projective. □

Remarks.

1. Projective modules are direct summands of free modules, and free modules are flat, and tensor products behave well under $\oplus$. So we get that projective modules

are flat.

2. In a PID, we know from the structure theorem for modules that direct summands of free modules are free. So projective modules are free.

Lemma 5.13. For an R-module E, the following are equivalent.

1. E is injective.
2. For every short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, the induced sequence $0 \to \mathrm{Hom}(M_1, E) \to \mathrm{Hom}(M, E) \to \mathrm{Hom}(M_2, E) \to 0$ is exact.
3. If $\mu : E \to M$ is monomorphism then there exists a map $\beta : M \to E$ such that $\beta \circ \mu =$ identity.
4. E is a direct summand in every module of which it is a submodule

Proof. Exercise. □

Given an R-module M there is certainly a free module F with $F \twoheadrightarrow M$ surjectively.

Definition 5.14. A **projective presentation** of M is a short exact sequence $0 \to K \to P \to M \to 0$ with P projective.

It is a **free presentation** in the case where P is free.

Definition 5.15. Given a projective presentation of M, apply $- \otimes_R N$ to get

$$K \otimes N \to P \otimes N \to M \times N \to 0$$

Define $\mathrm{Tor}^R(M, N) = \ker(K \otimes N \to P \otimes N)$.

Apply $\mathrm{Hom}(-, N)$ to get

$$0 \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(P, N) \to \mathrm{Hom}(K, N)$$

and define $\mathrm{Ext}(M, N) = \mathrm{coker}\big(\mathrm{Hom}(P, N) \to \mathrm{Hom}(K, N)\big)$.

Remarks.

1. This is actually independent of the choice of presentation.
2. One may also take a projective presentation for N and apply $M \otimes_R -$. The gives the same kernel.
3. One may take a short exact sequence $0 \to N \to E \to C \to 0$ with E injective and apply $\mathrm{Hom}(M, -)$. The cokernel arising is (the same as) $\mathrm{Ext}(M, N)$.
4. Ext denotes 'extensions' – there is an alternative description in terms of equivalence classes of extensions.

   Tor denotes 'torsion'.

Lecture 23

Example. We met the free presentation of $\mathbb{Z}/(2)$ (where $R = \mathbb{Z}$)

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\mathrm{mod}\, 2} \mathbb{Z}/(2) \longrightarrow 0$$

Apply $\otimes \mathbb{Z}/(2)$. Then we have $\mathrm{Tor}(\mathbb{Z}/(2), \mathbb{Z}/(2)) = \ker(\mathbb{Z} \otimes \mathbb{Z}/(2) \to \mathbb{Z} \otimes \mathbb{Z}/(2))$, induced by multiplication by 2, which is the zero map.

So $\mathrm{Tor}(\mathbb{Z}/(2), \mathbb{Z}/(2)) = \mathbb{Z}/(2)$.

Apply $\mathrm{Hom}(-, N)$ to our presentation. We have $\mathrm{Ext}(\mathbb{Z}/(2), N) = \mathrm{coker}(\mathrm{Hom}(\mathbb{Z}, N) \to \mathrm{Hom}(\mathbb{Z}, N))$, induced by multiplication by 2. Note $\mathrm{Hom}(\mathbb{Z}, N) \cong N$.

Remark. For any PID, we have a projective presentation $0 \to K \to P \to M \to 0$ for any finitely-generated R-module M in which K is also projective. (Projectives are free.)

Definition 5.16. A **projective resolution** of M is an exact sequence

$$\ldots \to P_n \to \ldots \to P_1 \to P_0 \to M \to 0$$

with each P_i projective.

Remark. If R is Noetherian and M is a finitely-generated R-module, we can produce a projective resolution with all of the P_i being finitely-generated projective modules.

Form a presentation $0 \to K_0 \to P_0 \to M \to 0$, and then take a presentation for K_0, say $0 \to K \to P_1 \to K_0 \to 0$, etc, ensuring that at each stage that P_i is finitely generated, and hence K_i is finitely generated.

Applying $\otimes_R N$ to a projective resolution for M yields a chain complex

$$\ldots \to P_n \otimes N \to \ldots \to P_1 \otimes N \to P \otimes N \to M \otimes N \to 0$$

(A **chain complex** is one where the image of one arrow is contained in the kernel of the next.)

At $P_i \otimes N$, we have $\ldots \xrightarrow{\theta_n} P_n \otimes N \xrightarrow{\theta_{n-1}} \ldots$

Then $\ker \theta_{n-1} / \mathrm{im}\, \theta_n$ is an R-module – it is known as the **homology** of the chain complex at $P_n \otimes N$.

Definition 5.17. $\mathrm{Tor}_n^R(M, N)$ is the homology group at $P_n \otimes N$.

Thus $\mathrm{Tor}_0(M, N) = M \otimes N$, and $\mathrm{Tor}_1(M, N) = \mathrm{Tor}(M, N)$.

(Use the chain complex $\ldots \to P_n \otimes N \ldots \to P_1 \otimes N \to P_0 \otimes N \to 0$, with the homology at $P_0 \otimes N$ being $M \otimes N$.)

Similarly, given a projective resolution for M, apply $\mathrm{Hom}(-, N)$ and get a cochain complex

$$\ldots \to \mathrm{Hom}(P_0, N) \to \mathrm{Hom}(P_1, N) \to \ldots$$

and we define $\mathrm{Ext}_R^n(M, N)$ to be the (co)homology group at $\mathrm{Hom}(P_n, N)$.

Thus $\mathrm{Ext}^0(M, N) = \mathrm{Hom}(M, N)$ and $\mathrm{Ext}^1(M, N) = \mathrm{Ext}(M, N)$.

Remark. In fact, this is all independent of the choice of projective resolution.

Moreover, one can obtain $\mathrm{Ext}^n(M, N)$ by considering an injective resolution of N

$$0 \to N \to E_0 \to E_1 \to \ldots \quad \text{(exact)}$$

with E_i injective R-modules. Applying $\mathrm{Hom}(M, -)$ to this and considering the homology groups of the resulting compex yields the same thing.

Lemma 5.18. The following are equivalent.

1. $\mathrm{Ext}^{n+1}(M,N) = 0$ for all R-modules N
2. M has a projective resolution of length n. I.e., $0 \to P_n \to P_{n-1} \to \ldots \to P_0 \to M \to 0$.

Proof. Omitted. □

Definition 5.19. The **homological dimension** of M is n if $\mathrm{Ext}^{n+1}(M,N) = 0$ for all N, and there is some N for which $\mathrm{Ext}^n(M,N) \neq 0$.

The **global dimension** of R is the supremum of all the homological dimensions of R-modules M.

Examples.

1. For a field k, all modules are free, and global dimension is 0.
2. The global dimension of $\mathbb{Z}$ is 1.

   In fact, this is also the case for any PID which isn't a field, such as $k[X]$.
3. The condition that gl.dim $= 0$ is equivalent to saying that all submodules of R are direct summands. In other words, R is semisimple – cf. complex representation theory of finite groups G, where the group algebra $\mathbb{C}G$ is semisimple.

Theorem 5.20. Given a short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, there are long exact sequences

$$\ldots \mathrm{Tor}_2(M_2,N) \to \mathrm{Tor}_1(M_1,N) \to \mathrm{Tor}_1(M,N) \to \mathrm{Tor}_1(M_2,N)$$
$$\to \mathrm{Tor}_0(M_1,N) \to \mathrm{Tor}_0(M,N) \to \mathrm{Tor}_0(M_2,N) \to 0$$

and

$$0 \to \mathrm{Ext}^0(M_2,N) \to \mathrm{Ext}^0(M,N) \to \mathrm{Ext}^0(M_1,N) \to \mathrm{Ext}^1(M_2,N)$$
$$\to \mathrm{Ext}^1(M,N) \to \mathrm{Ext}^1(M_1,N) \to \mathrm{Ext}^2(M_2,N) \to \ldots$$

Corollary 5.21 (Dimension shifting). Given a projective presentation $0 \to K \to P \to M \to 0$, one gets

$$\mathrm{Tor}_n(M,N) = \mathrm{Tor}_{n-1}(K,N) \quad \text{and} \quad \mathrm{Ext}^n(M,N) = \mathrm{Ext}^{n-1}(K,N) \quad \text{for } n > 0$$

Proof. Apply (5.20) to our presentation and observe that for a projective P, we have $\mathrm{Ext}^n(P,N) = \mathrm{Tor}_n(P,N) = 0$ for $n > 0$. □

For a polynomial algebra $k[X_1,\ldots,X_n]$, there is a well-chosen free resolution of the trivial module k with X_i acting like 0, known as the Koszul complex, based on the exterior algebra on n generators – in each degree we have the free R-module with generators being the exterior products $X_{i_1} \wedge X_{i_2} \wedge \ldots \wedge X_{i_m}$ of m of the n variables.

In general, Hilbert's syzygy theorem says that any ideal of R has a projective resolution of length $\leqslant n$. So gl.dim$R = n$.

Lecture 24

Hochschild Cohomology

Suppose for this lecture that we drdop the commutativity condition.

Bimodule (co)homology. A k-algebra R is a R-R bimodule. We need a projective resolution for R as a bimodule. An R-R-bimodule map may be viewed when convenient as a left $R \otimes R^{\mathrm{op}}$-module.

In R^{op}, the multiplication is $x\dot{y} = yx$ (the RHS being multiplication in R).

For R commutative, $R^{\mathrm{op}} \cong R$.

$R \otimes R \to R$ by $x \otimes y \mapsto xy$.

Hochschild resolution of R:

$$\ldots \to R \otimes R \otimes R \otimes R \to R \otimes R \otimes R \to R \otimes R \ \to R$$

This is a chain complex, exact.

The maps $R^{\otimes n} \to R^{\otimes n-1}$ involve alternating sums. E.g., $x \otimes y \otimes z \mapsto xy \otimes z - x \otimes yz$.

For Hochschild homology, one tensors this resolution with R.

If M is an R-R-bimodule, we can form $M \otimes_k R$, which is a bimodule, and consider the homology groups in the arising chain complex $HH_i(R, R)$.

If we apply $\mathrm{Hom}(-, R)$, the cohomology in the arising cocomplex is Hochschild cohomology $HH^i(R, R)$.

$HH^0(R, R)$ is the centre of R.

$HH^1(R, R)$ is (derivations of R)/(inner derivations of R).

Where: derivations are d such that $d(xy) = xdy + (dx)y$, and inner deriviations are those arising from ring commutators $x \mapsto [x, y] = xy - yx$ (multiplication in R).

For a commutative algebra, $HH^1(R, R) \cong \{\text{derivations}\}$.

The derivations form a Lie algebra – they can be regarded as infinitesimal automorphisms. ($HH^1(R, R)$ also has an interpretation in terms of differentials.)

Hochschild cohomology $HH^*(R, R)$ has a product defined on it – it forms a ring, but in practice it's hard to work with a particular example.

HH^2 has a meaning to do with deformations of the algebra.

Hochshild dimension

A k-algebra has **Hochschild dimension** n if and only if R has a free/projective resolution of length n and no shorter (analogous to the global dimension definition).

Hochschild dimension 0 iff R is a projective R-R-bimodule, iff R is a direct summand of $R \otimes R^{\mathrm{op}}$. (Separable k-algebra.)