11/10/13

Commutative Algebra ①

Prerequisites

- Experience in Ring Theory

Books

- Atiyah + Macdonald (concise)
- Sharp (details)
- Matsumura (not an introduction but includes homological material)
- Bourbaki
- Zariski, Samuel

) weighty

0 Introduction

David Hilbert, 1888 - 1893, wrote a series of papers on Invariant Theory. If k is a field, $k[x_1, \dots, x_n]$ the polynomial ring, and Σ_n the symmetric group on $\{1, 2, \dots, n\}$, then Σ_n acts on $k[x_1, \dots, x_n]$ by permuting variables.

The set of invariants $\{f \in k[x_1, \dots, x_n] : g(f) = f \ \forall g \in \Sigma_n\}$ forms a ring S.

Elementary Symmetric Functions $f_1(x_1, \dots, x_n) = x_1 + \dots + x_n$

$f_2(x_1, \dots, x_n) = \sum_{i<j} x_i x_j$

$f_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n$

In fact, S is generated as a ring by these f_i, i.e.

$S \cong k[f_1, \dots, f_n]$, i.e. the f_i have no algebraic dependence.

Hilbert showed that S is finitely generated, and for many other groups too. Along the way he proved 4 large theorems

1. Basis Theorem
2. Nullstellensatz
3. Polynomial nature of the Hilbert function
4. Syzygy Theorem.

Emmy Noether 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 (and other equivalent definitions).

Noether developed the theory of ideals for Noetherian rings, for example primary decomposition which generalises factorisation into primes in number theory.

<u>Link between commutative algebra and algebraic geometry:</u>

Fundamental theorem of algebra:

$f \in \mathbb{C}[x]$ is determined (up to scalar multiples) by its zeroes (up to multiplicity).

Given $f \in \mathbb{C}[x_1, \dots, x_n]$ there is a polynomial function

$f : \mathbb{C}^n \to \mathbb{C}$, $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$

Thus we get polynomial functions on affine n-space.

Given $I \subset \mathbb{C}[x_1, \dots, x_n]$ define $Z(I) = \{a \in \mathbb{C}^n : f(a) = 0 \ \forall f \in I\}$

Such a subset of $\mathbb{C}^n$ is an <u>algebraic set</u>.

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

Commutative Algebra ①

For a subset $S \subset \mathbb{C}^n$ define $I(S)$

$:= \{f \in \mathbb{C}[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \ \forall (a_1, \dots, a_n) \in S\}$

This is an ideal of $\mathbb{C}[x_1, \dots, x_n]$. Moreover it is <u>radical</u> i.e. if $f^r \in I(S)$ for some $r \geq 1$, then $f \in I(S)$.

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

$$\begin{array}{ccc} \text{Radical Ideals in } \mathbb{C}[x_1, \dots, x_n] & \longleftrightarrow & \text{Algebraic Subsets of } \mathbb{C}^n \\ I & \longmapsto & Z(I) \\ I(S) & \longmapsfrom & S \end{array}$$

In particular the maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$ correspond to points in $\mathbb{C}^n$.

<u>Remark</u>

There is a topology on $\mathbb{C}^n$ under which the closed sets are the algebraic ones : the <u>Zariski Topology</u>.

<u>Basis Theorem</u>

If R is Noetherian, then $R[X]$ is.

<u>Corollary</u>

If k is a field then $k[x_1, \dots, x_n]$ is Noetherian.

Quite a large section of the course is about dimension theory. There are (at least) 3 ways of defining dimension.

1. Maximal length of prime ideals.
2. In the geometric context, we look at growth rates (c.f. 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 4th method using homological algebra, which for "nice" Noetherian rings gives the same answer again.
Most of the theory is from 1920 - 1950.

Commutative Algebra ②

1 Noetherian Rings

In this chapter, R is a commutative ring with 1.

1.1

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

i) Every submodule of M is finitely generated

ii) Ascending Chain Condition: there is no strictly ascending chain of submodules.

iii) Every non-empty subset of submodules of M contains at least one maximal element.

Proofs

i) $\Rightarrow$ ii) Suppose $M_1 \subsetneq M_2 \subsetneq \dots$. Let $N = \bigcup M$. N is a submodule of M. Assuming i), N is finitely generated, but then the finite generating set lies in M_j for some j. Thus $N = M_j$, but this contradicts $M_j \subsetneq M_{j+1}$ ※

ii) $\Rightarrow$ iii) Assume ii). Let S be a non-empty subset of submodules. Choose $M_1 \in S$. If M_1 is maximal, we are done. If not, choose M_2 which is bigger, and repeat; eventually, by ii), the process stops.

iii) $\Rightarrow$ i) Assume iii). Let N be a submodule of M, and S be the set of all finitely generated submodules of N. S contains the zero module, so it is non-empty. Hence, it has a maximal element, say L. If $\exists x \in N \setminus L$, then $L + Rx$ is a finitely generated submodule of N, and $L + Rx \supsetneq L$.

But L was maximal ⚡. Hence $L = N$ and 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 $\Leftrightarrow$ N and M/N are both Noetherian

Proof

$\Rightarrow$) Every submodule of N is also a submodule of M, and so is finitely generated. M/N is finitely generated using the projection map $\Theta : M \to M/N$, since the preimage of a submodule of M/N is finitely generated.

$\Leftarrow$) Suppose that N and M/N are Noetherian and $L_1 \leq L_2 \leq \dots$ is an ascending chain of submodules of M. Set $\begin{cases} Q_i/N = (L_i + N)/N \\ N_i = L_i \cap N \end{cases}$. By the Ascending Chain Condition, there are r, s such that $Q_i/N = Q_r/N$, $N_j = N_s$ for $i \geq r$, $j \geq s$. Set $L = \max(r, s)$

For $i \geq L$, if $L_i \supsetneq L_L$, then $\exists x \in L_i \setminus L_L$

~~$x \neq n = y + n + N$, $y \in L_i$, $n \in N$.~~

But $Q_i/N = Q_L/N$ so $x + N = y + n + N$, $y \in L_L$, $n \in N$

Then $x - y \in N$, and since $L_L \subseteq L_i$, $x - y \in L_i$

But $L_i \cap N = L_L \cap N$, so $x - y$, hence $x \in L_L$ ⚡

Hence $L_i = L_L$ for $i \geq L$, and M is Noetherian.

Commutative Algebra ②

Lemma 1.4

Suppose that $M = M_1 + \dots + M_n$ (not necessarily a direct sum).
Then M is Noetherian $\Leftrightarrow$ Each M_i is Noetherian.

Proof

$\Rightarrow$) Any submodule of a given M_i is a submodule of M, and hence finitely generated.

$\Leftarrow$) If each M_i is Noetherian, then $M_1 \oplus M_2 \oplus \dots \oplus M_n$ is Noetherian, and so M is, since it is an image of $M_1 \oplus \dots \oplus M_n$ under the canonical map $M_1 \oplus \dots \oplus M_n \to M_1 + M_2 + \dots + M_n$

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 simply the ideals, so ACC for modules corresponds to ACC for ideals.

Lemma 1.6

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

Proof

Suppose that $M = Rm_1 + \dots + Rm_n$. We have surjective R-module maps $R \to Rm_i$, $r \mapsto rm_i$. R is Noetherian and so Rm_i is. Hence by 1.4, M is Noetherian.

Theorem 1.7 (Hilbert's 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 $I(n) = \{\text{polynomials in } I \text{ of degree} \leq n\}$. $0 \in I(n)$, so $I(n)$ is non-empty. $I(0) \subseteq I(1) \subseteq \ldots$.

Let $R(n)$ be the set of all leading coefficients of elements of $I(n)$. $R(0) \subseteq R(1) \subseteq \ldots$ and each is an ideal of R. R is Noetherian, so $\bigcup_n R(n) = R(N)$ for some $N \in \mathbb{N}$. Each of $R(0), R(1), \ldots, R(N)$ is finitely generated (second use of Noetherian). Each $R(j)$ is generated by $a_{j1}, \ldots, a_{jk_j}$ say, and these are leading coefficients of $f_{j1}, \ldots, f_{jk_j}$ in $I(j)$.

If $f \in R[x]$ of degree $j \leq N$, then the leading coefficient is generated by $a_{j1}, \ldots, a_{jk_j}$, so $f - r_1 f_{j1} - \ldots - r_{k_j} f_{jk_j}$ has degree $< j$. If $j > N$ then the leading coefficient is generated by $a_{N1}, \ldots, a_{Nk_N}$, so $f - x^t(r_1 f_{N1} + \ldots + r_{k_N} f_{Nk_N})$ has degree $< j$ (for the correct power of t).

Hence, by induction on j, $I = \langle f_{jk} \mid j \leq N, 1 \leq k \leq k_j \rangle$

Remark

In practice, Gröbner bases are used for ideals. They are generating sets with added properties that make algorithms efficient.

Examples

1. Fields are Noetherian (the only ideals are $\{0\}$, k).
2. PIDs e.g. $k[x]$, $\mathbb{Z}$ (k a field) are Noetherian.
3. $\{q \in \mathbb{Q} \mid q = \frac{m}{n},\ m, n \in \mathbb{Z},\ p \nmid n$ for fixed $p\}$ 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:
   $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$
5. By repeated application of 1.7, $k[x_1, \ldots, x_n]$ is Noetherian, and so is $\mathbb{Z}[x_1, \ldots, x_n]$. Any finitely generated ring is Noetherian (since such a ring is an image of $\mathbb{Z}[x_1, \ldots, x_n]$).
6. $R[[x]]$ (formal power series) is Noetherian for R Noetherian:
   Let $I \subset R[[x]]$ be an ideal and let $I(n)$ be the set of elements $a \in R$ such that for some $f \in I$, a is the trailing coefficient of f. Each $I(n)$ is an ideal and $I(0) \subseteq I(1) \subseteq \ldots$.
   R is Noetherian, so for some $N \in \mathbb{N}$, $I(N) = I(N+1) = \ldots$.
   Each $I(n)$ is finitely generated by $a_{n1}, \ldots, a_{nk_n}$, corresponding to $f_{n1}, \ldots, f_{nk_n}$ in I.
   Now let $f = \sum_{i=0}^{\infty} c_i x^i \in I$.
   By choosing the right linear combination of the f_{0k}, $f - (r_{01} f_{01} + \ldots + r_{0k} f_{0k})$ has constant term 0.
   Repeat for the f_{1k}, and so on. This expresses f in terms of the f_{jk} after infinitely many steps.

16/10/13

Commutative Algebra ③

(1.8) R Noetherian $\Rightarrow R[[x]]$ Noetherian

Proof

Either by using trailing coefficients and method analagous to the Basis Theorem

OR

Use Cohen's Theorem

Theorem 1.9 (Cohen's Theorem)

If every prime ideal is finitely generated, then R is Noetherian.

Proof

Suppose that R is not Noetherian, 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 that the family is non-empty and that an ascending chain of non f.g. ideals has union which is non f.g.)

Claim

I is prime (and hence we have a contradiction since we assumed all prime ideals to be f.g).

Suppose not. $\exists a \notin I, b \notin I$ but with $ab \in I$.

Then $I + Ra$ is an ideal strictly containing I. Maximality of I ensures that $I + Ra$ is f.g. by $i_1 + r_1 a, \ldots, i_n + r_n a$, say.

↑ so in particular $I+Ra$ really is an ideal since R cannot be f.g.

Let $J = \{s \in R : sa \in I\} \supsetneq I + Rb \supsetneq I$.

J is "I divided by a"

So by maximality of I, we know J is f.g.

$J = \{s \in R : sa \in I\} \supseteq I + Rb \supsetneq I$

We prove that $I = Ri_1 + \ldots + Ri_n + Ja$, a f.g ideal, a contradiction.

Take $t \in I \leq I + Ra$. So $t = u_1(i_1 + r_1 a) + \ldots + u_n(i_n + r_n a)$ for some $u_i \in R$. So $u_1 r_1 + \ldots + u_n r_n \in J$, so it is of the required form. □

To use Cohen's Theorem, we apply

Proposition 1.10

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

Then P is a f.g. ideal of $R[[X]] \iff \theta(P)$ is an f.g. ideal of R

Proof

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

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

Easy case — If $X \in P$ then P is generated by $a_1, \ldots, a_n$ and X. (since if $c_0 + c_1 X + \ldots \in P$ then $c_0 \in P$, but $c_0 \in \theta(P)$)

Harder, needs P prime — If $X \notin P$ then let $f_1, \ldots, f_n$ be power series with constant terms $a_1, \ldots, a_n$. Take $g \in P$, $g = b + \ldots$ (constant term).

Put $b = \sum_i b_i a_i$. So $g - \sum b_i f_i = g_1 X$ for some g_1.

Note $g_1 X \in P$. But P is prime, and $X \notin P$. $\therefore g_1 \in P$.

Similarly $g_1 = \sum c_i f_i + g_2 X$, $g_2 \in P$

Continuing, we get $h_1, \ldots, h_n \in R[[X]]$ such that

$h_i = b_i + c_i X + \ldots$ with $g = h_1 f_1 + \ldots + h_n f_n$. □

16/10/13

Commutative Algebra ③

1.11 (R commutative, not necessarily Noetherian)

The set $N(R)$ of all nilpotent elements of R is an ideal.

$R/N(R)$ has no non-zero nilpotent ideals.

Proof:

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

If x and $y \in N(R)$, $x^n = 0$, $y^m = 0$ for some m, n.

$(x+y)^{n+m+1} = 0$, so $x+y \in N(R)$.

If $S \in R/N(R)$, $S = x + N(R)$ then $S^n = x^n + N(R)$

If $S^n = N(R)$ then $x^n \in N(R)$, and $x^{mn} = 0$

(hence $x \in N(R)$, $S = N(R)$).

Definition 1.12

This ideal $N(R)$ is the nilradical of R.

1.13 (Krull)

$N(R)$ is the intersection of all 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. So $x \in P$. Hence $N(R) \leq I$.

Now suppose that x is not nilpotent. Set

$S = \{\text{ideals } J : \text{for } n > 0,\ x^n \notin J\}$.

S is non-empty as $(0) \in S$. We can apply Zorn's Lemma again to get a maximal member J_1 of S (if R is Noetherian, Zorn is not needed).

We claim that J_1 is prime:

Suppose that $yz \in J_1$ with $y \notin J_1$, $z \notin J_1$.
Then the ideals $J_1 + Ry$ and $J_1 + Rz$ strictly contain J.
Hence $x^n \in J_1 + Ry$, $x^n \in J_1 + Rz$ for some n.
So $x^{2n} \in J_1 + Ryz$, $= J_1$, so $yz \notin J_1$ ※ □

$\phi : R \to R/I$, $\sqrt{I} = \phi^{-1}(N(R/I))$

1.14 Definition
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

$$\sqrt{I} = \bigcap_{P \text{ prime}, P \supseteq I} P = \{x \in R : x^n \in I, \text{ some } n > 0\}$$

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

1.16 Nakayama's Lemma
If M is a finitely generated R-Module with $MJ = M$ $(J = J(R))$ then $M = 0$.

Proof (non-zero) We prove $M \neq 0 \Rightarrow MJ \subsetneq M$
In any f.g. R-module, Zorn (or Noetherian property) yields maximal (proper) submodules. Take M_1 maximal in M. Then M/M_1 is a simple (or irreducible) R-module, and taking a generator of M/M_1, $m + M_1$ say, then $M/M_1 \cong R/I$ with I a maximal ideal of R (via $R \to M/M_1$, $r \mapsto r(m + M_1)$, an R-module homomorphism ↳ generator used here with kernel necessarily a maximal ideal). But by definition $J \leq I$ ↳ or R/I has submodules
So $MJ \leq M_1 \subsetneq M$. So if $M \neq 0$ then $MJ \subsetneq M$ □

So works for any ideal $J' \leq J$ e.g. $N(R) \leq J(R)$

18/10/13

Commutative Algebra ④

For a commutative ring $N(R) = \bigcap_{P \text{ prime}} P \leq J(R) = \bigcap_{P \text{ maximal}} P$

These need not be equal.

e.g. $R = \{ \frac{m}{n} \in \mathbb{Q} : \text{a fixed prime } p \nmid n \}$ has unique maximal ideal $P = \{ \frac{m}{n} \in \mathbb{Q} : p \mid m, p \nmid n \}$

This is an integral domain, so there are no non-zero nilpotent elements.

$N(R) = 0$, $J(R) = P$.

However, for rings of the form $k[x_1, \dots, x_n]/I$, $k = \bar{k}$, I any ideal, we have $N(R) = J(R)$.

This is the context of the Nullstellensatz. There are "weak" and "strong" versions.

<u>Lemma 1.17</u> (Artin and Tate)

Let $R \subseteq S \subseteq T$ be (commutative) rings. Suppose that R is Noetherian, and T is generated by R and finitely many elements $t_1, \dots, t_n$. Suppose that T is a finitely generated S-module. Then S is generated by R and finitely many elements.

<u>Proof</u>

Let T be generated by $x_1, \dots, x_n \in T$ as an S-module i.e. $T = Sx_1 + \dots + Sx_n$. Then i) $t_i = \sum_j s_{ij} x_j$ for some $s_{ij} \in S$, ii) $x_i x_j = \sum s_{ijk} x_k$ for some $s_{ijk} \in S$.

Let S_0 be the ring generated by R and the s_{ij} and s_{ijk}.

Thus $R \subseteq S_0 \subseteq S$. Any element of T is a 'polynomial' in the t_i with coefficients in R. Using ① and ② we see that

each element of T 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.

S is a 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.

1.18 Lemma

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

Proof

Suppose that R is generated by k and $x_1, \ldots, x_n$ say, and is a field.

If R is not algebraic over k we can reorder our $x_1, \ldots, x_n$ so that $x_1, \ldots, x_m$ are algebraically independent.

(i.e. the ring generated by k and $x_1, \ldots, x_m$ ($\cong$ 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 f.g. module. (generated by $x_{m+1}, \ldots, x_n$ and products)

(R contains a copy of F since R is a field).

Apply 1.17 for $k \subseteq F \subseteq R$. It follows that F is a finitely generated k-algebra generated by k and $q_1, \ldots, q_e$ say with each $q_i = f_i/g_i$ with $f_i \in k[x_1, \ldots, x_m]$, $g_i \in$ ↗, $g_i \neq 0$

$\exists$ a polynomial h which is prime to each of the g_i (e.g. $g_1 \dots g_m + 1$) and the element $\frac{1}{h}$ cannot be in the ring generated by k and $q_1, \dots, q_t$ ⁂

Hence R is algebraic over K. □

Theorem 1.19 (Weak Nullstellensatz)

Let k be a field, S a finitely generated k-algebra. Let P be a maximal ideal. Then S/P is a finite algebraic extension of k. In particular if $k = \bar{k}$, then $S/P \cong k$.

Proof

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

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 of S. 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 $\bar{s}$ = image of S in $S/P = R$. S/P is an integral domain (since P is prime) and finitely generated as a k-algebra by $r_1, \dots, r_t$. Invert $\bar{s}$ to get $T = \langle R, \bar{s}^{-1} \rangle \subseteq$ fraction field

Take a maximal ideal Q of T. By 1.19 $T/Q \cong k$, and so $Q \cap R$ contains elements $r_i - \lambda_i$ for some $\lambda_i \in k$.

otherwise T/Q is an algebraic extension of k.

Hence $Q \cap R$ is a maximal ideal of R, not containing $\bar{S}$.
Thus $\exists$ a maximal ideal of S containing P but not s.
Thus $\bigcap \{\text{maximal ideals containing } P\} = P$.

1.21 Lemma

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

Proof

Suppose $x_1, \ldots, x_n$ 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 $x_1^{r_1} \ldots x_n^{r_n}$ with $\sum r_i = n$.
We must have some $r_i \geq n_i$. Hence all these products lie in I.

1.22

If R is Noetherian, a radical ideal is the intersection of finitely many prime ideals.

21/10/13

Commutative Algebra (5)

1.22

If R is Noetherian a radical ideal is the intersection of finitely many primes.

Proof

Suppose not, and take I to be a maximal member of the set of radical ideals not of this form. We claim that I is prime ~~Yields a contradiction~~

Suppose not. Then $\exists$ ideals $J_1, J_2 \not\geq I$ but with $J_1 J_2 \leq I$

So maximality of I gives that $\sqrt{J_1} = Q_1 \cap \dots \cap Q_s$,

$\sqrt{J_2} = Q_1' \cap \dots \cap Q_t'$, Q_i, Q_j' prime.

Set $J = \sqrt{J_1} \cap \sqrt{J_2} = Q_1 \cap \dots \cap Q_s \cap Q_1' \cap \dots \cap Q_t'$

So $J^{m_1} \leq J_1$ and $J^{m_2} \leq J_2$ for some m_1, m_2.

Hence $J^{m_1+m_2} \leq J_1 J_2 \leq I$. But I is radical and ~~so~~ $J \leq I$. But all $Q_i, Q_j' \geq I$ and so $J \geq I$.

Hence $J = I$ ※ □

Now suppose that $\sqrt{I} = P_1 \cap \dots \cap P_n$. We may remove any prime which contains one of the others and assume that $P_i \not\leq P_j$ for $i \neq j$ for $i \neq j$. If P is prime with $\sqrt{I} \leq P$ then $P_1 \dots P_m \leq \cap P_i = \sqrt{I} \leq P$ and so $P_i \leq P$.

1.23 Definition

The minimal primes over an ideal I of a Noetherian ring are those such that if P' prime, $I \leq P' \leq P$, 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 the intersection and hence in $\sqrt{I}$. Now 1.21 yields the final statement.

1.25 Definition

Let M be a finitely generated R-module, R Noetherian. A prime ideal P is an *associated prime of M* if it is the annihilator of an element of M ($\mathrm{Ann}(m) = \{r \in R : rm = 0\}$)

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

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

1.26 Definition

A sub-module N of M is *(P-) primary* if $\mathrm{Ass}(M/N) = \{P\}$ for a prime ideal P. An ideal I is (P-)primary if I is P-primary as a module.

1.27 Lemma

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 $\prod I_j \leq \mathrm{Ann}(M) = P$.
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

1.28 Lemma

Let Q be maximal among all annihilators of non-zero elements of M. Then Q is prime and so $Q \in \mathrm{Ass}(M)$.

Proof

~~Suppose that it is not prime.~~ Let $Q = \mathrm{Ann}(m)$ and $r_1 r_2 \in Q$ with $r_2 \notin Q$. We show that $r_1 \in Q$.

$r_1 r_2 \in Q \Rightarrow r_1 r_2 m = 0$, so $r_1 \in \mathrm{Ann}(r_2 m)$.

$r_2 \notin Q \Rightarrow r_2 m \neq 0$. But $Q \leq \mathrm{Ann}(r_2 m)$. Hence Q and r_1 lie in $\mathrm{Ann}(r_2 m)$. Maximality of Q among annihilators forces $r_1 \in Q$. □

1.29 Lemma

For a finitely generated, non-zero R-module M with R Noetherian, there is a chain of submodules $0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$ 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 $\mathrm{Ann}(m_1)$ prime, P_1 say. Set $M_1 = Rm_1$. Thus $M_1 \cong R/P_1$. Repeat for M/M_1 to find $M_2/M_1 \cong R/P_2$ for prime P_2. Repeat, and the

process terminates since R is Noetherian. □

1.30 Lemma

If $N \leq M$, $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$

Proof

Suppose that $P = \mathrm{Ann}(m)$ for some $m \in M$, P prime. Let $M_1 = Rm \cong R/P$. For any $0 \neq m_1 \in M_1$, $\mathrm{Ann}\, m_1 = P$ since P is prime. If $M_1 \cap N \neq 0$, then $\exists m_1 \in M_1 \cap N$ 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 f.g. R-module (when R is Noetherian)

Proof

Use 1.30 inductively on the chain in 1.29, recalling that $\mathrm{Ass}(R/P_i) = \{P_i\}$. So $\mathrm{Ass}(M) \subseteq \{P_1, \ldots, P_t\}$

23/10/13 Commutative Algebra ⑥

1.32 Proposition

Each minimal prime over I (an ideal) is an associated prime of R/I.

Proof

By 1.24 there is a product of minimal primes over I (possibly with repetition) contained in I. $P_1^{s_1} \dots P_n^{s_n} \leq I$ with $P_i \neq P_j$ for $i \neq j$.

Consider $\mathrm{Ann}\left(\frac{P_2^{s_2} \dots P_n^{s_n} + I}{I}\right) = J$. Certainly $J \geq P_1^{s_1}$.

Also $J P_2^{s_2} \dots P_n^{s_n} \leq I \leq P_1$, and since P_1 is prime, we have $J \leq P_1$ (since P_i are distinct minimal primes).

Let $M = \frac{P_2^{s_2} \dots P_n^{s_n} + I}{I}$. Use 1.29, and there is a chain of submodules in M; $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_t = M$ such that each factor $\frac{M_i}{M_{i-1}} \cong R/Q_j$ 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 Q_j ensures that $P_1 \leq Q_j$ for each j. Not all the $Q_j \supsetneq P_1$ since $\prod Q_j \leq J \leq P_1$. Hence some $Q_j \leq P_1$, so $P_1 = Q_j$, say Q_1.

Pick the least j such that $Q_j = P_1$, and then $\prod_{k<j} Q_k \not\leq P_1$.

Take $x \in M_j/M_{j-1}$. If $j = 1$, then $\mathrm{Ann}(x) = P_1$, and so $P_1 \in \mathrm{Ass}(R/I)$. ($\to Q_1 = P_1$, $x \in R/P_1 \cong M_1/M_0$)

If $j > 1$, 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 $P_1 \leq \mathrm{Ann}(rx)$, ~~since M_j/M_{j-1}~~. However, $rx \in M_{j-1}$ since $M_j/M_{j-1} \cong R/Q_j = R/P_1$.

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

Example

$P \in \mathrm{Ass}(R/I)$, but P is not minimal on I, taking

$R = K[X, Y]$, $P = (X, Y) > (X) = Q$

$I = PQ = (X^2, XY)$. Then $\mathrm{Ass}(R/I) = \{P, Q\}$

But Q is the only minimal prime over I. Not all associated primes are minimal.

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 $N \leq M$ a submodule. Then there exist $N_1, \ldots, N_t$ ← submodules with

$N = N_1 \cap \ldots \cap N_t$, with $\mathrm{Ass}(M/N_i) = \{P_i\}$ for some distinct $P_1, \ldots, P_t$ (i.e. N_i is a P_i-primary submodule of M).

Remark

In the example above, I is not Q-primary despite $\sqrt{I} = Q$.

But $I = Q \cap P^2$ is a primary decomposition

Alternative definition

A primary ideal I is such that

i) I is proper

ii) If $ab \in I$ but $a \notin I$, then $\exists n$ such that $b^n \in I$.

(Exercise: The two definitions match.)

If so, $\sqrt{I}$ is a prime ideal P and I is P-primary.

2 Localisation

Not necessarily Noetherian

Let R be a commutative ring with 1.

Let S be a multiplicatively closed subset of R, i.e.

i) S is closed under multiplication

ii) $1 \in S$ (by convention)

Define a relation '$\equiv$' on $R \times S$ by $(r_1, s_1) \equiv (r_2, s_2)$

$\Leftrightarrow (r_1 s_2 - r_2 s_1)x = 0$ for some $x \in S$.

This is reflexive, symmetric, and transitive.

For transitivity, suppose $(r_1, s_1) \equiv (r_2, s_2)$ and $(r_2, s_2) \equiv (r_3, s_3)$.

Then $\exists x, y \in S$ with $(r_1 s_2 - r_2 s_1)x = 0 = (r_2 s_3 - r_3 s_2)y$

Then $(r_1 s_3 - r_3 s_1) s_2 x y = 0$. S is multiplicatively closed so $s x y \in S$. 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 a ring with

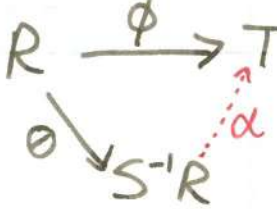
addition $(a_1/s_1) + (a_2/s_2) = (a_1 s_2 + a_2 s_1 / s_1 s_2)$,

multiplication $(a_1/s_1)(a_2/s_2) = a_1 a_2 / s_1 s_2$

$\theta : R \to S^{-1}R$, $r \mapsto r/1$ is a ring homomorphism.

2.1

Let $\phi : R \to T$ be a ring homomorphism, with $\phi(s)$ a unit of T for all $s \in S$. Then, there exists a unique ring homomorphism $\alpha : S^{-1}R \to T$ with $\phi = \alpha \circ \theta$



Proof

Exercise.

$\alpha : S^{-1}R \to T$

$r/s \mapsto \phi(r)$ …

Examples

1. Fraction fields of integral domains R: put $S = R \setminus \{0\}$
2. $S^{-1}R$ is the zero ring $\Leftrightarrow 0 \in S$
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 $S = R \setminus P$.

We write R_P for $S^{-1}R$ in this case. The process of passing from R to R_P is localisation.

The elements r/s with $r \in P$ form an ideal of R_P. This is a unique maximal ideal in R_P:

If r/s is such that $r \notin P$ then $r \in S$ and so has an inverse in R_P.

Def 2.2 A ring with a unique maximal ideal is local

Remark

Some authors require a local ring to be Noetherian.

Examples

1. $R = \mathbb{Z}$, $P = (p)$ a prime ideal (so p is prime).
   $R_P = \left\{ \frac{m}{n} : p \nmid n \right\} \subseteq \mathbb{Q}$, example from the introduction of a Noetherian ring
2. $R = k[X_1, \ldots, X_n]$, $P = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$
   R_P is a subring of $k(X_1, \ldots, X_n)$ where the rational functions are defined at $(a_1, \ldots, a_n) \in k^n$. The unique maximal ideal consists of those functions which are 0 at $(a_1, \ldots, a_n)$.

25/10/13

Commutative Algebra (7)

Modules

Given an R-module M, we can define '$\equiv$' on $M \times S$ with respect to a multiplicatively closed set S by $(m_1, s_1) \equiv (m_2, s_2)$ iff there is an $x \in S$ with $x(s_1 m_2 - s_2 m_1) = 0$.

This is an equivalence relation – check equivalence classes $m/s \in S^{-1}M$. $S^{-1}M$ is an $S^{-1}R$-module via.

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

$$(r_1/s_1)(r_2/s_2) = r_1 r_2 / s_1 s_2$$

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

If $\theta : M_1 \to M$ is an R-module map then

$S^{-1}\theta : S^{-1}M_1 \to S^{-1}M$ is an R-module map

$S^{-1}\theta : m/s \mapsto \theta(m)/s$

and if $\phi : M_1 \to M_2$ then $S^{-1}(\phi \circ \theta) = S^{-1}\phi \circ S^{-1}\theta$.

Definition

A sequence of R-modules $M_0 \to M_1 \to \dots \xrightarrow{\theta} M_i \xrightarrow{\phi} \dots \to M_t$ is exact at M_i if $\operatorname{Im}\theta = \ker\phi$. A short exact sequence is of the form $0 \to M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2 \to 0$ with exactness at M_1, M and M_2 and so θ is injective, ϕ is surjective, and $\operatorname{Im}\theta = \ker\phi$

2-3 Lemma

If M_1, M, M_2 are R-modules and $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2$ is exact at M, then $S^{-1}M_1 \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\phi} S^{-1}M_2$ is exact at $S^{-1}M$.

Proof

Since $\ker\phi = \mathrm{Im}\,\theta$ we have $\phi\circ\theta = 0$.

So $(S^{-1}\phi)\circ(S^{-1}\theta) = S^{-1}(0) = 0$ and hence

$\mathrm{Im}\,S^{-1}\theta \subseteq \ker S^{-1}\phi$. Now suppose that $m/s \in \ker S^{-1}\phi \subseteq S^{-1}M$

So $\phi(m)/s = 0$ in $S^{-1}M_2$, and there is $t\in S$ with

$t\phi(m) = 0$ in M_2. But $t\phi(m) = \phi(tm)$ since ϕ is an

R-module map. So $tm \in \ker\phi = \mathrm{Im}\,\theta$ and $tm = \theta(m_1)$

for some $m_1 \in M_1$.

Hence in $S^{-1}M$, $m/s = \theta(m_1)/ts = S^{-1}\theta(m_1/ts) \in \mathrm{Im}\,S^{-1}\theta$

Thus $\ker S^{-1}\phi = \mathrm{Im}\,S^{-1}\theta$. □

2.4 Lemma

Let N be a submodule of M.

Then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$

Proof

Apply 2.3 to the Short Exact Sequence $0 \to N \xrightarrow{\theta} M \xrightarrow{\phi} M/N \to 0$,

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

$\phi: R \to S^{-1}R, r \mapsto r/1$. If I is an ideal in R then $S^{-1}I$ is an

ideal of $S^{-1}R$.

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 $S^{-1}R$. If $\frac{r}{s} \in J$ then $\frac{r}{1} \in J$.
Let $I = \{r \in R : \frac{r}{1} \in J\}$. Thus $r \in I$. Clearly $J \subseteq S^{-1}I$
If $r \in I$ then $\frac{r}{1} \in J$ and hence $\frac{r}{s} \in J$, so $S^{-1}I = J$.
2. Let Q be a prime ideal in $S^{-1}R$. Then set $P = \{r \in R : \frac{r}{1} \in Q$

Q prime $\Rightarrow P$ prime, $P \cap S = \emptyset$

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

P does not meet S: if $r \in S$ then $\frac{r}{1}, \frac{1}{r} \in Q$, and $1 \in Q$ *

P prime, $P \cap S = \emptyset \Rightarrow S^{-1}P$ prime

Conversely, if $\frac{r}{s} \frac{x}{y} \in S^{-1}P$ then $\frac{rx}{sy} \in S^{-1}P$
So $z(rx) \in P$ for some $z \in S$.
$\Rightarrow rx \in P$ or $z \in P$ (impossible since $z \in S$).
$\Rightarrow r \in P$ or $x \in P \Rightarrow \frac{r}{s} \in S^{-1}P$ or $\frac{x}{y} \in S^{-1}P$ □

2.6

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

Proof

Any chain of ideals in $S^{-1}R$ is of the form $J_1 \subseteq J_2 \subseteq \dots$
Consider $I_k = \{r \in R : \frac{r}{1} \in J_k\}$. Then $I_1 \subseteq I_2 \subseteq \dots$
This must terminate since R is Noetherian. So $I_t = I_{t+1} = \dots$
for some t. Then $J_t = J_{t+1} = \dots$ since $J_k = S^{-1}I_k$ for each k □

2.7 Definition

A property $\mathcal{P}$ of a ring R (or an R-module M) is local if R (or M) has the property $\mathcal{P}$ $\Leftrightarrow$ R_p (or M_p) has property $\mathcal{P}$ for each prime ideal P.

2.8 Lemma

The following are equivalent:

i) $M = 0$

ii) $M_p = 0$ for all prime ideals P of R (i.e. being 0 is a local property)

iii) $M_Q = 0$ for all maximal ideals Q of R

Proof

i) $\Rightarrow$ ii) $\Rightarrow$ iii)

Suppose that iii) holds and $M \neq 0$. Take $0 \neq m \in M$. The annihilator of m is a proper ideal of R. Then, by Zorn's Lemma, it is contained within a maximal ideal Q.

Consider $m/1 \in M_Q$. By assumption $M_Q = 0$ and so $m/1 = 0$.

So $sm = 0$ for some $s \in S$, where $S = R \setminus Q$. But Q contains the annihilator of m ⚡ □

2.9

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

i) ϕ injective

ii) $\phi_p : M_p \to N_p$ injective for all prime ideals P of R

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

Proof: Apply 2.8 to $\ker \phi$, $(\ker \phi)_p$, $(\ker \phi)_Q$

28/10/13

Commutative Algebra (2)

2.10 Lemma

Let P be a prime ideal, 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 $P \subseteq Q$ then $(R_Q)_{PR_Q} \cong R_P$ (taking $S = R \setminus Q$).

Proof

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

Let $\phi = \theta_2 \circ \theta_1$. Then ϕ is a ring homomorphism, with $\phi(s)$ a unit for all $s \in S' = R \setminus P$. So we can apply our universal property

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

to give a unique ring homomorphism α

To show that α is injective, suppose that $r/s' \in \ker \alpha \subseteq R_P$ with $s' \in S'$. Then $r/1 \in \ker \alpha$ and hence $r \in \ker \phi$.

But if $\phi(r) = 0$ then $(r/1)(x/y) = 0$ in $S^{-1}R$ for some $x/y \notin S^{-1}P$, and so for some $s \in S$, $sx = 0$, $x \notin P$.

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. (use primeness of P; $y = sx$)

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

3 Dimension

All rings are commutative with a 1.

3.1 Definition

1. The spectrum $\mathrm{Spec}(R) = \{P : P \text{ a prime ideal of } R\}$

(3.2) 2. The length of a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n$ is n (note that the chain starts at 0).

(3.3) 3. The (Krull) dimension $\dim R$ of R is

$\dim R = \sup \{ n : \text{there is a chain of prime ideals of length } n \}$ if this exists

$= \infty$ if the sup does not exist

(3.4) 4. The height $ht(P)$ of $P \in \operatorname{Spec}(R)$

$= \sup \{ n : \text{there is a chain of prime ideals } P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n = P \}$

Note

The 1-1 correspondence between primes which do not meet $R \setminus P$ and the primes of R_P shows that $ht(P) = \dim R_P$.

Examples

1. An Artinian ring (e.g. a field) (ring with DCC on ideals) 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 $(0) \subsetneq (p)$, p prime. Similarly $\dim k[X] = 1$, k a field. These are both examples of Dedekind domains, integrally closed domains of dimension 1. See next chapter.
3. $\dim k[X_1, \dots, X_n] \geq n$ since we have a chain of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, \dots, X_n)$

In fact $\dim k[X_1, \dots, X_n] = n$ 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 sub-ring to the larger ring. First:

3.5 Lemma

The height 1 primes of $k[x_1, \ldots, x_n]$ are precisely those of the form (f) where f is irreducible.

Proof

Compare with Q3, Sheet 1. Height 1 primes in a UFD are the principal ideals generated by an irreducible.

3.6

Let $R \subset S$ be two rings. $x \in S$ is integral over R if it satisfies some monic polynomial with coefficients in R (i.e. algebraic if R is a field). e.g. the elements of $\mathbb{Q}^{alg}$ are integral over $\mathbb{Z}$ are precisely the elements of $\mathbb{Z}$.

3.7

The following are equivalent:

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

ii) $R[x]$ (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 a finitely generated R-module.

Remark

Some authors say that S is finite over R if S is a finitely generated R-module, and a k-algebra R is of finite height if

it is finitely generated as a k-algebra.

Proof (of 3.7)

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

ii) $\Rightarrow$ iii) Trivial.

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

$x y_i = \sum_j r_{ij} y_j$ for each i. So $\sum (x\delta_{ij} - r_{ij}) y_j = 0$

Multiply on the left by the adjugate of the matrix, $A_{ij} = x\delta_{ij} - r_{ij}$.

We deduce that $A y_j = 0$ for all j.

But 1 is an R-linear combination of the y_js. So $\det A = 0$.

But $\det A$ is of the form $x^n + r_{n-1}x^{n-1} + \dots + r_0$. $\square$

Remark

This proof is reminiscent of a proof often used for Nakayama's Lemma.

30/10/13

Commutative Algebra (9)

3.8 Lemma

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

Proof

Easy induction on n.

3.9 The set $T \subseteq S$ 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) $x \pm y$ and xy are integral over R.

3.10 Definitions

i) T is the integral closure of R in S.

ii) If $T = R$, then R is integrally closed in S

iii) If $T = S$, then S is integral over R.

iv) 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

i) $\mathbb{Z}$ is integrally closed

ii) $k[x_1, \ldots, x_n]$ is integrally closed

iii) In an algebraic number field k with $[k : \mathbb{Q}] < \infty$ then the integral closure of $\mathbb{Z}$ in k is $\mathcal{O}_k$, the ring of integers in k.

3.11 Lemma

If $R \subseteq T \subseteq S$, rings, with T integral over R, S integral over T, then S is integral over R.

Proof

Exercise.

3.12 Lemma

Let $R \subseteq T$ 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 $(R+J)/J$ subring of T).

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 $x^n + r_{n-1}x^{n-1} + \dots + r_0 = 0$ (*), $r_i \in R$.
Modulo J (writing $\bar{}$ for images in T/J) we have a monic equation $\bar{x}^n + \bar{r}_{n-1}\bar{x}^{n-1} + \dots + \bar{r}_0 = \bar{0}$ in T/J with $\bar{r}_i \in (R+J)/J$

ii) Suppose that $x/s \in S^{-1}T$. Then x satisfies an equation of the form (*). $(x/s)^n + (r_{n-1}/s)(x/s)^{n-1} + \dots + (r_0/s^n) = 0$ in $S^{-1}T$.
So x/s is integral over $S^{-1}R$.

3.13 Lemma

Suppose that $R \subseteq T$ are integral domains with T integral over R. Then T is a field iff R is a field.

Proof

Proof

Suppose that R is a field. Let $t \in T$, $t \neq 0$ and choose a monic polynomial of least degree of the form $t^n + r_{n-1}t^{n-1} + \dots + r_0 = 0$, $r_i \in R$. T is an integral domain and so $r_0 \neq 0$ (otherwise we note that $t(t^{n-1} + \dots + r_1) = 0$ giving a poly. of lower degree).

So t has an inverse, $-r_0^{-1}(t^{n-1} + r_{n-1}t^{n-2} + \dots + r_1) \in T$ and T is a field.

Conversely, suppose that T is a field. Let $x \in R$, $x \neq 0$.

Then x has inverse x^{-1} in T. So x^{-1} satisfies a monic equation

$x^{-m} + r'_{m-1}x^{-m+1} + \dots + r_0' = 0$

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

Thus R is a field. □

3.14

Let $R \subseteq T$ 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 $\Leftrightarrow$ P is maximal.

Proof

By 3.12 i), T/Q is integral over R/P, and since P, Q are prime, T/Q, R/P are integral domains. So 3.13 implies T/Q is a field $\Leftrightarrow$ R/P is a field. Hence Q maximal $\Leftrightarrow$ P maximal. □

3.15 Theorem (Incomparability)

Let $R \subseteq T$ be rings with T integral over R. Let $Q \subseteq Q_1$ 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 $T_p = S^{-1}T$ integral over R_p.

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. Also, there are $S^{-1}Q$ and $S^{-1}Q_1$ in T_p also prime and $\begin{cases} S^{-1}Q \cap S^{-1}R = S^{-1}P \\ S^{-1}Q_1 \cap S^{-1}R = S^{-1}P \end{cases}$

By 3.14, $S^{-1}Q$ and $S^{-1}Q_1$ are maximal since $S^{-1}P$ is. But $S^{-1}Q \subseteq S^{-1}Q_1$ 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 not meeting S yields $Q = Q_1$. □

3.16 (Lying Over) Theorem

Let $R \subseteq T$ be rings, 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, necessarily prime (primeness preserved under our 1-1 ideal correspondence). Then $S^{-1}Q \cap \overbrace{S^{-1}R}^{R_p}$ is maximal by 3.14. But R_p has a unique maximal ideal, namely $S^{-1}P$, and so $S^{-1}Q \cap S^{-1}R = S^{-1}P$. Therefore $Q \cap R = P$.

01/11/13

Commutative Algebra (10)

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

3.17 (Going Up Theorem)

Let $R \subseteq T$ be rings with T integral over R. Let $P_1 \subseteq \dots \subseteq P_n$ be a chain of prime ideals of R and $Q_1 \subseteq \dots \subseteq Q_m$ (with $m < n$) be a chain of ideals of T with $Q_i \cap R = P_i$ for $1 \leq i \leq m$. Then the chain of Q_i extends to a chain $Q_1 \subseteq \dots \subseteq Q_n$ with $Q_i \cap R = P_i$ for $1 \leq i \leq n$.

3.18 (Going Down Theorem)

Let $R \subset T$ be integral domains, R integrally closed, T integral over R. Let $P_1 \supseteq \dots \supseteq P_n$ be a chain of prime ideals of R and $Q_1 \supseteq \dots \supseteq Q_m$ $(m < n)$ be a chain of prime ideals of T with $Q_i \cap R = P_i$ for $1 \leq i \leq m$.

Then we can extend the chain of Q_i to $Q_1 \supseteq \dots \supseteq Q_n$ with $Q_i \cap R = P_i$ for $1 \leq i \leq n$.

Our major application of these is in the context of finitely generated k-algebras T. (a domain) Noether-normalisation yields $R \subset T$ with T integral over R and $R \equiv$ polynomial algebra and hence integrally closed.

Proof (Going Up Theorem)

By induction. It is enough to consider the case $n=2$, $n=1$.

Write $\bar{R}$ for R/P_1, $\bar{T}$ for T/Q_1. Then $\bar{R} \hookrightarrow \bar{T}$ with $\bar{T}$ integral over $\bar{R}$, using 3.12 ii). By Lying Over 3.16, there is a prime $\bar{Q}_2$ of $\bar{T}$ such that $\bar{Q}_2 \cap \bar{R} = \bar{P}_2$. Lifting back gives a prime ideal Q_2 of T with $Q_2 \supseteq Q_1$, $Q_2 \cap R = P_2$. □

3.19 Corollary (of Going Up)

Let $R \subseteq T$ with T integral over R. Then $\dim R = \dim T$.

Proof

Take a chain $Q_0 \subsetneq \dots \subsetneq Q_n$ of prime ideals in T. By Incomparability 3.15

$P_0 \subsetneq \dots \subsetneq P_n$, prime ideals of R with $Q_i \cap R = P_i$.

Thus $\dim R \geq \dim T$.

Conversely, if $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n$ is a chain of prime ideals of R, there is a prime Q_0 lying over P_0 by 3.16 and Going Up 3.17 gives a chain $Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_n$ with $Q_i \cap R = P_i$ and ~~Incomparability 3.15 ensures~~ with strict inequality. So $\dim R \leq \dim T$ □

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

$ht(Q \cap R) = ht(Q)$

Proof

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

So $ht(Q \cap R) \geq ht(Q)$.

Conversely, if $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n = Q \cap R$ then by the Going Down Theorem 3.18) we have $Q_0 \subsetneq \dots \subsetneq Q$ with $Q_i \cap R = P_i$

So $ht(R \cap Q) \leq ht(Q)$ □

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

3.21 Definition

i) If I is an ideal of R, $R \subset T$ and $x \in T$ is integral over I if x satisfies a monic equation $x^n + r_{n-1}x^{n-1} + \dots + r_0 = 0$ (*) with $r_i \in I$.

ii) The integral closure of I is the set of such x.

3.22 Lemma

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 $R = T$, we get that the integral closure of I in R is $\sqrt{I}$.

Proof

If x is integral over I, then (*) implies that $x^n \in TI$, and so $x \in \sqrt{(TI)}$. Conversely, if $x \in \sqrt{(TI)}$ then $x^n = \sum_{i=1}^{k} t_i r_i$ for some $r_i \in I$, $t_i \in K$. But each t_i is integral over R.

Then 3·8 shows that $M = R[t_1, \ldots, t_k]$ is a finitely generated R-module. Also $x^{\wedge} R[t_1, \ldots, t_k] \subseteq IM$. Let $y_1, \ldots, y_s$ be a generating set of M as an R-module. Then we have

$x^{\wedge} y_j = \sum_i r_{ji} y_i$ with $r_{ji} \in I$.

As in the proof of 3·7, $\sum (x^{\wedge} \delta_{ji} - r_{ji}) y_i = 0$ and we deduce that $x^{\wedge}$ satisfies a monic equation $(x^{\wedge})^s + \ldots + r_0' = 0$ namely $\det A = 0$. Note that all but the top coefficient is in I. Thus x is integral over I.

04/11/13

Commutative Algebra (11)

3.23 Lemma

Let $R \subset T$ be integral domains. R integrally closed and let $x \in T$ be integral over an ideal I of R. Then x is algebraic over the field of fractions k of R and its minimal polynomial over k

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

has its coefficients $r_{n-1}, \dots, r_0$ 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 of Claim: Take an extension field L of k containing all the conjugates $x_1, \dots, x_m$ of x, e.g. a splitting field of the minimal polynomial of x over k.

(Prop. 10.2, Stewart, Galois Theory) There is a k-automorphism of L sending $x \to x_i$ and so if $x^m + r'_{m-1}x^{m-1} + \dots + r_0' = 0$ with $r_i' \in I$, then $x_i^m + r'_{m-1}x_i^{m-1} + \dots + r_0' = 0$.

Thus each x_i is integral over I, and in particular lies in the integral closure T_1 of R in L. 3.12) implies that a polynomial with coefficients in $\mathbb{Z}$ in the x_is 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 of linking coefficients to roots of polynomials. This establishes our claim.

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

Proof (of 3.18. Going Down)

By induction it is enough to look at the case where $n = 2$, $m = 1$. We have $P_1 \supsetneq P_2$, Q_1, $Q_1 \cap R = P_1$. We want to find Q_2 with $Q_1 \supseteq Q_2$ and $Q_2 \cap R = P_2$.

Let $S_2 = R \setminus P_2$ and $S_1 = T \setminus Q_1$, and set $S = S_1 S_2$. $S = \{rt : r \in S_2, t \in S_1\}$. This S is multiplicatively closed and contains both S_1 and S_2 (since 1 is in both S_1 and S_2).

We will show that $TP_2 \cap S = \emptyset$.

Assume this. TP_2 is an ideal of T and so $S^{-1}(TP_2)$ is an ideal of $S^{-1}T$. It is proper since $TP_2 \cap S = \emptyset$ (our assumption). Hence $S^{-1}(TP_2)$ 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 $TP_2 \subseteq Q_2$. Hence $P_2 \subseteq TP_2 \cap R \subseteq Q_2 \cap R$ and since $Q_2 \cap S = \emptyset$ and $S_2 = R \setminus P_2 \subseteq S$, we have $P_2 = Q_2 \cap R$. Similarly, $S_1 = T \setminus Q_1 \subseteq S$ and so $Q_2 \subseteq Q_1$, as desired.

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

Take $x \in TP_2 \cap S$. By 3.22) x is in the integral closure of P_2 in T (using 3.22) in the case $I = P_2$). Hence by 3.23) it is algebraic over the field of factors k of R and its minimal polynomial $X^n + r_{n-1}X^{n-1} + \dots + r_0$ over k has coefficients in $\sqrt{P_2} = P_2$.

But $x \in S$ and so x is of the form rt with $r \in S_2$, $t \in S_1$

So $t = x/r$ has minimal polynomial over k given by

$X^n + r_{n-1}/r\, X^{n-1} + \dots + r_0/r^n$ and these coefficients are in R

(using 3.23) with $I = R$) since $t \in T$ is integral over R.

We write these coefficients as r_i' $(0 \le i \le n-1)$. But $r_i \in P_2$, $r \notin P_2$ and so $r_i' \in P_2$.

So by definition, t is integral over P_2, and so by 3.22), t is in $\sqrt{(TP_2)}$, a contradiction since $t \in S_1 = T \setminus Q_1$ and $TP_2 \subset Q_1$, (and hence $\sqrt{(TP_2)} \subseteq Q_1$). □

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

3.24 Theorem

Let T be a finitely generated k-algebra, which is an integral domain with fraction field L. Then $\dim T$ = Krull Dimension $= \operatorname{tr.deg}(L)$ = transcendence degree

What is transcendence degree? (K a field)

$x_1, \dots, x_n$ are algebraically independent over K if the map $K[X_1, \dots, X_n] \to K[x_1, \dots, x_n]$ $X_i \mapsto x_i$ is an isomorphism, and then $K[x_1, \dots, x_n]$ may be regarded as a polynomial algebra.

As in Linear Algebra, one wants to consider maximal independent sets; these all have the same cardinality.

Such a set is a transcendence basis of L over k and the transcendence degree the cardinality of the set.

Linearly Independent Set $\Leftrightarrow$ Algebraically Independent Set

Span (S) $\Leftrightarrow$ Algebraic Closure of S

Spanning Set $\Leftrightarrow$ S whose algebraic closure is L.

Example

If $L = k(x_1, \ldots, x_n)$ the fraction field of $k[x_1, \ldots, x_n]$ and f is an irreducible in $k[x_1, \ldots, x_n]$, $k = \mathrm{Frac}\left(\frac{k[x_1, \ldots, x_n]}{(f)}\right)$

Then $\mathrm{tr\,deg}\, L = n$, $\mathrm{tr\,deg}\, k = n-1$ since k is an algebraic extension of $k(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n)$ where x_i appears in some term of f.

The key result in proving the theorem is

3.25 Lemma (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.

3.25 Noether's Normalization Lemma

Let T be a finitely generated k-algebra. Then there exists a subring $R = k[x_1, \ldots, x_r]$ with $x_1, \ldots, x_r$ algebraically independent, and T integral over R.

Proof

Let $T = k[a_1, \ldots, a_n]$. Proof is by induction on n, the number of generators. Let r = max. no. of algebraically independent elements. Observe that we may assume that $r \geq 1$, otherwise T is a finite dimensional k-vector space. There is nothing to do if $a_1, \ldots, a_n$ are algebraically independent. We renumber the a_is 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 $f \neq 0$ in $k[x_1, \ldots, x_r, x_n]$ with $f(a_1, \ldots, a_r, a_n) = 0$. Thus $f(x_1, \ldots, x_r, x_n)$ is a sum of terms $\lambda_{\underline{\ell}} x_1^{\ell_1} \cdots x_r^{\ell_r} x_n^{\ell_n}$ where $\underline{\ell} = (\ell_1, \ldots, \ell_r, \ell_n)$ is an $(r+1)$ tuple.

Claim: $\exists$ +ve integers $m_1, \ldots, m_r$ such that $\phi : \underline{\ell} \mapsto m_1\ell_1 + \ldots + m_r\ell_r + \ell_n$ 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 $\lambda_{\underline{\ell}} \neq 0 \neq \lambda_{\underline{\ell}'}$.

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. Pick $(q_1, \ldots, q_r) \in \mathbb{Q}^r$ with each $q_i > 0$ so that $\sum q_i d_i \neq 0$ for all of the finitely many non-zero $(d_1, \ldots, d_r)$. Multiply by a positive integer to get $(m_1, \ldots, m_r)$, $m_i \in \mathbb{Z}_{>0}$ so that $|\sum m_i d_i| > |d_n|$ for all of the finitely many differences $\underline{d}$ with $(d_1, \ldots, d_r) \neq 0$. Thus if $\phi(\underline{\ell}) = \phi(\underline{\ell}')$ then $d_1 = \ldots = d_r = 0$, and so $\ell_n = \ell_n'$ and so $\underline{\ell} = \underline{\ell}'$.

Now for these $m_1, \ldots, m_r$, we set

$$g(X_1, \ldots, X_r, X_n) = f(X_1 + X_n^{m_1}, X_2 + X_n^{m_2}, \ldots, X_r + X_n^{m_r}, X_n)$$

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

Different terms have different powers of X_n, and so there will be a single term with a 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 $1 \leq i \leq r$, 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 coefficient shows that a_n is integral over $k[b_1, \ldots, b_r]$. So for each i with $1 \leq i \leq r$, $a_i = b_i + a_n^{m_i}$ 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.

Proofs of 3·24 (from 3·25)

Let T be a finitely generated k-algebra. Apply 3·25) to get $x_1, \ldots, x_r$ algebraically independent with T integral over $k[x_1, \ldots, x_r]$ ($\cong$ to a polynomial algebra)

By 3·19) $\dim T = \dim k[x_1, \ldots, x_r]$

Thus any finitely generated k-algebra T has dimension equal to the dimension of a polynomial algebra with r variables, where

$\operatorname{tr\,deg}$ (f. field of T) $= r$.
('fraction)

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

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

We prove equality by induction on r. $r = 0$ is trivial.

Assume that $r \geq 1$. If $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_s$ is a chain of prime ideals we may assume that $P_0 = 0$. Since P_1 contains (f), f irreducible, some f ($k[x_1, \ldots, x_r]$ is a UFD, Q3 Sheet 1) we may also assume that $P_1 = (f)$. But $\operatorname{tr\,deg}\left(\operatorname{frac} \frac{k[x_1, \ldots, x_r]}{(f)}\right) = r$.

So $\dim \frac{k[x_1, \ldots, x_r]}{(f)} = \dim k[y_1, \ldots, y_{r-1}]$ for some polynomial algebra with $r-1$ variables. $= r-1$ by induction.

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

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 $ht(Q) + \dim\left(T/Q\right) = n$.

Proof

Let $n = ht(Q)$ and pick a maximal chain $Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_n = Q$

By Noether (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),

$n = \dim R = \text{tr deg } R =$ no. of variables in our polynomial algebra.

Write $P_i = Q_i \cap R$. Observe that $ht(Q_1) = 1$, since otherwise we could find a longer chain. So by 3.20 (Corollary of Going Down) since R is integrally closed, and a polynomial algebra, $ht(P_1) = 1$.

So $P_1 = (f)$ as R is a UFD, f irreducible. Then $\text{tr deg}(\text{frac } R/P_1) = n$

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. Observe:

i) $ht\left(Q/Q_1\right) = n-1$

ii) $\dim\left(T/Q_1\right) = \dim\left(R/P_1\right) = n-1$ since R/P_1 embeds in T/Q_1 as $\frac{R+Q_1}{Q_1}$ and T/Q_1 is integral over it.

iii) $\dim\left(\frac{T/Q_1}{Q/Q_1}\right) = \dim\left(T/Q\right)$.

Induction gives that $(n-1) + \dim\left(T/Q\right) = n-1$.

Hence $ht(Q) + \dim\left(T/Q\right) = n$. □

28/11/13 Commutative Algebra (13)

Remarks

1. If $k \subseteq \mathbb{C}$ then the maximal ideals of $k[x_1, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ by the Nullstellensatz, and so they correspond to points of $\mathbb{C}^n$. But T/TP is finitely dimensional over $\mathbb{C}$, since T is a finitely generated $k[x_1, \ldots, x_r]$-module (integrality over R). So T/TP is Artinian and hence only has finitely many prime ideals, which are all maximal. They correspond to the maximal ideals of T lying over P. Thus there is a map

$$f : \{\text{maximal ideals of } T\} \longrightarrow \{\text{maximal ideals of } k[x_1, \ldots, x_r]\} \cong \mathbb{C}^r$$
$$Q \longmapsto P$$

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 $k = \mathbb{C}$. $g : \{\text{maximal ideals of } T_1\} \to \{\text{maximal ideals of } T\}$
(normal varieties)

and fibres $g^{-1}(Q)$ are finite and non-empty.

(for curves, normal $\equiv$ non-singular)

3.27

Let R be a Noetherian integral domain, integrally closed. $K = \mathrm{Frac}(R)$. 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 fie

is a finitely generated $\mathbb{Z}$-module.

'Proof' (of 3.27)

We use the trace function. $\mathrm{Tr}_{L/K}(x) = -[L : K(x)] \times$ (next to top coeff. in min. poly. of x over K)

for any finite degree field extension L of K.

Equivalently if L is Galois over K, $\mathrm{Tr}_{L/K}(x) = \sum_{g \in Gal(L/K)} g(x)$

the sum of conjugates of x with potential repetitions (the reason why we get a multiple of the polynomial coefficient).

Quote: If L is separable then $L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}(xy)$ is non-degenerate.

Pick a k-vector space basis of L, $y_1, \ldots, y_n$.

By multiplying by suitable elements of K, we may assume $y_i \in T$ (if the min. poly. 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 min. poly. of $\frac{y_i}{(\Pi s_i)}$ has coefficients in R).

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

Let $z \in T$. Then $z = \sum \lambda_i x_i$ with $\lambda_i \in k$.

So $\mathrm{Tr}(z y_j) = \mathrm{Tr}(\sum \lambda_i x_i y_j) = \sum \lambda_i \delta_{ij} = \lambda_j$

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

So $\lambda_j \in R$ for each j. Hence $T \subseteq \sum R x_i$, a Noetherian module.

Hence T is a finitely generated R-module.

08/11/13 Commutative Algebra (13)

Krull's Principal Ideal Theorem (from 1931) tells us about minimal primes over principal ideals.

3.28 (Principal Ideal Theorem)

Let R be a Noetherian ring, and let $a \in R$ be a non-unit. Let P be a minimal prime over (a). Then $ht(P) \leq 1$. Provides inductive step for

3.29 (Generalised Principal Ideal Theorem)

Let R be a Noetherian ring and I a proper ideal generated by n elements. Then $ht(P) \leq n$ for any minimal prime P over I.

3.30 Corollary

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

ii) Every Noetherian local ring has finite dimension

$\leq$ min. number of generators of the unique maximal ideal P

$= {}^{R}/_{P}$ vector space dimension of ${}^{P}/_{P^2}$

Proof (of 3.30 from 3.29)

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

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

$(3.28) \Rightarrow ht(P) \leq$ min. number of generators of P

The final equality follows from Nakayama. If P is generated by $x_1, \ldots, x_n \Leftrightarrow {}^{P}/_{P^2}$ is generated by $\bar{x}_1, \ldots, \bar{x}_n$ where $- : P \to P^2$. $(\Leftarrow)$ is trivial.

($\Leftarrow$) Suppose that $\bar{x}_1, \ldots, \bar{x}_n$ generate P/P^2.

Consider $I = (x_1, \ldots, x_n) \leq P$.

Clearly $I + P^2 = P$ and so $P(P/I) = P/I$

Nakayama $\Rightarrow P/I = 0$.

3.31 Corollary

A Noetherian ring satisfies the DCC on prime ideals.

Proof

If we have a strictly descending chain $P \supsetneq \ldots \supsetneq \ldots$ of prime ideals then the chain can have length at most $ht(P)$.

Using 3.30 i) gives the result.

3.29 (Generalised Principal Ideal Theorem)

Let R be a Noetherian ring, and I a proper ideal generated by n elements. Then $ht(P) \leq n$ for each minimal prime P over I.

3.32 Definition

i) A regular local ring is one where $\dim R = \dim P/P^2$, 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.

ii) In Corollary 3.30), $\dim_{\text{local ring}}^{\text{Noetherian}} \leq$ min # generators of the maximal ideal

The inequality can be strengthened for Noetherian local domains.

dim of the ring = min # generators of some ideal I with $\sqrt{I} = P$.

Proof (of 3.28) Principal Ideal Theorem)

Let P be a minimal prime over (a), $a \in R$ a non-unit.

First, localise at P to get R_P which has a unique maximal ideal $P_P = S_0^{-1}P$, where $S_0 = R \setminus P$. We observe that $S_0^{-1}P$ is a minimal prime over $S_0^{-1}A$ (following from the correspondence between ideals in R and in the localisation R_P). So we may assume that R is local with unique maximal ideal P.

Suppose that $ht(P) > 1$ and so we have a chain of prime ideals $Q' \subsetneq Q \subsetneq P$. Consider $R/(a)$. This has a unique maximal ideal $P/(a)$. Moreover, it is also a minimal prime ideal, so it is the only prime. So $N(R/(a)) = P/(a)$, which is also nilpotent. (R Noetherian)

So $P^n \leq (a)$ for some n. In the chain $R \supsetneq P \supseteq P^2 \supseteq \dots$ 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 $I_n = \{r \in R : \frac{r}{1} \in S^{-1}Q^n\}$ where $S = R/Q$.

Clearly $Q = I_1 \supseteq I_2 \supseteq \dots$ (*) and hence $\frac{(I_1+(a))}{(a)} \supseteq \frac{(I_2+(a))}{(a)} \supseteq \dots$ is a descending chain which necessarily terminates. Then $I_m + (a) = I_{m+1} + (a) = \dots$ for some m.

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

$Q = I_1 \supseteq I_m \supseteq Q^m$. So $x \in I_m$ since we have $S^{-1}R \supseteq S^{-1}Q \supseteq \dots \supseteq S^{-1}Q^m$ and if $\frac{x}{1} \notin S^{-1}Q^m$ then $\frac{xa}{1} \notin S^{-1}Q^m$. 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 $\Rightarrow I_m/I_{m+1} = 0$ and thus $I_m = I_{m+1} = \dots$.

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 $\subsetneq S^{-1}Q$ $\ast$ $\square$

Proof (of (3.29) Generalised Principal Ideal Theorem)

Let R be Noetherian, $I \subsetneq R$ generated by n elements. We're aiming to show that $ht(P) \leq n$ for each minimal prime P over I.

We argue by induction on n, with case $n=1$ the Principal Ideal Theorem

Assume that $n > 1$. We may assume by passing to R_P that R is local with unique maximal ideal P. Pick any prime Q maximal subject to $Q \subsetneq P$, and thus P is the only prime strictly containing Q. We show that $ht(Q) \leq n-1$.

It is sufficient to do this for all such Q as we then deduce that $ht(P) \leq n$.

Since P is minimal over I, $Q \not\supseteq I$. By assumption there are generators $a_1, \ldots, a_n$, and we may assume that $a_n \notin Q$ (reordering if necessary). P is the only prime containing $Q + (a_n)$ so as in the proof of (3.28) $R/(Q+(a_n))$ is Artinian. We 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 $1 \leq i \leq n-1$.

So $a_i^m = x_i + r_i a_n$ for some $x_i \in Q$, $r_i \in R$.

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

Claim:

$\bar{Q}$ is a minimal prime, where $\bar{R} = R/(x_1, \ldots, x_{n-1})$, and

$\bar{\ } : R \to \bar{R}$, $x \mapsto x + (x_1, \ldots, x_{n-1})$

Observe that the unique maximal ideal $\bar{P}$ of $\bar{R}$ is a minimal prime over $\overline{(a_n)}$. We apply the Principal Ideal Theorem to $\bar{P}$. We see that $ht(\bar{P}) \leq 1$ and thus $\bar{Q}$ must have height 0.

Thus $\bar{Q}$ is a minimal prime of $\bar{R}$.

From the claim, we can apply the inductive hypothesis to Q to get $ht(Q) \leq n-1$. □

We consider filtrations by powers of ideals I.

$R \supset I \supseteq I^2 \supseteq \dots$. This is an example of a more general situation where one filters a ring R by R_i satisfying $R_i R_j \subseteq R_{i+j}$. $R_{-j} = I^j$.

We can form the graded ring $\operatorname{gr} R = \bigoplus_{i \in \mathbb{Z}} R_i / R_{i-1}$

13/11/13 Commutative Algebra (15)

Filtrations

3.33 Definition

A ($\mathbb{Z}$) filtered ring R is one whose additive group is filtered by subgroups $\ldots \subseteq R_{-1} \subseteq R_0 \subseteq R_1 \subseteq R_2 \subseteq \ldots$

R_i additive subgroups with $\begin{cases} 1 \in R_0 \\ R_i R_j \subseteq R_{i+j} \end{cases}$ for $i, j \in \mathbb{Z}$.

$\cup R_i$ is a subring, and $\cap R_i$ is an ideal of $\cup R_i$.

We shall assume as is usual that $\cup R_i = R$ "exhaustive" and $\cap R_i = [0]$ "separated".

R_i for $i < 0$ are ideals of R_0.

Examples

i) I an ideal of R. $\begin{cases} R_i = R & \text{for } i \geq 0 \\ R_i = I^{-i} & \text{for } i < 0 \end{cases}$

ii) R a k-algebra generated by $x_1, \ldots, x_n$.

$R_i = 0$ for $i < 0$. $R_0 = k \cdot 1$

R_i = subspace spanned by polynomial expression in the x_js of total degree $\leq i$ for $i > 0$.

3.34 Definition

The associated graded ring $\operatorname{gr} R = \oplus R_i/R_{i-1}$ 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 $r \in R_i/R_{i-1}$

$\sigma(r) = r + R_{i-1}$

3·35 Definition

i) A ($\mathbb{Z}$) graded ring is a ring S with additive subgroups S_i, so that $S = \oplus S_i$ with $S_i S_j \subseteq S_{i+j}$ for $i, j \in \mathbb{Z}$

S_i is the i^{th} homogeneous component. S_0 is a subring and the S_i are S_0-modules.

ii) A graded ideal I is of the form $I = \oplus I_i$ with $I_i \subseteq S_i$.

Note

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

3·36 Definition

Let R be a filtered ring with filtration $\{R_i\}$, and M an R-module. Then M is a filtered R-module if there is a compatible filtration $\{M_i\}$ of M of additive subgroups such that $R_j M_i \subseteq M_{i+j}$.

3·37 Definition

i) The associated graded module of a filtered R-module $\hat{M}$ is $gr\, M = \oplus M_i/M_{i-1}$ as additive groups if M is a graded R-module. $(r + R_{i-1})(m + M_{j-1}) = rm + M_{i+j-1}$

ii) If $S \oplus S_i$ is a graded ring then a graded S-module V is of the form $\oplus V_j$ with $S_i V_j \subseteq V_{i+j}$

Given a filtered R-module M with filtration $\{M_0\}$ 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 $N \leq M$ allows the definition

$\phi_i : \frac{(N \cap M_i)}{(N \cap M_{i-1})} \to \frac{M_i}{M_{i-1}}$. Putting these together gives a map of additive groups $\phi : \bigoplus \frac{(N \cap M_i)}{(N \cap M_{i-1})} \to \bigoplus \frac{M_i}{M_{i-1}}$

Check that this is an R-module homomorphism.

Consider $\frac{N+M_i}{N} \cong \frac{M_i}{(N \cap M_i)}$

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

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

yielding $\Pi_i : \frac{M_i}{M_{i-1}} \to \frac{(N+M_i)/N}{(N+M_{i-1})/N}$

Putting these together gives $\Pi : gr\, M \to gr\, M/N$.

Check that this is an R-module homomorphism.

3.38 Lemma

If $N \leq M$, a filtered R-module, then

$0 \to gr\, N \xrightarrow{\phi} gr\, M \xrightarrow{\pi} gr\,(M/N) \to 0$ is exact when N and M/N are endowed with the filtrations induced from that of M.

Proof

$\ker \pi_i = \frac{M_{i-1} + (N+M_i)}{M_{i-1}} \cong \frac{N \cap M_i}{N \cap M_{i-1}}$

So we have $0 \to \frac{(N \cap M_i)}{N \cap M_{i-1}} \xrightarrow{\phi_i} \frac{M_i}{M_{i-1}} \xrightarrow{\pi_i} \frac{N+M_i/N}{N+M_{i-1}/N} \to 0$

is exact. Put these together. □

3.39 Definition

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

The Rees Ring of the filtration E is the subring $\bigoplus_{i\in\mathbb{Z}} R_i T^i$ of the Laurent polynomial ring $R[T^{-1}, T]$. Since $R_i R_j \subseteq R_{i+j}$, E is a graded ring, with homogeneous components $R_i T^i$ of degree i.

Observe that

i) $E/(T) \cong \operatorname{gr} R$

ii) $E/(1-T) \cong R$ since $(1-T) = \ker$ of the map $E \to R$, $\sum_i r_i T^i \mapsto \sum_i r_i$

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

Example

R Noetherian, $R_j = I^{-j}$ for $j>0$, I-adic filtration. Then I is finitely generated by $x_1, \dots, x_n$ say. Then $E = \bigoplus R_i T^i$ is generated by $R_0 \cong R$ and $T, x_1 T^{-1}, \dots, x_n T^{-1}$ as a ring. So E is a ring image of $R[Z_0, Z_1, \dots, Z_n]$, and so E is Noetherian.

3.40 Definition

The associated Rees-module is $\operatorname{Re}(M) = \bigoplus T^i M_i$ for a filtered R-module M. It is an E-module via $(\sum r_j T^j)(T^i m_i) = T^{i+j}(r_j m_i)$.

For $N \leq M$, given the induced filtrations,

3.38) $\Rightarrow \operatorname{Re}(M/N) = \operatorname{Re}(M)/\operatorname{Re}(N)$

3.41 Definition

A filtration of M is good if $\operatorname{Re}(M)$ is a finitely generated E-module

3.42 Lemma

Let $N \leq M$ with $\{M_i\}$ good for M. If E is Noetherian,

then the induced filtrations of N and M/N are also good.

Proof

$Re(N)$ is a finitely generated E-module, and hence Noetherian. So $Re(N)$ is finitely generated.

$Re(M/N) = Re(M)/Re(N)$ is also finitely generated. So the induced filtrations of N and M/N are both good.

Suppose that we have a good filtration and $Re(M)$ is a finitely generated E-module. If so, it is generated by a finite set of homogeneous elements $T^{k_1}m_{k_1}, \dots, T^{k_n}m_{k_n}$, with $m_{k_i} \in M_{k_i}$.

So the i^{th} homogeneous component

$$T^i M_i = R_{i-k_1} T^{i-k_1}(T^{k_1} m_{k_1}) + \dots + R_{i-k_n} T^{i-k_n}(T^{k_n} m_{k_n})$$

and so $M_i = R_{i-k_1} m_{k_1} + \dots + R_{i-k_n} m_{k_n}$ for these $m_{k_i} \in M_{k_i}$.

Example

For a finitely generated R-module M, R Noetherian, $M_i = I^{-i}M$ for $i<0$ take $N \leq M$. We deduce from (3.42) that the induced filtration $N \cap I^i M$ is a good filtration of N. So there is a generating set $n_{k_1}, \dots, n_{k_\ell}$ of N, negative integers k_i, with $n_{k_j} \in N \cap I^{-k}M$ and $N \cap I^{-i}M = I^{-i+k_1} n_{k_1} + \dots + I^{-i+k_\ell} n_{k_\ell}$

So for $i \leq \min(k_i) = k$, we have

$N \cap I^{-i}M = I^{-i+k}(N \cap I^{-k}M)$ for $i \leq k \leq 0$.

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

3.43 (Artin-Rees Lemma, 1956)

Let R be Noetherian. Given $N \leq M$ finitely generated R-modules, and $I \leq R$ an ideal, then $\exists c \geq 0$ such that

$N \cap I^a M = I^{a-c}(N \cap I^c M)$ for $a \geq c$.

Proof

Dimension

Suppose that R is a finitely generated k-algebra which is an integral domain. Let $I \leq R$ be 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 $\Rightarrow$ the minimal primes over the ideals $(1-T)$ and (T) in E are of height 1

3.26) Catenary Property ensures that $\dim E = 1 + \dim \left(\frac{E}{(T)}\right)$

$= 1 + \dim \left(\frac{E}{(1-T)}\right)$

Thus $\dim R = \dim \operatorname{gr} R$.

So it is useful to consider dimensions of graded rings.

We will consider positively graded rings $S = \bigoplus_{i=0}^{\infty} S_i$

and finitely generated graded S-module $V = \bigoplus_{i=0}^{\infty} S_i$

Remark

This all applies for 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 that S is Noetherian, generated by S_0, and homogeneous 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 $\lambda(u_2) = \lambda(u_1) + \lambda(u_3)$.

e.g. if S_0 is a field K then we can take λ = K-vector space dimension

More generally, if S_0 is local Artinian with maximal ideal P then each finitely generated S_0-module has a chain of submodules

$U \supseteq U_1 \supseteq U_2 \supseteq \dots \supseteq U_j = 0$ with each factor $\cong S_0/P$.

The number of terms in the chain is the composition length of U.

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

One can take λ to be the composition length.

3.44 Definition

The Poincaré series of V is the power series

$$P(V,t) = \sum \lambda(V_i)\, t^i \in \mathbb{Z}[[t]]$$

3.45 Theorem (Hilbert, Serre)

$P(V,t)$ is a rational function in t of the form $\dfrac{f(t)}{\prod_{i=1}^{n}(1-t^{k_i})}$

where $f(t) \in \mathbb{Z}[t]$ and k_i = degree of generator x_i.

Proof

By induction on the number of generators, n.

If $n = 0$ then $S = S_0$ and V is a finitely generated S_0-module

So $V_i = 0$ for large enough i. Clearly $P(V,t)$ is a polynomial.

For $n > 0$, assume true for $n-1$ generators.

We consider multiplication by x_n. $V_i \xrightarrow{\times x_n} V_{i+k_n}$

and so we can get an exact sequence

$$0 \to k_i \to V_i \xrightarrow{x_n} V_{i+k_n} \to L_{i+k_n} \to 0 \qquad (*)$$

where K_i is the kernel, and L_{i+km} is the cokernel of

$V_i \xrightarrow{x_m} V_{i+km}$.

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

L is a quotient. Both K and $L \left(\cong \frac{V}{x_m V}\right)$ are annihilated by x_m and so are $S_0[x_1, \ldots, x_{m-1}]$-modules.

Apply λ to $(*)$. $\lambda(K_i) - \lambda(V_i) + \lambda(V_{i+km}) - \lambda(L_{i+km}) = 0$.

Multiply by t^{i+km} and sum up.

$t^{km} P(K,t) - t^{km} P(V,t) + P(V,t) - P(L,t) = g(t)$

where $g(t) \in \mathbb{Z}[t]$ is a polynomial arising from the first few terms.

Apply inductive hypothesis to $P(K,t)$ and $P(L,t)$ $\square$

3.46 Corollary

If each k_i is 1, then for large enough i, $\lambda(V_i) = \phi(i)$ where $\phi(t) \in \mathbb{Q}[t]$ of degree $d-1$ where d = order of pole of $P(V,t)$ at $t = 1$.

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

3.47 Definition

$\phi(t)$ is the Hilbert polynomial.

$\chi(t)$ is the Samuel polynomial.

3.46 Corollary

If each $k_1, \ldots, k_n$ is 1 in 3.45), i.e. S is generated by S_0 and $x_1, \ldots, x_n$ of degree 1, then for large enough i $\lambda(V_i) = \phi(i)$ for some polynomial $\phi(t) \in \mathbb{Q}[t]$ of degree $d-1$, where d = order of pole of $P(V,t)$ at $t=1$.

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

Proof

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

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

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

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

$\phi(t) = \frac{f(1)}{(d-1)!} t^{d-1} +$ terms of lower degree

So $\phi(t)$ has degree $d-1$ since $f(1) \neq 0$.

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

The formula $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ yields

$\sum_{j=0}^{i} \binom{d+j-1}{d-1} = \binom{d+i}{d}$ and so

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

and this is equal to $\chi(i)$ for $i \geq s$, $\chi(t) \in \mathbb{Q}[t]$ 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 a good (negative) filtration $\{M_i\}$.

We form $V = \operatorname{gr} M$, $S = \operatorname{gr} R$ and renumber so that S is positively graded. We can apply our Hilbert-Serre analysis of dimension 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, $\chi(i) = \sum_{i}^{0} \dim_k \left(M_j/M_{j-1}\right)$ $i<0$.

$= \dim_k \left(M_0/M_{-i}\right)$ for $i<0$.

Remarks

① In fact, ~~everything~~ the degree is independent of which good filtration of M we pick (for a particular filtration of R).

3.48 Definition

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

3.49 Theorem

For a finitely generated k-algebra R that is an integral domain, $\dim R = \operatorname{tr\,deg}_k(\operatorname{Frac}(R)) = d(R)$, using P-adic filtration for any P a maximal ideal in R.

Remark

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

Proof of 3.49 (Sketchy)

We have established the first equality (3.24) and seen that $\dim R = \dim \operatorname{gr} R$ with respect to the P-adic filtration.

Then, it remains to show that for finitely generated graded k-algebras S, we have $\dim(S) = d(S)$.

We prove this by induction.

S is a finite dimensional k-vector space

$\Leftrightarrow \dim(S) = d(S) = 0$

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

The Principal Ideal Theorem (3.28) and Catenary Property (3.26) imply that $\dim(S/xS) = \dim(S) - 1$. We 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 equation involving $g(t)$ that

$d(L) = d(M) - 1$ where $L = S/xS$, $M = S$.

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

We 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.

We see that # monomials of total degree n is $\binom{n+m-1}{n-1}$ for all $n \geq 0$

Thus $\phi(t) = \frac{1}{(n-1)!}(t+n-1)\dots(t+1)$, Hilbert polynomial of degree $n-1$.

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)

For R a Noetherian local ring that is an integral domain, we have $d(R) = \dim(R) =$ least no. of generators of some ideal I such that $\sqrt{I} = P$ w.r.t. P-adic filtration, P is a unique maximal ideal.

4 Valuation Rings and Dedekind Domains

4.1 Definition

An integral domain A with field of fractions K is a valuation ring of K if for each $x \neq 0$, $x \in K$, either $x \in A$ or $x^{-1} \in A$ (or both)

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

4.2 Lemma

Let A be a valuation ring with fraction field K.

i) A is a local ring.

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

iii) A is integrally closed.

Proof:

i) Let P be the set of non-units in A. Thus $x \in P \Leftrightarrow x = 0$ or $x^{-1} \notin A$

We see that P is an ideal:

- If $a \in A$, $x \in P$, then $ax \in P$.

This is true since otherwise $(ax)^{-1} \in A$ so $x^{-1} = a(ax)^{-1} \in A$.

- 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, and similarly if $x^{-1}y \in A$.

ii) Is very simple.

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

Suppose that $x \notin A$. Then $x = -(a_{n-1} + a_{n-2}x^{-1} + \dots + a_0 x^{-n+1})$

and this lies in A since x^{-1} does $\not\in$ $\square$

The reason for the terminology 'valuation ring' is that one may associate a non-Archimedean valuation

$v: K^* \to \Gamma$ where Γ is a (well chosen) ordered abelian group. (i.e. every pair of elements satisfies $r_1 \leq r_2$ or $r_2 \leq r_1$ and we only get both if $r_1 = r_2$. $r_1 \leq r_2 \Rightarrow r + r_1 \leq r + r_2$) satisfying:

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

ii) $v(x+y) \geq \min(v(x), v(y))$ (ultrametric inequality)

so that $A = \{x \in K : x = 0 \text{ or } v(x) \geq 0\}$

and given such a v, A is a valuation ring.

4.3 Definition

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

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

ii) $v_f : K(x)^* \to \mathbb{Z}$, $f^{g/h} \mapsto n$ where f is an irreducible polynomial and g, h are coprime to f. $f, g, h \in K[x]$. We have discrete valuation ring $K[x]_{(f)}$.

Recipe for Valuation Rings

Given R, an integral domain with $K = \text{frac}(R)$, take an algebraically closed field F.

Consider pairs (R', ϕ') where R' is a subring of K, and $\phi : R' \to F$ is a ring homomorphism.

We partially order these pairs by

$(R_1, \phi_1) \leq (R_2, \phi_2) \Leftrightarrow \begin{cases} R_1 \leq R_2 \\ \phi_2|_{R_1} = \phi_1 \end{cases}$

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

Apply Zorn. There are maximal such pairs, (A, θ) say.

Claim: Such an A is a valuation ring of K.

Step 1

We choose F so that such pairs actually exist.

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

$\theta(A)$ 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 $\phi: A_P \to F$, $\frac{a}{s} \mapsto \frac{\theta(a)}{\theta(s)}$, $S = A \setminus P$.

Maximality of the pair (A, θ) ensures that $A = A_P \leq K$.

Hence A is a local ring with maximal ideal P.

Take $x \neq 0$ in K. We must show that either $x \in A$ or $x^{-1} \in A$

i.e. $A[x]$ or $A[x^{-1}]$ is equal to A.

Step 2

First we show either $PA[x] \neq A[x]$ or $PA[x^{-1}] \neq A[x^{-1}]$

Proof

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

So $1 \in PA[x]$, $1 = a_n x^n + \dots + a_0$, $a_i \in P$ ①

$1 \in PA[x^{-1}]$, $1 = b_n x^{-n} + \dots + b_0$, $b_i \in P$ ②

Pick m, n minimal and assume that $m \geq n$.

Multiply ② by x^n to get $(1-b_0)x^n = b_n + \dots + b_1 x^{n-1}$ ③

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

So ③ gives $x^n = c_n + \dots + c_1 x^{n-1}$ with $c_i \in P$,

and so $x^m = c_n x^{m-n} + \dots + c_1 x^{m-1}$

Substituting in ① gives an equation contradicting minimality of n.

Step 3

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

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

Let Q be a maximal ideal of B containing I.

Thus $Q \cap A = P$ since $Q \cap A \subsetneq A$ and P is in it.

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

$k_1 = k[\bar{x}]$ where $\bar{x}$ is the image of x in B/Q.

Thus k_1 is an algebraic extension of k. But θ induces a map $\bar{\theta} : \underset{k}{A/P} \to F$, extending to a map $\bar{\phi} : k_1 \to F$, since F is algebraically closed.

$\bar{\phi}$ lifts back to a map $B \to F$. Maximality of the pair (A, θ) ensures that $A = B$.

4.4 Theorem

YRIS 4-5

Let R be an integral domain with $K = \mathrm{frac}(R)$. Then the integral closure of R in K is the intersection of all the valuation rings of K containing R.

e.g. $\mathbb{Z} = \bigcap_{p \text{ prime}} \mathbb{Z}_{(p)}$ ← valuation ring

Proof:

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

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 $\phi: R_1 \to R_1/P_1 \subseteq F$ 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, $\theta(x^{-1}) = \phi(x^{-1}) = 0$. 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). Let A have unique maximal ideal P.

If we have a (surjective) discrete valuation $v: K^* \to \mathbb{Z}$ so that $A = \{x \in K : x = 0 \text{ or } v(x) \geq 0\}$ (often $v(0) := \infty$)

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

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

Then $(a) = (b)$

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 $v(b) \geq k$ (since $b = a(b/a)$ and $v(b/a) \geq 0$, so $b/a \in A$)

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

Thus, there is only one chain of ideals

$A \supsetneq P = I_1 \supsetneq I_2 \supsetneq \ldots$ and therefore A is Noetherian. Thus P is the only non-zero prime, so $\dim A = 1$.

4·5 Lemma

Let A be a Noetherian local integral domain of dimension 1.

Set $k = A/P$ where P is the unique maximal ideal.

The following are equivalent:

i) A is a discrete valuation ring.

ii) A is integrally closed.

iii) P is principal

iv) $\dim P/P^2 = 1$

v) Every non-zero ideal ($\neq A$) is a power of P.

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

Proof:

i) $\Rightarrow$ ii) is 4·2 iii)

ii) $\Rightarrow$ iii) Let $0 \neq a \in P$. Then $\dim A = 1$ and A is local. P is the only minimal prime over (a), and we know that $P^n \leq (a)$ for some n. Pick n minimal so that $P^{n-1} \not\leq (a)$ and we may pick $b \in P^{n-1}$ with $b \notin (a)$.

Set $x = a/b$. We claim that $P = (x)$.

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

- If $x^{-1}P \leq P$, then P would be a $\mathbf{A}[x^{-1}]$-module, finitely generated as an $\mathbf{A}$-module. Any $\mathbf{A}[x^{-1}]$-submodule will also be finitely generated as an $\mathbf{A}$-module (since $\mathbf{A}$ is Noetherian). But any non-zero cyclic $A[x^{-1}]$-submodule of A is isomorphic to $A[x^{-1}]$, and this gives a contradiction as $A[x^{-1}]$ is not a finitely generated A-module (x^{-1} not integral). So $x^{-1}P \lneq P$. Thus $x^{-1}P \leq A$ by construction, so $x^{-1}P = A$. Hence $P = (x)$.

iii) $\Rightarrow$ iv) P principal $\Rightarrow P/P^2$ principal $\Rightarrow \dim P/P^2 \leq 1$.

$P \neq P^2$ by Nakayama.

iv) $\Rightarrow$ v) If $I \overset{\neq 0}{\neq 0}$ is an ideal of A, then $P^n \leq I$ (as in ii) $\Rightarrow$ iii)). But $\dim_k (P/P^2) = 1 \Rightarrow P$ principal (application of Nakayama). $P = (x)$, say.

$\exists r$ such that $I \leq P^r$, $I \not\leq P^{r-1}$ and hence

$\exists y \in I$ such that $y = ax^r$, $y \notin P^{r-1}$. So $a \notin P$ and hence a is a unit of A.

So $x^r \in I$ and $P^r \subseteq I$. Then $I = P^r$.

v) $\Rightarrow$ vi) 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. Hence $I = (x^r)$.

vi) $\Rightarrow$ i) From vi), $P = (x^r)$, some r.

But P prime $\Rightarrow r = 1$. $P = (x)$. By Nakayama, $P^k \neq P^{k+1}$ for any k.

- A is a valuation ring:

If $y \in K$, $y \notin A$ then consider $\{x \in A : xy \in A\}$, an ideal of A.

This ideal is (x^k), 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^* by $v(ab^{-1}) = v(a) - v(b)$

Exercise: this gives a well defined discrete valuation $v : K^* \to \mathbb{Z}$.

Dedekind Domains

4.6 Definition

An integrally-closed, Noetherian integral domain of dimension 1 is a Dedekind domain.

Examples

1. Integral closure of $\mathbb{Z}$ in a finite field extension of $\mathbb{Q}$.
2. Coordinate 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 discrete valuation ring. using 4.5).

4.7 Lemma

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, where $S = R \setminus Q$. By 4.5) applied to the discrete valuation ring R_Q,

$$S^{-1}I = (S^{-1}Q)^r = S^{-1}(Q^r) \quad \text{for some } r.$$

The bijective correspondence between ideals 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 — Artinian only has finitely many primes all of which are maximal. Since $\dim R = 1$. So R/I is a direct product of Artinian rings (Sheet 1). Thus $I = \bigcap I_j$ with $\sqrt{I_j} = Q_j$, maximal. But by 4.7), $I_j = Q_j^{n_j}$ for some n_j. Thus $I = \bigcap_j Q_j^{n_j}$. But for copime ideals products are the same as intersections (proved by induction).

So $I = \prod_j Q_j^{n_j}$.

For uniqueness, the Q_j are the minimal primes over I, In any other similar expression for I, the same Q_j must appear and the powers must be the same because the powers are unique (see 4.5). □

4.9 Definition

Given an integral domain R, $K = \mathrm{Frac}(R)$, any R-submodule M of K is a fractional ideal of R if $xM \subseteq R$ for some $x \in R \setminus \{0\}$.

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.

5.1 Definition

$\phi : M \times N \to L$ is R-bilinear if

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

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

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

If $\phi : M \times N \to T$ is bilinear and $\theta : T \to L$ is linear then the composition is bilinear. Thus, composition with ϕ gives a well-defined function ϕ^* $\left\{ \begin{matrix} R\text{-module maps} \\ T \to L \end{matrix} \right\} \to \left\{ \begin{matrix} \text{bilinear maps} \\ M \times N \to L \end{matrix} \right\}$

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

5.2 Lemma

1. Given M, N, there is an R-module T and a universal map $\phi : M \times N \to T$.

2. Given two such maps $\phi_i : M \times N \to T_i$, $i = 1, 2$, then there is a unique isomorphism $\beta : T_1 \to T_2$ with $\beta \circ \phi_1 = \phi_2$.

Proof.

1. 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 form $e_{(r_1 m_1 + r_2 m_2, n)} - r_1 e_{(m_1, n)} - r_2 e_{(m_2, n)}$

and $e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m, n_1)} - r_2 e_{(m, n_2)}$

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

$\phi : M \times N \to T, \quad (m,n) \mapsto m \otimes n$

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

Any map $\alpha : M \times N \to L$ extends to a map $\bar{\alpha} : F \to L$ sending $e_{(m,n)} \mapsto \alpha(m,n)$. If α is bilinear, then $\bar{\alpha}$ vanishes on X and we have an induced map $\alpha' : T \to L$, with $\alpha'(m \otimes n) = \alpha(m,n)$, and α' uniquely defined by this.

2. Follows from universality □

S.3 Definition

T is written $M \otimes_R N$, the tensor product of M, N over R. (We often drop R if it is clear from context).

Warning

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

e.g. If $R = k$, a field, M, N k-vector spaces of dimension s, t, then $M \otimes_k N$ is a k-vector space of dimension st.

S.4 Lemma

We have unique isomorphisms

i) $M \otimes N \to N \otimes M, \quad m \otimes n \mapsto n \otimes m$

ii) $M \otimes (N \otimes L) \to (M \otimes N) \otimes L, \quad m \otimes (n \otimes l) \mapsto (m \otimes n) \otimes l$

iii) $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L)$

iv) $R \otimes M \to M, \quad r \otimes m \mapsto rm$

If $\phi: R \to T$ is a ring homomorphism and N is a T-module, it may be regarded as an R-module via $rn = \phi(r)n$. "Restriction of Scalars". 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 the R-module map $S^{-1}R \otimes M \to S^{-1}M$.

Check that this is an isomorphism.

5.5 Definition

Given $\Theta: M_1 \to M_2$, $\phi: N_1 \to N_2$, R-module maps, we define the tensor product of Θ and ϕ:

$\Theta \otimes \phi: M_1 \otimes N_1 \to M_2 \otimes N_2$, $m_1 \otimes n_1 \mapsto \Theta(m_1) \otimes \phi(n_1)$

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

5.6 Lemma

Given L, M, N, R-modules, we have

$\mathrm{Hom}(M \otimes N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, L))$

Proof

Given a bilinear $\phi : M \times N \to L$ we have

$\Theta : M \to \mathrm{Hom}(N, L)$, $m \mapsto \Theta_m : N \to L$

Conversely, given $\Theta : M \to \mathrm{Hom}(N, L)$ we have a bilinear

$M \times N \to L$, $(m, n) \to \Theta(m)(n)$

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 left hand side corresponds to the linear maps

$M \otimes N \to L$.

S.7

so that T_1, T_2 are R-algebras

Given $\phi_1 : R \to T_1$, $\phi_2 : R \to T_2$, the tensor product of the two R-algebras is defined to be $T_1 \otimes_R T_2$ (as an R-module)

$T_1 \otimes_R T_2$ 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. $1 \otimes 1$ is the multiplicative identity.

Check that $R \to T_1 \otimes T_2$, $r \mapsto \phi_1(r) \otimes 1 = 1 \otimes \phi_2(r)$ is a ring homomorphism.

Examples

1. k a field. $k[x]$ is a k-algebra.

$k[x_1] \otimes_k k[x_2] \cong k[x_1, x_2]$

2. $\mathbb{Q}[x]/(x^2+1) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[x]/(x^2+1)$.

3. $\frac{K[x_1]}{(f(x_1))} \otimes_K \frac{K[x_2]}{(g(x_2))} \cong \frac{K[x_1, x_2]}{(f(x_1), g(x_2))}$

5.8 Lemma ← n.b. not a short exact sequence

If $M_1 \to M \to M_2 \to 0$ is an exact sequence, and N is an R-module then $M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$ is also exact,

and similarly $N \otimes M_1 \to N \otimes M \to N \otimes M_2 \to 0$.

(n.b. can prove directly, but often knowledge of exactness of Hom and then 5.6 is used)

Remark

Not short exact sequences. Given a short exact sequence, applying $\otimes N$ does not necessarily preserve the injectivity of the left-hand map. e.g. $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\text{reduce}} \mathbb{Z}/(2) \to 0$

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

Tensoring with N, $\mathbb{Z}/(2) \to \mathbb{Z}/(2) \to \mathbb{Z}/(2) \to 0$

(the zero map, not injective)

Thus exactness is not preserved.

5.9 Definition

N is a flat R-module if given any short exact sequence $0 \to M_1 \to M \to M_2 \to 0$ then

$0 \to M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$ is exact.

Examples

1. R itself is a flat R-module.
2. R^n (free module on n-generators) is a flat R-module.
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 statement only things are now contravariant rather than covariant.

~~5.10 Lemma~~

i) If $0 \to M_1 \to M \to M_2$ is exact then

restriction

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

ii) $M_1 \to M \to M_2 \to 0$ is exact $\Leftrightarrow 0 \to \mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M_1$

exact for all N.

5.10 Lemma

i) $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2 \to 0$ is exact, (*)

$\Leftrightarrow 0 \to \mathrm{Hom}(M_2, N) \xrightarrow{\bar{\phi}} \mathrm{Hom}(M, N) \xrightarrow{\bar{\theta}} \underset{(**)}{\mathrm{Hom}(M_1, N)}$ exact $\forall N$.

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

$\Leftrightarrow 0 \to \mathrm{Hom}(N, M_1) \to \mathrm{Hom}(N, M) \to \mathrm{Hom}(N, M_2)$ exact $\forall N$.

Proof

i) Suppose that $0 \to \mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M_1, N)$ is exact, for all N. Since $\mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M, N)$ is injective $\forall N$, the map $M \to M_2$ is injective. So we have exactness at M_2 in (*)

We need to check exactness at M.

$\mathrm{Im}\,\theta \subseteq \ker \phi$: Take $N = M_2$, $f = \mathrm{id} : M_2 \to M_2$.

Then $\bar{\theta}(\bar{\phi}(f)) = 0$. So $f \circ \phi \circ \theta = 0$ and so $\phi \circ \theta = 0$.

Finally, take $N = M/\mathrm{Im}\,\theta$ and $\pi : M \to N$ surjective.

Then $\pi \in \ker \bar{\theta}$ and hence $\exists\, \psi$ such that $\pi = \bar{\phi}(\psi)$, $\pi \in \mathrm{Hom}(M_2, N)$.

Rest of proof : exercise. □

Now we ~~proof~~ prove 5.8) using 5.6) and 5.10).

Proof of 5.8

Given a sequence $M_1 \to M \to M_2 \to 0$ which is exact,

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

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 by 5.10) again, $M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$ is exact. ☐

Observe that in general a short exact sequence

$0 \to M_1 \to M \to M_2 \to 0$ does not necessarily mean that

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

is not necessarily exact.

5.11 Definition

A module P is <u>projective</u> if whenever we have a injective map $M \to M_2$ and a map $P \to N$ then we can complete the diagram with a map $P \to M$

$$\begin{array}{ccccc} & & P & & \\ & \swarrow & \downarrow & & \\ M & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

so that it commutes.

Similarly, we define <u>injective</u> modules by 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. For an integral domain R with $K = \mathrm{Frac}(R)$ then K is an injective R-module, e.g. $\mathbb{Q}$ an injective $\mathbb{Z}$-module.

5.12 Lemma

For an R-module P the following are equivalent:

i) P projective

ii) 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.

iii) If $\varepsilon : M \twoheadrightarrow P$ is surjective then $\exists$ a map $\beta : P \to M$ such that $\varepsilon \circ \beta = \mathrm{identity}$

iv) P is a direct summand in every module of which it is a quotient.

v) P is a direct summand of a free module.

Proof

i) $\Rightarrow$ ii) follows from the definition of projective P.

ii) $\Rightarrow$ iii) 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. So $\exists\ \beta : P \to M$ such that $\varepsilon \circ \beta = \mathrm{id}$.

iii) $\Rightarrow$ iv) Let $P = M/M_1$, a quotient of M, and so we have $0 \to M_1 \to M \xrightarrow{\alpha} P \to 0$ a short exact sequence.
By iii) $\exists\ \beta : P \to M$ such that $\alpha \circ \beta = \mathrm{id}$. Therefore P is a direct summand of M.

iv) $\Rightarrow$ v) P is a quotient of a free module with basis indexed by $\{e_x\}$ $x \in X$ and map basis elements $e_x \mapsto x$.

v) $\Rightarrow$ i) By v) $F = P \oplus Q$. Since free modules are projective and we have good behaviour under $\oplus$, P is projective. $\square$

There is a similar list for injective modules.

Remarks

1. Projectives are direct summands of free modules, and free modules are flat. $\otimes$ behaves well under $\oplus$, so we see 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 projectives are free

5.13 Lemma

For an R-module E, TFAE:

i) E injective.

ii) For every short exact sequence $0 \to M_1 \to M \to M_2 \to 0$ then $0 \to \mathrm{Hom}(M_2, E) \to \mathrm{Hom}(M, E) \to \mathrm{Hom}(M_1, E) \to 0$ is exact.

iii) If $\mu : E \to M$ is a monomorphism, then $\exists\, \beta : M \to E$ such that $\beta \circ \mu = \mathrm{id}$.

iv) E is a direct summand of every module containing it as a submodule.

Proof

Exercise. □

Given an R-module M, there is certainly a free module F with $F \twoheadrightarrow M$ surjectively.

5.14 Definition

A projective presentation of M is a short exact sequence $0 \to K \to P \to M \to 0$ with P projective.

This is a free presentation in the case where P is free.

5.15 Definition

Given a projective presentation of M then we apply $- \otimes_R N$ to get $K \otimes N \to P \otimes N \to M \otimes N \to 0$.

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

$\mathrm{Ext}(M, N) = \mathrm{coker}(\mathrm{Hom}(P, N) \to \mathrm{Hom}(K, N))$

Remark

1. This is actually independent of the choice of presentation.
2. One may also take a projective presentation for N and apply $M \otimes_R -$. This 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', giving an alternative description in terms of equivalence classes of extensions.

Tor denotes 'torsion'.

Example

We met the free presentation of $\mathbb{Z}/(2)$ (where $R = \mathbb{Z}$)

$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/(2) \to 0$

Apply $- \otimes \mathbb{Z}/(2)$. Then we have

$\mathrm{Tor}(\mathbb{Z}/(2), \mathbb{Z}/(2)) = \ker(\mathbb{Z} \otimes \mathbb{Z}/(2) \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/(2))$

(the map is induced by multiplication by 2 which is the 0 map)

So $\mathrm{Tor}(\mathbb{Z}/(2), \mathbb{Z}/(2)) = \mathbb{Z}/(2)$

Apply $\mathrm{Hom}(-, N)$ to our presentation.

$\mathrm{Ext}(\mathbb{Z}/(2), N) = \mathrm{coker}(\mathrm{Hom}(\mathbb{Z}, N) \to \mathrm{Hom}(\mathbb{Z}, N))$

(induced by multiplication by 2)

Note that $\mathrm{Hom}(\mathbb{Z}, N) \cong N$.

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).

S.16 Definition

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 P_i projective.

Remark

If R is Noetherian and M is a finitely generated R-module then we can produce a projective resolution with all the P_i finitely generated projective modules. We form a presentation $0 \to K_0 \to P_0 \to M \to 0$ and then take a presentation for K_0 $\quad 0 \to K_1 \to P_1 \to K_0 \to 0$ and so on, ensuring 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:

$$\ldots \to P_n \otimes N \to \ldots \to P_1 \otimes N \to P_0 \otimes N \to M \otimes N \to 0$$

(A chain complex one where the image of one arrow is in the kernel of the next).

At $P_n \otimes N$, $\ldots \xrightarrow{\theta_n} P_n \otimes N \xrightarrow{\theta_{n-1}} \ldots$

$\ker \theta_{n-1} / \operatorname{Im} \theta_n$ is an R-module, known as the homology of the chain complex at $P_n \otimes N$.

5.17 Definition

$\operatorname{Tor}_n^R(M, N)$ is the homology group at $P_n \otimes N$. Thus

$\operatorname{Tor}_0(M, N) = M \otimes N$

$\operatorname{Tor}_1(M, N) = \operatorname{Tor}(M, N)$

(Use the chain complex $\ldots \to P_n \otimes N \to \ldots \to P_1 \otimes N \to P_0 \otimes N \to 0$ with the homology at $P_0 \otimes N$ being $M \otimes N$).

Similarly, given a projective resolution for M, apply $\operatorname{Hom}(-, N)$ and get a cochain complex

$$0 \to \operatorname{Hom}(P_0, N) \to \operatorname{Hom}(P_1, N) \to \ldots$$

and we define $\operatorname{Ext}_R^n(M, N)$ to be the (co)-homology group at $\operatorname{Hom}(P_n, N)$. Thus

$\operatorname{Ext}^0(M, N) = \operatorname{Hom}(M, N)$

$\operatorname{Ext}^1(M, N) = \operatorname{Ext}(M, N)$

Remark

In fact, this is all independent of the choice of projective resolution. Moreover, one can obtain $Ext^n(M,N)$ by considering an injective resolution of N

$0 \to N \to E_0 \to E_1 \to \dots$ exact

with E_i injective resolutions. Apply $Hom(M,-)$ to this and considering the homology groups of the resulting complex yields the same thing.

5.18 Lemma

The following are equivalent:

i) $Ext^{n+1}(M,N) = 0$ $\forall$ R-modules N

ii) M has a projective resolution of length n.

$0 \to P_n \to P_{n-1} \to \dots \to P_0 \to M \to 0$

(Unproved here)

5.19 Definition

1. The homological dimension of M is n if $Ext^{n+1}(M,N)=0$ $\forall N$ and there is some N for which $Ext^n(M,N) = 0$.
2. The global dimension of R is the supremum of all the homological dimensions of R-modules M.

Examples

i) For a field K, all modules are free and the global dimension is 0.

ii) The global dimension of $\mathbb{Z}$ is 1. In fact, this is also the case

for any PID which is not a field.

iii) The condition that global dimension = 0 is equivalent to saying that all submodules of R are direct summands. In other words, R is semi-simple. Compare with Complex Representation theory of finite groups G - the group algebra $\mathbb{C}G$ is semi-simple.

5.20

Given a short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, there are long exact sequences:

$$\cdots \to \mathrm{Tor}_1(M_1, N) \to \mathrm{Tor}_1(M, N) \to \mathrm{Tor}_1(M_2, N) \xrightarrow{\text{connecting maps}}$$
$$\to \mathrm{Tor}_0(M_1, N) \to \mathrm{Tor}_0(M, N) \to \mathrm{Tor}(M_2, N) \to 0$$

and

$$0 \to \mathrm{Ext}^0(M_2, N) \to \mathrm{Ext}^0(M, N) \to \mathrm{Ext}^0(M_1, N)$$
$$\to \mathrm{Ext}^1(M_2, N) \to \mathrm{Ext}^1(M, N) \to \mathrm{Ext}^1(M_1, N) \to \cdots$$

5.21 Corollary (Dimension Shifting)

Given a projective presentation $0 \to K \to P \to M \to 0$ we have

$\mathrm{Tor}_n(M, N) = \mathrm{Tor}_{n-1}(K, N)$ (for $n > 0$)

$\mathrm{Ext}^n(M, N) = \mathrm{Ext}^{n-1}(K, N)$ (for $n > 0$)

Proof

Apply 5.20) to our presentation and observe that for a projective P, $\mathrm{Ext}^n(P, N) = 0$, $\mathrm{Tor}_n(P, N) = 0$ 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.

This is based on the exterior algebra on n-generators; in each degree m we have the free module with generators being the exterior products $X_{i_1} \wedge \dots \wedge X_{i_m}$ of m of the n variables.

In general, Hilbert's syzygy theorem says that any ideal of R has a projective resolution of length $\leq n$.

So global dim $R = n$.

04/11/13

Commutative Algebra

Hochschild Cohomology * NON-EXAMINABLE *

This is bi-module cohomology. We drop commutativity.

A k-algebra R is an R-R bi-module.

We need a projective resolution for R as a bi-module.

An R-R bi-module may be viewed, when convenient, as a left $R \otimes R^{op}$-module. In R^{op}, $x \circ y := yx$

For R commutative $R^{op} \cong R$.

$R \otimes R \longrightarrow R$, $x \otimes y \mapsto xy$

Hochschild resolution of R:

free $R \otimes R$ module

free $R \otimes R$-module

$$\ldots \longrightarrow R \otimes R \otimes R \otimes R \longrightarrow R \otimes R \otimes R \longrightarrow R \otimes R \longrightarrow R$$

clain complex exacto

The map $R^{\otimes^n} \to R^{\otimes^{n-1}}$ involves alternate sums.

e.g. $x \otimes y \otimes z \longmapsto xy \otimes z - x \otimes yz$

For Hochschild homology one tensors this resolution with R.

If M is an R-R bi-module, we can form a bi-module $M \otimes_R R$ and consider the homology groups in the arising chain complex, $HH_i(R, R)$.

If we apply $\mathrm{Hom}(-, R)$ then the cohomology in the arising co-complex is the Hochschild cohomology $HH^i(R, R)$.

$HH^0(R, R)$ = centre of R

$HH^1(R, R) = \dfrac{\text{derivations of } R}{\text{inner derivations of } R}$

A derivation d is such that $d(xy) = x(dy) + (dx)y$

Inner derivations are those arising from ring commutators.

$$x \mapsto [x, y] = xy - yx$$

For commutative Algebra, $HH'(R,R) \cong$ 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 has a product defined on it; it forms a ring, but in practice this is hard to work with in particular examples.

HH^2 has a meaning to do with deformations of the algebra.

Hochschild 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 global definition of dimension).

Hochschild dimension $0 \iff R$ is a projective R-R-bimodule

$\iff R$ is a direct summand of $R \otimes R^{op}$

a separable k-algebra.