COMMUTATIVE ALGEBRA

NOTES BY WENQI LI

Contents

Date: December 20, 2023.

1. Lecture 1: 2023.9.5

Basic conventions: all rings have 1, 1 could be 0 but only when $R = \{0\}$. Ring homomorpisms send 1 to 1.

If there is a ring morphism $f : R \to S$, call S an R-algebra. The data of a R-algebra includes the structural morphism f. Examples includes the inclusion $\mathbf{Z} \hookrightarrow \mathbf{Q}$, or the quotient ring $R \to R/I$. A basic example is the polynomial algebra $R[x_1, \cdots, x_n]$ over a ring R, and the formal power series $R[\![x_1, \cdots, x_n]\!]$. A short hand notation is x^I where $I = (a_1, \cdots, a_n)$ is a tuple in $\mathbf{Z}_+^n$, and x^I means $x_1^{a_1} \cdots x_n^{a_n}$. The notation $|I|$ means $\sum_i a_i$. So another way of writing elements in $R[x_1, \cdots, x_n]$ is

$$\sum_d P_d, \text{ where } P_d = \sum_{|I|=d} r_I x^I$$

grouping together homogenous of degree d parts.

Definition 1.1. Let S_1, S_2 be R algebras. A ring morphism $f : S_1 \to S_2$ is an R-algebra morphism if f commutes with the structural homomorphisms.

For example, if J is an ideal in S and S is an R-algebra, then S/J is also an R-algebra.

Suppose S is an R-algebra. Let $s_1, \cdots, s_n \in S$. Then we have an R-algebra homomorphism

$$R[x_1, \cdots, x_n] \to S$$

by evaluating at $s_1, \cdots, s_n$.

Basic fact: every R-algebra homomorphism from $e : R[x_1, \cdots, x_n] \to S$ is of this form. (Take s_i to be $e(x_i)$.) So there is a bijection $\mathrm{Hom}(R[x_1, \cdots, x_n], S) \cong S^n$ as sets.

This doesn't work for $R[\![x_1, \cdots, x_n]\!]$ since one can't evaluate a power series unless there is some notion of convergence.

Definition 1.2. If an R-algebra S is isomorphism as R-algebras to $R[x_1, \cdots, x_n]/I$, then say S is a finitely generated R-algebra. If I is a finitely generated ideal, then say S is finitely presented.

The second basic object is R-modules.

Definition 1.3. M is an R-module if $(M, +)$ is an abelian group, and $\cdot : R \times M \to M$ is a ring action.

Definition 1.4. $N \subset M$ is an submodule if it is a subgroup and closed under action of R. The quotient M/N inherits the structure of a R-module.

Definition 1.5. A function $f : M_1 \to M_2$ is an R-module homomorphism if it is a homomorphism of abelian groups, and $f(rm) = rf(m)$ for all $r \in R$ and $m \in M_1$.

Given a homomorphism f, the kernel, the image, and the cokernel are all naturally R-modules. f is injective if the kernel is 0, and f is surjective if the cokernel is 0. f is a isomorphism if and only if f is bijective, which implies f^{-1} is also a homomorphism, hence also an isomorphism.

Example 1.1.

(1) If k is a field, then a k-module is a k-vector space.

(2) An R-algebra is naturally an R-module.

(3) A $\mathbf{Z}$-module is the same thing as an abelian group.

(4) An R-submodule of R is an ideal.

(5) Free modules R^n

(6) Let X be any set and M an R-module. The set of all functions

$$M^X = \{f : X \to M\}$$

is an R-module under pointwise addition and multiplication.

(7) Direct sums/products. Let M_1, M_2 be R-modules. The direct sum is

$$M_1 \oplus M_2 = \{(m_1, m_2) \mid m_i \in M_i\}$$

More generally, let A be a set (might be infinite), and suppose M_α is a R-module for all $\alpha \in A$. Define the direct product

$$\prod_{\alpha \in A} M_\alpha$$

to be the set of functions $f : A \to \coprod_{\alpha \in A} M_\alpha$ such that $f(\alpha) \in M_\alpha$. The addition and multiplication by r is pointwise. The direct sum is a submodule

$$\bigoplus_{\alpha \in A} M_\alpha \subseteq \prod_{\alpha \in A} M_\alpha$$

consists of functions f such that $f(\alpha) = 0$ for all but finitely many α's.

Another basic object is ideals. Let R be a fixed ring. Let A be a set and I_α be an ideal of R for all $\alpha \in R$. The intersection

$$\bigcap_{\alpha \in A} I_\alpha$$

is an ideal, and it is the largest ideal contained in all the I_α's.

Let I, J be ideals in R. The ideal product is

$$IJ = \left\{ \sum_{i=1}^{N} r_i s_i \mid r_i \in I, s_i \in J \right\}$$

It is obvious that $IJ \subseteq I \cap J$ and in general they are different. For examples, in $\mathbf{Z}$ we have $(n) \cap (n) = (n)$, but $(n)(n) = (n^2)$. It is easy to check that $(IJ)K = I(JK)$ and $IJ = JI$. There is no way to take an infinite product of ideals.

The ideal sum is

$$I + J = \{r + s \mid r \in I, s \in J\}$$

We see that $I, J \subset I + J$, and it is the smallest ideal containing I and J. The union $I \cup J$ is almost never an ideal, and it is only when one ideal is contained in the other.

It is possible to sum up infinitely many ideals. Suppose we have ideals $I_\alpha, \alpha \in A$. The sum is defined to be

$$\sum_\alpha I_\alpha = \left\{ \sum_\alpha r_\alpha \mid r_\alpha \in I_\alpha, r_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

Definition 1.6. Given $r \in R$, the set of all multiples of r, denoted by (r), is the principal ideal generated by r. Given $r_1, \cdots, r_k \in R$, define the ideal generated by $r_1, \cdots, r_k$ to be

$$(r_1, \cdots, r_k) = \left\{ \sum_{i=1}^k t_i r_i \mid t_i \in R \right\} = (r_1) + \cdots + (r_k)$$

Infinitely generated ideal is defined to be the set of all finite sums, or the infinite sum of principal ideals.

These constructions have analogues for R-modules. Fix an R-module M. Suppose there is a collection M_α of submodules. One may define the intersection and the sum, but in general one can't take the product. However, if I is an ideal in R, and N a submodule in M, one can form the product

$$IN = \left\{ \sum_{i=1}^n r_i m_i \mid r_i \in I, m \in M \right\}.$$

Let R be a ring. A unit in R is an element with an multiplicative inverse. $R^\times$ is the set of all units, and it is a group under multiplication. A zero divisor in R is an $r \in R$ such that $rs = 0$ for some $s \neq 0$.

Definition 1.7. R is a domain if $R \neq \{0\}$ and the only zero divisor is 0.

Example 1.2.

(1) A field is a domain.

(2) A subring of a domain is a domain.

(3) If R is a domain, then $R[x]$ is also a domain.

Definition 1.8. An ideal $P \subset R$ is a prime ideal if $P \neq R$, and $rs \in P$ implies $r \in P$ or $s \in P$ for all $r, s \in R$.

Fact: P is a prime ideal if and only if R/P is a domain.

Observation: Suppose $f : R \to S$ is a ring homomorphism, and $Q \subset S$ is a prime ideal. Then $f^{-1}(Q)$ is a prime ideal in R.

Proof. Let $\overline{f}$ be the composition $R \to S \to S/Q$. The kernel of $\overline{f}$ is $\{r \in R \mid f(r) \in Q\} = f^{-1}(Q)$. The induced homomorphism $R/f^{-1}(Q) \to S/Q$ is injective, so $R/f^{-1}(Q)$ is isomorphic to some subring of S/Q, a domain. Hence $R/f^{-1}(Q)$ is a domain, so $f^{-1}(Q)$ is a prime ideal. ■

2. Lecture 2: 2023.9.7

Definition 2.1. A maximal ideal M in a ring R is an ideal not equal to R, and if J is an ideal in R and $M \subseteq J \subseteq R$, then $J = M$ or $J = R$.

M is maximal if and only if R/M is a field. If R is a ring, I is an ideal, then there is a 1-1 correspondence between ideals J containing I and ideals of R/I. Hence M is a maximal ideal in R if and only if $k = R/M$ is non-zero and has no proper non-trivial ideals, so it is a field.

Theorem 2.2. *Let R be a ring and I a proper ideal. Then there exists a proper ideal M containing I.*

Proof. Zorn's lemma. ■

Corollary 2.3. *If $R \neq \{0\}$, there exists a maximal ideal in R.*

Proof. Apply the theorem to $I = \{0\}$. ■

Corollary 2.4. *If $R \neq \{0\}$ and $r \in R$, then r is a unit if and only if r is not contained in any maximal ideal.*

Proof. If r is not a unit, we can apply the theorem to $I = (r)$ to get a maximal ideal containing r. ■

We move on to the topic of radical of ideals. If I is an ideal in R, we defined

$$I = \{r \in R \mid \text{ there exists } n \text{ such that } r^n \in I\}$$

The radical of 0 is the set of nilpotent elements in R.

Lemma 2.5. *The radical of an ideal is an ideal of R. Taking radical is an idempotent operation.*

Proof. Let $r, s \in \operatorname{rad}(I)$. Then exists a n such that $r^n, s^n \in I$. We can expand

$$(r+s)^N = \sum_{k=0}^{N} \binom{N}{k} r^k s^{N-k}$$

so for $N \geq 2n-1$, each term is in I. ■

Theorem 2.6. *If $I \neq R$, then the radical of I is the intersection of all prime ideals containing I.*

Proof. If $r \in \operatorname{rad}(I)$, and P is a prime ideal containing I, then $r^n \in I \subset P$, which implies $r \in P$. Hence $\operatorname{rad}(I) \subset \cap_{P \supseteq I} P$.

Now we must show that if $r \notin \operatorname{rad}(I)$, then there exists a prime ideal P containing I such that $r \notin P$. Under this assumption, we have that $r^n \notin I$ for any n. Let X be the set of all ideals J such that $I \subset J$ and $r^n \notin J$ for any n. Note that X is not empty since I is in X. Let M be a maximal element in this set X. We claim M is prime. To see this, suppose a, b are elements not in M. Then by the maximality of M, the ideal generated by a and M contains r^n and the ideal generated by b and M contains r^m. Therefore their product (ab, M) contains r^{n+m}. This shows $ab \notin M$, so M is a prime ideal. ■

Proposition 2.7. *The Jacobson radical of a ring R is the set $\{r \in R \mid 1 + rs$ is a unit for any $s \in R\}$.*

Proof. Suppose $1 + rs$ is not a unit for some s. Then there is a maximal ideal $\mathfrak{m}$ containing $1 + rs$. If $\mathfrak{m}$ also contains r, then $\mathfrak{m}$ contains $1 + rs - rs = 1$, which is impossible. So $r \notin \mathfrak{m}$. This shows that the Jacobson radical is contained in the proposed set.

Now assume $1 + rs$ is a unit for any $s \in R$. Suppose r is not in $\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. We know that the ideal generated by r and $\mathfrak{m}$ is the entire ring, so there exists $s \in R$ and $t \in \mathfrak{m}$ such that $sr + t = 1$. But then $t = 1 - sr$ is a unit in $\mathfrak{m}$, a contradiction. Therefore r is in the Jacobson radical. ■

3. Lecture 3: 2023.9.12

Theorem 3.1. *Let R be a Noetherian domain. Then the following are equivalent:*

(1) *R is a UFD*

(2) *if $r \in R$ non-zero non-unit, then r is irreducible if and only if (r) is a prime ideal*

Theorem 3.2. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Let K be the field of fractions of R. We will show that the irreducible elements in $R[x]$ are either $r \in R$ irreducible in r, or $f \in R[x]$ primitive and f is irreducible in $K[x]$.

Recall that $f \in R[x]$ non-zero is called *primitive* if the gcd of its coefficients is equal to 1. In general, if $f \neq 0$, define $c(f)$, the *content* of f, to be the gcd of its coefficients. So for any $f \neq 0$, we can write $f = c(f)f_0$ where f_0 is primitive.

Lemma 3.3. *If f, g are primitive polynomials in $R[x]$. If $f = \alpha g$ with $\alpha \in K^\times$, then $\alpha \in R^\times$.*

Proof. Let $\alpha = r/s$, so then $sf = rg$. The content of sf is s, and the content of rg is r, which means r is an associate of s, so $\alpha = r/s$ is a unit in R. ■

Lemma 3.4. *If $f \in k[x]$ is non-zero, then there exists $\alpha \in K^\times$ such that $\alpha f \in R[x]$ and αf is primitive.*

Proof. Let $f = \sum_{i=0}^{d} a_i x^i$ where $a_i = r_i/s_i$. Let s be the product of all s_i. Then $sf \in R[x]$. Now $\alpha = s/c(sf)$ does the job. ■

Lemma 3.5 (Gauss lemma)**.** *If $f, g \in R[x]$ are primitive, then fg is primitive.*

Proof. Suppose not. Then there exists a $r \in R$ irreducible such that r divides all coefficients of fg. Now work in the ring $R/(r)$. The ideal (r) is a prime ideal since R is a UFD, so $R/(r)$ is a domain. Now we have $\overline{f}\overline{g} = 0$ in $R/(r)$, so $\overline{f} = 0$ or $\overline{g} = 0$. This means r divides f or g, contradicting the hypothesis that both f and g are primitive. ■

Proposition 3.6.

(1) *If $g \in R[x]$ is primitive, $f \in R[x]$, then $g|f$ in $R[x]$ if and only if $g|f$ in $K[x]$.*

(2) *if $f \in R[x]$ primitive and $f = gh$ in $K[x]$, then there exists $g_0 = \alpha g$, $h_0 = \beta h$, $\alpha, \beta \in K$ such that g_0, h_0 are primitive and $f = g_0 h_0$.*

Proof. For (1), suppose $f = gh$ with $h \in K[x]$. We may assume f is primitive. There exists some $\alpha \in K^\times$ such that $\alpha h = h_0$ is primitive. Then $\alpha f = gh_0$ which is primitive by the Gauss lemma. Now by Lemma, we get that $\alpha \in R^\times$, so $h = \alpha h_0 \in R[x]$.

For (2), just choose α, β as suggested and observe the polynomials are primitive. ■

Corollary 3.7.

(1) *If $f \in R[x]$ is primitive and f is irreducible in $K[x]$, then f is irreducible in $R[x]$.*

(2) *if $r \in R$ is irreducible, then r is irreducible in $R[x]$.*

This identifies a collection of irreducible elements in $R[x]$.

Now we claim that any $f \in R[x]$ not 0 or unit can be factored into a product $r_1 \cdots r_a g_1 \cdots g_b$ such that r_i is irreducible in R and g_i are primitive and irreducible in $K[x]$. Indeed, write $f = c(f) f_0$ with f_0 primitive, then $r_1 \cdots r_a$ is just the factorization of $c(f)$ in R. Then in $K[x]$, we can factor f_0 into a product of irreduicbles in $K[x]$, but by part (2) of the Proposition, this gives a factorization in g_i's primitive in $R[x]$ and irreducible in $K[x]$.

The uniqueness of such factorizations follows from the uniqueness of factorizations in R and $K[x]$. ■

4. Lecture 4: 2023.9.14

We move on to affine algebraic geometry, which is the study of the polynomial ring $k[x_1, \cdots, x_n]$ where k is an algebraically closed field. Define $\mathbf{A}_k^n$ to be the affine n-space over k, which is just k^n as a set (or vector space). We think of $k[x_1, \cdots, x_n]$ as the ring of functions on $\mathbf{A}_k^n$.

Given $f_1, \cdots, f_N \in k[x_1, \cdots, x_n]$, define

$$V(f_1, \cdots, f_N) = \{x \in \mathbf{A}_k^n \mid f_1(x) = \cdots = f_N(x) = 0\}.$$

In generate, one can define $V(A)$ for any subset $A \subset k[x_1, \cdots, x_n]$ to be the set of all points on which every polynomial in A vanishes. It is easy to see that if I is the ideal generated by A, then $V(I) = V(A)$.

The Hilbert Basis Theorem says every ideal in $k[x_1, \cdots, x_n]$ is finitely generated, so there is no gain in considering infinite subset A. We will prove this theorem.

Theorem 4.1. *If R is Noetherian, then $R[x]$ is also Noetherian.*

This immediately implies $R[x_1, \cdots, x_n]$ is Noetherian if R is. And if S is a finitely generated R-algebra for R Noetherian, then S is Noetherian and finitely presented. This is because S is realized as $R[x_1, \cdots, x_n]/I$, but now we know $R[x_1, \cdots, x_n]$ is Noetherian and thus I is finitely generated, and as a quotient S is also Noetherian.

proof of theorem. Let I be an ideal in $R[x]$. Define

$$I_k = \{r \in R \mid \exists f = \sum_{i=0}^{k} r_k x^k \in I, r = r_k\}$$

which is the set of all leading coefficients of polynomials of degree at most k (could be 0). It is clear that I_k is an ideal. In particular, for any $f \in I$, $xf \in I$, so any $r \in I_k$ is also in I_{k+1}. Hence I_k is an increasing sequence of ideals, so R Noetherian implies $I_k = I_N$ for some N and all $k \geq N$.

For all $k \leq N$, choose $g_1^{(k)}, \cdots, g_{a_k}^{(k)} \in I$ polynomials of degree k such that their leading coefficients generates I_k (I_k is finitely generated in R).

We claim that I is generated by $g_i^{(k)}$, $0 \leq k \leq N$. It is clear that $(g_i^{(k)}) \subseteq I$ since all the $g_i^{(k)}$ are in I. Conversely, let $f \in I$. We proceed by induction on the degree d of f. If $d = 0$, then $f \in I \cap R = I_0$, so f is a linear combination of $g_i^{(0)}$'s.

For the inductive step, if $d \leq N$, then the leading coefficient of f is in I_d, so there exists some $s_i \in R$ such that

$$f - \sum_i s_i g_i^{(d)}$$

has degree less than d, because the $g_i^{(d)}$ can produce the leading coefficient. Then f is a linear combination of all $g_i^{(k)}$'s by the inductive hypothesis.

If $d > N$, the leading coefficient of f is in I_N, which is again produced by $g_i^{(N)}$'s. Consider

$$f - \sum_i s_i x^{d-N} g_i^{(N)}$$

which is a polynomial of smaller degree to finish. ■

Definition 4.2. A closed algebraic subset of $\mathbf{A}_k^n$ is a subset of the form $V(I)$ for some ideal I in $k[x_1, \cdots, x_n]$.

Lemma 4.3.

(1) $I_1 \subset I_2$ *implies* $V(I_2) \subset V(I_1)$

(2) $V(0) = \mathbf{A}_k^n$ *and* $V(1) = \varnothing$

(3) $V(\sum_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$

(4) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

Proof. The proof is just set theory, except for the inclusion $V(IJ) \subset V(I) \cap V(J)$. To see this, suppose $x \notin V(I) \cap V(J)$, so there exist $f_1 \in I, f_2 \in J$ such that $f_1(x) \neq 0$ and $f_2(x) \neq 0$. Then $f_1 f_2$ doesn't vanish at x, and $f_1 f_2 \in IJ$. This means $V(IJ) \subset V(I) \cap V(J)$. ■

This lemma shows that the algebraic sets form the closed sets of a topology. This is the Zariski topology.

Given any $X \subset \mathbf{A}_k^n$, define $I(X)$ to be the set of all polynomials that vanishes on all of X. This is an ideal.

Lemma 4.4.

(1) $X_1 \subseteq X_2$ *implies* $I(X_2) \subseteq I(X_1)$

(2) $X \subseteq V(I(X))$

(3) $I \subseteq I(V(I))$ *for any ideal* I *in* $k[x_1, \cdots, x_n]$

(4) $I(\mathbf{A}_k^n) = (0)$.

Proof. Definitions. ■

Lemma 4.5. *$V(I(X))$ is the smallest closed subset of $\mathbf{A}_k^n$ containing X, i.e. the Zariski closure of X. In particular, if $X = V(I)$ is closed, then $V(I(X)) = X$.*

Proof. Of course $V(I(X))$ is closed and $X \subseteq V(I(X))$. If $X \subset V(J) = Y$, then $J \subseteq I(Y) = I(V(J)) \subseteq I(X)$. Then $V(I(X)) \subset V(J) = Y$. ■

The question in the opposite direction is what is $I(V(I))$. Clearly $\mathrm{rad}(I)$ is contained in $I(V(I))$ since if $f \in \mathrm{rad}(I)$, then $f^N \in I$, so $f^N(x) = 0$ for every $x \in V(I)$. Hence $f(x) = 0$ for every $x \in V(I)$, so $f \in I(V(I))$. The **Nullstellensatz** shows this inclusion is an equality.

A special case is the following: if $\mathfrak{m}$ is a maximal ideal of $k[x_1, \cdots, x_n]$, then there exists $a_1, \cdots, a_n \in k$ such that $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$. In other words, $\mathfrak{m}$ is the kernel of the evaluation map at the point $(a_1, \cdots, a_n)$.

Conversely, assuming the Nullstellensatz, we have $V(\mathfrak{m}) \neq \varnothing$, so there is some point $a = (a_1, \cdots, a_n)$ such that $a \in V(\mathfrak{m})$, so $\mathfrak{m} \subset I(\{a\})$. By maximality they are equal.

We already know that $k[x_1, \cdots, x_n]$ is a UFD, and the non-zero minimal prime ideals are generated by a single irreducible polynomial f. We call $V(f)$ is an irreducible hypersurface. For any f, by factoring it into irreducibles $f = f_1 \cdots f_N$, we get $V(f) = V(f_1) \cup \cdots \cup V(f_N)$, so every hypersurface is a union of irreducible hypersurfaces.

The operations V and I give a one-to-one correspondence between affine algebraic sets and radical ideals of $k[x_1, \cdots, x_n]$.

Let X be a set in $\mathbf{A}_k^n$. What are the functions on X? They come from function on $\mathbf{A}_k^n$, but two such function are the same on X if their difference vanishes on X. Thus we defined the affine coordinate ring of X, $A(X)$, to be $k[x_1, \cdots, x_n]/I(X)$. We see that $A(X)$ is reduced.

Lemma 4.6. *Maximal ideals of $A(X)$ are in bijection with points of X.*

Proof. Maximal ideals of $A(X)$ are in bijection with maximal ideals of $k[x_1, \cdots, x_n]$ containing $I(X)$. Those are of the form $\mathfrak{n} = (x_1 - a_1, \cdots, x_n - a_n)$, and $I(X) \subset \mathfrak{n}$ mean $(a_1, \cdots, a_n)$ is in X. ■

5. Lecture 5: 2023.9.19

Definition 5.1. Let X be a topological space. X is irreducible if when $X = X_1 \cup X_2$ a union of closed subsets, then $X = X_1$ or $X = X_2$. Equivalently, every two non-empty open subsets have a non-empty intersection.

Proposition 5.2. *Let $X = V(I)$ be a closed subset of $\mathbf{A}_k^n$. X is irreducible if and only if $I(X)$ is prime.*

Proof. If X is not irreducible then we can write $X = X_1 \cup X_2$ where $X_i \neq X$. So there exist functions f_i that vanishes on X_i but not on X, i.e. $f_i \notin I(X)$. But $f_1 f_2$ vanishes on X, so $I(X)$ is not a prime ideal.

If $I(X)$ is not a prime ideal, then there exists f_1, f_2 not in $I(X)$ but $f_1 f_2 \in I(X)$. This implies that $X \subset V(f_1 f_2)$ but X is not contained in $V(f_i)$. Now take $X_i = X \cap V(f_i)$, which is a proper closed subset of X. Thus X is not irreducible. ■

By the correspondence, X is irreducible if and only if $X = V(I(X)) = V(\mathfrak{p})$ where $\mathfrak{p}$ is a prime ideal.

Example 5.1.

(1) $\mathbf{A}_k^n$ is irreducible since $\mathbf{A}_k^n = V(0)$

(2) A point is irreducible since it is the vanishing locus of a maximal ideal.

Definition 5.3. X is a (affine $k-$)variety if X is irreducible closed subset of $\mathbf{A}_k^n$.

Equivalently, $I(X)$ is a prime ideal, which is equivalent to $A(X)$ being a domain.

Remarks about the Zariski topology:

(1) On $\mathbf{A}_k^1$, the Zariski topology is the finite complement topology, i.e. the closed sets are $\varnothing$, finite sets, and $\mathbf{A}_k^1$. As topological spaces, this only depends on the cardinality of k.

(2) If $n, m > 0$, of course **as sets** $\mathbf{A}_k^{n+m} = \mathbf{A}_k^n \times \mathbf{A}_k^m$. But the topologies are never the same, i.e. $\mathbf{A}_k^{m+n}$ always has more open sets than $\mathbf{A}_k^n \times \mathbf{A}_k^m$ with the product topology.

Let $D_f = \mathbf{A}_k^n - V(f)$, i.e. the non-vanishing locus of a polynomial f. This is called a basic open set. It is easy to see that $D_f \cap D_g = D_{fg}$, and

$$\bigcup_{\alpha \in A} D_{f_\alpha} = \mathbf{A}_k^n - V(f_\alpha : \alpha \in A).$$

In particular, if $\{D_{f_\alpha}\}$ cover the whole space if and only if $\{f_\alpha\}$ generates the unit ideal. This is the same as saying there exist $f_{\alpha_1}, \cdots, f_{\alpha_N}$ that generates 1. This in turn means $D(f_{\alpha_1}), \cdots, D(f_{\alpha_N})$ also cover the whole space. The space $\mathbf{A}_k^n$ is quasi-compact.

More generally, any open set is a complement of some $V(I)$, and I is finitely generated so it is finite union of D_f's. This shows that D_f's are a basis of the Zariski topology.

The Zariski topology is not Hausdorff because every two open sets have non-empty intersection, but it is true that points are closed.

Definition 5.4. X is called a Noetherian topological space if every decreasing sequence of closed subsets $X_1 \supset X_2 \supset \cdots \supset X_n \supset \cdots$ is eventually constant.

The affine space $\mathbf{A}_k^n$ is Noetherian since $k[x_1, \cdots, x_n]$ is. Any closed subset of $\mathbf{A}_k^n$ is quasi-compact and Noetherian.

We now turn to morphisms. A natural notion of a morphism from X to $\mathbf{A}_k^1$ is just an element in $A(X)$. A morphism $\mathbf{A}_k^n \to \mathbf{A}_k^m$ is a m-tuple of polynomials $F = (f_1, \cdots, f_m)$. We get a map $F^* : k[y_1, \cdots, y_m] \to k[x_1, \cdots, x_n]$ by $g \mapsto g \circ F$. This is specified by $F^*(y_i) = f_i$ which uniquely determines a k-algebra homomorphism.

An ad hoc definition of a general morphism would be this: If $X \subset \mathbf{A}_k^n$ and $Y \subset \mathbf{A}_k^m$, a morphism $X \to Y$ is a function $G : X \to Y$ which is the restriction of a morphism $F : \mathbf{A}_k^n \to \mathbf{A}_k^m$.

Proposition 5.5. *There is a bijection between morphisms $G : X \to Y$ and k-algebra homomorphisms $G^* : A(Y) \to A(X)$.*

Proof. Start from a morphism $F : \mathbf{A}_k^n \to \mathbf{A}_k^m$ such that $F(X) \subset Y$. This defines a $F^* : k[y_1, \cdots, y_m] \to k[x_1, \cdots, x_n]$. We claim that $F^*(I(Y)) \subset I(X)$. Granting this claim, the map F^* induces a map

$$k[y_1, \cdots, y_m]/I(Y) \to k[x_1, \cdots, x_n]/I(X)$$

i.e. a map $A(Y) \to A(X)$. So now we prove the claim. Suppose $F(X) \subset Y$. Then for all $x \in X$, $F(x) = (f_1(x), \cdots, f_m(x)) \in Y$. So for every $g \in I(Y)$, we have $g(f_1(x), \cdots, g_m(x)) = 0$. This means $F^*(g)(x) = 0$, so $F^*(g) \in I(X)$.

In the other direction, if $\phi : A(Y) \to A(X)$ is a k-algebra homomorphism, then we have

$$\begin{tikzcd}
k[y_1, \cdots, y_m] \arrow[r, dashed] \arrow[d, two heads] & k[x_1, \cdots, x_n] \arrow[d, two heads] \\
A(Y) \arrow[r, "\varphi"] & A(X)
\end{tikzcd}$$

Let $f_i = \phi(y_i)$. This uniquely defines a map $F^* : k[y_1, \cdots, y_m] \to k[x_1, \cdots, x_n]$. Now define $F(x) = (f_1(x), \cdots, f_m(x))$. We easily see that $F^*(I(Y)) \subset I(X)$. Namely, for any $g \in I(Y)$, $g(F(x)) = 0$ for all $x \in X$, so $F(x) \in Y$. This means $F(X) \subset Y$. ■

This correspondence is contravariant, and the morphisms are continuous in the Zariski topology. We obtained an equivalence of categories between the category of affine algebraic sets and the category of reduced finitely generated k-algebras.

But the category of reduced finitely generated k-algebras has a lot of adjective. Our goal will be to generalize to all commutative rings.

Given a commutative ring R, define $\operatorname{Spec} R$ to be the set of all prime ideals in R. Given a ring morphism $f : R \to S$, we get $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ since the preimage of a prime ideal is prime. If $I \subset R$ is an ideal, define $V(I)$ to be the set of prime ideals that contain I.

Lemma 5.6.

(1) *If $I_1 \subset I_2$, then $V(I_2) \subset V(I_1)$.*

(2) $V(0) = \operatorname{Spec} R$. *$V(r) = \varnothing$ if and only r is a unit.*

(3) $V(\sum_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$.

(4) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

This proves the $V(I)$'s form closed set of a topology. This is the Zariski topology.

Example 5.2. Suppose R is a PID (e.g. $k[x], \mathbf{Z}$). If r is not a unit or 0, then $V(r) = V(r_1) \cup V(r_N)$ where $r_1, \cdots, r_N$ are distinct irreducible factors of r. Each $V(r_1)$ is a single point since (r_i) is maximal. So the elements of $\operatorname{Spec} R$ are the irreducibles (mod R^*) together with (0).

Note that in any domain R, (0) is not in any proper closed subsets, because that happens exactly when $(r) \subset (0)$ which means $r = 0$. Thus the closure of the point $(0) = \eta$ is the entire $\operatorname{Spec} R$. We say that it is a generic point.

In the case $R = k[x]$, $\operatorname{Spec} k[x]$ and the usual $\mathbf{A}^1_k$ have the same open sets, because non-zero prime ideals of $k[x]$ are in bijection with point in $\mathbf{A}^1_k$. But there is an extra generic point $\eta = (0)$ that is in every non-empty open set.

Example 5.3. Let $R = k[x_1, x_2]$ with $k = \overline{k}$. Prime ideals are $(0), (f)$ for f irreducible, and $(x_1 - a_1, x_2 - a_2)$. The closed points are ones of the form $(x_1 - a_1, x_2 - a_2)$, and the generic point is (0). The ones of the form (f) have closure $\{(f)\}$ union all the points lying on f.

6. Lecture 6: 2023.9.21

Definition 6.1. A ring is graded is $R = \oplus_{d \geq 0} R_d$ as abelian groups such that $R_d R_e \subset R_{d+e}$. A homomorphism of graded rings $f : R \to S$ is a ring homomorphism such that $f(R_d) \subset S_d$.

Any ring R is trivially graded by setting $R = R_0$. The polynomial ring $S = R[x_1, \cdots, x_n]$ is graded where S_d is the set of homogenous degree d polynomials. The natural map $R \to S$ is a graded homomorphism. In this grading, each x_i has weight 1, but it is possible to assign different weights to x_i, and define the grading of a monomial to be the sum of all these weights.

For a general graded ring R, say $r \in R$ is homogenous of degree d if $r \in R_d$. In general, $r = \sum_d r_d$ where r_d is the d-th homogenous piece. Here are some observations:

(1) $1 \in R_0$, so R_0 is a subring. This is non-obvious but here's the proof. Let r_0 be the 0-th homogeneous part of 1. If s is homogenous, then $s = 1 \cdot s = r_0 s$. Writing any element as a sum of homogenous ones, we see that $s = r_0 s$ for any $s \in R$. Thus r_0 is the multiplicative identity.

(2) R_d are R_0-submodules of R.

(3) $R_+ = \oplus_{d>0} R_d$ is an ideal. This is called the irrelevant ideal.

Definition 6.2. Let I be an ideal of R. I is a homogenous ideal if $I = \oplus_{d \geq 0}(I \cap R_d)$.

Equivalently, homogenous ideals I are those which can be generated by homogenous elements. For any $r \in R$ write $r = \sum_d r_d$, then $r \in I$ if and only if $r_d \in I$ for any d. We have that $R/I = \oplus_{d \geq 0} R_d / I_d$ so it is also graded.

If I, J are graded, then so are $I + J, I \cap J, IJ$ and $\operatorname{rad}(I)$.

Graded rings arise in nature in the context of projective spaces. For simplicity let k be an algebraically closed field. The projective space $\mathbf{P}^1_k$ as a set is

$$(k^{n+1} - \{0\})/k^*$$

A point a has homogenous coordinates $(a_0, \cdots, a_n)$. There is an inclusion $\mathbf{A}^n_k \to \mathbf{P}^n_k$ given by $(x_1, \cdots, x_n) \mapsto (1, x_1, \cdots, x_n)$.

Let $f \in k[x_0, \cdots, x_n]$ be a polynomial. It defines a closed set $V(f)$ in $\mathbf{A}^n_k$, but this has no meaning in $\mathbf{P}^n_k$ since points can have different representatives. But if f is homogenous of degree d, then $f(tx) = t^d f(x)$, so it is well-defined to say at which points f vanishes.

More generally, if $I \subset k[x_0, \cdots, x_n]$ is a homogenous ideal, we can define $V_+(I) \subset \mathbf{P}^n_k$ to be the set of points on which all of I vanish. If $f \in k[x_0, \cdots, x_n]$ is homogenous of degree d, we can define

$$f^{\text{inh}} \in k[y_1, \cdots, y_n]$$

to be $f^{\text{inh}}(y) = f(1, y)$. So $V(f^{\text{inh}}) = V_+(f) \cap \mathbf{A}^n_k$. The upshot is that the $V_+(I)$'s for I homogenous defines a topology on $\mathbf{P}^n_k$ and it induces the Zariski topology on $\mathbf{A}^n_k$. Note that $\mathbf{A}^n_k = \mathbf{P}^n_k - \{V_+(x_0)\}$, so it is an open subset of $\mathbf{P}^n_k$. In fact, $n+1$ copies of $\mathbf{A}^n_k$ cover $\mathbf{P}^n_k$.

Note that in $\mathbf{P}^n_k$ there is no such point as $(0, \cdots, 0)$, so $V_+(x_0, \cdots, x_n) = \varnothing = V(1)$, so the usual Nullstellensatz is false. The correct version is just to ignore this bad example: there is a bijection between closed sets in $\mathbf{P}^n_k$ and homogenous radical ideals not equal to $(x_0, \cdots, x_n)$.

A projective variety X is an irreducible closed set, which corresponds to $V_+(\mathfrak{p})$ where $\mathfrak{p}$ is a homogenous prime ideal. For any $X = V(I)$ (can take I radical), we have the homogenous coordinate ring $A_+(X) = k[x_0, \cdots, x_n]/I$, which is graded since I is homogeneous. It is an domain if and only if X is a projective variety.

In the affine case, $A(X)$ is intrinsic to X, i.e. $X \cong Y$ if and only if $A(X) \cong A(Y)$. In the projective case, one can define morphisms of closed projective sets (by doing so locally), but $A_+(X)$ is not intrinsic, since it depends on the embedding $X \subset \mathbf{P}^n_k$. Morphisms from $A_+(Y) \to A_+(X)$ don't necessarily come from morphisms $X \to Y$. For example, if $m > n$ we have

$$k[x_0, \cdots, x_n] \hookrightarrow k[x_0, \cdots, x_m]$$

but there is no morphism $\mathbf{P}^m_k \to \mathbf{P}^n_k$: the map $(x_0, \cdots, x_m) \mapsto (x_0, \cdots, x_n)$ is not defined at points of the form $(0, \cdots, 0, x_{n+1}, \cdots, x_m)$.

Let R be a graded ring. Define $\operatorname{Proj} R$ to be the set of homogenous prime ideals $\mathfrak{p}$ in R which doesn't contain R_+. If I is a homogenous ideal, we can still define $V_+(I)$ to be the set of prime ideals in $\operatorname{Proj} R$ that contain I. This defines a Zariski topology on $\operatorname{Proj} R$. For example,

$$\operatorname{Proj} R[x_0, \cdots, x_n] = \mathbf{P}^n_R$$

with the usual grading. When R is a field k, we get

$$\operatorname{Proj} k[x_0, \cdots, x_n] = \mathbf{P}^n_k$$

but this is not the same as the $\mathbf{P}^n_k$ before, in a similar manner how $\operatorname{Spec} k[x_1, \cdots, x_n]$ is not the same as the classical $\mathbf{A}^n_k$.

Modules. We have define the sums, intersections, and quotients of modules. If $I \subset R$ is an ideal, then IM is a submodules of M. The quotient M/IM is naturally an R/I-module. As an example, given M_α, $\alpha \in A$ some index set, we defined the objects $\prod_\alpha M_\alpha$ and $\oplus_\alpha M_\alpha$. If A is any set and $M_\alpha = M$ for all α, then

$$\prod_\alpha M \cong M^A = \text{set of all functions } A \to M$$

The direct sum is the functions which are 0 for all but finitely many α. Also, if $m \in M$, the cyclic R-module Rm is the obvious thing. More generally the submodule generated by $m_1, \cdots, m_n$ is $Rm_1 + \cdots + Rm_n$.

Definition 6.3. The module M is finitely generated if there exist some $m_1, \cdots, m_n$ such that $M = Rm_1 + \cdots + Rm_n$.

Another way to produce new modules is by taking Homs. If M, N are R-modules, $\mathrm{Hom}_R(M, N)$ is the set of all R-module homomorphisms. This is itself an R-module by pointwise addition and multiplication. In particular, we define the dual module $M^\vee$ to be $\mathrm{Hom}_R(M, R)$. Hom is a functor in both arguments, covariant in the codomain and contravariant in the domain.

For $\prod_\alpha M_\alpha$, we have projections $\pi_\alpha : \prod_\alpha M_\alpha \to M_\alpha$; for direct sum $\oplus_\alpha M_\alpha$ we have inclusions $i_\alpha : M_\alpha \to \oplus_{M_\alpha}$. Suppose a module N is equipped with maps $f_\alpha : N \to M_\alpha$, then there exists a unique map $f : N \to \prod_\alpha M_\alpha$ such that $\pi_\alpha \circ f = f_\alpha$. On the other hand, if N is equipped with maps $g_\alpha : M_\alpha \to N$, then there is a unique map $g : \oplus_\alpha M_\alpha \to N$ such that $g_\alpha = g \circ i_\alpha$. In other words,

$$\mathrm{Hom}_R(N, \prod_\alpha M_\alpha) = \prod_\alpha \mathrm{Hom}_R(N, M_\alpha)$$

$$\mathrm{Hom}_R\left(\bigoplus_\alpha M_\alpha, N\right) = \prod_\alpha \mathrm{Hom}_R(M_\alpha, N)$$

In particular, if A is a set, we have the free module $F_R(A) = \oplus_{\alpha \in A} R$. Then we see that

$$\mathrm{Hom}_R(F_R(A), M) = \mathrm{Hom}_R\left(\bigoplus_{\alpha \in A} R, M\right) = \prod_{\alpha \in A} \mathrm{Hom}_R(R, M) = \prod_{\alpha \in A} M = M^A$$

Lemma 6.4. *Every R-module M is a quotient of a free R-module. An R-module M is finitely generated if and only if M is a quotient of R^n for some n.*

Proof. Take $A = M$ and consider $F_R(A)$. There is an identity map $A \to M$, which induces a map $F_R(M) \to M$ a surjection.

In general, given a finite set $m_1, \cdots, m_n \in M$, there is a map $R^n \to M$ where $(r_1, \cdots, r_n)$ is sent to $\sum_i r_i m_i$. So M is finitely generated if and only if this map is surjective.

■

Definition 6.5. Say M is finitely presented if there is a surjection $R^n \to M$ such that the kernel is also finitely generated.

7. Lecture 7: 2023.9.26

A complex $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is exact at M if the image of α is equal to the kernel of β. A complex is exact if it is exact at every spot where it makes sense (not the head or tail). A short exact sequence is an exact complex of the form

$$0 \to M' \to M \to M'' \to 0.$$

A morphism of short exact sequences of short exact sequences are maps in the three spots such that the entire diagram commutes.

Given a morphism $\alpha : M_1 \to M_2$, we get an exact sequence

$$0 \to \ker(\alpha) \to M_1 \xrightarrow{\alpha} M_2 \to \operatorname{coker}(\alpha)$$

The cokernel of the kernel is the same as the kernel of the cokernel, which are both the image of α.

Lemma 7.1. *Let $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ be a short exact sequence of R-modules. The following are equivalent:*

(1) *there exists $s : M'' \to M$ such that $\pi \circ s = id_{M''}$*

(2) *there exists $r : M \to M'$ such that $r \circ i = id_{M'}$*

(3) *there exists an isomorphism $f : M \to M' \oplus M''$ such that*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "i"] \arrow[d] & M \arrow[r, "\pi"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] & M' \oplus M'' \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

is an isomorphism of short exact sequences.

Proof. 3 to 1: Let s be the map given by $M'' \to M' \oplus M'' \xrightarrow{f^{-1}} M$. 3 to 2 is of course the same.

1 to 3: Suppose there exists $s : M'' \to M$ such that $\pi \circ s = id_M$. Observe that

$$M = \ker(\pi) \oplus \operatorname{Im}(s)$$

For each $m \in M$, let $m_2 = s(\pi(m))$ and let $m_1 = m - m_2$, then $m_2 \in \operatorname{Im}(s)$ and $m_1 \in \ker(\pi)$. If $m \in \ker(\pi) \cap \operatorname{Im}(s)$, then let $m = s(m_1)$ and $m_1 = \pi(s(m_1)) = 0$, so $m = 0$. ■

Definition 7.2. A short exact sequence is called split if the conditions of the lemma is met.

Example 7.1. $0 \to \mathbf{C}[x] \xrightarrow{x} \mathbf{C}[x] \to \mathbf{C}[x]/(x) \to 0$ is not split. Let $R = \mathbf{C}[x, y]$.

$$0 \to R \to R^{\oplus 2} \to (x, y) \to 0$$

given by $c \mapsto (cy, -cx)$ and $(a, b) \mapsto xa + yb$ is a short exact sequence. It is not split since the first map has no left inverse.

Lemma 7.3. *If $0 \to M' \to M \to M'' \to 0$ if short exact, and M'' is free, then it is split.*

Proof. Let $\{e_i\}$ be a basis of M''. Let m_i be such that $e_i = \pi(m_i)$. Let s be defined by $s(e_i) = m_i$. ■

Lemma 7.4 (snake)**.** *Given a map of short exact sequences, we get a 6-term exact sequence.*

$$0 \to \ker \to \ker \to \ker \to \operatorname{coker} \to \operatorname{coker} \to \operatorname{coker} \to 0.$$

Proposition 7.5. *Suppose* $0 \to M' \to M \to M'' \to 0$ *is a short exact sequence. Then for any* R*-module* N*, the following are exact*

$$0 \to \operatorname{Hom}_R(N, M') \to \operatorname{Hom}_R(N, M) \to \operatorname{Hom}_R(N, M'')$$
$$0 \to \operatorname{Hom}_R(M'', N) \to \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M', N)$$

Definition 7.6. An R-module P is called projective if for any surjection $\pi : M' \to M$ of R-modules, every map $\phi : P \to M$ can be lifted to a map $\phi' : P \to M'$. In other words, given any solid diagram, there exists a dashed map like this:

$$\begin{tikzcd}
& M'' \arrow[d, two heads] \\
P \arrow[ur, dashed] \arrow[r] & M
\end{tikzcd}$$

Lemma 7.7. *Every short exact sequence* $0 \to M' \to M \to P \to 0$ *with* P *projective splits.*

Proof.

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & P \arrow[r] & 0 \\
& & & P \arrow[u, "id"'] \arrow[ul, dashed, "s"] &
\end{tikzcd}$$

■

We proved that every free module is projective, so every module is a quotient of a projective module. This means that the category of R-modules has enough projectives.

Example 7.2. If $R = R_1 \times R_2$, we can write $1 = (1, 0) + (0, 1)$ a sum of idempotents. The R-module $R_1 \times 0$ is projective but not free. As a concrete example, $\mathbf{C}[x]/(x(x-1))$ isomorphic to $\mathbf{C} \times \mathbf{C}$, but $\mathbf{C}[x]/(x)$ is not free over $\mathbf{C}[x]/(x(x-1))$.

Lemma 7.8. *A module* P *is projective if and only if it is a summand of a free module.*

Proof. Assume P is projective. Pick a surjection $F \to P$ with F free. Using the definition of projective modules, this surjection splits, so P is a direct summand.

On the other hand, suppose $P \oplus Q = F$ for some free module F. Suppose there a surjection $M' \to M$ and a map $\phi : P \to M$. We can extend ϕ by 0 on Q to get a map $F \to M$. But F is projective, so it lifts to a map $\psi : F \to M''$. Then $\psi|_P$ is what we want. ■

Definition 7.9. An R-module I is injective if for any injection $i : M \to M'$, every map $\psi : M \to I$ can be extended to a map $\psi' : M' \to I$.

$$\begin{tikzcd}
M \arrow[r] \arrow[d, hook] & I \\
M' \arrow[ur, dashed] &
\end{tikzcd}$$

Projective modules are easier than injectives because of the presence of free modules. Injectives are not so easy. A characterization of injective **Z**-modules is that I is injective if and only if it is *divisible*: for any $x \in I$ and $n \in \mathbf{Z}$ non-zero, there exists $y \in I$ such that $ny = x$. In fact, this works over any PID.

Lemma 7.10. *Suppose R is a ring and a is not a zero divisor. Then if I is injective, then I is a-divisible: $a : I \to I$ is surjective.*

Proof.

$$\begin{tikzcd}
R \arrow[r, "r\mapsto rx"] \arrow[d, hook, "a"'] & I \\
R \arrow[ur, dashed] &
\end{tikzcd}$$

■

8. Lecture 8: 2023.9.28

Definition 8.1. An R-module M is artinian if it satisfies the descending chain condition.

Lemma 8.2. *Let M be an R-module. Then M is noetherian if and only every submodule of M is finitely generated. This is also equivalent to every non-empty collection of submodules has a maximal element.*

Proof. Easy. ■

Lemma 8.3. *Let M be an R-module. The following are equivalent:*

(1) *M is artinian*

(2) *every non-empty collection of submodules has a minimal element.*

Proof. Easy. ■

Example 8.1. If R is a k-algebra, k is a field, and $\dim_k(M) < \infty$, then M is artinian as a R-module.

An artinian module not of this form is this: let $R = k[x]$. Let $M - k[x, x^{-1}]/k[x]$ where the quotient is as k-vector spaces. This has the basis $\frac{1}{x^n}$ as a vector space. The only submodules are 0, $\frac{1}{x^n}k[x]/k[x], M$.

Another example is $\mathbf{Q}/\mathbf{Z}$ as a **Z**-module.

Lemma 8.4. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules. Then M is noetherian if and only if M' and M'' are noetherian. M is artinian if and only if M' and M'' are artinian.*

Proof. If there is a chain in M, one can look at its image in M'' which stabilizes, and then look at the intersection of it with M', which will also stabilize. ■

Corollary 8.5. *Finite direct sums of noetherian(artinian) modules are also noetherian(artinian).*

Corollary 8.6. *If R is a noetherian ring, then $R^{\oplus n}$ is noetherian, so any quotient of $R^{\oplus n}$ is noetherian, i.e. any finitely generated R-module is noetherian.*

Corollary 8.7. *If R is noetherian and M is an R-module. The following are equivalent:*

(1) *M is noetherian*

(2) *M is finitely generated*

(3) *M is finitely presented.*

It is true that artinian rings are noetherian, but it is not so obvious.

Lemma 8.8. *Let M be an R-module. The following are equivalent:*

(1) *M is both noetherian and artinian*

(2) *M has a composition series, i.e. there exists a filtration*

$$0 \subset M_1 \subset \cdots \subset M_n = M$$

such that for each i, M_i/M_{i-1} is a simple R-module.

Lemma 8.9. *M simple if and only if $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.*

Proof. If $S \subset R/\mathfrak{m}$ is a submodule, then the inverse of S in R is an ideal containing $\mathfrak{m}$. So $S = R/\mathfrak{m}$ or $S = 0$.

Now suppose M is a simple R-module. Let $m \in M$ be any non-zero element. Then Rm is a non-zero submodule, so $Rm = M$ by simplicity. Thus $M \cong R/I$ where I is the annihilator of m. As before there is no ideal that strictly contains I, so I is maximal.

■

Lemma 8.10. *Let M be an R-module and let I be an ideal of R. If M is finitely generated and $IM = M$, then there exists $f \in 1 + I$ such that $fM = 0$.*

Proof. Use induction to reduce to the case of cyclic modules where this is clear.

Here is another proof with matrices. Let M be generated by $m_1, \cdots, m_n$. Then each $m_i \in IM$, so $m_i = \sum_j x_{ij}m_j$ for some $x_{ij} \in I$. This means that the matrix $I-(x_{ij})_{ij}$ kills the vector $(m_1, \cdots, m_n)$.

For any matrix T over any ring R, there is another matrix T^{adj} such that

$$\det(T)I = T^{\text{adj}}T$$

Therefore we see that $\det(T) \in R$ kills $(m_1, \cdots, m_n)$. Furthermore, $\det(I)$ is in $1 + I$ because $x_{ij} \in I$. ■

Lemma 8.11 (Nakayama's Lemma, first version)**.** *Let M be a finitely generated R-module and let I be an ideal of R. If $IM = M$ and I is in the Jacobson radical $J(R)$ of R, then $M = 0$.*

Proof. Use the previous lemma to find a $f \in 1 + I$ such that $fM = 0$. But any element in $1 + J(R)$ is a unit, so $M = 0$. ■

As an application, let's prove the following: Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field k, Let M be a finitely generated R-module. Let $x_1, \cdots, x_r$ be elements whose images generate the k-vector space $M/\mathfrak{m}M$. Then $x_1, \cdots, x_r$ generates M.

The proof is like this. Let $N = M/(Rx_1 + \cdots + Rx_r)$. The goal is to show $N = 0$. N is finitely generated because it is a quotient of M. Pick $y \in N$, then y is the image of some $z \in M$ modulo $Rx_1 + \cdots + Rx_r$. By assumption, the image of z in $M/\mathfrak{m}M$ is a sum $\sum \lambda_i x_i$ for some $\lambda_i \in k$. Say λ_i has a lift ξ_i in R. Then

$$z - \xi_1 x_i - \cdots - \xi_r x_r \in \mathfrak{m}M$$

This means $y \in \mathfrak{m}N$, i.e. $N = \mathfrak{m}N$. So we are done by Nakayama's lemma.

A variant: if $(R, \mathfrak{m}, k)$ is a local ring and $\phi : M \to N$ is a map of finitely generated modules. Then ϕ is surjective if and only if $\phi : M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective.

Corollary 8.12. *Over a local ring $(R, \mathfrak{m}, k)$, a finitely generated projective module P is free.*

Proof. Pick $x_1, \cdots, x_r \in P$ which maps to a basis of $P/\mathfrak{m}P$. The by the previous lemma we obtain a surjection

$$\phi : R^{\oplus r} \to P$$

This splits because P is projective. Let s be its right inverse. Note that s is an isomorphism on the level of k-vector spaces because it is a surjection between vector spaces with the same dimension. This proves that s is a surjection by the previous statement. Think to see s is actually the inverse of ϕ, or use the FREDHOLD ALTERNATIVE. ■

Lemma 8.13. *Let R be any ring and M a finitely generated R-module. Then any surjective map $\phi : M \to M$ is an isomorphism*

Proof. Let $A = R[x]$. Then M is an A-module where x acts via ϕ. Then ϕ being surjective is equivalent to $(x)M = M$. Then there exists $f = 1 + i$ for $i \in I$ such that $fM = 0$. Let $i = r_1 x + \cdots + r_t x^t$. We see that for all $m \in M$,

$$(1 + r_1 x + \cdots + r_t x^t)m = 0$$

so

$$m = -(r_1 + \cdots + r_t x^{t-1})xm$$

This proves that ϕ has an inverse given by $r_1 + \cdots + r_t \phi^{(t-1)}$. ■

9. Lecture 9: 2023.10.3

Definition 9.1. If M_1, M_2, N are R-modules, a bilinear map is a map $f : M_1 \times M_2 \to N$ such that it is linear in both variables. Denote by $\mathrm{Bil}(M_1, M_2; N)$ the set of all bilinear maps.

As an example, $\mathrm{Hom}_R(M, N) \times M \to N$ given by evaluation is bilinear.

Definition 9.2. A tensor product $M_1 \otimes_R M_2$ is an object that satisfies the universal property: it is equipped with a R-bilinear map $t : M_1 \times M_2 \to M_1 \otimes_R M_2$, and for any bilinear map $f : M_1 \times M_2 \to N$, there exists a unique R-linear map $F : M_1 \otimes_R M_2 \to N$ such that $f = F \circ t$. In other words, $\mathrm{Bil}(M_1, M_2; N) \cong \mathrm{Hom}_R(M_1 \otimes M_2, N)$.

As a solution to a universal property, any 2 tensor products are isomorphic by a unique isomorphism.

Proposition 9.3. *Tensor product exists for any R-modules M_1, M_2.*

Proof. Start with the free module $F_R(M_1 \times M_2)$. There is an R-linear map $M_1 \times M_2 \to F_R(M_1 \times M_2)$ by doing nothing. Let Q be the submodule of $F_R(M_1 \times M_2)$ generated by $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, etc. the relations of bilinearity. Then let $M_1 \otimes_R M_2$ be $F_R(M_1 \times M_2)/Q$. Denote the image of (m_1, m_2) by $m_1 \otimes m_2$. Then we get a map $t : M_1 \times M_2 \to M_1 \otimes M_2$ such that $t(m_1, m_2) = m_1 \otimes m_2$ that is bilinear.

Given $f : M_1 \times M_2 \to N$ bilinear, we obtain a map $F_R(M_1 \times M_2) \to N$. The fact that f is bilinear exactly means $f(Q) = 0$, so it induces a unique map $M_1 \otimes_R M_2 \to N$ that commutes with f and t (check on generators (m_1, m_2)). ■

From the construction we see that tensor product $M_1 \otimes_R M_2$ is generated by pure tensors $m_1 \otimes m_2$. This implies, for example, if two maps agrees on pure tensors then the two maps are equal.

Similarly, we can define a tensor product of k modules as the object having the universal property with bilinear replaced with multilinear.

Some comments: $\mathrm{Bil}(M_1, M_2; N) \cong \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, N))$ by the obvious correspondence. Likewise, multilinear maps can be iteratively written as linear maps.

Using the universal property of tensor products, we get some properties:

(1) $M_1 \otimes_R M_2 \cong M_2 \otimes M_1$

(2) $M_1 \otimes_R (M_2 \otimes_R M_3) \cong (M_1 \otimes_R M_2) \otimes_R M_3 \cong M_1 \otimes_R M_2 \otimes_R M_3$. (Use the universal property of 3-tensor and 3-linear maps.)

(3) $(M_1 \oplus M_2) \otimes_R M_3 \cong M_1 \otimes_R M_3 \oplus M_2 \otimes_R M_3$

(4) $R \otimes_R M \cong M$.

(5) $R^{\oplus n} \otimes_R R^{\oplus m} \cong R^{\oplus mn}$

(6) Let $f_1 : M_1 \to N_1$ and $f_2 : M_2 \to N_2$ be R-module homomorphisms. Then we get a unique map $f_1 \otimes f_2 : M_1 \otimes_R M_2 \to N_1 \otimes_R N_2$ such that $(f_1 \otimes f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$.

The first application of tensor product is change of rings. Let S be an R-algebra, and let M be an R-module. We can form the tensor product $S \otimes_R M$, which is of course an R-module. But it is in fact an S-module. The S-module structure is $(s_1, s_2 \otimes m) \mapsto (s_1 s_2) \otimes m$. Now note that $S \otimes_R M$ have 2 R-module structures: the other one is through the ring map $R \to S$ and the S-module structure. The two structures are the same.

As an example, there is an canonical isomorphism $S \otimes_R (R^{\oplus n}) \cong S^{\oplus n}$. In particular, if $k \subset K$ are fields and V is a k-vector space, then $K \otimes_k V$ is a K-vector space.

The second application is the tensor product of two R-algebras. Let S and T be R-algebras. We allow them to be non-commutative (but the image of R should be in the center of each). We can $S \otimes_R T$ an R-module. We want to define multiplication

$$(S \otimes_R T) \otimes_R (S \otimes_R T) \to S \otimes_R T$$

(It is a map from the tensor product since multiplication needs to be bilinear and commutes with the R action, so that $S \otimes_R T$ is an R-algebra.) The way to define it is to define a multilinear map

$$(s_1, t_1, s_2, t_2) \mapsto (s_1 s_2) \otimes (t_1 t_2).$$

As an example, let $T = R[x]$. Then $S \otimes_R R[x] \cong S[x]$ as rings and as R-algebras. Applying this to $S = R[y]$, we get $R[x] \otimes_R R[y] \cong R[x, y]$. For a non-commutative example, $S \otimes \mathrm{Mat}_n(R) \cong \mathrm{Mat}_n(S)$.

A fun problem: Let $\mathbf{H}$ be the quaternion algebra over $\mathbf{R}$ with basis $1, i, j, k$. What is $\mathbf{H} \otimes_R \mathbf{H}$? Answer: $\mathrm{Mat}_4(\mathbf{R})$.

Note: if S and T are R-algebras (commutative), then $S \otimes_R T$ is a coproduct in the category of commutative R-algebras. In other words, there exists R-algebra maps $i_1 : S \to S \otimes_R T$ and $i_2 : T \to S \otimes_R T$, and given any $f_1 : S \to A$ and $f_2 : T \to A$, there exists a unique map $F : S \otimes_R T \to A$ such that $f_1 = F \circ i_1$ and $f_2 = F \circ i_2$. To prove this, the tensor product universal property gives the correct R-module map, but still need to check it is an R-algebar map. This requires A being commutative.

Exactness properties of tensor products.

Proposition 9.4. *If $M' \to M \to M'' \to 0$ is an exact sequence of R-modules and N is an R-module, then*

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$$

is exact.

Note $\otimes_R N$ is not exact on the left: an injection $M' \to M$ doesn't give an injection $M' \otimes_R N \to M \otimes_R N$. Tensor products preserves surjections but not injections.

Examples: If I is an ideal in R and M is an R-module, then $R/I \otimes_R M \cong M/IM$ as R/I-modules. The proof is to consider $I \to R \to R/I \to 0$. Tensoring by M to get

$$I \otimes_R M \to R \otimes_R M \to (R/I) \otimes_R M \to 0$$

The middle term is isomorphism to M. The left term is not necessarily IM, but its image in M is IM.

10. Lecture 10: 2023.10.5

Example 10.1. Let k be a field, and K a finite extension of k. We can form $K \otimes_k K$, which is a k-algebra. If K is a Galois extension over k, then $K \otimes_k K \cong K^d$ as rings where $d = [K : k]$. This is not a domain, but it is reduced. If we just assume that K/k is separable, then $K \otimes_k K$ is still a product of fields, so it is reduced. If K/k is not separable, then $K \otimes_k K$ may not be reduced.

Example 10.2. Let k be algebraically closed. If X and Y are closed algebraic sets of $\mathbf{A}^n_k$ and $\mathbf{A}^m_k$ defined by $I(X)$ and $I(Y)$, then it is easy to see that $X \times Y \subset \mathbf{A}^{m+n}_k$ is a closed algebraic subset.

If we denote the ring of $\mathbf{A}_k^n$ by $k[x_1, \cdots, x_n] = k[X]$, and similarly the ring of $\mathbf{A}_k^m$ by $k[y_1, \cdots, y_m] = k[Y]$, then the ring of $\mathbf{A}_k^{m+n}$ is $k[X, Y] = k[X] \otimes_k k[Y]$. The subset $X \times Y$ is then $V(I(X)k[X, Y] + I(Y)k[X, Y])$. The affine coordinate ring of $X \times Y$ is isomorphic to $A(X) \otimes_k A(Y)$.

It is also easy to see that if X and Y are irreducible, then $X \times Y$ is an irreducible subset of $\mathbf{A}_k^{m+n}$. This is saying that if $A(X)$ and $A(Y)$ are domains, then so is $A(X) \otimes_k A(Y)$. More generally, if R, S are any k-algebras, then R, S reduced implies $R \otimes_k S$ reduced; if R, S are domains, then $R \otimes_k S$ is a domain.

Suppose $R = A(Z)$, $S = A(X)$, $T = A(Y)$. Suppose S, T are R-algebras, i.e. there are maps $A(Z) \to A(X)$ and $A(Z) \to A(Y)$. This corresponds to morphisms (of algebraic sets) $f : X \to Z$ and $g : Y \to Z$. As sets, the *fiber product* $X \times_Z Y$ is by definition

$$\{(x, y) \in X \times Y \mid f(x) = g(y)\}$$

This comes with a morphism $h : X \times_Z Y \to Z$ by $h(x, y) = f(x) = g(y)$. This is called the fiber product for the following reason. Let $X_z = f^{-1}(z)$ and $Y_z = g^{-1}(z)$. Then $(X \times_Z Y)_z = X_z \times Y_z$.

The idea is that $A(X) \otimes_{A(Z)} A(Y)$ "is" the ring $A(X \times_Z Y)$. But in general this tensor product is not reduced. The general picture is that $\operatorname{Spec} S \times_{\operatorname{Spec} R} \operatorname{Spec} T = \operatorname{Spec}(S \otimes_R T)$.

Now we go back to the exactness properties of tensor products. We prove that $\otimes_R N$ is a right exact functor.

Proof. The situation is that

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

The first thing to check is that $g \otimes id$ is surjective. The tensor product $M'' \otimes_R N$ is generated by $m \otimes n$, and g is surjective, so $m = g(x)$ for some $x \in M$. Thus the image contains generators, so $g \otimes id$ is surjective.

We then check $\operatorname{Im}(f \otimes id) = \ker(g \otimes id)$. Certainly the composition is 0, so we just need to show $\ker(g \otimes id) \subset \operatorname{Im}(f \otimes id)$. Let $I = \operatorname{Im}(f \otimes id)$. Since I is contained in the kernel, we get a map $(M \otimes_R N)/I \to M'' \otimes N$. It suffices to show that this is an isomorphism. To do this, we need to find $h : M'' \otimes N \to (M \otimes_R N)/I$. Define

$$\widetilde{h} : M'' \times N \to (M \otimes_R N)/I$$
$$(m, n) \mapsto (\tilde{m} \otimes n) \bmod I$$

where $\tilde{m}$ is a lift of m, i.e. $g(\tilde{m}) = m$. This is well-defined, since any other choice of a lift of m is of the form $\tilde{m} + f(x)$ for some $x \in M'$ by the exactness of the original sequence, so the difference is $f(x) \otimes n$ which is in I. This is clearly R-bilinear, so we obtain the map h. Checking on pure tensors shows that h is the inverse.

■

The application we mentioned last time is $(R/I) \otimes_R M \cong M/IM$. As an example,

$$(\mathbf{Z}/n\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/m\mathbf{Z}) \cong (\mathbf{Z}/m\mathbf{Z})/(n\mathbf{Z}/m\mathbf{Z}) \cong \mathbf{Z}/d\mathbf{Z}$$

where $d = \gcd(m, n)$. Warning: $I \otimes_R M$ is not necessarily isomorphic to IM. It is only when $I \otimes_R M \to M$ is injective. An example of such failure is: $I = n\mathbf{Z} \cong \mathbf{Z}$ as $\mathbf{Z}$-modules. We have

$$0 \to I \to \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \to 0$$

Tensoring by $\mathbf{Z}/n\,\mathbf{Z}$, we get

$$n\,\mathbf{Z} \otimes \mathbf{Z}/n\,\mathbf{Z} \to \mathbf{Z}/n\,\mathbf{Z} \to (\mathbf{Z}/n\,\mathbf{Z}) \otimes_Z (\mathbf{Z}/n\,\mathbf{Z}) \to 0$$

but the first map is the zero map.

Note that $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}/n\,\mathbf{Z} = 0$ for any n. Question: what is $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Q}$?

Corollary 10.1. *If M, N are finitely generated R-modules, then so is $M \otimes_R N$.*

Proof. Tensor the surjection $R^k \to M$ by N to get a surjection $R^k \otimes_R N \to M \otimes_R N$. We know that $R^k \otimes_R N \cong N^k$ is finitely generated. ∎

Corollary 10.2. *If M is a finitely generated R-module and J is an ideal contained in the Jacobson radical of R, then so is $M \otimes_R (R/J) = 0$ implies $M = 0$. In particular, if R is local with maximal ideal $\mathfrak{m}$, and $k = R/\mathfrak{m}$, then $M \otimes_R k = 0$ implies $M = 0$.*

Proof. $M \otimes_R (R/J) \cong M/JM$, so it becomes the usual statement of Nakayama's lemma. ∎

Corollary 10.3. *Let R be local with maximal ideal $\mathfrak{m}$ and k be its residue field. Let M, N be finitely generated R-modules. Then $M \otimes_R N = 0$ implies $M = 0$ or $N = 0$.*

Proof. Suppose $N \neq 0$. Then the k-vector space $N/\mathfrak{m}N \neq 0$ by the previous corollary. Choose a surjection $N \to N/\mathfrak{m}N \to k \to 0$ and tensor with M. We get

$$M \otimes_R N \to M \otimes_R N/\mathfrak{m}N \to M \otimes_R k \to 0$$

Thus $M \otimes_R k = 0$, so the previous corollary implies $M = 0$. ∎

We switch gears to flatness.

Definition 10.4. An R-module M is flat if tensoring with M preserves injections. In other words, tensoring with M is exact.

A trivial example is that R is a flat R-module, since tensoring with R does nothing.

Example 10.3. $\oplus_\alpha N_\alpha$ is a flat R-module if and only if each N_α is flat. If $M' \to M$ is injection, then tensoring gives

$$\bigoplus_\alpha (M' \otimes_R N_\alpha) \to \bigoplus_\alpha (M \otimes_R N_\alpha)$$

which is injective if and only if it is injective on each factor. In particular, R^k is flat.

This also implies a projective module P is flat. This is because $P \oplus P' = F_R(A)$ for some free module $F_R(A)$, the free module is flat, so its direct summand P is flat. In summary, free implies projective implies flat. As an example, **Q** is a flat **Z**-module but not projective or free.

Definition 10.5. Let R be a domain. An R-module M is torsion free if whenever $rm = 0$, either $r = 0$ or $m = 0$.

If R is a domain, a flat R-module M is torsion free. This is because we can tensor the injection $0 \to R \xrightarrow{r} R$ by N.

If R is a PID, then flatness is equivalent to torsion free. This fails when R is not a PID. Consider $R = k[x, y]$ and $\mathfrak{m} = (x, y) \subset R$. This is torsion free but not flat.

11. Lecture 11: 2023.10.10

Proposition 11.1. *For an R-module N, the following are equivalent:*

(1) *N is flat*

(2) *for all finitely generated R-modules M' and all injections $M' \to M$, $M' \otimes_R N \to M \otimes_R N$ is injective*

(3) *for all ideals $I \subset R$, $I \otimes_R N \to N$ is injective.*

(4) *for all finitely generated ideals $I \subset R$, $I \otimes_R N \to N$ is injective.*

Proof. It is clear that 1 implies all the rest. The first step is to prove 2 implies 1. Assume 2. Suppose $M' \xrightarrow{f} M$ is an injection for arbitrary R-modules. Let $\sum m_i \otimes n_i$ be in the kernel of $f \otimes id_N$. We need to show that $\sum m_i \otimes n_i = 0$ in $M' \otimes_R N$. We want to find finitely generated modules $M_0' \subset M'$, $M_0 \subset M$ such that $m_i \in M_0'$ and $f(m_i) \in M_0$, together with a map $g : M_0' \to M_0$. Take M_0' to be the submodule generated by m_i's. We know that $M \otimes_R N$ is a quotient of the free module $F_R(M \times N)$ by some relations, so the formal sum

$$\sum (f(m_i), n_i)$$

is in the submodule generated in these relations. We can thus write $\sum (f(m_i), n_i)$ as a finite sum of the relations. Now let M_0 be the submodule of M generated by $f(m_i)$ and all the first coordinates of the relations used to express $\sum (f(m_i), n_i)$. This is finitely generated.

Therefore the restriction of f to M_0' maps into M_0, and $\sum f(m_i) \otimes n_i = 0$ since the relations used to make it 0 is in M_0. This means that $\sum m_i \otimes n_i$ is in the kernel of the restriction of f to M_0'. By assumption 2, we get that $\sum m_i \otimes n_i = 0$.

4 implies 3 is the same proof. It remains to show 3 implies 2.

Step 1: We claim that if S is a submodule of R^k, then $S \otimes_R N \to R^k \otimes_R N = N^k$ is injective. The proof is by induction on k. If $k = 1$, then S is an ideal of R, so the statement is by hypothesis. Assume this is true for $k - 1$. Then let S'' be the image of S under the projection $R^k \to R^{k-1}$. Let S' be the kernel. So we have the diagram

$$\begin{tikzcd}
0 \arrow[r] & S' \arrow[r] \arrow[d, hook] & S \arrow[r] \arrow[d, hook] & S'' \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & R \arrow[r] & R^k \arrow[r] & R^{k-1} \arrow[r] & 0
\end{tikzcd}$$

Tensoring with N, we get

$$\begin{tikzcd}
 & S' \otimes_R N \arrow[r] \arrow[d, hook] & S \otimes_R N \arrow[r] \arrow[d] & S'' \otimes_R N \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & N \arrow[r] & N^k \arrow[r] & N^{k-1} \arrow[r] & 0
\end{tikzcd}$$

where the left and right vertical arrows are injections by induction hypothesis and the base case. This implies the middle arrow is also injective by chasing the diagram.

Step 2: General case: Let M' be a submodule of M and M is finitely generated, so there is a surjection $R^k \to M$. Let S_0 be the kernel of $R^k \to M$. Let S be the preimage of M' in R^k. We obtain

$$\begin{tikzcd}
0 \arrow[r] & S_0 \arrow[r] \arrow[d] & S \arrow[r] \arrow[d, hook] & M' \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & S_0 \arrow[r] & R^k \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Tensoring by N, we see that the left and middle arrows remain injective, which then implies the right arrow is also injective.

■

Corollary 11.2. *If R is a PID and M is an R-module, then M flat if and only if M is torsion free.*

Proof. Assume M is torsion free. For any non-zero $I \subset R$, we know that $I = (a)$, so $I \cong R$ as R-modules. Then the map $I \otimes_R M \to M$ is identified with $R \otimes_R M \to M$ where the map is multiplication by a. Torsion-freeness impleis multiplication by a is injective, so we are done. ■

Theorem 11.3. *Let N be an R-module. The following are equivalent:*

(1) *N is flat*

(2) *for every $r_1, \cdots, r_k \in R$, $m_1, \cdots, m_k \in N$, if $\sum_i r_i m_i = 0$ in N, then there exists some $s_{ij} \in R$ and some $n_j \in N$ for $1 \leq i \leq k$ and $1 \leq j \leq \ell$, such that $\sum_i r_i s_{ij} = 0$ and $m_i = \sum_j s_{ij} n_j$. In other words, every relation in N is a consequence of a relation in R.*

Proof. Assume N is flat. Suppose $\sum_i r_i m_i = 0$. Then there is a map $R^k \to R$ by sending $(t_1, \cdots, t_k)$ to $\sum r_i t_i$. Let K be the kernel of this map. Tensoring everything with N, we get

$$0 \to K \otimes_R N \to N^k \to N \to 0$$

and the last map sends $(x_1, \cdots, x_n)$ to $\sum r_i x_i$. The hypothesis is that $\sum_i r_i m_i$ is in the image of $K \otimes_R N$. Therefore, there exists $\sigma_j \in K$ and $n_j \in N$ such that

$$\sum_j \sigma_j \otimes n_j \mapsto (m_1, \cdots, m_k)$$

Since $\sigma_j \in K$, we know that $\sigma_j = (s_{1j}, \cdots, s_{kj}) \in R^k$ such that $\sum_i r_i s_{ij} = 0$. Substituting this in, we get what we want.

Now assume 2 is true. To prove N is flat, we want to show $I \otimes_R N \to N$ is injective for all ideals I in R. An element in the kernel of this map is some element $\sum_i r_i \otimes m_i$ and $\sum_i r_i m_i = 0$ in N. The hypothesis provides n_j, s_{ij} such that $\sum_i r_i s_{ij} = 0$ and $m_i = \sum_j s_{ij} n_j$. Therefore

$$\sum_i r_i \otimes m_i = \sum_i r_i \otimes (\sum_j s_{ij} n_j) = \sum_j \sum_i (r_i s_{ij}) \otimes n_j = 0$$

■

Corollary 11.4. *Let R be a local ring. Let M be a finitely generated R-module. Then M is flat if and only if M is projective, if and only if M is free.*

Proof. We know that free implies projective implies flat. So assume M is flat. Let $\mathfrak{m}$ be the maximal ideal and k be the residue field. Then $M/\mathfrak{m}M = M \otimes_R k$ is finitely generated over k, so it is a finite dimensional vector space. Choose a basis $e_1, \cdots, e_n$, and choose lifts $m_1, \cdots, m_n \in M$. Then we get a map $f : R^n \to M$ given by $(r_1, \cdots, r_n) \mapsto \sum r_i m_i$, and the composition $R^n \to M \to M/\mathfrak{m}M$ is surjective. By Nakayama's lemma, this implies f is surjective. We get

$$0 \to K \to R^n \to M \to 0$$

We want to show $K = 0$, namely if $\sum_i r_i m_i = 0$ then $r_i = 0$ for all i. We will use induction to prove $\sum_{i=1}^k r_i m_i = 0$ then $r_i = 0$. For $k = 1$, if $r_1 m_1 = 0$, then by the previous theorem, we know that there exists $s_j \in R$ and $n_j \in M$ such that $r_1 s_j = 0$ and $m_1 = \sum_j s_j n_j$. Note that m_1 is not in $\mathfrak{m}M$ since it maps to $e_1 \neq 0$, so there exists some j such that $s_j \notin \mathfrak{m}$. This means s_j is a unit, so $r_1 s_j = 0$ implies $r_1 = 0$. The inductive step is similar. ■

Now we start the topic of localization.

Definition 11.5. Let R be any ring. S is a multiplicative subset of R if it contains 1, and if $s_1, s_2 \in S$ then $s_1 s_2 \in S$. Denote the localization by $S^{-1}R$.

12. Lecture 12: 2023.10.12

Example 12.1. Let p be a prime in $\mathbf{Z}$. Write $\mathbf{Z}_n$ for $\mathbf{Z}$ localized at $\{1, n, n^2, \cdots\}$ which is just $\mathbf{Z}[1/n]$. Note that for example $\mathbf{Z}[1/6] = \mathbf{Z}[1/72]$. Write $\mathbf{Z}_{(p)}$ for the localization of $\mathbf{Z}$ at the prime ideal (p).

Example 12.2. Let $R = k[x_1, \cdots, x_n]$ where k is algebraically closed. Let $f \in R$. The localization R_f is $k[x_1, \cdots, x_n, 1/f]$. Let $\mathfrak{m}$ be the maximal ideal $(x_1 - a_1, \cdots, x_n - a_n)$. Then $R - \mathfrak{m}$ is the set of functions that doesn't vanish at $a = (a_1, \cdots, a_n)$. The localization $R_{\mathfrak{m}}$ is then $\{f/g \mid g(a) \neq 0\}$, which is the set of rational functions defined on some open neighborhood of a.

Similarly, if $\mathfrak{p}$ is a prime ideal, then $V(\mathfrak{p})$ is an affine variety X. Then $R_{\mathfrak{p}}$ is the set

$$\{f/g \mid g \text{ is not identically } 0 \text{ on } X\}.$$

All rational functions defined at some point on X, i.e. defined on some open subset of X.

Example 12.3. Let R be any ring. The localization R_r can be thought of as $R[x]/(1 - xr)$. $R_r = \{0\}$ if and only if r is a nilpotent, equivalent to $1 - xr$ is a unit in $R[x]$.

Proposition 12.1. *Let S be a multiplicative subset of R. Let $f : R \to T$ be a ring homomorphism such that $f(S) \subseteq T^\times$. Then there exists a unique homomorphism $\widetilde{f} : S^{-1}R \to T$ of R-algebras.*

Proof. Define $\widetilde{f}(r/s) = f(r)f(s)^{-1}$. If $r_1/s_1 = r_2/s_2$, then there exists some $t \in S$ such that $ts_2 r_1 = ts_1 r_2$. Then $f(t)f(s_2)f(r_1) = f(t)f(s_1)f(r_2)$. Since $f(t)$ is a unit in T, we can cancel it and see that $\widetilde{f}$ is well-defined. ■

Corollary 12.2. *The only R-algebra automorphism on $S^{-1}R$ is the identity.*

An application: given $r_1, r_2 \in R$, we can localize twice $(R_{r_1})_{r_2}$, or $(R_{r_2})_{r_1}$, or just form $R_{r_1 r_2}$. These are all canonically isomorphic since they satisfy the same universal property.

Ideals in a localization.

Let $\phi : R \to S^{-1}R$ be the natural map. If I is an ideal in R, let $IS^{-1}R$ be the ideal in $S^{-1}R$ generated by the image of I. Then $IS^{-1}R = \{r/s \mid r \in I, s \in S\}$ because the right side is an ideal.

Proposition 12.3. *Let J be an ideal in $S^{-1}R$. Let $I = \phi^{-1}(J) \subseteq R$. Then $J = IS^{-1}R$.*

Proof. The inclusion $IS^{-1}R \subsetneq J$ is clear by definition. Now let $r/s \in J$. Then $s(r/s) \in J$, so $r/1 \in J$. This means $r \in I$ by definition of ϕ, so $r/s \in IS^{-1}R$ by the previous discussion. ■

Proposition 12.4. *Let $\mathfrak{p}$ be a prime ideal in R. If $\mathfrak{p} \cap S$ is not empty, then $\mathfrak{p}S^{-1}R = S^{-1}R$. If $\mathfrak{p} \cap S = \varnothing$, then $\mathfrak{p}S^{-1}R$ is a prime ideal in $S^{-1}R$, and $\phi^{-1}(\mathfrak{p}S^{-1}R) = \mathfrak{p}$. So there is a bijection between prime ideals in $S^{-1}R$ and prime ideals in R avoiding S.*

Proof. Assume $\mathfrak{p} \cap S = \varnothing$. Suppose $\phi(r) \in \mathfrak{p}S^{-1}R$. Then $r/1 = r'/s$ for some $r' \in \mathfrak{p}$. So $tsr = tr'$ for some $t \in S$. Thus $tsr \in \mathfrak{p}$, but $s, t \notin \mathfrak{p}$, so $r \in \mathfrak{p}$. This proves that $\phi^{-1}(\mathfrak{p}S^{-1}R) = \mathfrak{p}$. The same reasoning shows that $\mathfrak{p}S^{-1}R$ is a prime ideal.

On the other hand, if Q is a prime ideal in $S^{-1}R$, then $\phi^{-1}(Q)$ is a prime ideal in R. The previous proposition tells us that $Q = \phi^{-1}(Q)S^{-1}R$. This establishes the bijection. ■

Corollary 12.5. *R noetherian implies $S^{-1}R$ noetherian. R artinian implies $S^{-1}R$ artinian.*

Proof. Chain of ideals is preserved. ■

Corollary 12.6. *If $\mathfrak{p}$ is a prime ideal in R, then $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. The residue field is $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, which is also the field of fractions of $R/\mathfrak{p}$.*

Localization of Modules.

Let S be a multiplicative set of R and M be an R-module. Define $S^{-1}M$ to be fractions m/s for $s \in S$, and $m_1/s_1 = m_2/s_2$ if and only if there exists some $t \in s$ such that $t(m_1 s_2 - m_2 s_1) = 0$. The action $\frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}$ makes $S^{-1}M$ an $S^{-1}R$-module. There is a natural map $\phi : M \to S^{-1}M$. If $S = R - \mathfrak{p}$, denote by $M_{\mathfrak{p}}$ the localization.

Localization is functorial: if $f : M \to N$, there is a map $\widetilde{f} : S^{-1}M \to S^{-1}N$ by sending m/s to $f(m)/s$.

Given R, S, M, there are two ways of producing $S^{-1}R$-module. One is $S^{-1}M$, and the other is $(S^{-1}R) \otimes_R M$.

Lemma 12.7. *$S^{-1}M$ is functorially isomorphic to $(S^{-1}R) \otimes_R M$ as $S^{-1}R$-modules.*

Proof. On one hand, there is an R bilinear map

$$(r/s, m) \mapsto rm/s$$

On the other hand, we can define $S^{-1}M \to (S^{-1}R) \otimes_R M$ by sending $(m, s) \mapsto (1/s) \otimes m$. ■

Proposition 12.8. *$M \mapsto S^{-1}M$ is an exact functor.*

Proof. Suppose $M' \xrightarrow{g} M \xrightarrow{f} M''$ is exact. Consider $\widetilde{f}$ and $\widetilde{g}$. The clearly $\widetilde{g} \circ \widetilde{f} = 0$. Suppose $\widetilde{g}(m/s) = 0$. Then $g(m)/s = 0$, so there exists $t \in S$ such that $tg(m) = 0$. This means $g(tm) = 0$, so by exactness $tm = f(n)$ for some $n \in M'$. Thus $m/s = \widetilde{f}(n/ts)$. ■

Corollary 12.9. *$S^{-1}R$ is a flat R-module.*

Proof. Tensoring with $S^{-1}R$ is the same as localizing at S, which is exact. ■

For example, **Q** is a flat **Z**-module.

There are all sorts of properties. E.g.

(1) $S^{-1}(M_1 + M_2) = S^{-1}M_1 + S^{-1}M_2$

(2) $S^{-1}(M_1 \cap M_2) = S^{-1}M_1 \cap S^{-1}M_2$

(3) $S^{-1}(M/N) = S^{-1}N/S^{-1}M$

13. Lecture 13: 2023.10.19

We look into local properties of a ring R or a module M: a property P is said to be local if P holds for R if and only if P holds for $R_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$. (or all maximal ideal)

Proposition 13.1. *Let M be an R-module. Then $M = \{0\}$ if and only if $M_\mathfrak{p} = \{0\}$ for all prime ideals $\mathfrak{p}$ in R, if and only if $M_\mathfrak{m} = \{0\}$ for all maximal ideals $\mathfrak{m}$ in R.*

Proof. Suppose $M_\mathfrak{m} = \{0\}$ for all maximal ideals $\mathfrak{m}$ in R. Assume M is non-zero. Choose some $x \in M$ non-zero. Let I be the annihilator of m, i.e. $I = \{r \in R \mid rm = 0\}$. Since m is non-zero, we know $1 \notin I$, so I is a proper ideal. Then there exists a maximal ideal $\mathfrak{m}$ containing I. We know that $M_\mathfrak{m} = 0$, so there exists $s \notin \mathfrak{m}$ such that $sm = 0$. But $s \in I \subseteq \mathfrak{m}$, which is a contradiction. ■

Corollary 13.2. *Let M, N be R-modules. Let $f : M \to N$ be a homomorphism. Then f is injective if and only if for all prime ideals $\mathfrak{p}$ (or all maximal $\mathfrak{m}$), $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective. Surjectivity can also be checked locally this way. Same is true for isomorphism.*

Proof. Let $K = \ker f$, then there is an exact sequence $0 \to K \to M \to N$. Localizing we get $0 \to K_\mathfrak{p} \to M_\mathfrak{p} \to N_\mathfrak{p}$. Now whether K is zero can be checked locally. ■

A non-trivial fact is that

Proposition 13.3. *Let R be a ring and M an R-module. Then M is flat over R if and only if $M_\mathfrak{p}$ is flat over $R_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$, if and only if $M_\mathfrak{m}$ is flat over $R_\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$.*

We need some lemmas to prove the above proposition.

Lemma 13.4. *Let R be a ring and T an R-algebra. Let M_1 be an R-module and M_2 be a T-module (and hence an R-module). Then for all T-modules N, we have*

$$(M_1 \otimes_R M_2) \otimes_T N \cong M_1 \otimes_R (M_2 \otimes_T N)$$

Lemma 13.5. *Let R be a ring, T an R-algebra, and M an R-module. Then M is flat over R then $M \otimes_R T$ is flat over T.*

Proof. Let N be a T-module. Then

$$(M \otimes_R T) \otimes_T N \cong M \otimes_R (T \otimes_T N) \cong M \otimes_R N$$

If $N' \to N$ is an injection of T-modules, then tensoring with $M \otimes_R T$ we just get

$$M \otimes_R N' \to M \otimes_R N$$

This is injective since M is R-flat. ■

Lemma 13.6. *Let R be a ring and T an R-algebra. Let M_1, M_2 be R-modules. We have*

$$(M_1 \otimes_R M_2) \otimes_R T \cong (M_1 \otimes_R T) \otimes_T (M_2 \otimes_R T).$$

Proof. Omitted. ■

Proof of 13.3. If M is flat, then $M \otimes_R R_\mathfrak{p} = M_\mathfrak{p}$ is flat over $R_\mathfrak{p}$ by Lemma 13.5.

Now suppose $M_\mathfrak{m}$ is flat over $R_\mathfrak{m}$ for all maximal $\mathfrak{m}$. Let $N' \to N$ be an injection of R-modules. We know that $N'_\mathfrak{m} \to N_\mathfrak{m}$ is injective. By flatness of $M_\mathfrak{m}$, we get

$$N'_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \to N_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m}$$

is an injection. Using Lemma 13.6 with $T = R_\mathfrak{m}$, we see that

$$N_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \cong (M \otimes_R N) \otimes R_\mathfrak{m} = (M \otimes_R N)_\mathfrak{m}$$

So we get that $(N' \otimes_R M)_\mathfrak{m} \to (N \otimes_R M)_\mathfrak{m}$ is injective for all maximal ideal $\mathfrak{m}$, so then $N' \otimes_R M \to N \otimes_R M$ is an injection. ■

Note: Projective or finitely generated are not local properties.

Proposition 13.7. *Let M be an R-module. TFAE:*

(1) *M is projective and finitely generated.*

(2) *M is flat and finitely presented.*

(3) *M is finitely presented and locally free ($M_\mathfrak{m}$ is free over $R_\mathfrak{m}$ for all maximal ideal $\mathfrak{m}$).*

Some remarks: M finitely presented means that there is an exact sequence $R^n \to R^m \to M \to 0$, but it is not true that the first map can be made injective. If R is noetherian, finitely generated is equivalent to finitely presented. In the finitely presented case, projective = locally free = flat.

Proof. 1 to 2: We know that projective implies flat. If M is projective and finitely generated, then R is finitely presented (this is hw).

2 to 3: If M is flat and finite presented, then M is projective. We know that when M is finitely generated, projective implies locally free (we proved in a local ring, projective is same as free).

3 to 1: If M is finitely presented then M is finitely generated. We need to show that M is projective. Let $N \to N''$ be a surjection of R-module. We want to show $\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M, N'')$ is surjective. We check locally. So for every maximal ideal $\mathfrak{m}$, we want to check

$$\operatorname{Hom}_R(M, N) \otimes_R R_{\mathfrak{m}} \to \operatorname{Hom}_R(M, N'') \otimes_R R_{\mathfrak{m}}$$

is surjective. In the case where M is finitely presented and $R_{\mathfrak{m}}$ is flat over R, we have an isomorphism

$$\operatorname{Hom}_R(M, N) \otimes_R R_{\mathfrak{m}} \to \operatorname{Hom}_{R_{\mathfrak{m}}}(M \otimes_R R_{\mathfrak{m}}, N \otimes_R R_{\mathfrak{m}})$$

Now $M_{\mathfrak{m}}$ projective (it is free) implies

$$\operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, N_{\mathfrak{m}}) \to \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, N''_{\mathfrak{m}})$$

is surjective. So we are done. ■

Remark: in the case where M is finitely presented, localization commutes with Hom:

$$S^{-1} \operatorname{Hom}_R(M, N) \cong \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Stuff about sheaf and stalks. Skipping in notes.

14. Lecture 14: 2023.10.24

Theorem 14.1. *Suppose D_{f_α} is an open cover of $\operatorname{Spec} R$. Then*

$$0 \to R \to \prod_\alpha R_{f_\alpha} \to \prod_{\alpha,\beta} R_{f_\alpha f_\beta}$$

is exact. In particular $\mathcal{O}_{\operatorname{Spec} R}(\operatorname{Spec} R) = R$. Similarly, if M is an R-module, then same statement is true.

Proof. By quasi-compactness we assume this is a finite cover $D(f_1), \cdots, D(f_n)$. So $(f_1, \cdots, f_n)$ generates (1), and thus $(f_1^N, \cdots, f_n^N)$ generates 1 for any $N \geq 1$.

The desired exactness is the following: given $r_i \in R$ such that $r_i/1 = r_j/1$ in $R_{f_i f_j}$ for all i, j, then there exists a unique $r \in R$ such that $r/1 = r_i/1$ in R_{f_i} for all i.

Uniqueness: say $r \in R$ such that $r/1 = 0$ in R_{f_i} for all i. Then there exists f_i^N such that $f_i^N r = 0$ for all i. Then $r = r \cdot 1 = r(\sum_i a_i f_i^N) = 0$.

Existence: Suppose $h_i/f_i^N \in R_i$ (can assume the exponent is the same since there are finitely many of them) and h_i/f_i^N whose images in $R_{f_i f_j}$ are equal, i.e.

$$(f_i f_j)^{m_{ij}} f_j^N h_i = (f_i f_j)^{m_{ij}} f_i^N h_j$$

Choose $M \geq m_{ij} + N$ for all ij, then

$$f_j^M f_i^{M-N} h_i = f_i^M f_j^{M-N} h_j.$$

Let $H_i = f_i^{M-N} h_i$. Then

$$f_j^M H_i = f_i^M H_j$$

We have $1 = \sum_i a_i f_i^M$, so

$$f_j^M \sum_i a_i H_i = \sum_i a_i f_j^m H_i = \sum_i a_i f_i^M H_j = H_j$$

so $r = \sum_i a_i H_i$ has image $H_j / f_j^M = h_i / f_j^N$ in all R_{f_i}. ■

Definition 14.2. A Zariski local property of R or an R-module M is a property inherited by localizations, and holds for R (or M) if and only if there exists $f_1, \cdots, f_n$ that generates 1 and the property holds for all R_{f_i}.

Proposition 14.3. *Suppose M is an R-module, and $f_1, \cdots, f_n$ generates 1. TFAE:*

(1) $M = 0$

(2) $M_{f_1} = 0$ *for all i*

Proof. $M_{f_i} = 0$ for all i means that for all $m \in M$, there exists N such that $f_i^N m = 0$. Then $m = 1 \cdot m = \sum_i a_i f_i^N m = 0$. ■

Proposition 14.4. *Let R, M, f_i be as above. Then M is finitely generated (resp. finitely presented) if M_{f_i} are finitely generated (resp. finitely presented).*

Proof. Localization is exact (preserves surjection, etc.) so the forward direction is obvious.

Assume M_{f_i} is finitely generated for all f_i. Since there are finitely many M_{f_i}'s, there exists $m_1, \cdots, m_k \in M$ such that the images of m_i in M_{f_i} generate M_{f_i}. We claim these elements generate M. Let $R^k \to M$ be the map and let Q be the cokernel, so we get

$$R^k \to M \to Q \to 0$$

Localizing we get

$$R^k_{f_i} \to M_{f_i} \to Q_{f_i} \to 0$$

So $Q_{f_i} = 0$ for all i, which implies $Q = 0$.

Assume M_{f_i} is finitely presented for all f_i. So by the previous proof M is finitely generated. Let K be the kernel of the surjection $R^k \to M \to 0$. We want to show that K is finitely generated. By the previous paragraph we can check K_{f_i} is finitely generated. This is true by Schaneul's lemma in homework, since $0 \to K_{f_i} \to R^r_{f_i} \to M_{f_i} \to 0$ are exact sequences. ■

We change topic to integral homomorphisms. In number theory, this is relevant to algebraic integers. In algebraic geometry, this is connected to studying varieties by projecting onto linear spaces.

Definition 14.5. Let T be an R-algebra. Let $\overline{R}$ be the image of R in T. An element $t \in T$ is integral over R is there exists a monic polynomial $p(x) \in \overline{R}[x]$ such that $p(t) = 0$.

Proposition 14.6. *Keep the notation above. TFAE:*

(1) *t is integral over R*

(2) *$\overline{R}[t]$ is a finitely generated R-module*

(3) *there exists a R-subalgebra T_0 of T containing $\overline{R}$ and t which is a finitely generated R-module (or $\overline{R}$-module, same thing)*

(4) *there exists an $\overline{R}[t]$-module M which is finitely generated as an R-module and is a faithful $\overline{R}[t]$-module, i.e. if $\alpha m = 0$ for all m then $\alpha = 0$.*

Remark: if $p(x)$ is monic, then $R[x]/p(x)$ is a free R-module with basis $1, x, \cdots, x^{d-1}$ where $d = \deg p$.

Proof. 1 to 2 is obvious. 2 to 3: take $T_0 = \overline{R}[t]$. 3 to 4: take $M = T_0$. It contains $\overline{R}[t]$ and has 1, so it is faithful as an $\overline{R}[t]$-module.

4 to 1: look multiplication by t: $M \xrightarrow{t} M$. Then there exists monic $p(x)$ such that $p(t)M = 0$. This is true becuase: Suppose $m_1, \cdots, m_k$ generate M, and suppose $tm_i = \sum_j q_{ij} m_j$. Take $p(x)$ to be $\det(x - (q_{ij}))$. Now faithfulness of M implies $p(t) = 0$. ■

Corollary 14.7. *Notation as before. Then $t_1, \cdots, t_n$ all integral over R if and only if $\overline{R}[t_1, \cdots, t_n]$ is a finitely generated R-module.*

Proof. For the forward direction, use induction on n. The base case $n = 1$ is the equivalence 1 and 2 in the previous proposition. For the inductive step, assume $R[t_1, \cdots, t_{n-1}]$ is generated by $\alpha_1, \cdots, \alpha_d$ over R. If t_n is integral over R, then it is integral over $\overline{R}[t_1, \cdots, t_{n-1}]$, so $\overline{R}[t_1, \cdots, t_{n-1}, t_n]$ is a finitely generated $\overline{R}[t_1, \cdots, t_{n-1}]$, say by $\beta_1, \cdots, \beta_k$. Then $\{\alpha_i \beta_j\}$ generates $\overline{R}[t_1, \cdots, t_n]$ over R. ■

Corollary 14.8. *Integral elements of T form a subring of T containing $\overline{R}$, and hence an R-algebra.*

Definition 14.9.

(1) Integral elements of T is called the integral closure of R in T.

(2) If $f : R \to T$ is injective and T is integral over R, then T is called an integral extension.

(3) Say R is integrally closed in T if its integral closure is $\overline{R}$.

(4) If R is a domain, say R is integrally closed if it integrally closed in $\mathrm{Frac}(R)$.

Lemma 14.10. *Let $f : R \to T_1$ and $g : T_1 \to T_2$. If T_1 is integral over R and T_2 is integral over T_1, then T_2 is integral over R via $g \circ f$.*

Proof. Given $t \in T_2$, there exists a monic polynomial $p(x) \in \overline{T_1}[x]$ such that $p(t) = 0$. Write

$$p(x) = x^n + \overline{a_{n-1}} x^{n-1} + \cdots + \overline{a_0}$$

where $a_i \in T_1$. Now $\overline{R}[a_0, \cdots, a_{n-1}] \subset T_1$ is a finitely generated R-module since a_i are integral over R, and $\overline{R}[a_0, \cdots, a_{n-1}][t]$ is a finitely generated $\overline{R}[a_0, \cdots, a_{n-1}]$-module. Then $\overline{R[a_0, \cdots, a_{n-1}]}[t]$ is a finitely generated R-module, so t is integral over R. ■

Corollary 14.11. *The integral closure of R in T is integrally closed in T.*

Example 14.1.

(1) Let $R \subset R[x]$. The element x is not integral over R.

(2) If R is a UFD, then R is integrally closed. Proof: given $r/s \in \mathrm{Frac}(R)$ where $r \neq 0$ and $\gcd(r, s) = 1$, if $p(r/s) = 0$ for monic $p \in R[x]$, then

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_n s^n = 0$$

This implies s divides r, so s is a unit in R.

15. Lecture 15: 2023.10.26

Example 15.1.

(1) If R is a field and F is an extension, then F is integral over R if and only if F is algebraic over R.

(2) The integral closure of $\mathbf{Z}$ in $\mathbf{Q}(i)$ is $\mathbf{Z}[i]$, but the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{-3})$ is $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$. In general for d squarefree, the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{d})$ is

$$\begin{cases} Z[\sqrt{d}], & d \neq 1 \bmod 4 \\ Z[\frac{1+\sqrt{d}}{2}], & d = 1 \bmod 4 \end{cases}.$$

(3) Let k be a field. Then $y^2 - x^3$ is irreducible in $k[x, y]$ because it is monic and primitive. (Factors only if x^3 is a square, which it is not). This means $k[x, y]/(y^2 - x^3)$ is a domain. It is not integrally closed. Consider y/x which is not in R. We have

$$(y/x)^2 = y^2/x^2 = x^3/x^2 = x \in R$$

So y/x satisfies $t^2 - x = 0$, hence integral. In fact, there is an inclusion $R \hookrightarrow k[t]$ by setting $t^2 = x$ and $t^3 = t^2 \cdot t = x(y/x) = y$. The image of R is then $k[t^2, t^3]$. This is connected to the fact that $y^2 = x^3$ is not a "smooth curve".

Proposition 15.1. *Let T be an R-algebra. Let S be a multiplicative subset of R. The image of S in T is still a multiplicative set, which we still call S. Then*

(1) *for $t \in T$ and $s \in S$, $t/s \in S^{-1}T$ is integral over $S^{-1}R$ if and only if there exists some $v \in S$ such that vt is integral over R.*

(2) *if T is integral over R, then $S^{-1}T$ is integral over $S^{-1}R$.*

(3) *the integral closure of $S^{-1}R$ in $S^{-1}T$ is the integral closure of R in T localized by S.*

"Taking integral closure is compatible with localization, and localization preserves integrality." Also, 1 trivially implies 2 and 3.

Proof. We prove 1. Let $t/s \in S^{-1}T$. If vt is integral over R, then

$$(vt)^n + \cdots + a_1(vt) + a_0 = 0$$

Multiplying by $(vs)^{-n}$, we get

$$(t/s)^n + \cdots + a_0(vs)^{-n} = 0.$$

This is a monic polynomial with coefficients in $S^{-1}R$, so t/s is integral over $S^{-1}R$.

Conversely, suppose t/s is integral over $S^{-1}R$. Then

$$(t/s)^n + (b_{n-1}/w_{n-1})(t/s)^{n-1} + \cdots + b_0/w_0 = 0$$

Multiply through by $s^n w_0 \cdots w_{n-1}$, we see that

$$t^n + sb_1' t^{n-1} + \cdots + s^n b_0' = 0$$

in $S^{-1}T$ (not in T!). But this means there exists some $v \in S$ such that

$$v(t^n + sb_1' t^{n-1} + \cdots + s^n b_0') = 0$$

in T. Multiplying by v^{n-1} gives the desired equation. ■

Proposition 15.2. *If R is a domain, the following are equivalent:*

(1) *R is integrally closed*

(2) *for all prime ideals $\mathfrak{p}$, $R_\mathfrak{p}$ is integrally closed*

(3) *for all maximal ideals $\mathfrak{m}$, $R_\mathfrak{m}$ is integrally closed.*

Being integrally closed is a local property.

Proof. Let $\widetilde{R}$ be the integral closure of R in K, the field of fractions. Then $R = \widetilde{R}$ if and only if for all $\mathfrak{p}$ prime, $R_\mathfrak{p} = \widetilde{R}_\mathfrak{p} = \widetilde{R_\mathfrak{p}}$, where the last equality is by the previous proposition. ■

We consider situations of interest in number theory. Let R be a domain, K its field of fractions, and F an extension of K.

Lemma 15.3. *If F/K is algebraic, then for all $\alpha \in F$, there exists $r \in R$ non-zero such that $r\alpha$ is integral over R.*

Proof. Clear denominators. ■

Proposition 15.4. *Let R be integrally closed. Let $\alpha \in F$ be algebraic over K. Then α is integral over R if and only if the minimal polynomials of α actually lies in $R[x]$.*

Proof. Backwards is obvious. For the forward direction, first assume that $K(\alpha)$ is separable over K, which means that if $d = [K(\alpha) : K]$, then there exists $\sigma_1, \cdots, \sigma_d$ distinct embeddings of $K(\alpha)$ into $\overline{K}$ (i.e. the minimal polynomial of α has d distinct roots). Then the minimal polynomials of α is

$$\prod_{i=1}^{d} (x - \sigma_i(\alpha)).$$

Thus the coefficients of this polynomials are symmetric functions in $\sigma_i(\alpha)$. Since α is integral over R, there exists $p(x) \in R[x]$ such that $p(\alpha) = 0$. Applying σ_i, we get $p(\sigma_i(\alpha)) = 0$ too. So $\sigma_i(\alpha)$ are all integral, so the symmetric functions are also integral over R. Because R is integrally closed, the coefficients are in R.

If $K(\alpha)$ is not separable over K, then coefficients of $\prod_{i=1}^{d}(x - \sigma_i(\alpha))$ lies in some purely inseparable extensions. Taking the product to some p^N solves the problem. ■

Example 15.2. Let $R = \mathbf{Z}$, $K = \mathbf{Q}$, and $F = \mathbf{Q}(\sqrt{d})$. If $\alpha = a + b\sqrt{d}$, then the minimal polynomial of α is $x^2 - 2ax + a^2 - db^2$.

Proposition 15.5. *Let R be integrally closed. Suppose F/K is a finite separable extension. Let $\widetilde{R}_F$ be the integral closure of R in F. Then there exists $\alpha_1, \cdots, \alpha_d \in F$ a basis of F over K such that $\widetilde{R}_F \subseteq R\alpha_1 + \cdots + R\alpha_d$. In other words, $\widetilde{R}_F$ is contained in a finitely generated free R-submodule of F.*

In particular, if R is noetherian, then $\widetilde{R}_F$ is a finitely generated R-submodule of F.

Example 15.3. Let $R = \mathbf{Z}$, $K = \mathbf{Q}$. The ring of integers $\mathcal{O}_F$ is a free $\mathbf{Z}$-module of rank $d = [F : \mathbf{Q}]$. (torsion free, $\mathbf{Z}$ is PID, so free).

Proof. If $\alpha \in F$, multiplication by α is a linear map $F \to F$, so it has a trace $\mathrm{tr}(\alpha)$. Trace is K-linear, and $\mathrm{tr}(1) = d$. If the characteristic of K doesn't divide d then $\mathrm{tr}(1) \neq 0$. The separability hypothesis guarantees that tr is not identically zero, so the bilinear form

$$\langle \alpha, \beta \rangle = \mathrm{tr}(\alpha\beta)$$

is non-degenerate, so it identifies F with its dual as K-vector spaces.

Let $\sigma_1, \cdots, \sigma_d$ be distinct embeddings $F(\alpha) \to \overline{K}$, then $\mathrm{tr}(\alpha) = \sum_i \sigma_i(\alpha)$. In particular, if α is integral over R, then $\mathrm{tr}(\alpha)$ is integral over R and is also in K. Since R is integrally closed, $\mathrm{tr}(\alpha) \in R$.

Now let $\beta_1, \cdots, \beta_d$ be a K-basis of F. After clearing denominators, we can assume $\beta_1, \cdots, \beta_d$ are integral over R, i.e. in $\widetilde{R}_F$. Let $\alpha_1, \cdots, \alpha_d$ be the dual basis under the trace, i.e. $\mathrm{tr}(\alpha_i\beta_j) = \delta_{ij}$.

Suppose $\gamma = \sum_i c_j\alpha_j$ with $c_j \in K$ and γ is integral over R. Then

$$\mathrm{tr}(\gamma\beta_i) = c_i$$

Since $\gamma, \beta_i \in \widetilde{R}_F$, we have $\gamma\beta_i \in \widetilde{R}_F$, so $\mathrm{tr}(\gamma\beta_i) \in R$. This means $\gamma \in \sum_i R\alpha_i$. ■

We start the going up theorem.

Theorem 15.6 (Going up). *Suppose $R \subset S$ are rings, and S is integral over R. Let $\mathfrak{p}$ be a prime ideal of R. The going up theorem says that there exists a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q} \cap R = \mathfrak{p}$. (i.e. $\operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.) Also, if $\mathfrak{q}_1, \mathfrak{q}_2$ are prime ideals of S, $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$, then $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Corollary 15.7. *Suppose $\mathfrak{p}_1 \subset \mathfrak{p}_2$ are prime ideals in R, $\mathfrak{q}$ is a prime ideal in S and $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Then there exists a prime ideal $\mathfrak{q}_2$ in S such that $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$ and $\mathfrak{q}_1 \subset \mathfrak{q}_2$.*

Proof. Applying going up to $R/\mathfrak{p}_1 \subset S/\mathfrak{q}_1$ and the prime ideals $\mathfrak{p}_2/\mathfrak{p}_1$. ■

Lemma 15.8. *Let $R \subset S$ be domains and S is integral over R. Then R is a field if and only if S is a field.*

Proof. Assume R is a field. Let $s \in S$ be non-zero. The subring $R[s]$ is a domain, and it is a finitely generated R-module. Since R is a field, this is a finite dimensional vector space. A domain that is finite dimensional vector space is a field, so $R[s]$ is a field.

Assume S is a field. Take $r \in R$ non-zero. Then $r^{-1} \in S$ is integral over R, so there is an equation

$$r^{-n} + \cdots + a_0 = 0$$

with $a_i \in R$. Multiplying by r^{n-1}, we get that r^{-1} is a polynomial in r with R coefficients, so $r^{-1} \in R$. ■

Lemma 15.9. *Let $R \subset S$ be rings and S integral over R. Let $\mathfrak{q}$ be a prime ideal in S and $\mathfrak{p} = \mathfrak{q} \cap R$. Then $\mathfrak{p}$ is a maximal ideal in R if and only if $\mathfrak{q}$ is maximal in S.*

Proof. Look at the induced map $R/\mathfrak{p} \to S/\mathfrak{q}$ which is injective since $\mathfrak{p} = \mathfrak{q} \cap R$. These are both domains, and $R/\mathfrak{p} \to S/\mathfrak{q}$ is an integral extension by just writing down the equation and mod $\mathfrak{p}$. Then we are done by the previous lemma. ■

16. Lecture 16: 2023.10.31

Lemma 16.1. *Let $R \subset S$ be rings and S integral over R. If $\mathfrak{q}_1, \mathfrak{q}_2$ are prime ideals of S, $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$, then $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. Let $\mathfrak{p} = \mathfrak{q}_i \cap R$ be the same intersection. Then $R - \mathfrak{p}$ is a multiplicative subset of both R and S. Localization preserves inclusion and intersection of submodules, so we have $R_\mathfrak{p} \subset S_\mathfrak{p} = (R - \mathfrak{p})^{-1}S$. The local ring $R_\mathfrak{p}$ has a unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$. Also,

$$\mathfrak{q}_i S_\mathfrak{p} \cap R_\mathfrak{p} = (\mathfrak{q}_i \cap R)_\mathfrak{p} = \mathfrak{p}_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}.$$

This means $\mathfrak{q}_i S_\mathfrak{p}$ are maximal ideals in $S_\mathfrak{p}$ by Lemma 15.9 and the fact that localization preserves integrality. Now $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ implies $\mathfrak{q}_1 S_\mathfrak{p} = \mathfrak{q}_2 S_\mathfrak{p}$ since they are maximal ideals. We also know that

$$(R - \mathfrak{p}) \cap \mathfrak{q}_i \subseteq (R \cap \mathfrak{q}_i) \cap (R - \mathfrak{p}) = \mathfrak{p} \cap (R - \mathfrak{p}) = \varnothing.$$

So $\mathfrak{q}_1 S_\mathfrak{p} = \mathfrak{q}_2 S_\mathfrak{p}$ are prime ideals in $S_\mathfrak{p}$ that corresponds to both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ under the bijection between prime ideals in $S_\mathfrak{p}$ and prime ideals in S that avoids $R - \mathfrak{p}$, so we must have $\mathfrak{q}_1 = \mathfrak{q}_2$. ■

Proof of the going up theorem. Start with R, S an integral ring extension and $\mathfrak{p}$ a prime ideal in R. As before, we have $R_\mathfrak{p} \subseteq S_\mathfrak{p} = (R - \mathfrak{p})^{-1}S$ which is still an integral extension. Choose a maximal ideal $\mathfrak{m}$ in $S_\mathfrak{p}$. Consider $\mathfrak{m} \cap R_\mathfrak{p}$. Lemma 15.9 implies that this is a maximal ideal in $R_\mathfrak{p}$. The ring $R_\mathfrak{p}$ is local, so we must have

$$\mathfrak{m} \cap R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}.$$

Let $\mathfrak{q} = i_S^{-1}(\mathfrak{m})$ where $i_S : S \to S_\mathfrak{p}$. We have the commutative diagram

$$\begin{tikzcd}
R_\mathfrak{p} \arrow[r, "j_\mathfrak{p}"] & S_\mathfrak{p} \\
R \arrow[u, "i_R"] \arrow[r, "j"] & S \arrow[u, "i_S"']
\end{tikzcd}$$

So $\mathfrak{q} \cap R = j^{-1}(i_S^{-1}(\mathfrak{m})) = i_R^{-1} j_\mathfrak{p}^{-1}(\mathfrak{m}) = i_R^{-1}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}$. ■

What does the going up theorem mean?

(1) For an integral ring extension S over R, the affine scheme map $\operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.

(2) Suppose $f : R \to S$ is just an integral homomorphism and let I be the kernel of f. Then R/I is a subring of S. Then $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ factors as

$$\operatorname{Spec} S \to \operatorname{Spec} R/I \to \operatorname{Spec} R$$

The first step is surjective and the second step is a closed immersion.

(3) If $f : R \to S$ an integral homomorphism, then f^* is a closed map: if $Z \subset \operatorname{Spec} S$ is closed, then $f^*(Z)$ is closed in $\operatorname{Spec} R$.

(4) If $f : R \to S$ an integral homomorphism and S is a finitely generated R-algebra (so by integrality S is a finite R module), then $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ has finite fibers.

Geometrically, if $g : X \to Y$ is a map of affine algebraic sets over k which corresponds to a k-algebra homomorphism $f : A(Y) \to A(X)$, then f being integral implies that g is a closed map, and g has finite fibers.

Dimension in rings.

Let R be any ring. A chain in R is a sequence of strictly increasing prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k$$

Note that the index starts at 0 and ends at k, and k is called the length of the chain.

Definition 16.2. The Krull dimension of a ring R is the maximal length of chains in R. It is denoted by $\dim R$.

The Krull dimension could be infinity, even in noetherian rings.

Example 16.1.

(1) If R is a domain then (0) is a prime ideal. Thus, $\dim R = 0$ if and only if R is a field.

(2) If R is a PID that is not a field, then every non-zero prime ideal is maximal. So every maximal chain looks like

$$(0) \subsetneq \mathfrak{p}$$

which has length 1. So the dimension of PIDs is 1.

(3) Let $R = k[x, y]$ where k is algebraically closed. We proved in homework that the prime ideals are (0), (f) for f irreducible, or $\mathfrak{m} = (x - a, x - b)$. Therefore a maximal chain looks like

$$(0) \subsetneq (f) \subsetneq \mathfrak{m}$$

Therefore $\dim k[x, y] = 2$.

(4) In $k[x_1, \cdots, x_n]$, we have a chain

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \cdots, x_n)$$

Later we will prove that this is a maximal chain.

If follows from the going up theorem that

Corollary 16.3. *If $R \subset S$ is an integral extension, then* $\dim R = \dim S$.

Proof. Given a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k$$

in R, the going up theorem implies that it can be lifted to a chain

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

where $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. Therefore $\dim S \geq \dim R$. On the other hand, given a chain

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

in S, we can let $\mathfrak{p}_i = \mathfrak{q}_i \cap R$. The second state of going up implies $\mathfrak{q}_i \neq \mathfrak{q}_{i+1}$ for any i. Therefore we get a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k$$

in R. So $\dim R \geq \dim S$. Hence they are equal. ■

There is also the going down theorem.

Theorem 16.4 (Going down). *Let $R \subset S$ be an integral extension. Assume also that R, S are domains and R is integrally closed (in its field of fractions). Suppose $\mathfrak{p}_2 \subset \mathfrak{p}_1$ are prime ideals in R, and $\mathfrak{q}_1$ is a prime ideal in S such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Then there exists a prime ideal $\mathfrak{q}_2 \in S$ such that $\mathfrak{q}_2 \subset \mathfrak{q}_1$ and $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$.*

We will not prove it.

Definition 16.5. If $\mathfrak{p}$ is a prime ideal in R, the height of $\mathfrak{p}$ is the maximal length of a chain that ends at $\mathfrak{p}$. We denote it by $\operatorname{ht}\mathfrak{p}$. The coheight of $\mathfrak{p}$ is the maximal length of a chain that starts at $\mathfrak{p}$. This is sometimes denoted by $\dim \mathfrak{p}$.

We easily see that the height is $\dim R_{\mathfrak{p}}$, and the coheight is $\dim R/\mathfrak{p}$. From the definitions, $\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p}$ is the max length of chains that contain $\mathfrak{p}$. In particular,

$$\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p} = \dim R.$$

If I is an arbitrary ideal in R, we define

$$\operatorname{ht} I = \min\{\operatorname{ht}\mathfrak{p} \mid I \subset \mathfrak{p}\}$$

and

$$\operatorname{coht} I = \max\{\operatorname{coht}\mathfrak{p} \mid I \subset \mathfrak{p}\}$$

The going up theorem says that if $R \subset S$ is an integral extension, $\mathfrak{q} \in \operatorname{Spec} S$ and $\mathfrak{p} = \mathfrak{q} \cap S$, then $\operatorname{ht}\mathfrak{q} \leq \operatorname{ht}\mathfrak{p}$ and $\operatorname{coht}\mathfrak{p} = \operatorname{coht}\mathfrak{q}$.

We move on to the topic of Noether normalization theorem. We need some field theory first. Let K/k be a field extension. We say elements $\alpha_1, \cdots, \alpha_n \in K$ are algebraically independent over k if the evaluation map $k[x_1, \cdots, x_n] \to K$ is injective. This means $k(x_1, \cdots, x_n)$ embeds into K.

Definition 16.6. A transcendence basis of K/k is a set of algebraically independent elements

$$\alpha_1, \cdots, \alpha_n \in K$$

such that K is algebraic over $k(\alpha_1, \cdots, \alpha_n)$.

Fact: these always exists if suitably defined (i.e. maybe you need infinitely many of them), and the number of these is independent of the choice of $\alpha_1, \cdots, \alpha_n$. Then n is the transcendence degree of K/k.

Suppose R is a k-algebra that is also a domain. We then think of R as a subring of K, its field of fractions, and K/k is an field extension. We say elements in R are algebraically independent over k if they are when considered in K.

Theorem 16.7 (Noether normalization)**.** *Let k be a field and $R = [x_1, \cdots, x_N]/\mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal in $k[x_1, \cdots, x_N]$ (i.e. R is a finitely generated domain over k). Then there exists $\alpha_1, \cdots, \alpha_d$ in R which are algebraically independent over k such that R is an integral extension of the ring $k[\alpha_1, \cdots, \alpha_d]$.*

We will only prove this if k is infinite (e.g. k is algebraically closed). In this case, α_i are the images of linear combinations of x_i's with coefficients in k. In fact,"almost all" linear combinations will work.

What is a geometric interpretation of Noether normalization? Suppose $k = \overline{k}$. A ring R as in the theorem corresponds to $X \subset \mathbf{A}_k^N$, and there is a linear projection $\mathbf{A}_k^N \to \mathbf{A}_k^d$. This gives a map $X \to \mathbf{A}_k^d$ that is surjective with finite fibers. We say X is a "finite branch cover" of $\mathbf{A}_k^d$.

As a special case, let $f \in k[x, y]$ and $X = V(f)$. After choosing coordinates correctly, $X \to \mathbf{A}_k^1$ is a cover. For example, let $X = V(xy - 1)$ be a hyperbola. If we just project to the x-axis then the image doesn't contain 0, so this is an incorrect way of projecting. In fact, if we look at

$$k[x] \hookrightarrow k[x, y]/(xy - 1) = k[x, x^{-1}]$$

then this is not an integral extension. However, projecting to almost all other lines will work (not the y-axis).

17. Lecture 17: 2023.11.2

Proof of Noether Normalization. Assume $R = k[\alpha_1, \cdots, \alpha_N]$ where $\alpha_1, \cdots, \alpha_N$ are generators (not the final answers!). The proof is by induction on N the number of generators. The base case $N = 0$ is trivial.

Assume now the statement is true for all k-algebras that can be generated by $N-1$ elements. Again let $R = k[\alpha_1, \cdots, \alpha_N]$. If $\alpha_1, \cdots, \alpha_N$ are algebraically independent, then we are simply done. So assume $\alpha_1, \cdots, \alpha_N$ are not algebraically independent. We claim that there exists $N-1$ linear combinations α_i' of α_i's such that $R = k[\alpha_1', \cdots, \alpha_{N-1}', \alpha_N]$, and α_N is integral over $k[\alpha_1', \cdots, \alpha_{N-1}']$. If so, the inductive hypothesis implies there exists $\beta_1, \cdots, \beta_d$ algebraically independent in $k[\alpha_1', \cdots, \alpha_{N-1}']$. Then we have the tower of integral extensions

$$k[\beta_1, \cdots, \beta_d] \subset k[\alpha_1', \cdots, \alpha_{N-1}'] \subset k[\alpha_1', \cdots, \alpha_{N-1}'][\alpha_N]$$

which implies R is integral over $k[\beta_1, \cdots, \beta_d]$.

So now we prove the claim. Let P be a non-zero polynomial such that $P(\alpha_1, \cdots, \alpha_N) = 0$. Write

$$P = \sum_{\nu=0}^{D} P_\nu$$

where P_ν is the degree ν homogenous part of P, and $P_D \neq 0$. Because k is infinite(!), there exists $\lambda_1, \cdots, \lambda_N \in k$ such that $P_D(\lambda_1, \cdots, \lambda_N) \neq 0$. This implies the polynomial $P(\lambda_1, \cdots, \lambda_{N-1}, t)$ in t is not identically 0. Therefore we may choose $\lambda_N \neq 0$ such that $P_D(\lambda_1, \cdots, \lambda_N) \neq 0$. Since

P_D is homogenous, we may assume $\lambda_N = 1$ by just dividing through. Set $\alpha_i' = \alpha_i - \lambda_i \alpha_N$ for $1 \leq i \leq N-1$. Then of course

$$k[\alpha_1, \cdots, \alpha_N] = k[\alpha_1', \cdots, \alpha_{N-1}', \alpha_N]$$

since $\alpha_i = \alpha_i' + \lambda_i \alpha_N$. Plugging back in P_D, we get

$$P_D(\alpha_1, \cdots, \alpha_N) = P_D(\alpha_1' + \lambda_1 \alpha_N, \cdots, \alpha_{N-1}' + \lambda_{N-1}\alpha_N, \alpha_N)$$

The monomial of α_N^D must be $P_D(\lambda_1, \cdots, \lambda_{N-1}, 1)\alpha_N^D$. The assumption was that $P_D(\lambda_1, \cdots, \lambda_{N-1}, 1)$ is non-zero in k, so after dividing by it we obtain a monic polynomial in α_N of degree d with coefficients in $k[\alpha_1', \cdots, \alpha_{N-1}']$. This shows α_N is integral over $k[\alpha_1', \cdots, \alpha_{N-1}']$, and we are done. ■

What happens if k is finite? We can still use induction, but instead of $\alpha_i' = \alpha_i - \lambda_i \alpha_N$, we use $\alpha_i' = \alpha_i + \alpha_N^{D_i}$ for some large power. So the β's won't be linear combinations.

Corollary 17.1. *Let K be a field extension over k which is a finitely generated k-algebra. Then K is a finite extension.*

Proof. Apply Noether normalization. There exists a subring $k[\alpha_1, \cdots, \alpha_d]$ where α_i's are algebraically independent such that K is integral over $k[\alpha_1, \cdots, \alpha_d]$. But by going up, $k[\alpha_1, \cdots, \alpha_d]$ is a field since K is integral over it. Thus $d = 0$, so K is integral over k, or equivalently algebraic over k. Now finite generatedness of K implies K is finite over k. ■

Corollary 17.2. *Let k be algebraically closed and K be a finitely generated extension over k. Then $K = k$.*

Proof. Follows trivially from the previous corollary. ■

Corollary 17.3. *Let k be algebraically closed and R be a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal in R. Then the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism.*

Corollary 17.4 (Nullstellensatz)**.** *Let k be algebraically closed. If $\mathfrak{m}$ is a maximal ideal in the polynomial ring $k[x_1, \cdots, x_n]$, then $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$ for some $a_1, \cdots, a_n \in k$.*

Proof. Consider $k \to k[x_1, \cdots, x_n]/\mathfrak{m}$, which is an isomorphism. So for all i, there exists $a_i \in k$ such that $x_i = a_i \bmod \mathfrak{m}$. So $x_i - a_i \in \mathfrak{m}$ for all i, so $\mathfrak{m}$ contains $(x_1 - a_1, \cdots, x_n - a_n)$, but the latter is obviously maximal (e.g. because it is the kernel of the evaluation map at $(a_1, \cdots, a_n)$). ■

When k is not algebraically closed, let $I \subseteq k[x_1, \cdots, x_n]$ be any ideal. Then I is not the unit ideal if and only if there exists $a_1, \cdots, a_n \in \overline{k}$ such that $f(a_1, \cdots, a_n) = 0$ for all $f \in I$.

Theorem 17.5 (Nullstellensatz)**.** *Let k be algebraically closed and let I be an ideal in $k[x_1, \cdots, x_n]$. Then $f(a) = 0$ for all $a \in V(I)$ if and only if there exists N such that $f^N \in I$ (i.e. $f \in \sqrt{I}$). Namely, $I(V(I)) = \sqrt{I}$.*

Proof. Suppose f^N is not in I for any N. Consider the localization

$$k[x_1, \cdots, x_n]_f = k[x_1, \cdots, x_n, 1/f]$$

which is a finitely generated k-algebra. Since $f^N \notin I$ for all N, we know that I_f is not the unit ideal. Choose a maximal ideal $\mathfrak{M}$ in $k[x_1, \cdots, x_n]_f$ containing I_f. Now $\mathfrak{m} = \mathfrak{M} \cap k[x_1, \cdots, x_n]$ contains I and is a prime ideal. Now

$$k \to k[x_1, \cdots, x_n]/\mathfrak{m} \hookrightarrow k[x_1, \cdots, x_n]_f/\mathfrak{M} \cong k$$

where the last isomorphism is by the previous corollary. The ring $k[x_1, \cdots, x_n]/\mathfrak{m}$ is captures in the sequence of injections that composes to an isomorphism, so it must also be k, which means $\mathfrak{m}$ is a maximal ideal. We then get $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$ for some $a_1, \cdots, a_n \in k$. The fact that $I \subset \mathfrak{m}$ means $(a_1, \cdots, a_n)$ is in $V(I)$. We know that $f \notin \mathfrak{M}$, so $f \notin \mathfrak{m}$, which means $f(a) \neq 0$. This finishes the proof. ■

Some related results:

(1) Finiteness of integral closure. Suppose R is a domain and K is its field of fractions. Let $\widetilde{R}$ be the integral closure of R. In general, little can be said about $\widetilde{R}$ even when R is noetherian. Akizuki showed that there exists R noetherian such that $\widetilde{R}$ is not noetherian, and in particular not a finitely generated R-module. But

Theorem 17.6 (Noether)**.** *Let R be a domain which is a finitely generated algebra over k. If K is the field of fractions of R and L is a finite extension of K, then the integral closure $\widetilde{R}_L$ in L is a finitely generated R-module. In particular $\widetilde{R}$ is a finitely generated R-module.*

Geometrically, if $k = \overline{k}$ and X is an affine algebraic variety over k, then the coordinate ring $A(X)$ is a domain that is a finitely generated k-algebra. The integral closure $\widetilde{A(X)}$ corresponds to another variety $\widetilde{X}$, and we have an integral morphism $\widetilde{X} \to X$. This is called the normalization. The map $\pi : \widetilde{X} \to X$ has finite fibers, and is also birational: there is a non-empty open subset U of X such that $\pi^{-1}(U) \to U$ is an isomorphism. As an example, $k[x, y]/(y^2 - x^3)$ is a cusp $X = V(y^2 - x^3)$ in the plane, and it injects into $k[t]$ by mapping y to t^3 and x to t^2. This corresponds to the parametrization $\mathbf{A}^1_k \to X$ given by $t \mapsto (t^2, t^3)$.

(2) Generalization of Noether normalization. Let k be a field and R be a domain that is finitely generated over k. Suppose there exists a sequence of ideals

$$I_0 \subset \cdots \subset I_k \subsetneq R$$

Then there exists $\alpha_1, \cdots, \alpha_d \in R$ algebraically independent over k and a non-decreasing sequence of integers $0 \leq h_0 \leq h_k$ such that R is integral over $k[\alpha_1, \cdots, \alpha_d]$ and for all i, $k[\alpha_1, \cdots, \alpha_d] \cap I_i = (\alpha_1, \cdots, \alpha_{h_i})$.

What does this mean? In $k[x_1, \cdots, x_d]$, there is a standard filtration $(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \cdots, x_d)$. This statement says in finitely generated domain over k this is somewhat true.

Corollary 17.7. $\dim k[x_1, \cdots, x_n] = n$. $\mathrm{ht}(x_1, \cdots, x_i) = i$, *and* $\mathrm{coht}(x_1, \cdots, x_i) = n - i$.

Proof. We know a chain of lenght n, so we just need to show the opposite. Given a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k,$$

we apply the above result, so we obtain an integral extension $k[\alpha_1, \cdots, \alpha_d] \subset k[x_1, \cdots, x_n]$ where $\alpha_1, \cdots, \alpha_d$ are algebraically independent, and $\mathfrak{p}_i \cap k[\alpha_1, \cdots, \alpha_d]$ is equal to $(\alpha_1, \cdots, \alpha_{h_i})$.

First of all $d = n$ because $\alpha_1, \cdots, \alpha_d$ is a transcendence basis. Moreover, by going up, we know that $\mathfrak{p}_i \cap k[\alpha_1, \cdots, \alpha_d]$ is not equal to $\mathfrak{p}_{i+1} \cap k[\alpha_1, \cdots, \alpha_d]$. This shows that the numbers h_i are strictly increasing. The maximal possible value for h_i is $d = n$, so we must have $k \neq n$.

The statements about height and coheight of $(x_1, \cdots, x_i)$ follows from the the fact that

$$\operatorname{ht}(x_1, \cdots, x_i) + \operatorname{coht}(x_1, \cdots, x_i) \leq \dim k[x_1, \cdots, x_n] = n.$$

■

Corollary 17.8. *If R is a domain that is fintiely generated over a field k, then the dimension of R is equal to the transcendence degree of its field of fractions. If $\mathfrak{p}$ is a prime ideal in R, then $\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p} = \dim R$.*

Proof. Generalized version of Noether normalization and going down. ■

Geometrically, R corresponds to some variety X. The prime ideal $\mathfrak{p}$ corresponds to some closed subvariety $Z \subset X$. The the corollary implies $\operatorname{coht}\mathfrak{p} = \dim Z$ and $\operatorname{ht}\mathfrak{p} = \dim R - \dim Z$.

18. Lecure 18: 2023.11.9

We start talking about the Picard group and the ideal class group of a ring R.

Definition 18.1. An invertible R-module M is a finitely generated R-module such that there exists an R-module M' such that $M \otimes_R M' \cong R$ as R-modules.

We will show that if M' exists then it is also finitely generated. If M' exists, then it is unique up to isomorphism. In fact, M' will be the dual of M.

Theorem 18.2. *M is invertible if and only if M is finitely generated, projective, and for all prime ideals $\mathfrak{p}$, $M_\mathfrak{p} \cong R_\mathfrak{p}$.*

We say M is "locally free of rank 1". This is the algebraic version of line bundles on $\operatorname{Spec} R$. It is in fact enough to consider all maximal ideals. There is a Zariski local criterion which is in the HW.

Proof. Assume M is invertible. Fix M' such that $M \otimes_R M' \cong R$. First we show that $M_\mathfrak{p} \cong R_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$. The first step is to do this in the case where R is local and $\mathfrak{m}$ is its maximal ideal. Let $k = R/\mathfrak{m}$. We have

$$(M \otimes_R M') \otimes_R k \cong k$$

The left side is isomorphic to

$$(M \otimes_R k) \otimes_k (M' \otimes_R k).$$

So as k-vector spaces, $(M \otimes_R k) \otimes_k (M' \otimes_R k) \cong k$. Considering the dimension, we obtain that

$$M/\mathfrak{m}M \cong M \otimes_R k \cong k \text{ and } M'/\mathfrak{m}M \cong M' \otimes_R k \cong k$$

So there exists $m \in M$ that generates $M/\mathfrak{m}M$. Using the assumption that M is finitely generated, we can use Nakayama's lemma to conclude $Rm = M$, so $M \cong R/I$ where I is the annhilator of m. Let $r \in I$, so $rM = 0$. This implies $r(M \otimes_R M') = rR = 0$, so $r = 0$. Hence $I = 0$ and $M \cong R$.

In the general case, obesrve that M is invertible implies $M_\mathfrak{p}$ is invertible over $R_\mathfrak{p}$. This is because we can localize the isomorphism $M \otimes_R M' \cong R$. Now by the local case discussion, we get $M_\mathfrak{p} \cong R_\mathfrak{p}$ for all $\mathfrak{p}$.

To prove M is projective, we need

Lemma 18.3. *If M is invertible, then M is flat over R. In fact, M is faithfully flat: it is flat, and for all R-modules N, $N = 0$ if and only if $M \otimes_R N = 0$.*

Proof. We have that $M_\mathfrak{p}$ is free, and hence flat over $R_\mathfrak{p}$. Flatness is a local property, so M is flat. If $M \otimes_R N = 0$, then $0 = M' \otimes_R M \otimes_R N \cong N$. ∎

Lemma 18.4. *If M is invertible and $M \otimes_R M' \cong R$, then M' is also finitely generated, and therefore invertible.*

Proof. There exists $m_1, \cdots, m_k \in M$ and $m'_1, \cdots, m'_k \in M'$ such that $\sum m_i \otimes m'_i$ maps to 1 in R. We claim that $m'_1, \cdots, m'_k$ generate M'. There is map $R^k \to M'$ defined by sending the basis to $m'_1, \cdots, m'_k$. Let Q be the cokernel of this map. We have

$$R^k \to M' \to Q \to 0$$

Tensoring with M, we get

$$M^k \xrightarrow{\psi} M \otimes_R M' \to M \otimes_R Q \to 0$$

The image of the first map ψ contains $\sum m_i \otimes m'_i$, so it is surjective since it contains 1 if we pass to the isomorphism to R. This implies $M \otimes_R Q$ is zero, and faithfully flatness of M implies Q is zero. Hence $R^k \to M'$ is a surjection and M is finitely generated. ∎

Lemma 18.5. *If M is invertible, then M is in fact finitely presented.*

Proof. Finitely generatedness gives an exact sequence

$$0 \to K \to R^n \to M \to 0$$

Let M' be such that $M \otimes_R M' \cong R$. We know that M' is also invertible, so it is faithfully flat. Tensoring with M', we get

$$0 \to K \otimes_R M' \to (M')^n \to M \otimes_R M' \to 0$$

We have that $M \otimes_R M' \cong R$, so in particular it is projective, and thus the exact sequence splits. Hence

$$(M')^n \cong R \oplus (K \otimes_R M')$$

This implies $K \otimes_R M'$ is finitely generated. Hence $K \otimes_R M' \otimes_R M$ is also finitely generated, but this is just isomorphic to K. ∎

These lemmas in summary says that M is finitely presented and locally free. A previous result (Proposition 13.7) implies M is projective (in fact these condition is equivalent to projective and finitely generated). This completes of the first half of the theorem.

Now we assume M is finitely generated, projective, and locally free of rank 1. Again Proposition 13.7 implies M is finitely presented. We claim that $M' = \mathrm{Hom}_R(M, R)$ is an inverse. We always have a natural map

$$M \otimes_R \mathrm{Hom}_R(M, R) \to R$$

by evaluation. We want to show this is an isomorphism. Isomorphism can be checked locally at all prime ideals, so consider the localization

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} \mathrm{Hom}_R(M, R)_\mathfrak{p} \to R_\mathfrak{p}$$

Because M is finitely presented, we have $\mathrm{Hom}_R(M,R)_\mathfrak{p} \cong \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p},R_\mathfrak{p})$. (Localization commutes with Hom when the source is finitely presented.) After these identification,

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p},R_\mathfrak{p}) \to R_\mathfrak{p}$$

is the evaluation map, and it is an exercise to show it is an isomorphism. This finishes the proof of the Theorem. ■

Proposition 18.6. $\mathrm{Pic}(R)$ *is an abelian group under tensor products.*

Proof. Routine. ■

As an example, if R is a noetherian UFD, then $\mathrm{Pic}(R)$ is trivial group. But this converse is not true. In fact, a theorem is that if R is a noetherian domain, then R is a UFD if and only if $R_\mathfrak{p}$ is a UFD for all primes $\mathfrak{p}$ and $\mathrm{Pic}(R) = 1$.

Assume now R is a domain, and K is its field of fractions.

Definition 18.7. A fractional ideal of R is an R-submodule M of K such that there exists $r \in R$ non-zero such that $rM \subseteq R$.

If M is a finitely generated submodule of K, then M is a fractional ideal since we can clear the denominators of the finitely many generators. If a fractional ideal M is already in R, then it is an ideal. If $\lambda \in K^\times$, we can define (λ) to be the principal fractional ideal $R\lambda \subseteq K$. It is a principal fractional ideal. If M is a fractional ideal and $rM \subseteq R$, then rM is an ideal in R.

Lemma 18.8. *if M_1, M_2 are two fractional ideals, so are $M_1 + M_2, M_1 \cap M_2, M_1M_2$. So is*

$$(M_1 : M_2) = \{\lambda \in K, \lambda M_2 \subseteq M_1\}.$$

Definition 18.9. R, K as above. An R-submodule M of K is invertible if there exists an R-submodule M' of K such that $MM' = R$.

Lemma 18.10. *If M is invertible, then M is finitely generated, and hence a fractional ideal.*

Proof. The equality $MM' = R$ implies there exists a finite list $\alpha_i \in M$ and $\beta_i \in M'$ such that $1 = \sum_i \alpha_i\beta_i$. We claim that M is generated by α_i's. Take $m \in M$. Then

$$m = 1 \cdot m = \sum_i \alpha_i(\beta_i m).$$

Notice that $\beta_i m \in MM' = R$, so m is generated by α_i's. ■

Lemma 18.11. *If M and M' are such that $MM' = R$, then $M' = (R : M)$.*

Proof. If $MM' = R$, then $M' \subseteq (R : M)$ by definition. Conversely, we know that $M(R : M) \subseteq R$. Multiplying by M', we get $R(R : M) = (R : M) \subseteq M'$. ■

Lemma 18.12. *If $M_1, \cdots, M_n$ are invertible, then so is $M = M_1 \cdots M_n$. Conversely, if M is invertible, then so are the M_i's.*

Proof. If M is invertible, we can consider $M^{-1}(\prod_{i\neq j} M_i)$. This is obviously the inverse of M_j. ■

Let $\mathcal{I}$ be the set of all invertible fractional ideals. Then $\mathcal{I}$ is an abelian group under multiplication of fractional ideals. We have a group homomorphism $K^\times \to \mathcal{I}$ sending λ to the principal fractional ideal (λ). The kernel of this map is just $R^\times$.

Definition 18.13. The ideal class group $\mathrm{Cl}(R)$ is defined to be the cokernel of the map $K^\times \to \mathcal{I}$.

19. Lecture 19: 2023.11.14

Theorem 19.1. *For a domain R, we have $\mathrm{Cl}(R) \cong \mathrm{Pic}(R)$.*

Proof. If M is an invertible fractional ideal, we can consider it as an R-module. We want to show it is an invertible R-module. We know it is finitely generated. So we need to show that M is projective, and locally free of rank 1.

There exists a fractional ideal M' such that $MM' = R$. Write $1 = \sum_{i=1}^n m_i m_i'$ where m_i, m_i' are in M, M' but ultimately in $K = \mathrm{Frac}(R)$. We define

$$f : R^n \to M$$
$$f(r_1, \cdots, r_n) = \sum_i r_i m_i$$

In the reverse direction we have

$$g : M \to R^n$$
$$g(m) = (mm_1', \cdots, mm_n')$$

Then easily $f \circ g$ is the identity on M, so M is a direct summand of R^n, hence projective.

We know that finitely generated and projective implies M is locally free. We must show that it is rank 1 at every prime ideal. We have

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} K \cong R_\mathfrak{p}^d \otimes_{R_\mathfrak{p}} K \cong K^d$$

But $M_\mathfrak{p} \otimes_{R_\mathfrak{p}} K$ is contained in $K \otimes_{R_\mathfrak{p}} K = K_{(0)} = K$. Thus $d = 1$.

Conversely, given an invertible R-module M, we have

$$M \otimes_R K \cong (M \otimes R_\mathfrak{p}) \otimes_{R_\mathfrak{p}} K \cong R_\mathfrak{p} \otimes_{R_\mathfrak{p}} K \cong K$$

Also M injects into $M \otimes_R K \cong K$ because it is torsion free. Thus, M is isomorphic (but not canonically) to some R-submodule of K. We know that M is finitely generated, so M is now seen to be a fractional ideal.

Lemma 19.2. *If M_1, M_2 are two non-zero fractional ideals, then $M_1 \cong M_2$ as R-modules if and only if there exists $\lambda \in K^\times$ such that $\lambda M_1 = M_2$. In fact, $\mathrm{Hom}_R(M_1, M_2) \cong \{\lambda \in K \mid \lambda M_1 \subset M_2\}$.*

Proof. Let $\phi : M_1 \to M_2$ be an R-linear map. Choose $\alpha \in M_1$ non-zero. Then $\phi(\alpha)/\alpha$ is some element in K. Observe that for any $r \in R$ non-zero, then $\phi(r\alpha)/(r\alpha) = \phi(\alpha)/\alpha$. Let β be another non-zero element. Then $\phi(\beta)/\beta = \phi(\alpha)/\alpha$. This is simply because $\beta = (r/s)\alpha$ for some non-zero $r, s \in R$. This shows that if we let $\lambda = \phi(\alpha)/\alpha$, then $\phi(\alpha)$ is just multiplication by λ. ■

Lemma 19.3. *If M_1, M_2 are two fractional ideals which are invertible as R-modules, then*

$$M_1 M_2 \cong M_1 \otimes_R M_2.$$

Proof. We have a natural map $M_1 \otimes_R M_2 \to M_1 M_2$. On pure tensors it is $m_1 \otimes m_2 \mapsto m_1 m_2$. Thus it is surjective. We want to show that it is injective. We check locally at every prime $\mathfrak{p}$.

We know that $(M_1M_2)_{\mathfrak{p}}$ is a non-zero $R_{\mathfrak{p}}$-module, because M_1M_2 is non-zero R-module and M_1M_2 is torsion free, so it injects into $(M_1M_2)_{\mathfrak{p}}$. On the other hand

$$(M_1 \otimes_R M_2)_{\mathfrak{p}} \cong (M_1)_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} (M_2)_{\mathfrak{p}} \cong R_{\mathfrak{p}} \cong R_{\mathfrak{p}} \cong R_{\mathfrak{p}}$$

So we obtain a surjection

$$R_{\mathfrak{p}} \to (M_1M_2)_{\mathfrak{p}}$$

by exactness of localization. Thus $(M_1M_2)_{\mathfrak{p}}$ is a quotient of $R_{\mathfrak{p}}$ by some proper ideal I. If $I \neq (0)$, then $(M_1M_2)_{\mathfrak{p}}$ has I-torsion, but $(M_1M_2)_{\mathfrak{p}} \subset K$ is torsion free. Thus $I = (0)$ and $R_{\mathfrak{p}} \cong (M_1M_2)_{\mathfrak{p}}$. In particular $(M_1 \otimes_R M_2)_{\mathfrak{p}} \to (M_1M_2)_{\mathfrak{p}}$ is injective. ■

Corollary 19.4. *If M is a fractional ideal that is invertible as an R-module, then M is an invertible fractional ideal.*

Proof. We know that there exists another invertible R-module M' such that $M \otimes_R M' \cong R$. By the discussion before the lemmas, we know that M' can be viewed as a fractional ideal. Then the above lemma implies $MM' \cong M \otimes_R M' \cong R$. As such, we must have $MM' = \lambda R$ for some $\lambda \in K$. Now $M(\lambda^{-1}M') = R$, so M is an invertible fractional ideal. ■

Note that in the corollary there is an ambiguity of a constant $\lambda \in K^{\times}$, so this establishes the isomorphism between $\mathrm{Cl}(R)$ and $\mathrm{Pic}(R)$ since we mod out by principal fractional ideals.

■

A brief digression.

Let R be a ring and M be an R-module. Recall that M is noetherian if any increasing chain of submodules is eventually constant. This is equivalent to that every non-empty collection of submodules has a maximal element. M is artinian if the reverse condition is true.

Definition 19.5. An R-module M is simple if it is non-zero and there is no non-zero proper submodule.

If M is simple and $m \in M$ non-zero, then $Rm = M$. Hence $M \cong R/I$ for some ideal I. But also this says R/I is simple, so any J containing I must be just I or R, so I is maximal and R/I is a field.

Definition 19.6. M is of finite length if it has a composition series

$$0 = M_0 \subseteq \cdots \subseteq M_n = M$$

with M_i/M_{i-1} are all simple.

This is a very special property. If a composition series exists, then the length of such composition series is independent of the choice of the composition series. Such length is then defined to be the length of M. Also the quotient M_i/M_{i-1} are independent of the choice of the composition series, up to reordering.

Now we turn to ideals in noetherian rings.

Theorem 19.7. *If I is a proper radical ideal in R a noetherian ring, then I is an intersection of finitely prime ideals. Let $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ be a non-redundant intersection, then $\mathfrak{p}_i$'s are unique up to order.*

Proof. Let X be the set of proper radical ideals which are not a finite intersection of prime ideals. Assume for contradiction that X is non-empty. Choose a maximal element I in X which exists since R is noetherian. First I is not prime, so there exists $r, s \in R$ such that $r, s \notin I$ but $rs \in I$. Consider the ideal $I + (r)$. This is a proper ideal, because otherwise $a + tr = 1$ and then $sa + trs = s \in I$, a contradiction. Also $I + (r)$ strictly contains I. Likewise $I + (s)$ have these same properties. However, we claim that $I = (I + (r)) \cap (I + (s))$. If $x \in (I + (r)) \cap (I + (s))$, then

$$x = a_1 + t_1 r = a_2 + t_2 s$$

Then

$$x^2 = (a_1 + t_1 r)(a_2 + t_2 r) = a_1 C + a_2 D + t_1 t_2 (rs) \in I$$

Since I is radical, we get that $x \in I$. Hence $I = (I + (r)) \cap (I + (s))$. Hence

$$I = \sqrt{I} = \sqrt{(I + (r)) \cap (I + (s))} = \sqrt{I + (r)} \cap \sqrt{I + (s)}.$$

Both $\sqrt{I + (r)}$ and $\sqrt{I + (s)}$ are proper radical ideals strictly containing I, so they are intersections of finitely prime ideals. This implies I is also an intersection of finitely many prime ideals. This is a contradiction.

For uniqueness, say

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

This is a subset of $\mathfrak{q}_i$ for all i, so

$$\mathfrak{q}_i \in V(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_n)$$

So there exists some j such that $\mathfrak{q}_i \subset \mathfrak{p}_j$. Similarly $\mathfrak{p}_j \subset \mathfrak{q}_l$ for some l. But there is no redundancy, so $\mathfrak{q}_i \subseteq \mathfrak{p}_j \subseteq \mathfrak{q}_l$ implies all three are equal. ■

Corollary 19.8. *If R is noetherian and $X \subset \operatorname{Spec} R$ closed, then there are finitely many irreducible subsets $Y_1, \cdots, Y_n$ such that $X = Y_1 \cup \cdots \cup Y_n$. Then Y's are unique is there is no redundancy.*

We say that Y's are the irreducible components of X. Geometrically if X is a closed algebraic subset of $\mathbf{A}_k^n$, then there exists closed irreducible subset $Y_1, \cdots, Y_l$ such that $X = Y_1 \cup \cdots \cup Y_l$. A typical example: let $f \in k[x_1, \cdots, x_m]$ is a non-constant polynomial, then we can factor $f = p_1 p_2 \cdots p_l$ into irreducible polynomials, and $V(f) = V(p_1) \cup \cdots \cup V(p_l)$.

Corollary 19.9. *If R is noetherian, there are finitely many minimal (i.e. height zero) prime ideals. If $\sqrt{0} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ with no redundancy, then $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ are the minimal primes.*

The case for non-radical ideals is the theory of primary decomposition. We will skip. We start a discussion of artinian rings.

Theorem 19.10. *A ring $R \neq 0$ is artinian if and only if R is noetherian and* $\dim R = 0$ (*i.e. every prime ideal is maximal*)

For example, a field is artinian, and a finite product of fields is artinian. If R is a noetherian ring and $\mathfrak{m}$ a maximal ideal, then quotient $R/\mathfrak{m}^N$ is noetherian and has dimension 0 because every prime ideal in $R/\mathfrak{m}^N$ corresponds to a prime ideal $\mathfrak{p}$ containing $\mathfrak{m}^N$ and thus $\mathfrak{m}$. So $R/\mathfrak{m}^N$ has a unique prime ideal that is maximal.

Proof.

Lemma 19.11. *An artinian domain is a field.*

Proof. Let R be an artinian domain. Let $r \in R$ be non-zero. We have a decreasing sequence of ideals

$$(r) \supseteq (r^2) \supseteq \cdots$$

So there exists an n such that $(r^{n+1}) = (r^n)$. So $r^n = cr^{n+1}$ for some unit c, so $1 = cr$ since we are in a domain. ∎

Lemma 19.12. *If R is artinian, every prime ideal is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal. Then $R/\mathfrak{p}$ is an artinian domain, so it is a field, and so $\mathfrak{p}$ is a maximal ideal. ∎

Lemma 19.13. *If R is artinian, then R has only finitely many maximal ideals*

Proof. Let X be the collection of all ideals of the form $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$ where m_i's are maximal. X is not empty since there is a maximal ideal, and the artnian condition gives a minimal element in X. Say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. We claim that any maximal ideal is some m_i. Let $\mathfrak{n}$ be a maximal ideal. Then $\mathfrak{n} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$ is some element in X, so we have

$$\mathfrak{n} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$$

This implies $\mathfrak{n}$ contains $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. Then $\mathfrak{n}$ contains some $\mathfrak{m}_i$ because it is prime (think about V's), and so $\mathfrak{n} = \mathfrak{m}_1$. ∎

Lemma 19.14. *If R is artinian, the nilradical $N = \sqrt{0}$ is a nilpotent ideal, i.e. $N^k = (0)$ for some $k \geq 0$.*

Proof. The decreasing chain $N \supseteq N^2 \supseteq \cdots$ stabilizes, so $N^k = N^{k+1} = \cdots$. Let $I = N^k$, so $I^2 = N^{2k} = I$. If I is not (0), let X be the collection of ideals J such that $JI \neq 0$. Note that X is not empty because $I^2 = I \neq (0)$. So X has a minimal element, say J_0. Then there is some $r \in J_0$ such that $rI \neq (0)$, and thus $(r)I \neq (0)$. Hence $J_0 = (r)$ by minimality. But also $(rI)I = rI^2 = rI \neq 0$, so rI is also in X. This implies $rI = (r)$ by minimality again. So there exists some $s \in I$ such that $sr = r$. Replacing r by sr, we obtain that $s^n r = r$ for all $n > 0$. Since $I = N^k \subset \sqrt{0}$, we know that for some n, $s^n = 0$. so in fact $r = 0$. Hence $J_0 = 0$ but that's a contradiction. ∎

Now we are almost done proving an artinian R is noetherian. We know that $\sqrt{0}$ is the intersection of all prime ideals, and when R is artinian we showed that this is the same as the intersection of all maximal ideals, and there are only finitely many. So let $\sqrt{0} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. We have that for some N,

$$\sqrt{0}^N = (0) = (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k)^N \supseteq \mathfrak{m}_1^N \cdots \mathfrak{m}_k^N.$$

Thus $\mathfrak{m}_1^N \cdots \mathfrak{m}_k^N = 0$.

Let I be an ideal of the form $\mathfrak{m}_1^{a_1} \cdots \mathfrak{m}_k^{a_k}$. Then I is an artinian R-module. Consider $I/\mathfrak{m}_i I$. It is an artinian R-module, but also an artinian $R/\mathfrak{m}_i$-module, which is a vector space. Being artinian implies $I/\mathfrak{m}_i I$ is finite dimensional. So $I/\mathfrak{m}_i I$ has a composition series.

Consider the filtration by ideals

$$R \supseteq \mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{m}^N \cdots \mathfrak{m}^N = 0$$

and call them $I_0, \cdots, (0)$, and each I_n/I_{n+1} has a composition series. This implies R has a composition series, which implies R is noetherian.

Now we prove the converse. Assume R is noetherian and $\dim R = 0$. In a noetherian ring, every radical ideal is an intersection of *finitely many* prime ideals. So let $\sqrt{0} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$ where each is maximal because we assume $\dim R = 0$. Every ideal contains a power of its radical, so we have

$$(0) \supseteq (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k)^N \supseteq \mathfrak{m}^N \cdots \mathfrak{m}^N.$$

Doing the composition series proof again to see that R has a composition series, and thus artinian. ■

20. Lecture 20: 2023.11.16

Corollary 20.1. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$. Then either $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for any n, or R is artinian.*

Proof. If $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for any n then clearly R is not artinian. Otherwise, $\mathfrak{m}^n = \mathfrak{m} \cdot \mathfrak{m}^n$. The ideal $\mathfrak{m}^n$ is a finitely generated R-module, so Nakayama's lemma implies $\mathfrak{m}^n = 0$. Let $\mathfrak{p}$ be any prime ideal, then $\mathfrak{p}$ contains $\sqrt{0}$ which contains $\mathfrak{m}$ because $\mathfrak{m}^n = 0$, so $\mathfrak{p} = \mathfrak{m}$. ■

Theorem 20.2. *If R is any artinian ring, then R is a product $R_1 \times \cdots \times R_k$ where R_i's are artin local. The product is unique up to order and isomorphism.*

We turn to Dedekind domains. We keep the basic assumption that R is noetherian domain with dimension 1. In this case, the dimension assumption is equivalent to saying that every non-zero prime ideal is maximal.

Theorem 20.3. *Let R be as above. Assume R is local, with $\mathfrak{m}$ its maximal ideal, k the residue field, and let K be its field of fractions. Then the following are equivalent:*

(1) *R is integrally closed*

(2) *$\mathfrak{m}$ is principal*

(3) $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$

(4) *there exists some $t \in R$ such that if $I \neq (0)$ is an ideal, then $I = (t^k)$*

(5) *every non-zero ideal in R is $\mathfrak{m}^k$ for some k.*

Definition 20.4. If R satisfies any (all) conditions in Theorem 20.3, we say R is a discrete valuation ring (DVR). t is called a local uniformizing parameter (uniformizer).

Proof of Theorem 20.3. First, some remarks: if $I \neq (0)$ is an ideal in R, then $\sqrt{I}$ is the intersection of all prime (hence maximal, by $\dim R = 1$) ideals containing it, but there is only one maximal ideal, so $\sqrt{I} = \mathfrak{m}$. Also $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for any $\mathfrak{n}$ since otherwise R is artinian and has dimension 0.

We first show 1 implies 2. Choose $r \in \mathfrak{m}$ non-zero, then $\sqrt{(r)} = \mathfrak{m}$. Hence there exists some $\mathfrak{m}^n \subseteq (r)$. By taking the smallest we can assume $\mathfrak{m}^{n-1} \subsetneq (r)$. So choose $s \in \mathfrak{m}^{n-1} - (r)$. Let $t = r/s \in K^\times$ ($s \neq 0$ since $0 \in (r)$). Then $rt^{-1} = s$ is not in (r), so t^{-1} is not in the ring R. Now consider $t^{-1}\mathfrak{m}$. We have

$$t^{-1}\mathfrak{m} = \frac{s}{r}\mathfrak{m} \subset \frac{1}{r}\mathfrak{m}^{n-1}\mathfrak{m} = \frac{1}{r}\mathfrak{m} \subset \frac{1}{r}(r) \subset R$$

Therefore $t^{-1}\mathfrak{m}$ is an actual ideal of R. We claim that $t^{-1}\mathfrak{m}$ is not contained in $\mathfrak{m}$, because otherwise $t^{-1}\mathfrak{m} \subset \mathfrak{m}$ is finitely generated, so t^{-1} is integral over R. By assumption 1 we have $t^{-1} \in R$, but we showed $t^{-1} \notin R$. Thus $t^{-1}\mathfrak{m} = R$, so $\mathfrak{m} = tR = (t)$.

Now we do 2 to 3. If $\mathfrak{m} = (t)$, then t mod $\mathfrak{m}^2$ spans $\mathfrak{m}/\mathfrak{m}^2$. Also $t \notin \mathfrak{m}^2$ because $\mathfrak{m}/\mathfrak{m}^2 = 0$ will make $\dim R = 0$. It is also clear that 3 implies 2. Take some basis vector of $\mathfrak{m}/\mathfrak{m}^2$ and lift to some $t \in \mathfrak{m}$. Nakayama's lemma implies $\mathfrak{m} = (t)$.

Next we show that 2 if and only if 4. Clearly 4 implies 2. Assume $\mathfrak{m} = (t)$ is principal. Let I be a non-zero proper ideal. We claim that there exists $\mathfrak{n}$ such that $I \subset \mathfrak{m}^n$ but not in $\mathfrak{m}^{n+1}$. If not, then $I \subseteq \mathfrak{m}^{k+1}$ for all k. We know that there is some k such that $\mathfrak{m}^k \subset I$ because $\sqrt{I} = \mathfrak{m}$, but then $\mathfrak{m}^k \subset \mathfrak{m}^{k+1} \subset \mathfrak{m}^k$, which implies $\mathfrak{m}^k = \mathfrak{m}^{k+1}$ which we know is not the case.

So we can choose some $s \in I - \mathfrak{m}^{n+1}$ but in $\mathfrak{m}^n = (t^n)$. So let $s = at^n$ for some $a \in R$. The choice $s \notin \mathfrak{m}^{n+1}$ means that $a \notin \mathfrak{m}$. But R is local so a is a unit. Thus $(s) = (t^n) \subseteq I \subset \mathfrak{m}^n = (t^n)$, so $I = (t^n)$, as desired.

We want to show 4 if and only if 5. 4 implies 5 is obvious. Assume 5. Choose $t \in \mathfrak{m} - \mathfrak{m}^2$ which is non-empty. Then $(t) = \mathfrak{m}^k$ by assumption 5. We must have $k < 2$ and so $k = 1$, which means $\mathfrak{m} = (t)$. So 2 is true and so 4 is true.

It remains to show any of $2 - 5$ implies 1. Assume 4, then R is a PID and hence a UFD, which is integrally closed. ■

For a DVR R, we can define a function $v : R - \{0\} \to \mathbf{Z}_{\geq 0}$ by $v(r) = k$ where $(r) = (t^k)$ where t is the uniformizer ($\mathfrak{m} = (t)$). It is easy to see that $v(rs) = v(r) + v(s)$, $v(t) = 1$, and $v(a) = 0$ if and only if a is a unit in R. This extends to a function $v : K^\times \to \mathbf{Z}$ by $v(r/s) = v(r) - v(s)$. By construction v is a surjection $K^\times \to \mathbf{Z}$. This is the discrete valuation.

Some properties:

(1) $v(\alpha) \geq 0$ if and only if $\alpha \in R - \{0\}$, and $v(\alpha) > 0$ if and only if $\alpha \in \mathfrak{m} - \{0\}$.

(2) If $\alpha + \beta \neq 0$, then $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$. This is seen by writing α, β in terms of the uniformizer t.

Example 20.1. Let $R = \mathbf{Z}_{(p)}$. It is a local, noetherian, dimension 1. For $\alpha \in K^\times$, write $\alpha = p^k\beta$ where $\beta = r/s$ and r, s are not divisible by p. Then $v(\alpha) = k$.

Example 20.2. Let $R = k[x]_{(x-a)}$. The field of fraction is $k(x)$, the field of rational functions. Any such function h can be written as

$$(x-a)^k \frac{f}{g}$$

Then $v(h) = k$. This measures the zero/pole of h at a.

The above is the local picture. Globally, we have

Theorem 20.5. *Let R be a noetherian domain that is not a field. Then the following are equivalent:*

(1) $\dim R = 1$ *and R is integrally closed*

(2) *for all non-zero prime ideals $\mathfrak{p}$, $R_\mathfrak{p}$ is a PID*

(3) *Given a prime ideal $\mathfrak{p}$, there exists a $t \in R$ such that every ideal in $R_\mathfrak{p}$ is (t^k) for some k*

Definition 20.6. If R satisfies any (all) conditions in Theorem 20.5, we say R is a Dedekind domain.

Proof. 3 to 2 is obvious. 1 implies 2 because $R_\mathfrak{p}$ is integrally closed with dimension 1 by property of localization, so 2 is true by the previous theorem. 1 implies 3 is also by the previous theorem and that $\dim R_\mathfrak{p} = 1$.

It remains to prove 2 implies 1. We claim that $\dim R = 1$. Let $\mathfrak{p}$ be a prime ideal in R that is non-zero. It is then contained in some maximal ideal $\mathfrak{m}$. By assumption 2 we know that $R_\mathfrak{m}$ is a PID that is local, so it contains a unique non-zero prime ideal $\mathfrak{m}R_\mathfrak{m}$. Using the correspondence of prime ideals, we see that $\mathfrak{p}$ must be $\mathfrak{m}$. So every non-zero prime ideal is maximal, and hence $\dim R = 1$. Also, R is integrally closed because being integrally closed is a local property. ■

21. Lecture 21: 2023.11.21

Theorem 21.1. *Let R be a Dedekind domain. Then every non-zero fractional ideal of R is invertible. In particular, if $\mathcal{I}$ is the set of non-zero fractional ideals, then $\mathcal{I}$ is a group under multiplication. If I is a non-zero proper ideal, then I is a product of prime ideals, unique up to order.*

If R is just a domain (not necessarily noetherian), then these conditions may not be true but they are all equivalent, and they are equivalent to the condition of being a Dedekind domain.

Proof. Let I be a non-zero ideal of R. Since R is noetherian, I is finitely presented. For any prime ideal $\mathfrak{p}$, the ideal $I_\mathfrak{p}$ is a non-zero ideal in $R_\mathfrak{p}$, which is a PID. Thus $I_\mathfrak{p}$ is free of rank 1. The conditions finitely presented + locally free of rank 1 implies I is invertible. Now if M is a non-zero fractional ideal, it is isomorphic as an R-module to an actual ideal, so M is an invertible R-module. Hence it is also an invertible fractional ideal. This proves the first statement.

Suppose there exists a non-zero proper ideal I_0 which is not a product of prime ideals. Since R is noetherian, we may take I_0 to be a maximal element with such property. I_0 cannot be a maximal ideal since that's a one-term product of prime ideals. So there exists some maximal ideal $\mathfrak{m}$ with

$I_0 \subset \mathfrak{m}$. Using the previous statement, $\mathfrak{m}$ and I_0 are invertible, so $\mathfrak{m}^{-1}I_0 \subset R$. But $R \subsetneq \mathfrak{m}^{-1} = (R : \mathfrak{m})$, so we get

$$I_0 \subset \mathfrak{m}^{-1}I_0 \subset R.$$

Notice that $\mathfrak{m}^{-1}I_0 \neq R$ since otherwise $I_0 = \mathfrak{m}$. Also $\mathfrak{m}^{-1}I_0 \neq I_0$ because otherwise $I_0 = \mathfrak{m}I_0$ (and we can then localize at $\mathfrak{m}$, by Nakayama's lemma $I_0 \subset (I_0)_{\mathfrak{m}} = 0$, a contradiction). Then $\mathfrak{m}^{-1}I_0$ is a proper ideal that strictly contains I_0, so it is a product of primes. But then so is I_0, a contradiction. This proves the existence of prime ideal factorization.

For uniqueness, if

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_l$$

then $\mathfrak{q}_1$ must be contained in $\mathfrak{p}_i$ for some i, but the dimension 1 property means this is an containment of maximal ideals, so they must be equal. These prime ideals are all invertible, so we can cancel them from both sides. Keep going we get uniqueness. ■

Corollary 21.2. *Any fractional ideal $M \neq 0, R$ is uniquely (up to order) written as a product*

$$\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$$

where $\mathfrak{p}_i$'s are distinct prime ideals, and $a_i \in \mathbf{Z} - \{0\}$.

Definition 21.3. If I, J are two non-zero ideals, say $J|I$ if there exists an ideal J' such that $I = JJ'$.

Lemma 21.4. *Let R be a Dedekind domain. Then $J|I$ if and only if $I \subset J$.*

Proof. $J|I$ implies $I \subset J$ trivially, in any ring. If $I \subset J$, then $J^{-1}I \subset R$ is an ideal. So $I = J(J^{-1}I)$. ■

Proposition 21.5. *Let R be a Dedekind domain. The following are equivalent:*

(1) $\mathrm{Cl}(R) = 0$

(2) *R is a PID*

(3) *R is a UFD*

Proof. The equivalence of 1 and 2 is just the definition of $\mathrm{Cl}(R)$. Any PID is UFD. So assume R is a UFD. Let $\mathfrak{p}$ be a non-zero prime ideal. Pick some $r \in \mathfrak{p}$ non-zero. Since R is a UFD, we factor r into irreducible, and one of the irreducible factors is in $\mathfrak{p}$. Thus we may assume r is irreducible. The ideal (r) is then a prime ideal contained in $\mathfrak{p}$, and the dimension 1 condition says this is a containment of maximal ideals, so $\mathfrak{p} = (r)$. Hence all prime ideals are principal. Now if I is any ideal in R, writing it as a product of prime ideals implies that it is principal. ■

Let R be a Dedekind domain. Let $\mathfrak{p}$ be a non-zero prime ideal. Then on $K^\times$, we have a valuation $v_{\mathfrak{p}} : K^\times \to \mathbf{Z}$: if $r \in R_{\mathfrak{p}}$ and $rR_{\mathfrak{p}} = (t^k)$, then $v_{\mathfrak{p}}(r) = k$. Also, if I is a non-zero fractional ideal, then write

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$$

then we can define $v_{\mathfrak{p}}(I) = a_i$ if $\mathfrak{p} = \mathfrak{p}_i$. This is multiplicative, and it agrees with the valuation on elements: $(r) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$, then $rR_{\mathfrak{p}_i} = (t_i^{a_i})$ where t_i is the uniformizer. Thus $v_{\mathfrak{p}}(r) = v_{\mathfrak{p}}((r))$.

If $R = \mathbf{Z}$ and $\mathfrak{p} = (p)$, then v_p is the p-adic valuation. If $R = A(Y)$ where Y is an affine algebraic curve (variety of dimension 1) and $A(Y)$ is integrally closed (Y is smooth), then the maximal ideals of R corresponds to points on Y. If $\mathfrak{m}$ corresponds to a point x, and t is a uniformizer at x (i.e. $\mathfrak{m}R_{\mathfrak{m}} = (t)$), then $v_x(f)$ measures the order of the zero (or minus the order of the pole) of f at x.

Facts: Let M be a non-zero fractional ideal.

(1) $v_{\mathfrak{p}}(M) = 0$ for all but finitely many $\mathfrak{p}$

(2) $v_{\mathfrak{p}}(M) = 0$ for all $\mathfrak{p}$ if and only if $M = R$.

(3) $v_{\mathfrak{p}}(M) \geq 0$ for all $\mathfrak{p}$ if and only if $M \subseteq R$.

(4) $v_{\mathfrak{p}}(M_1M_2) = v_{\mathfrak{p}}(M_1) + v_{\mathfrak{p}}(M_2)$, and $v_{\mathfrak{p}}(M^{-1}) = -v_{\mathfrak{p}}(M)$.

(5) $M_1 \subseteq M_2$ if and only if $v_{\mathfrak{p}}(M_1) \geq v_{\mathfrak{p}}(M_2)$ for all $\mathfrak{p}$.

(6) $v_{\mathfrak{p}}(M_1 + M_2) = \min\{v_{\mathfrak{p}}(M_1), v_{\mathfrak{p}}(M_2)\}$

(7) $v_{\mathfrak{p}}(M_1 \cap M_2) = \max\{v_{\mathfrak{p}}(M_1), v_{\mathfrak{p}}(M_2)\}$

To see (6), notice that $M_1 + M_2$ is the smallest fractional ideal containing M_1 and M_2. If $M_1 = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$ and $M_2 = \mathfrak{p}^{b_1} \cdots \mathfrak{p}^{b_k}$, then the smallest fractional ideal containing M_1, M_2 is $\mathfrak{p}_1^{c_1} \cdots \mathfrak{p}^{c_k}$ where $c_i = \min\{a_i, b_i\}$. For (7) it is the reverse argument.

Extensions of Dedekind domains.

Let R be a Dedekind domain, and K its field of fractions. Let L be a finite separable extension over K. Let $\widetilde{R}$ be the integral closure of R in L. We have seen that $\widetilde{R}$ is a finitely generated R-module, so $\widetilde{R}$ is also noetherian. An integral extension has the same dimension, so $\dim \widetilde{R} = 1$. Thus $\widetilde{R}$ is also a Dedekind domain.

The Krull-Akizuki theorem says that this is true even if L is not separable.

Let n denote the degree of L/K. The basic issue to compare factorization of ideals in R and $\widetilde{R}$. We introduce some notation. Let $\mathfrak{p}$ be a non-zero prime ideal in R. Then $\mathfrak{p}\widetilde{R}$ is some ideal in $\widetilde{R}$, so we can factor

$$\mathfrak{p}\widetilde{R} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Definition 21.6. In the above factorization, we say $\mathfrak{P}$ lies over $\mathfrak{p}$ if $\mathfrak{P}$ appears in the factorization.

Lemma 21.7. *The following are equivalent:*

(1) $\mathfrak{P}$ *lies over* $\mathfrak{p}$

(2) $\mathfrak{p}\widetilde{R} \subseteq \mathfrak{P}$

(3) $\mathfrak{p} \subseteq \mathfrak{P} \cap R$

(4) $\mathfrak{p} = \mathfrak{P} \cap R$

Proof. 1, 2, 3 are trivially equivalent. If $\mathfrak{p} \subseteq \mathfrak{P} \cap R$, then since $\mathfrak{P} \cap R$ is a non-zero prime ideal in R which is maximal, they must be equal. ∎

Definition 21.8. In the situation
$$\mathfrak{p}\widetilde{R} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$
we say e_i is the ramification index of $\mathfrak{p}$ at $\mathfrak{P}_i$. If $e_i = 1$ we say $\mathfrak{p}$ is unramified at $\mathfrak{P}_i$. Otherwise we say $\mathfrak{p}$ ramifies at $\mathfrak{P}_i$.

We have field extensions $R/\mathfrak{p} \hookrightarrow \widetilde{R}/\mathfrak{P}_i$. Let f_i be the degree of this field extension. This is called the residue field degree.

If $\mathfrak{p}\widetilde{R} = \mathfrak{P}^e$ (has only one term in the factorzation) and $f = 1$, we say $\mathfrak{p}$ is totally ramified. If $e_i = f_i = 1$ for all i, we say $\mathfrak{p}$ splits completely. If $\mathfrak{p}\widetilde{R} = \mathfrak{P}$, we say $\mathfrak{p}$ is undecomposed (inert?).

In the geometric case, for simplicity let k be algebraically closed and let $R = k[x]$, which is the affine coordinate ring of $\mathbf{A}^1_k$. (One can replace $\mathbf{A}^1_k$ by some irreducible smooth curve X, so $A(X)$ has dimension 1 and integrally closed.) Assume $R \subset A(Y) = \widetilde{R}$ where Y is an irreducible smooth curve. $A(Y)$ is also a Dedekind domain. We have the corresponding finite field extension $K(X) \subset K(Y)$. In this case, the Nullstellensatz implies that $R/\mathfrak{p}$ and $\widetilde{R}/\mathfrak{P}$ are always just k, so the residue field degree are always 1. Prime ideals in $A(X)$ corresponds to points $\mathfrak{m}_x, x \in X$, and prime ideals in $A(Y)$ corresponds to points $\mathfrak{m}_y, y \in Y$. The inclusion $A(X) \hookrightarrow A(Y)$ corresponds to a map $\pi : Y \to X$, and $\mathfrak{m}_y$ lies over $\mathfrak{m}_x$ if and only if $\pi(y) = x$.

Say
$$\mathfrak{m}_x A(Y) = \mathfrak{m}_{y_1}^{e_1} \cdots \mathfrak{m}_{y_k}^{e_k}.$$
Let t be the uniformizer at x. Then
$$\pi^*(t) A(Y)_{\mathfrak{m}_{y_i}} = \mathfrak{m}_{y_i}^{e_i} A(Y)_{\mathfrak{m}_{y_i}}$$
This is analogous to "branching" on Riemann surfaces.

Theorem 21.9. *In the situation*
$$\mathfrak{p}\widetilde{R} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$
we have
$$n = \sum_i e_i f_i.$$

Proof. Fix $\mathfrak{p}$. The localization $\widetilde{R}_\mathfrak{p}$ is torsion-free, and hence a flat $R_\mathfrak{p}$-module. $R_\mathfrak{p}$ is a local ring, so $\widetilde{R}_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module. Thus $\widetilde{R}_\mathfrak{p} = (R_\mathfrak{p})^n$ by tensoring with K.

The quotient $\widetilde{R}/\mathfrak{p}\widetilde{R}$ is a vector space over $R/\mathfrak{p}$ of dimension n by tensoring with K. On the other hand,
$$\widetilde{R}/\mathfrak{p}\widetilde{R} \cong \widetilde{R}/\mathfrak{P}^{e_1} \times \cdots \times \widetilde{R}/\mathfrak{P}^{e_r}$$
So it suffices to show that $\widetilde{R}/\mathfrak{P}^{e_i}$ has dimension $e_i f_i$ over $R/\mathfrak{p}$. Consider
$$0 \subset \mathfrak{P}_i^{e_i} \subset \mathfrak{P}_i^{e_i - 1} \subset \cdots \subset R$$
Each $\mathfrak{P}_i^a / \mathfrak{P}_i^{a+1}$ is a vector space over $R/\mathfrak{p}$ and over $\widetilde{R}/\mathfrak{P}_i$. We have
$$\dim_{R/\mathfrak{p}} \mathfrak{P}_i^a / \mathfrak{P}_i^{a+1} = f_i \dim_{\widetilde{R}/\mathfrak{P}_i} \mathfrak{P}_i^a / \mathfrak{P}_i^{a+1}$$

But $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ is one-dimensional (after localizing it is principal). Going through the filtration we see that $\widetilde{R}/\mathfrak{P}^{e_i}$ has dimension $e_i f_i$ over $R/\mathfrak{p}$. ■

As an example, $R = \mathbf{Z}$ and $\widetilde{R} = \mathbf{Z}[i]$. The primes are $1+i$, p congruent to 3 mod 4, and π where $N(\pi)$ is prime congruent to 1 mod 4. The prime 2 ramifies: $(2) = (1+i)^2$, here $r = 1$, $e = 2$, $f = 1$. If p is 3 mod 4, then p remains prime in $\mathbf{Z}[i]$ is inert, but $\mathbf{Z}[i]/p\,\mathbf{Z}[i]$ is $\mathbf{F}_{p^2}$. If p is 1 mod 4, then $(p)\,\mathbf{Z}[i] = (\pi)(\overline{\pi})$, so p splits completely.

22. Lecture 22: 2023.11.28

The last topic of the course will be dimension theorems and applications. First we discuss graded rings. Recall that a graded ring is a direct sum (as abelian groups) $R = \oplus_{n\geq 0} R_n$ where $R_n R_m \subseteq R_{m+n}$. The piece R_0 is a subring, and $R_+ = \oplus_{n>0} R_n$ is an ideal. A graded module is similar: $M = \oplus_{n\geq 0} M_n$, where M_n are abelian group summands and not R-submodules. However, they are R_0-modules.

Let R be any ring and I an ideal. We define the blowup algebra $B_I(R) = R \oplus I \oplus I^2 \oplus \cdots = \oplus_{n\geq 0} I^n$ with the convention $I^0 = R$. It is clear that $I^n I^m = I^{m+n}$, so this is a graded ring.

View I as an ideal in $B_I(R)$. It has degree zero, and $IB_I(R) = I \oplus I^2 \oplus \cdots$ living inside $B_I(R)$ compatibly. We can then take the quotient and define

$$\mathrm{gr}_I(R) = (R/I) \oplus (I/I^2) \oplus \cdots$$

The multiplication gives $(I^n/I^{n+1})(I^m/I^{m+1}) \subseteq I^{n+m}/I^{n+m+1}$, so this is a graded ring.

Similarly constructions can be done for modules, and we can obtain graded modules over $B_I(R)$ and $\mathrm{gr}_I(R)$.

Example 22.1. Let $R = k[x_1, \cdots, x_n]$ and let $\mathfrak{m} = (x_1, \cdots, x_n)$. Then $\mathrm{gr}_{\mathfrak{m}}(R)$ is R itself again, because $R/\mathfrak{m}$ is k, and $\mathfrak{m}/\mathfrak{m}^2 = kx_1 \oplus \cdots \oplus kx_n$ the degree 1 monomials, and so on.

Lemma 22.1. *Let $R = \oplus_{n\geq 0} R_n$ be a graded ring.*

(1) *R is noetherian if and only if R_0 is noetherian and R is a finitely generated R_0-algebra.*

(2) *If R is noetherian and $M = \oplus_{n\geq 0} M_n$ is a finitely generated R-module, then M_n is a finitely generated R_0-module for all $n \geq 0$.*

Proof. If R is noetherian then any quotient of it is noetherian, so R_0 is noetherian. Also, R_+ is an ideal in R, so R_+ is finitely generated, say by $s_1, \cdots, s_k$. We can assume s_i are homogeneous of degree d_i (if not, just take the homogenous components). Then any $r \in R_n$ for $n > 0$ is of the form $\sum r_i s_i$ with $r_i \in R_{n-d_i}$ by considering the degree. Inductively doing this (replace r_i's with sums of smaller degree ones), we get that r is a sum of monomials in s_i's with coefficients in R_0. This means that the map $R_0[s_1, \cdots, s_r] \to R$ is surjective since it is surjective in every degree, so R is finitely generated over R_0.

Conversely, suppose R_0 is noetherian and R is finitely generated as a R_0-algebra. Then R is a quotient of $R_0[x_1, \cdots, x_n]$, which is noetherian by the Hilbert basis theorem, so R is noetherian.

For the second statement, again let $s_1, \cdots, s_k$ be homogenous generators for R_+ of degree d_i. Similarly since M is finitely generated, let $m_1, \cdots, m_l$ be homogenous generators of M of degree e_j.

Then M_n is generated by

$$\{s_1^{a_1} \cdots s_k^{a_k} m_j \mid \sum_i a_i d_i + e_j = n\}$$

This is a finite set. ■

Corollary 22.2. *Let R be a ring and I an ideal. If R is noetherian, then $B_I(R)$ and $\mathrm{gr}_I(R)$ are also noetherian. And if $B_I(R)$ is noetherian, then R is noetherian.*

Proof. If R is noetherian, then I is a finitely generated ideal generated by $r_1, \cdots, r_k$. We have $B_I(R)_0 = R$, and $B_I(R)_+$ is generated $r_1, \cdots, r_k$ as an ideal in $B_I(R)$. Then $B_I(R)$ is a finitely generated R-algebra, so we are done by the lemma above.

If $B_I(R)$ is noetherian, then $R = B_I(R)/B_I(R)_+$ is noetherian. ■

Definition 22.3. Let M be an R-module. A decreasing filtration $\{M_n\}$ in M is a sequence of submodules $M_0 = M \supseteq M_1 \supseteq \cdots$. We call M is a filtered R-module. (Note that we are not in the graded setting now, so M_n are indeed submodules.) The associated graded module is $\mathrm{gr}M = \oplus_{n\geq 0} M_n/M_{n+1}$.

As an example, if R is a ring and I is an ideal, then there is a filtration $R \supseteq I \supseteq I^2 \supseteq \cdots$. Then $\mathrm{gr}R = \mathrm{gr}_I(R)$. Similarly for $M \supseteq IM \supseteq I^2M \supseteq \cdots$.

As an aside, if A is an abelian group with a filtration $A = A_0 \supseteq A_1 \cdots$, then we can define a topology on A by defining $\{A_i\}$ to be a base of open neighborhoods of 1. Under this topology, addition is continuous, so A is made into a topological group. This topology is Hausdorff if and only if $\cap_{n\geq 0} A_n = \{0\}$. In the situation with R and $\{I^n\}$, this is called the I-adic topology on R.

Definition 22.4. We say that two filtrations $\{M_n\}$ and $\{M'_n\}$ on M have bounded difference if and only if there exists N_1, N_2 such that $M_{N_1+n} \subset M'_n$ and $M'_{N_2+n} \subset M_n$. One can take $N_1 = N_2$ by taking the maximum of the two. This means that they define the same topology.

Definition 22.5. Let R be a ring, I an ideal, and M an R-module. $\{M_n\}$ is an I-filtration if for any $n \geq 0$, $IM_n \subseteq M_{n+1}$, which is equivalent to that $I^k M_n \subseteq M_{n+k}$ for any $n \geq 0, k \geq 1$. An I-filtration is stable if $IM_n = M_{n+1}$ for all sufficiently large n.

For example, $M_n = I^n M$ is a stable I-filtration.

Lemma 22.6. *If $\{M_n\}$ is a stable I-filtration, then $\{M_n\}$ and $\{I^n M\}$ have bounded difference.*

Proof. By definition, $I^n M = I^n M_0 \subseteq M_n$. On the other hand, since $\{M_n\}$ is stable, we know that there exist some N such that for $n \geq N$, we have $I^n M_N = M_{N+n}$. But $I^n M_N \subset I^n M$, so $I^n M \subset M_{N+n}$. ■

Theorem 22.7 (Artin-Rees Lemma). *Suppose R is noetherian, I is an ideal, and M is a finitely generated R-module. Let M_n be a stable I-filtration on M. Then for any submodule M' of M, the induced filtration $\{M' \cap M_n\}$ is a stable I-filtration on M'.*

Corollary 22.8. *With R, I, M, M' as above, we have $(I^n M) \cap M' = I^{n-N}(I^N M \cap M')$.*

This means that the subspace topology on M' is the I-adic topology on M'.

Proof of Artin-Rees Lemma. Define

$$M^* = \oplus_{n\geq 0} M_n.$$

If M_n is an I-filtration, then M^* is graded $B_I(R)$-module because $I^k M_n \subseteq M_{n+k}$. The key lemma is the following:

Lemma 22.9. *If R is noetherian, I an ideal in R, and M a finitely generated R-module. Let $\{M_n\}$ be an I-filtration on M. Then $\{M_n\}$ is a stable I-filtration if and only if M^* is a finitely generated $B_I(R)$-module.*

Proof. Since R is noetherian, we know that $B_I(R)$ is noetherian. Consider the submodule

$$M_n^* = M_0 \oplus M_1 \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots$$

of M^* (because each $I^k M_n$ is contained in M_{n+k}). More efficiently,

$$M_n^* = \bigoplus_{k\neq n} M_k \oplus \bigoplus_{k\geq n+1} I^{k-n} M_n$$

Note that M_n^* are increasing, and $\cup_n M_n^* = M^*$. Hence, $M_N^* = M^*$ for some N if and only if $M_k = I^{k-N} M_N$ for all $k \geq N$. Reindexing, this is $M_{N+j} = I^j M_N$ for all j. This is the definition of being a stable I-filtration, so we indeed have $M_N^* = M^*$ for some N. On the other hand, M_n^* is a finitely generated $B_I(R)$-module since it is generated by $M_0 \oplus \cdots \oplus M_n$, each of which is a finitely generated module over R. Hence M^* is a finitely generated $B_I(R)$-module if and only if $\{M_n\}$ is a stable I-filtration. ■

Returning to the proof of Artin-Rees, we now know that M^* is a finitely generated $B_I(R)$-module. Consider the induced filtration $\{M' \cap M_n\}$ on M'. We have

$$I(M' \cap M_n) \subset IM' \cap IM_n \subseteq M' \cap M_{n+1}$$

so $\{M' \cap M_n\}$ is an I-filtration on M'. Thus we can construction $(M')^* \subseteq M^*$, which is a $B_I(R)$-submodule. We know that $B_I(R)$ is noetherian and M^* is finitely generated, so M^* is noetherian, and any submodule is finitely generated. Hence $(M')^*$ is finitely generated over $B_I(R)$ and thus $\{M' \cap M_n\}$ is a stable I-filtration.

■

Corollary 22.10 (Krull)**.** *Let R be noetherian, I an ideal, and M a finitely generated R-module. Then*

$$\bigcap_{n=1}^{\infty} I^n M = \{m \in M \mid \text{ there exists } r \in I, (1+r)m = 0\}.$$

In particular, this intersection is zero if I is contained in the Jacobson radical of R, or R is a domain, I is a proper ideal, and M is torsion free.

Proof. Let $M' = \cap_{n=1}^{\infty} I^n M$. Artin-Rees Lemma implies that

$$(I^{N+1}M) \cap M' = I(I^N M \cap M')$$

but $I^k M' \supseteq M'$ just because it is the intersection over all power. So we get

$$M' = IM'$$

By Nakayama's lemma, this means there exists $r \in I$ such that $(1+r)M' = 0$. Hence

$$M' \subseteq \{m \in M \mid \text{ there exists } r \in I, (1+r)m = 0\}.$$

For the other inclusion, we have

$$m = -rm = r^2 m = \cdots$$

so $m \in I^n M$ for all n. ■

For example, $M = R = C^\infty(R)_0$ be the germs of smooth function at $0 \in R$. Let $\mathfrak{m}$ be the maximal ideal of germs vanishing at 0. The ring R is local, so the condition of Krull's theorem is satisfied except for noetherianness.

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n M$$

is the C^∞ functions whose Taylor series at 0 is identically 0. We know that this is not zero, so the Krull's theorem fails for non-noetherian rings.

23. Lecture 23: 2023.11.30

We will discuss Hilbert functions.

Let k be a field. Let $S = k[x_0, \cdots, x_d]$, a graded ring. The dimension of the n-th piece is

$$\dim_k S_n = \binom{n+d}{d} = \frac{1}{d!}(n+d)\cdots(n+1)$$

This is a polynomial in n of degree d with leading coefficient $\frac{1}{d!}$.

If M is a finitely generated graded S-module, so $M = \oplus_{n\geq 0} M_n$, we obtain a function

$$H_M(n) = \dim_k M_n.$$

When $M = S/I$ where I is a homogenous ideal (so I corresponds to some subset X of the projective space), we write $H_X(n)$.

In general, let $S = \oplus_{n\geq 0} S_n$ be a graded noetherian ring. Let χ be a function on the set of isomorphism class of finitely generated S_0-modules, to **Z**. For example, if S_0 is a field, we can take χ to be the dimension of M. If S_0 is artinian, then we can take χ to be the length of M. Note that if k is algebraically closed and S_0 is a finitely generated k-algebra, then S_0 is artinian, and in this case the length is equal to the dimension.

We assume χ is additive over exact sequences: given an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of finitely generated S_0 modules, then $\chi(M) = \chi(M') + \chi(M'')$. Here are some consequences:

(1) If we have an exact sequence

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

of finitely generated S_0 modules, we get

$$\sum_{i=0}^{n} (-1)^i \chi(M_i) = 0$$

(2) Given a filtration $M_0 = M \supseteq \cdots \supseteq M_n$ where each M_i/M_{i+1} is a finitely generated module over S_0, then

$$\chi(M/M_n) = \sum_{i=0}^{n-1} \chi(M_i/M_{i+1}).$$

If M is a finitely generated S-module, then each M_n is a finitely generated S_0-module, and we can define

$$H_{\chi,M}(n) = \chi(M_n).$$

This is called the *Hilbert function*.

There is another version. Let R be a noetherian ring (no grading), and let M be a R-module with a filtration $\{M_n\}$ (not graded pieces). We might be able to define

$$P_{\chi,M}(n) = \chi(M/M_n).$$

The point is that given M, we associated $\mathrm{gr} M = \oplus M_n/M_{n+1}$, then

$$P_{\chi,M}(n+1) - P_{\chi,M}(n) = H_{\chi,\mathrm{gr}M}(n)$$

once everything is defined.

Let R be a noetherian ring, $\mathfrak{m}$ a maximal ideal, and k the residue field.

Definition 23.1. An ideal $\mathfrak{q}$ is $\mathfrak{m}$-primary if $\sqrt{\mathfrak{q}} = \mathfrak{m}$.

In a noetherian ring, this is equivalent to that there exists some k such that $\mathfrak{m}^k \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, because in a noetherian ring any ideal contains some power of its radical.

Let M be a finitely generated R-module and $\mathfrak{q}$ a $\mathfrak{m}$-primary ideal. Let $S = \mathrm{gr}_{\mathfrak{q}} R = \oplus_{n \geq 0} \mathfrak{q}^n/\mathfrak{q}^{n+1}$. Then $S_0 = R/\mathfrak{q}$ is artinian because $\mathfrak{q}$ contains some $\mathfrak{m}^k$. If M is a finitely generated, we have $\mathrm{gr}_{\mathfrak{q}} M = \oplus_{n \geq 0} \mathfrak{q}^n M/\mathfrak{q}^{n+1} M$. This is a finitely generated S-module.

Let χ be the length function as S_0-modules. If $M_n = \{\mathfrak{q}^n M\}$ or any stable $\mathfrak{q}$-filtration, then M_n/M_{n+1} is a finitely generated S_0-module, so it has finite length. This implies that M/M_{n+1} also has finite length. We define

$$H_{\mathfrak{q},M} = H_{\chi,M}$$

and $P_{\mathfrak{q},M}$ similarly. This depends on the filtration. Concretely, $H_{\mathfrak{q},M}(n)$ is the length of $\mathfrak{q}^n M/\mathfrak{q}^{n+1} M$.

We need some knowledge on numerical polynomials. Consider functions $f : \mathbf{Z}_{\geq 0} \to \mathbf{Z}$. We say $f_1 \sim f_2$ if $f_1(n) = f_2(n)$ for sufficiently large n. This is an equivalence relation. We identify functions under this equivalence relation.

For example, a polynomial in $\mathbf{Z}[t]$ defines such a function. Sometimes a polynomial p in $\mathbf{Q}[t]$ defines a function $\mathbf{Z}_{\geq 0} \to \mathbf{Z}$. If so, we call p a numerical polynomial. If $f \sim p$, then we also say f is a numerical polynomial. Note that if p_1, p_2 are polynomials and $p_1 \sim p_2$, then $p_1 = p_2$ because their difference has infinitely many zeros. A numerical polynomial has a well-defined degree and leading coefficient. We adapt the convention that $\deg 0 = -1$.

If f is a function $\mathbf{Z}_{\geq 0} \to \mathbf{Z}$, we define $\Delta f(n) = f(n+1) - f(n)$. Then $f_1 \sim f_2$ implies $\Delta f_1 \sim \Delta f_2$. For example, $\Delta P_{\chi,M} = H_{\chi,\mathrm{gr}M}$.

Lemma 23.2. *f is a numerical polynomial of degree d if and only if Δf is a numerical polynomial of degree $d-1$. A $\mathbf{Z}$-basis for numerical polynomials in $\mathbf{Q}[t]$ is given by*

$$\binom{t}{i} = \frac{1}{i!}t(t-1)\cdots(t-i+1).$$

In other words, any numerical polynomial in $\mathbf{Q}[t]$ is uniquely of the form

$$\sum_{i=0}^{n} a_i \binom{t}{i}$$

where $a_i \in \mathbf{Z}$.

Proposition 23.3. *Let R be a graded noetherian ring. Assume that R is generated by elements in degree 1 over R_0, i.e. $R = R_0[r_1, \cdots, r_k]$ with $\deg r_i = 1$. Let M be a finitely generated graded R-module, and χ an additive function. Then $H_{\chi,M}$ is a numerical polynomial of degree $k-1$.*

Proof. We use induction on k. When $k = 0$, there is no generator, so $R = R_0$. This means M is a finitely generated R_0-module. This means that $M_n = \{0\}$ for all sufficiently large n. Hence $H_{\chi,M} \sim 0$, whence $\deg H_{\chi,M} = -1$.

For the inductive step, assume the statement is true for R' generated by at most $k-1$ elements. Consider $R' = R/r_kR$. We have an exact sequence

$$0 \to K \to M \xrightarrow{r_k} M \to L \to 0$$

where K, L are the kernel and cokernel of multiplication by r_k. They are graded R'-modules. We have exact sequences

$$0 \to K_n \to M_n \xrightarrow{r_k} M_{n+1} \to L_{n+1} \to 0$$

We know that

$$\Delta H_{\chi,M}(n) = \chi(M_{n+1}) - \chi(M_n) = \chi(L_{n+1}) - \chi(K_n) = H_{\chi,L}(n+1) - H_{\chi,K}(n)$$

By the induction hypothesis, this has degree at most $k-2$, so $H_{\chi,M}$ has degree at most $k-1$. ■

Corollary 23.4. *Let R be noetherian, $\mathfrak{m}$ a maximal ideal, $\mathfrak{q}$ a $\mathfrak{m}$-primary ideal, and M a finitely generated R-module.*

(1) *If $\mathfrak{q}$ is a generated by at most k elements, then $H_{\mathfrak{q},M}$ is a numerical polynomial of degree at most $k-1$.*

(2) *If $P_{\mathfrak{q},M}(n)$ is the length of $M/\mathfrak{q}^{n+1}M$, then $P_{\mathfrak{q},M}$ is a numerical polynomial of degree at most k.*

(3) *If $\{M_n\}$ is a stable $\mathfrak{q}$-filtration, and we define $P(n)$ to be the length of M/M_{n+1}, then P is a numerical polynomial of degree at most k.*

Proof. The graded ring $\mathrm{gr}_{\mathfrak{q}}R$ is generated in degree 1 as a $R/\mathfrak{q}$-algebra by images of generators of $\mathfrak{q}$. ■

Lemma 23.5. *Same hypothesis as in the previous corollary. If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of R-modules, then $H_{\mathfrak{q},M} - H_{\mathfrak{q},M''} = F$ where F is a numerical polynomial and F and $H_{\mathfrak{q},M'}$ have the same degree and leading coefficient.*

Proof. We have an exact sequence

$$0 \to \mathfrak{q}^n M \cap M' \to \mathfrak{q}^n M \to \mathfrak{q}^n M'' \to 0.$$

This gives

$$0 \to \mathfrak{q}^n M \cap M'/\mathfrak{q}^{n+1} M \cap M' \to \mathfrak{q}^n M/\mathfrak{q}^{n+1} M \to \mathfrak{q}^n M''/\mathfrak{q}^{n+1} M'' \to 0.$$

Let

$$F(n) = \ell(\mathfrak{q}^n M \cap M'/\mathfrak{q}^{n+1} M \cap M')$$

Then $H_{\mathfrak{q},M} - H_{\mathfrak{q},M''} = F$. Observe that $F = \Delta P$, where

$$P(n) = \ell(M'/M' \cap \mathfrak{q}^{n+1} M')$$

Also as usual, $H_{\mathfrak{q},M'} = \Delta P_{\mathfrak{q},M'}$ where $P_{\mathfrak{q},M'}(n) = \ell(M'/\mathfrak{q}^{n+1} M')$.

By Artin-Rees, the filtrations $\{\mathfrak{q}^n M \cap M'\}$ and $\{\mathfrak{q}^n M'\}$ have bounded difference. So there exists some constants N such that

$$P(n-N) \le P_{\mathfrak{q},M'}(n) \le P(n+N).$$

This is only possible if P and $P_{\mathfrak{q},M'}$ have the same degree and leading coefficient. Thus so do ΔP and $\Delta P_{\mathfrak{q},M'}$, which is the desired result. ■

We will proceed to the dimension theorem. Let R be a local noetherian ring, $\mathfrak{m}$ its maximal ideal, and k the residue field. There are three possible notions of dimension. The first one is the Krull dimension $\dim R$. The second one is $d(R) = \deg H_{\mathfrak{m},R} + 1$. The third one is $\delta(R)$, the minimal possible number of generators of an $\mathfrak{m}$-primary ideal $\mathfrak{q}$. (Here, if (0) is $\mathfrak{m}$-primary, we set $\delta(R) = 0$.) The dimension theorem says that these are all the same.

In the dimension 0 case, R is artinian and $\mathfrak{m}$ is nilpotent, so (0) is $\mathfrak{m}$-primary. Also, $\deg H_{\mathfrak{m},R} = -1$ if and only if it is the zero polynomials, which means $\mathfrak{m}^n/\mathfrak{m}^{n+1} = 0$ for all large n. This happens if and only if $\mathfrak{m}^n = 0$ for all large n, which is equivalent to R being artinian. Hence we see that in dimension 0 indeed these are all the same.

We will prove the dimension theorem next time. Now we make some side remarks. Let k be algebraically closed, and let $R = k[x_0, \cdots, k_N]/I$ where I is some homogeneous prime ideal. So R is the projective coordinate ring of some projective variety X. We have the Hilbert polynomial $H_X(n) = \dim_k R_n$, which is a numerical polynomial. A fact is that if r is the dimension of X (which we haven't defined for the moment), then $\deg H_X$ is r, and its leading coefficient is $d/r!$ for some positive integer d. This integer d is called the *degree* of X. We saw that the degree of $\mathbf{P}^n_k$ is 1.

An easy exercise is that if $X = V(f)$ where f is homogenous irreducible of degree d, then the degree of X is d. More generally (and harder), if $X \subset \mathbf{P}^N_k$ with dimension r, then cutting X with r hyperplanes will generally give a finite set of d points where d is the degree of X.

24. Lecture 24: 2023.12.5

Recall that we want to prove the dimension theorem for a local noetherian ring R. Let $\mathfrak{m}$ be its maximal ideal and $k = R/\mathfrak{m}$ its residue field.

An immediate corollary of the dimension theorem is that the dimension of a local noetherian ring is finite, as can be seen using the quantity $\delta(R)$, the minimal number of generators of a $\mathfrak{m}$-primary ideal.

The easiest step is to show

Lemma 24.1. *$d(R) \leq \delta(R)$.*

Proof. Recall that $d(R) = \deg H_{\mathfrak{m},R} + 1$. Let $\mathfrak{q}$ be a $\mathfrak{m}$-primary ideal generated by t elements where $t = \delta(R)$. We want to prove that $\deg H_{\mathfrak{m},R} + 1 \leq t$. By Corollary 23.4, we know that $\deg H_{\mathfrak{q},R} \leq t-1$. So it is enough to observe that $H_{\mathfrak{m},R}$ and $H_{\mathfrak{q},R}$ have the same degree. Since $\mathfrak{q}$ is $\mathfrak{m}$-primary, we know that there exists some k such that $\mathfrak{m}^k \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, and therefore

$$\mathfrak{m}^{kn} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n.$$

We then have surjections

$$R/\mathfrak{m}^{kn} \to R/\mathfrak{q}^n \to R/\mathfrak{m}^n$$

This means $\ell(R/\mathfrak{kn}) \geq \ell(R/\mathfrak{q}^n) \geq \ell(R/\mathfrak{m}^n)$. By definition, this gives

$$P_{\mathfrak{m},R}(kn) \geq P_{\mathfrak{q},R}(n) \geq P_{\mathfrak{m},R}(n)$$

For large values of n these are all polynomials, so such an inequality is only possible if they have the same degree. Applying the difference operators gives the result. ■

Let $\overline{R} = R/\sqrt{0}$, and its maximal ideal is denoted by $\overline{\mathfrak{m}}$. This is a reduced ring.

Lemma 24.2. *With $\overline{R}$ as above, we have*

(1) $\dim R = \dim \overline{R}$

(2) $\delta(R) = \delta(\overline{R})$

(3) $d(\overline{R}) \leq d(R)$

Proof.

(1) Prime ideals in $\overline{R}$ corresponds to prime ideals in R that contains $\sqrt{0}$, but all prime ideals contain $\sqrt{0}$. Hence there is a bijection between chains of prime ideals.

(2) If $\mathfrak{q}$ is $\mathfrak{m}$-primary in R generated by t elements, then the image $\overline{\mathfrak{q}}$ in $\overline{R}$ is also $\overline{\mathfrak{m}}$-primary and generated by t elements. Thus $\delta(R) \geq \delta(\overline{R})$. Conversely, if $\overline{\mathfrak{q}}$ in $\overline{R}$ is $\overline{\mathfrak{m}}$-primary and generated by t elements $\overline{r_1}, \cdots, \overline{r_t}$, we can lift the generators to $r_1, \cdots, r_t$. There is certainly a surjection

$$\sqrt{(r_1, \cdots, r_t)} \to \sqrt{\overline{q}} = \overline{\mathfrak{m}}$$

On the other hand, $\sqrt{0} \subset \sqrt{(r_1, \cdots, r_t)}$, so the kernel of the above map is exactly $\sqrt{0}$, meaning that $\sqrt{(r_1, \cdots, r_t)} = \mathfrak{m}$. Hence $\delta(R) = \delta(\overline{R})$.

(3) The surjection $\mathfrak{m} \to \overline{\mathfrak{m}}$ gives surjections

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} \to \overline{\mathfrak{m}}^n/\overline{\mathfrak{m}}^{n+1}$$

Hence $H_{\mathfrak{m},R}(n) \geq H_{\overline{\mathfrak{m}},R}(n)$, so we have the degree inequality.

■

This allows us to reduce to the case where R is reduced. Here are some facts we will use

(1) If R is any ring, I is an ideal, and $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$ are prime ideal, then I is contained in the union $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_k$ if and only if I is contained in one of them.

(2) If R is a reduced noetherian ring, and $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$ are the minimal primes of R (so their intersection is 0), then the set of zero divisors of R is the union $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_k$. If R is not assumed to be reduced, then the minimal primes are contained in the set of zero divisors. (More generally the zero divisors are union of associated prime, but we won't use that.)

Lemma 24.3. *Let $\mathfrak{q}$ be a $\mathfrak{m}$-primary ideal in a local noetherian ring R. If M is an R-module, and $r \in R$ is not a zero divisor on M (i.e. multiplication by r is an injection), then*

$$\deg H_{\mathfrak{q},M/rM} \leq \deg H_{\mathfrak{q},M} - 1.$$

In particular, if r is not a zero divisor, then $d(R/rR) \leq d(R) - 1$.

Proof. We have a short exact sequence

$$0 \to M \xrightarrow{r} M \to M/rM \to 0$$

By Lemma 23.5, we know that $H_{\mathfrak{q},M} - H_{\mathfrak{q},M/rM} = F$ where F has the same degree and leading coefficient as $H_{\mathfrak{q},M}$. In other words, $H_{\mathfrak{q},M.rM}$ has smaller degree than $H_{\mathfrak{q},M}$. ■

We know prove $\dim R \leq d(R)$ for reduced R. We have seen that if any of the three dimensions is 0, then all of them are 0. So we induct on the value of $d = d(R)$ and the base case is known. Assume that $\dim R' \leq d(R') = d'$ is true for all rings R' with $d' < d$. Let

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_k$$

be a maximal (strictly increasing) chain of prime ideals in R. We can assume $k \geq 1$, since we know the case where $k = 0$. Then $\mathfrak{p}_1$ is not a minimal prime. So there exists $r \in \mathfrak{p}_1$ not a zero divisor (otherwise $\mathfrak{p}_1$ is contained in the union of minimal primes (here we used R reduced!), and thus in one of the minimal primes, a contradiction.) Consider $R' = R/rR$, and let $\mathfrak{p}_i'$ be the image of $\mathfrak{p}_i$ in R'. We get a chain

$$\mathfrak{p}_1' \subset \cdots \subset \mathfrak{p}_k'$$

So $\dim R' \geq k-1$. On the other hand, Lemma 24.3 implies that $d(R') \leq d(R) - 1$. By the inductive hypothesis, we know that $\dim R' \leq d(R')$, so

$$k - 1 \leq \dim R' \leq d(R') \leq d(R) - 1$$

Thus $k \leq d(R)$, giving $\dim R \leq d(R)$. Note that this already implies $\dim R < \infty$.

It remains to prove $\delta(R) \leq \dim R$. The finiteness of $\dim R$ allows us to use induction of $\dim R = d$. The base case is again known. Assume the results for all $d' < d$.

Lemma 24.4. *If R is local noetherian, and $r \in R$ is not a zero divisor or a unit, then*

(1) $\delta(R) \leq \delta(R/rR) + 1$

(2) $\dim R \geq \dim(R/rR) + 1$

Note that this lemma implies the inductive step. If $\dim R > 0$, then the maximal ideal $\mathfrak{m}$ is not minimal. By the same reasoning as before, there exists some $r \in \mathfrak{m}$ that is not a zero divisor, and clearly also not a unit. Then the lemma gives

$$\dim(R/rR) \leq \dim R - 1 = d - 1$$

The induction hypothesis says $\delta(R/rR) \leq \dim(R/rR)$, and the lemma gives $\delta(R) - 1 \leq \delta(R/rR)$. Putting them all together yields $\delta(R) \leq d$.

Proof of Lemma 24.4.

(1) Suppose $s_1, \cdots, s_t$ generate an $\mathfrak{m}'$-primary ideal in $R' = R/rR$, where $\mathfrak{m}'$ is the image of $\mathfrak{m}$. Lift s_i to $r_i \in R$ and consider $(r, r_1, \cdots, r_t)$. We claim that this is $\mathfrak{m}$-primary. This is because we have equality
$$R/(r, r_1, \cdots, r_t) = (R/rR)(s_1, \cdots, s_t)$$
and the right side is artinian, so $(r, r_1, \cdots, r_t)$ contains some power of $\mathfrak{m}$, and hence is $\mathfrak{m}$-primary. Therefore $\delta(R) \leq \delta(R/rR) + 1$.

(2) Start with a chain
$$\mathfrak{p}_1' \subset \cdots \subset \mathfrak{p}_k'$$
in $R' = R/rR$. We can lift it to a chain
$$\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_k$$
that is also strictly increasing. We know that $r \in \mathfrak{p}_1$ and r is not a zero divisor, so $\mathfrak{p}_1$ cannot be minimal. Thus there is some $\mathfrak{p}_0$ that is strictly contained in $\mathfrak{p}_1$, so $\dim R \geq \dim R' + 1$.

■

This finishes the proof of the dimension theorem.

Applications of the dimension theorem.

Corollary 24.5. *Let R be a local noetherian ring, $r \in R$ not a zero divisor or a unit. Then* $\dim(R/rR) = \dim R - 1$

Proof. By Lemma 24.4 and the dimension theorem, we have
$$\dim(R/rR) \leq \dim R - 1 = \delta(R) - 1 \leq \delta(R/rR) = \dim(R/rR)$$
So all inequalities are equalities. ■

Proposition 24.6. *Let R be a noetherian ring but not necessarily local. Let $r_1, \cdots, r_k \in R$. Let $\mathfrak{p}$ be a minimal prime in the set of ideals that contains $(r_1, \cdots, r_k)$ (so $\mathfrak{p}$ corresponds to a minimal prime in the quotient $R/(r_1, \cdots, r_k)$). Then $\operatorname{ht} \mathfrak{p} \leq k$.*

Proof. Recall that $\operatorname{ht} \mathfrak{p}$ is the length of the longest chain that ends at $\mathfrak{p}$, which is $\dim R_{\mathfrak{p}}$. The minimality of $\mathfrak{p}$ means that if we write
$$\sqrt{(r_1, \cdots, r_k)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_a$$
with no containment relations (a decomposition into irreducible components), then $\mathfrak{p}$ is one of them, say $\mathfrak{p}_1$. An easy fact is that $\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$, so here we have
$$\sqrt{(r_1, \cdots, r_k)R_{\mathfrak{p}}} = (R - \mathfrak{p})^{-1}(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_a) = \bigcap_{i=1}^{a} \mathfrak{p}_i R_{\mathfrak{p}} = \mathfrak{p} R_{\mathfrak{p}}$$
Thus $(r_1, \cdots, r_k)R_{\mathfrak{p}}$ is $\mathfrak{p}R_{\mathfrak{p}}$-primary in the local ring $R_{\mathfrak{p}}$. The dimension theorem then implies
$$k \geq \delta(R_{\mathfrak{p}}) = \dim R_{\mathfrak{p}}.$$

■

Corollary 24.7 (Krull's principal ideal theorem = Hauptidealsatz)**.** *Let R be a noetherian ring. Let $r \in R$ that is not a unit or a zero divisor. Let $\mathfrak{p}$ be a minimal prime ideal in the set of ideals containing (r). Then* $\operatorname{ht} \mathfrak{p} = 1$*.*

Proof. The Proposition implies $\operatorname{ht} \mathfrak{p} \leq 1$. If $\mathfrak{p}$ has height 0, then $\mathfrak{p}$ is a minimal prime, so $\mathfrak{p}$ is contained in the set of zero divisors. But $r \in \mathfrak{p}$ is not a zero divisor, so $\mathfrak{p}$ cannot have height 0. Thus $\mathfrak{p}$ has height 1. ■

There are some other applications that we will not prove in class:

Theorem 24.8. *Let R be noetherian. Then* $\dim R[x] = \dim R + 1$*.*

This sounds obvious but in fact fails when R is not noetherian. As a corollary, if k is a field then the dimension of $k[x_1, \cdots, x_n]$ is n.

Theorem 24.9. *If R is a noetherian domain, then the following are equivalent:*

(1) *R is a UFD*

(2) *every height 1 prime ideal is principal*

(3) *if $\mathfrak{m}$ is maximal (equivalently, prime) then $R_\mathfrak{m}$ is a UFD and* $\operatorname{Pic} R = 0$

25. Lecture 25: 2023.12.7

Theorem 25.1. *Let k be a field, which is algebraically closed. Then* $\dim k[x_1, \cdots, x_n]_\mathfrak{m} = n$ *for any maximal ideal $\mathfrak{m}$.*

Proof. Assume $\mathfrak{m} = (x_1, \cdots, x_n)$. Then $\operatorname{gr}_\mathfrak{m} k[x_1, \cdots, x_n]_\mathfrak{m}$ is $\oplus_{k \geq 0} \mathfrak{m}^k / \mathfrak{m}^{k+1}$. The piece $\mathfrak{m}^k / \mathfrak{m}^{k+1}$ is the homogenous degree k polynomials, which has dimension $\binom{n+k-1}{k}$. This is a polynomial of degree $n-1$ in k. So $\deg H_{\mathfrak{m}, k[x_1, \cdots, x_n]_\mathfrak{m}} = n - 1$, and it follows that the dimension is n.

Any other maximal ideal is $(x_1 - a_1, \cdots, x_n - a_n)$, which is the same. ■

Corollary 25.2. $\dim k[x_1, \cdots, x_n] = n$*.*

Proof. For any ring, $\dim R$ is $\max\{\dim R_\mathfrak{m}\}$ because the longest chain must end at a maximal ideal. ■

Corollary 25.3. *Let $A = A(X)$ for X an affine variety over $k = \overline{k}$. Then $\dim A$ is equal to the transcendence degree of A over k. More precisely, there is an integral extension of $k[x_1, \cdots, x_d] \hookrightarrow A(X)$, so $\dim A = d$.*

From now on, R is a local noetherian ring with maximal ideal $\mathfrak{m}$ and residue field k.

Lemma 25.4. $\dim R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$*. This quantity is referred to as the embedding dimension of R.*

Proof. Let $e_1, \cdots, e_n$ be a k-basis of $\mathfrak{m}/\mathfrak{m}^2$. Lift them to $r_1, \cdots, r_n$. Then $r_1, \cdots, r_n$ generate $\mathfrak{m}$ mod $\mathfrak{m}^2$, so Nakayama's lemma implies $\mathfrak{m} = (r_1, \cdots, r_n)$. $\mathfrak{m}$ is itself $\mathfrak{m}$-primary, so $\delta(R) \leq n$. The proof is then finished by the dimension theorem. ■

Definition 25.5. We say R is a regular local ring if $\dim R = \dim_k \mathfrak{m}/\mathfrak{m}^2$. If R is noetherian but not necessarily local, we say R is regular if $R_\mathfrak{m}$ is regular for all maximal ideals $\mathfrak{m}$.

It is a non-trivial fact that $R_\mathfrak{m}$ is regular for all maximal ideals $\mathfrak{m}$ if and only if $R_\mathfrak{p}$ is regular for all prime ideals $\mathfrak{p}$..

As an example, the polynomial ring $k[x_1, \cdots, x_n]$ is regular. If R is a local noetherian domain of dimension 1, then R is regular if and only if R is a DVR. If R is a noetherian domain of dimension 1, then R is regular if and only if R is a Dedekind domain. We then see that in dimension 1, regularity is equivalent to being integrally closed. In higher dimensions, regularity implies integrally closed.

Proposition 25.6. *Let R be a local noetherian ring. Then R is regular of dimension n if and only if $\mathrm{gr}_\mathfrak{m} R \cong k[x_1, \cdots, x_n]$ as graded algebras.*

Proof. Assume $\mathrm{gr}_\mathfrak{m} R \cong k[x_1, \cdots, x_n]$ as graded algebras. Then the graded piece of degree 1 is $\mathfrak{m}/\mathfrak{m}^2$ but also just the linear polynomials, so it is of dimension n.

Assume R is regular of dimension n. We have a homomorphism $k[x_1, \cdots, x_n] \to \mathrm{gr}_\mathfrak{m} R$ defined by sending x_i to e_i where e_i is a basis of $\mathfrak{m}/\mathfrak{m}^2$. The piece $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is generated by monomials in e_i's, so this map is a surjection.

Let f be in the kernel of this map. Then we would have a surjection $k[x_1, \cdots, x_n]/(f) \to \mathrm{gr}_\mathfrak{m} R$, so the dimension of $k[x_1, \cdots, x_n]/(f)$ is at least n. But if f is not 0, then it is not a zero divisor, so $\dim k[x_1, \cdots, x_n]/(f) \leq n-1$, a contradiction. Hence $f = 0$ and we have an isomorphism. ■

In higher dimensions, we have the so called Jacobian criterion.

Proposition 25.7. *Suppose R is a regular local ring of dimension n. Let $f_1, \cdots, f_k \in \mathfrak{m}$. Let $S = R/(f_1, \cdots, f_k)$. Suppose $\dim S = d$. Then S is regular if and only if the images of the f_i's in $\mathfrak{m}/\mathfrak{m}^2$ span a subspace of dimension $n - d$. These images are typically denoted by $df_1, \cdots, df_k$.*

For example, if $k = 1$ and $f = f_1 \neq 0$, then $\dim S = n - 1$. S is regular if and only if f is not zero in $\mathfrak{m}/\mathfrak{m}^2$, i.e. $f \notin \mathfrak{m}^2$. In the case $R = k[x_1, \cdots, x_n]_\mathfrak{m}$, $f \in \mathfrak{m}^2$ if and only if $\frac{\partial f}{\partial x_i}(0) = 0$ for all i.

Proposition 25.8. *A regular local ring R is a domain.*

Proof. We know that $\mathrm{gr}_\mathfrak{m} R \cong k[x_1, \cdots, x_n]$ is a domain. Given $f \in R$ not equal to 0, then there exists a unique a such that $f \in \mathfrak{m}^a - \mathfrak{m}^{a+1}$ (because $\cap \mathfrak{m}^n = 0$). Then we define $\mathrm{in}(f) \in \mathfrak{m}^a/\mathfrak{m}^{a+1}$ to be the image of f in $\mathfrak{m}^a/\mathfrak{m}^{a+1}$. We see that $\mathrm{in}(fg) = \mathrm{in}(f)\,\mathrm{in}(g)$ is non-zero for f, g non-zero, so fg is non-zero. ■

In fact, regular local rings are UFDs, but this is a hard theorem of Serre.

Finally we will talk about completions. Let A be an abelian group and $A = A_0 \supset A_1 \supset \cdots$ be a sequence of subgroups. This defines a topology on A, where a sequence $\{x_k\}$ converges to some b if and only if for any n, there exists N such that $k \geq N$ implies $x_k - b \in A_n$. This is Hausdorff if and only if $\cap_{k \geq 0} A_k = \{0\}$. Cauchy sequences are defined similarly.

The completion $\widehat{A}$ is a complete and Hausdorff space produced out of A. The construction is standard, namely the set of all Cauchy sequences in A modulo the equivalence relation $\{x_n\} \sim \{y_n\}$ if $\{x_n - y_n\}$ converges to 0. There is a group homomorphism $A \to \widehat{A}$ sending a to the constant sequence with dense image, and the kernel is $\cap_{k \geq 0} A_k$.

Algebraically, for each k we have surjections $A/A_{k+1} \to A/A_k$. so we can take the inverse limit

$$\varprojlim A/A_k$$

Concretely this is the set of tuples $(a_0, a_1, \cdots)$ such that the image of a_{k+1} in A/A_k is a_k. There is a natural map $A \to \varprojlim A/A_k$, with kernel $\cap_{k \geq 0} A_k$. This identifies the completion with $\varprojlim A/A_k$.

Say $0 \to A' \to A \to A'' \to 0$ is an exact sequence of abelian groups. Start with a decreasing sequence of subgroups $A_k \subset A$. This induces a sequence A''_k in A'', and $A'_k = A_k \cap A'$ in A'. With these filtration we have an exact sequence

$$0 \to \widehat{A'} \to \widehat{A} \to \widehat{A''} \to 0.$$

Note that for a fixed k, we have $0 \to A_k \to A$, and the filtration induces a filtration on A_k. Then $\widetilde{A}/\widehat{A_k} \cong A/A_k$.

The basic example in ring theory is the filtration $\{I^n\}$ in R where I is an ideal. If M is an R-module then we can take $\{I^n M\}$. It is a basic fact that $\widehat{R}$ is a ring, and $\widehat{M}$ is a $\widehat{R}$-module.

Example 25.1. Let $R = \mathbf{Z}$ and $I = (p)$. Then $\widehat{R}$ is usually denoted by $\mathbf{Z}_p$, the p-adic integers. Let $R = k[x_1, \cdots, x_n]$ and $I = \mathfrak{m} = (x_1, \cdots, x_n)$, then $\widehat{R} = k[\![x_1, \cdots, x_n]\!]$ the formal power series.

Some properties:

(1) If R is noetherian, then $\widehat{R}$ is noetherian. The main point is that $\mathrm{gr}_{\widehat{I}} \widehat{R} \cong \mathrm{gr}_I R$, which is then seen to be noetherian.

(2) If R is noetherian, M is finitely generated, then

$$0 \to M' \to M \to M'' \to 0$$

is exact implies

$$0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$$

is exact. The proof is to use Artin-Rees lemma to identify filtrations and apply the abelian group fact.

(3) If R is noetherian, M is finitely generated, then $\widehat{M} = M \otimes_R \widehat{R}$. This is obvious when $M = R^n$ since both sides are $\widehat{R}^n$. In general, we pick

$$0 \to K \to R^n \to M \to 0$$

where K is finitely generated by noetherianness. Then

$$K \otimes_R \widehat{R} \to \widehat{R}^n \to M \otimes_R \widehat{R} \to 0$$

is exact, and on the other hand

$$0 \to \widehat{K} \to \widehat{R}^n \to \widehat{M} \to 0$$

is exact. There are natural vertical maps, and by diagram chase we get that $M \otimes_R \widehat{R} \to \widehat{M}$ is surjective for all finitely generated R-module, in particular this is true for K. Chasing diagrams again gives the desired isomorphism.

(4) For R noetherian, $\widehat{R}$ is R-flat, because flatness can be checked only against finitely generated modules.

(5) Let $\mathfrak{m}$ be a maximal ideal and let $\widehat{R}$ be the completion in the $\mathfrak{m}$-adic topology. Then $\widehat{R}$ is a local ring, because for $r \in \mathfrak{m}$,

$$\frac{1}{1+r} = 1 - r + r^2 - \cdots$$

which converges in $\widehat{R}$. Thus $1 + r$ is a unit, which implies all things not in $\mathfrak{m}$ are units.

(6) Assume R is local. Then $\dim R = \dim \widehat{R}$. R is regular if and only if $\widehat{R}$ is regular. If there exists a field k in R mapping isomorphically to $R/\mathfrak{m}$, then $\widehat{R}$ is regular if and only if $\widehat{R}$ is the power series $k[\![x_1, \cdots, x_n]\!]$.

The Cohen structure theorem says that if R is local noetherian with maximal ideal $\mathfrak{m}$ and residue field k, and R is complete with respect to the $\mathfrak{m}$-adic topology, and most importantly if R contains a subring which is a field, then R contains a subring isomorphic to k via $R \to R/\mathfrak{m} = k$. This is called a coefficient field. Then $R \cong k[\![x_1, \cdots, x_n]\!]/I$.

What does this mean? Let M be a smooth or complex manifold. Then locally they all look like $\mathbf{R}^n$ or $\mathbf{C}^n$. In algebraic geometry, if X is an affine variety, it has local rings $A(X)_{\mathfrak{m}}$, but they don't look alike. If $A(X)_{\mathfrak{m}}$ is regular, then $\mathrm{gr}_{\mathfrak{m}} A(X)_{\mathfrak{m}}$ and completions $\widehat{A(X)_{\mathfrak{m}}}$ do look alike.