Commutative algebra

Excerpted and modified from the Stacks Project
(principal author: Johan de Jong) by David Savitt

Contents

Homological algebra

Introduction

These are the notes for a one-semester course in commutative algebra. They have been created by copying, rearranging, and modifying portions of the Stacks Project, `http://stacks.math.columbia.edu`, and especially parts of the chapter entitled "Commutative Algebra".

1. Finiteness conditions

Definition 1.1. Let R be a ring. Let M be an R-module.

(1) We say M is a *finite R-module*, or a *finitely generated R-module* if there exists a surjection $R^{\oplus n} \to M$ for some $n \in \mathbf{N}$.
(2) We say M is a *finitely presented R-module* or an *R-module of finite presentation* if there exist integers $n, m \in \mathbf{N}$ and an exact sequence

$$R^{\oplus m} \longrightarrow R^{\oplus n} \longrightarrow M \longrightarrow 0.$$

Informally, M is a finitely presented R-module if and only if it is finitely generated and the module of relations among these generators is finitely generated as well. A choice of an exact sequence as in the definition is called a *presentation* of M.

The *snake lemma* and its variants reside naturally in the setting of abelian categories.

Lemma 1.2. *Suppose given a commutative diagram*

$$\begin{tikzcd} & X \arrow[r] \arrow[d, "\alpha"] & Y \arrow[r] \arrow[d, "\beta"] & Z \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & U \arrow[r] & V \arrow[r] & W & \end{tikzcd}$$

of abelian groups with exact rows, then there is a canonical exact sequence

$$\ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma)$$

Moreover, if $X \to Y$ is injective, then the first map is injective, and if $V \to W$ is surjective, then the last map is surjective.

Lemma 1.3. *Let R be a ring. Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence of R-modules.

(1) *If M_1 and M_3 are finite R-modules, then M_2 is a finite R-module.*
(2) *If M_1 and M_3 are finitely presented R-modules, then M_2 is a finitely presented R-module.*

(3) *If M_2 is a finite R-module, then M_3 is a finite R-module.*
(4) *If M_2 is a finitely presented R-module and M_1 is a finite R-module, then M_3 is a finitely presented R-module.*
(5) *If M_3 is a finitely presented R-module and M_2 is a finite R-module, then M_1 is a finite R-module.*

Proof. (1), (3), and (4) are easy.

Proof of (2). Assume that M_1 and M_3 are finitely presented. The argument in the proof of part (1) produces a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & R^{\oplus n} \arrow[r] \arrow[d] & R^{\oplus n+m} \arrow[r] \arrow[d] & R^{\oplus m} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & M_3 \arrow[r] & 0 \end{tikzcd}$$

with surjective vertical arrows (and where the left-hand and right-hand vertical arrows come from presentations of M_1 and M_3). By the snake lemma we obtain a short exact sequence

$$0 \to \ker(R^{\oplus n} \to M_1) \to \ker(R^{\oplus n+m} \to M_2) \to \ker(R^{\oplus m} \to M_3) \to 0$$

By since the two modules are finite, the middle one is finite too, by (1). By (4) we see that M_2 is of finite presentation.

Proof of (5). Assume M_3 is finitely presented and M_2 finite. Choose a presentation

$$R^{\oplus m} \to R^{\oplus n} \to M_3 \to 0$$

There exists a map $R^{\oplus n} \to M_2$ such that the solid diagram

$$\begin{tikzcd} & R^{\oplus m} \arrow[r] \arrow[d, dotted] & R^{\oplus n} \arrow[r] \arrow[d] & M_3 \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & M_3 \arrow[r] & 0 \end{tikzcd}$$

commutes. Since the composite map $R^{\oplus m} \to M_3$ is the zero map we obtain the dotted arrow. By the snake lemma (Lemma 1.2) we see that we get an isomorphism

$$\mathrm{coker}(R^{\oplus m} \to M_1) \cong \mathrm{coker}(R^{\oplus n} \to M_2)$$

Since M_2 is finite by hypothesis, so is $\mathrm{coker}(R^{\oplus n} \to M_2)$, and therefore so also is $\mathrm{coker}(R^{\oplus m} \to M_1)$. Since $\mathrm{im}(R^{\oplus m} \to M_1)$ is finite by (3), we see that M_1 is finite by part (1). $\square$

Definition 1.4. Let $R \to S$ be a ring map.

(1) We say $R \to S$ is of *finite type*, or that S *is a finite type R-algebra* if there exists an $n \in \mathbf{N}$ and an surjection of R-algebras $R[x_1, \ldots, x_n] \to S$.
(2) We say $R \to S$ is of *finite presentation* if there exist integers $n, m \in \mathbf{N}$ and polynomials $f_1, \ldots, f_m \in R[x_1, \ldots, x_n]$ and an isomorphism of R-algebras $R[x_1, \ldots, x_n]/(f_1, \ldots, f_m) \cong S$.

Informally, $R \to S$ is of finite presentation if and only if S is finitely generated as an R-algebra and the ideal of relations among the generators is finitely generated. A choice of a surjection $R[x_1, \ldots, x_n] \to S$ as in the definition is sometimes called a *presentation* of S.

Exercise 1.5. Suppose that $R \to S$ is of finite presentation. Then any surjection $\psi\colon R[x_1, \ldots, x_n] \to S$ is a presentation of S, i.e., has finitely generated kernel. (Hint: if $\psi' : R[y_1, \ldots, y_m] \to S$ is any presentation, construct another presentation $R[x_1, \ldots, x_n, y_1, \ldots, y_m] \to S$ that factors through both ψ and ψ'.)

Definition 1.6. Let $\varphi : R \to S$ be a ring map. We say $\varphi : R \to S$ is *finite* if S is finite as an R-module.

Lemma 1.7. *Let $R \to S$ be a finite ring map. Let M be an S-module. Then M is finite as an R-module if and only if M is finite as an S-module.*

Proof. The "only if" direction is trivial. To see the "if" direction assume that M is finite as an S-module. Pick $x_1, \ldots, x_n \in S$ which generate S as an R-module. Pick $y_1, \ldots, y_m \in M$ which generate M as an S-module. Then $x_i y_j$ generate M as an R-module. □

Corollary 1.8. *Suppose that $R \to S$ and $S \to T$ are finite ring maps. Then $R \to T$ is finite.*

2. Colimits

Definition 2.1.

(1) A *partially ordered set* is a set I together with a relation $\leq$ which is transitive (if $i \leq j$ and $j \leq k$ then $i \leq k$) and reflexive ($i \leq i$ for all $i \in I$).
(2) A *directed set* $(I, \leq)$ is a partially ordered set $(I, \leq)$ such that I is not empty and such that $\forall i, j \in I$, there exists $k \in I$ with $i \leq k, j \leq k$.

It is customary to drop the $\leq$ from the notation when talking about a partially ordered set (that is, one speaks of the partially ordered set I rather than of the partially ordered set $(I, \leq)$).

The notion "partially ordered set" is commonly abbreviated as "poset".

Definition 2.2. Let $(I, \leq)$ be a partially ordered set. A *system* (M_i, μ_{ij}) *of R-modules over I* consists of a family of R-modules $\{M_i\}_{i \in I}$ indexed by I and a family of R-module maps $\{\mu_{ij} : M_i \to M_j\}_{i \leq j}$ such that for all $i \leq j \leq k$

$$\mu_{ii} = \mathrm{id}_{M_i} \quad \mu_{ik} = \mu_{jk} \circ \mu_{ij}$$

We say (M_i, μ_{ij}) is a *directed system* if I is a directed set.

Definition 2.3. Let (M_i, μ_{ij}) be a system of R-modules over I. A *colimit* of this system is an R-module M together with maps $\mu_i : M_i \to M$ for all $i \in I$ satisfying $\mu_i = \mu_j \circ \mu_{ij}$ for all $i \leq j$, with the following universal property: for any R-module N together with maps $\nu_i : M_i \to N$ such that $\nu_i = \nu_j \circ \mu_{ij}$ for all $i \leq j$, there exists a unique map $\psi : M \to N$ such that $\nu_i = \psi \circ \mu_i$ for all i. We write $M = \operatorname{colim} M_i$.

If the system (M_i, μ_{ij}) is directed, we may say *direct limit* in lieu of colimit.

Colimits always exist. We give two constructions, one which is general, and a second which is simpler but applies only to the directed case. The proofs are straightforward and we omit them.

Lemma 2.4. *Let (M_i, μ_{ij}) be a system of R-modules over the partially ordered set I. The colimit of the system (M_i, μ_{ij}) is the quotient R-module $(\bigoplus_{i\in I} M_i)/Q$ where Q is the R-submodule generated by all elements*

$$\iota_i(x_i) - \iota_j(\mu_{ij}(x_i))$$

where $\iota_i : M_i \to \bigoplus_{i\in I} M_i$ is the natural inclusion.

Lemma 2.5. *Let (M_i, μ_{ij}) be a system of R-modules over the partially ordered set I. Assume that I is directed. The colimit of the system (M_i, μ_{ij}) is canonically isomorphic to the module M defined as follows:*

$$M = \left(\coprod\nolimits_{i\in I} M_i\right) / \sim$$

where for $m \in M_i$ and $m' \in M_{i'}$ we have

$$m \sim m' \Leftrightarrow \mu_{ij}(m) = \mu_{i'j}(m') \text{ for some } j \geq i, i'.$$

The canonical maps $\mu_i : M_i \to M$ are induced by the canonical maps $M_i \to \coprod_{i\in I} M_i$.

Corollary 2.6. *Let (M_i, μ_{ij}) be a directed system. Let $M = \operatorname{colim} M_i$ with $\mu_i : M_i \to M$. Then, $\mu_i(x_i) = 0$ for $x_i \in M_i$ if and only if there exists $j \geq i$ such that $\mu_{ij}(x_i) = 0$.*

Proof. This is clear from the description of the directed colimit in Lemma 2.5. $\square$

Definition 2.7. Let (M_i, μ_{ij}), (N_i, ν_{ij}) be systems of R-modules over the same partially ordered set I. A *homomorphism of systems* Φ from (M_i, μ_{ij}) to (N_i, ν_{ij}) is by definition a family of R-module homomorphisms $\phi_i : M_i \to N_i$ such that $\phi_j \circ \mu_{ij} = \nu_{ij} \circ \phi_i$ for all $i \leq j$.

This is the same notion as a transformation of functors between the associated diagrams $M : I \to \text{Mod}_R$ and $N : I \to \text{Mod}_R$, in the language of categories.

Lemma 2.8. *Let (M_i, μ_{ij}), (N_i, ν_{ij}) be systems of R-modules over the same partially ordered set. A morphism of systems $\Phi = (\phi_i)$ from (M_i, μ_{ij}) to (N_i, ν_{ij}) induces a unique homomorphism*

$$\operatorname{colim} \phi_i : \operatorname{colim} M_i \longrightarrow \operatorname{colim} N_i$$

such that

$$\begin{tikzcd} M_i \arrow[r] \arrow[d, "\phi_i"'] & \operatorname{colim} M_i \arrow[d, "\operatorname{colim} \phi_i"] \\ N_i \arrow[r] & \operatorname{colim} N_i \end{tikzcd}$$

commutes for all $i \in I$.

Proof. Use the explicit description of $\operatorname{colim} M_i$ and $\operatorname{colim} N_i$ in Lemma 2.4. $\square$

Exercise 2.9. (Directed colimits are exact.) Let I be a directed partially ordered set. Let (L_i, λ_{ij}), (M_i, μ_{ij}), and (N_i, ν_{ij}) be systems of R-modules over I.

Let $\varphi_i : L_i \to M_i$ and $\psi_i : M_i \to N_i$ be morphisms of systems over I. Assume that for all $i \in I$ the sequence of R-modules

$$L_i \xrightarrow{\varphi_i} M_i \xrightarrow{\psi_i} N_i$$

is a complex with homology H_i. Then the R-modules H_i form a system over I, the sequence of R-modules

$$\mathrm{colim}_i\, L_i \xrightarrow{\varphi} \mathrm{colim}_i\, M_i \xrightarrow{\psi} \mathrm{colim}_i\, N_i$$

is a complex as well, and denoting H its homology we have

$$H = \mathrm{colim}_i\, H_i.$$

Example 2.10. (Taking colimits is not exact in general.) Consider the partially ordered set $I = \{a, b, c\}$ with $a < b$ and $a < c$ and no other strict inequalities. A system $(M_a, M_b, M_c, \mu_{ab}, \mu_{ac})$ over I consists of three R-modules M_a, M_b, M_c and two R-module homomorphisms $\mu_{ab} : M_a \to M_b$ and $\mu_{ac} : M_a \to M_c$. The colimit of the system is just

$$M := \mathrm{colim}_{i \in I}\, M_i = \mathrm{coker}(M_a \to M_b \oplus M_c)$$

where the map is $\mu_{ab} \oplus -\mu_{ac}$.

Consider the map of systems $(0, \mathbf{Z}, \mathbf{Z}, 0, 0) \to (\mathbf{Z}, \mathbf{Z}, \mathbf{Z}, 1, 1)$. The colimit of the first system is $\mathbf{Z} \oplus \mathbf{Z}$ and the colimit of the second is $\mathbf{Z}$. Thus the associated map of colimits $\mathbf{Z} \oplus \mathbf{Z} \to \mathbf{Z}$ is not injective, even though the map of systems is injective on each object. Hence the result of Lemma 2.9 is false for general systems.

Definition 2.11. Let R be a ring. Let M be an R-module. Let $n \geq 0$ and $x_i \in M$ for $i = 1, \ldots, n$. A *relation* between $x_1, \ldots, x_n$ in M is a sequence of elements $f_1, \ldots, f_n \in R$ such that $\sum_{i=1,\ldots,n} f_i x_i = 0$.

Lemma 2.12. *Let R be a ring and let M be an R-module. Then M is the colimit of a directed system (M_i, μ_{ij}) of R-modules with all M_i finitely presented R-modules.*

Proof. Let I be the set of pairs (S, E) where

- $S \subset M$ is any finite subset, and
- E is a finite collection of relations among the elements of S,

ordered by inclusion. So each $e \in E$ consists of a vector of elements $f_{e,s} \in R$ such that $\sum f_{e,s} s = 0$. Let $M_{S,E}$ be the cokernel of the map

$$R^{\#E} \longrightarrow R^{\#S}, \quad (g_e)_{e \in E} \longmapsto (\sum g_e f_{e,s})_{s \in S}.$$

The reader can check that the colimit of the directed system $(M_{S,E})$ is M. $\square$

Recall that if R is a ring, and M, N are R-modules, then

$$\mathrm{Hom}_R(M, N) = \{\varphi : M \to N\}$$

is the set of R-linear maps from M to N. This set comes with the structure of an abelian group by setting $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$, as usual. In fact, $\mathrm{Hom}_R(M, N)$ is also an R-module via the rule $(x\varphi)(m) = x\varphi(m) = \varphi(xm)$.

Exercise 2.13. Show that M is of finite presentation if and only if $\mathrm{Hom}_R(M,-)$ commutes with direct limits, i.e., if and only if

$$\operatorname{colim} \mathrm{Hom}_R(M, N_i) \cong \mathrm{Hom}_R(M, \operatorname{colim} N_i)$$

for any directed system (N_i).

3. Tensor products

Definition 3.1. Let R be a ring, M, N, P be three R-modules. A mapping $f : M \times N \to P$ (where $M \times N$ is viewed only as Cartesian product of two R-modules) is said to be *R-bilinear* if for each $x \in M$ the mapping $y \mapsto f(x, y)$ of N into P is R-linear, and for each $y \in N$ the mapping $x \mapsto f(x, y)$ is also R-linear.

Lemma 3.2. *Let M, N be R-modules. Then there exists a pair (T, g) where T is an R-module, and $g : M \times N \to T$ an R-bilinear mapping, with the following universal property: For any R-module P and any R-bilinear mapping $f : M \times N \to P$, there exists a unique R-linear mapping $\tilde{f} : T \to P$ such that $f = \tilde{f} \circ g$. In other words, the following diagram commutes:*

$$\begin{tikzcd}
M \times N \arrow[rr, "f"] \arrow[dr, "g"'] & & P \\
& T \arrow[ur, "f'"'] &
\end{tikzcd}$$

Moreover, if (T, g) and (T', g') are two pairs with this property, then there exists a unique isomorphism $j : T \to T'$ such that $j \circ g = g'$.

The R-module T which satisfies the above universal property is called the *tensor product* of R-modules M and N, denoted as $M \otimes_R N$.

Proof. We give the construction of such an R-module T. Let T be the quotient module P/Q, where P is the free R-module $R^{(M\times N)}$ and Q is the R-module generated by all elements of the following types: $(x \in M, y \in N)$

$$\begin{aligned}
(x + x', y) - (x, y) - (x', y),\\
(x, y + y') - (x, y) - (x, y'),\\
(ax, y) - a(x, y),\\
(x, ay) - a(x, y)
\end{aligned}$$

Let $\pi : M \times N \to T$ denote the natural map. This map is R-bilinear, as implied by the above relations when we check the bilinearity conditions. Denote the image $\pi(x, y) = x \otimes y$. The reader can check that T has the desired universal property. $\square$

Exercise 3.3. Let M, N, P be R-modules, then the bilinear maps

$$\begin{aligned}
(x, y) &\mapsto y \otimes x\\
(x + y, z) &\mapsto x \otimes z + y \otimes z\\
(r, x) &\mapsto rx
\end{aligned}$$

induce unique isomorphisms

$$\begin{aligned} M \otimes_R N &\to N \otimes_R M, \\ (M \oplus N) \otimes_R P &\to (M \otimes_R P) \oplus (N \otimes_R P), \\ R \otimes_R M &\to M \end{aligned}$$

We may generalize the tensor product of two R-modules to finitely many R-modules, and set up a correspondence between the multi-tensor product with multilinear mappings.

LEMMA 3.4. *The homomorphisms*

$$(M \otimes_R N) \otimes_R P \to M \otimes_R N \otimes_R P \to M \otimes_R (N \otimes_R P)$$

such that $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ *and* $g(x \otimes y \otimes z) = x \otimes (y \otimes z)$, $x \in M, y \in N, z \in P$ *are well-defined and are isomorphisms.*

Doing induction we see that this extends to multi-tensor products. Combined with Exercise 3.3 we see that the tensor product operation on the category of R-modules is associative, commutative and distributive.

LEMMA 3.5. *For any three R-modules M, N, P,*

$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$

PROOF. An R-linear map $\hat{f} \in \mathrm{Hom}_R(M \otimes_R N, P)$ corresponds to an R-bilinear map $f : M \times N \to P$. For each $x \in M$ the mapping $y \mapsto f(x, y)$ is R-linear by the universal property. Thus f corresponds to a map $\phi_f : M \to \mathrm{Hom}_R(N, P)$, easily checked to be R-linear.

Conversely, any $f \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$ defines an R-bilinear map $M \times N \to P$, namely $(x, y) \mapsto f(x)(y)$. So this is a natural one-to-one correspondence between the two modules $\mathrm{Hom}_R(M \otimes_R N, P)$ and $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. □

LEMMA 3.6 (Tensor products commute with colimits). *Let (M_i, μ_{ij}) be a system over the partially ordered set I. Let N be an R-module. Then*

$$\mathrm{colim}(M_i \otimes N) \cong (\mathrm{colim}\, M_i) \otimes N.$$

Moreover, the isomorphism is induced by the homomorphisms $\mu_i \otimes 1 : M_i \otimes N \to M \otimes N$ *where* $M = \mathrm{colim}_i M_i$ *with natural maps* $\mu_i : M_i \to M$.

PROOF. This is a special case of a very general phenomenon. Lemma 3.5 shows that the functor $- \otimes_R N$ is left adjoint to the left exact functor $\mathrm{Hom}_R(N, -)$. But any left adjoint functor commutes with all colimits. We make this precise below. □

DEFINITION 3.7. Let $\mathcal{C}$, $\mathcal{D}$ be categories. Let $u : \mathcal{C} \to \mathcal{D}$ and $v : \mathcal{D} \to \mathcal{C}$ be functors. We say that u is a *left adjoint* of v, or that v is a *right adjoint* to u if there are bijections

$$\mathrm{Mor}_{\mathcal{D}}(u(X), Y) \longrightarrow \mathrm{Mor}_{\mathcal{C}}(X, v(Y))$$

functorial in $X \in \mathrm{Ob}(\mathcal{C})$, and $Y \in \mathrm{Ob}(\mathcal{D})$.

LEMMA 3.8. *Let u be a left adjoint to v as in Definition 3.7. Suppose that* $M : \mathcal{I} \to \mathcal{C}$ *is a system, and suppose that* $\mathrm{colim}_{\mathcal{I}} M$ *exists in* $\mathcal{C}$. *Then* $u(\mathrm{colim}_{\mathcal{I}} M) = \mathrm{colim}_{\mathcal{I}}\, u \circ M$. *In other words, u commutes with (representable) colimits.*

Proof. A morphism from a colimit into an object is the same as a compatible system of morphisms from the constituents of the limit into the object. So

$$\begin{array}{rcl} \mathrm{Mor}_{\mathcal{D}}(u(\mathrm{colim}_{i\in\mathcal{I}} M_i), Y) & = & \mathrm{Mor}_{\mathcal{C}}(\mathrm{colim}_{i\in\mathcal{I}} M_i, v(Y)) \\ & = & \mathrm{colim}_{\mathcal{I}} \mathrm{Mor}_{\mathcal{C}}(M_i, v(Y)) \\ & = & \mathrm{colim}_{\mathcal{I}} \mathrm{Mor}_{\mathcal{D}}(u(M_i), Y) \\ & = & \mathrm{Mor}_{\mathcal{D}}(\mathrm{colim}_{i\in\mathcal{I}} u(M_i), Y) \end{array}.$$

□

Since cokernels are a colimit, it follows in particular that left adjoint functors are always right-exact (in contexts where exactness makes sense).

Corollary 3.9. *Let u be a left adjoint to v as in Definition 3.7, and where $\mathcal{C}$, $\mathcal{D}$ are abelian categories. Then u is right-exact, in the sense that if*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

is a right-exact sequence in $\mathcal{C}$ then

$$u(M_1) \xrightarrow{u(f)} u(M_2) \xrightarrow{u(g)} u(M_3) \to 0$$

is a right-exact sequence in $\mathcal{D}$.

We re-state this for tensor products.

Lemma 3.10. *Let*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

be an exact sequence of R-modules and homomorphisms, and let N be any R-module. Then the sequence

$$M_1 \otimes N \xrightarrow{f\otimes 1} M_2 \otimes N \xrightarrow{g\otimes 1} M_3 \otimes N \to 0 \tag{3.11}$$

is exact. In other words, the functor $-\otimes_R N$ is right exact.

Remark 3.12. However, tensor product does NOT preserve exact sequences in general. In other words, if $M_1 \to M_2 \to M_3$ is exact, then it is not necessarily true that $M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N$ is exact for arbitrary R-module N.

Example 3.13. Consider the injective map $2 : \mathbf{Z} \to \mathbf{Z}$ viewed as a map of $\mathbf{Z}$-modules. Let $N = \mathbf{Z}/2$. Then the induced map $\mathbf{Z} \otimes \mathbf{Z}/2 \to \mathbf{Z} \otimes \mathbf{Z}/2$ is NOT injective. This is because for $x \otimes y \in \mathbf{Z} \otimes \mathbf{Z}/2$,

$$(2 \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$$

Therefore the induced map is the zero map while $\mathbf{Z} \otimes N \neq 0$.

Definition 3.14. For R-modules N, if the functor $-\otimes_R N$ is exact, i.e. tensoring with N preserves all exact sequences, then N is said to be *flat* R-module.

Remark 3.15. In the above setup, the right adjoint functor v always commutes with (representable) limits, and is thus left-exact. This applies in particular to the functor $\mathrm{Hom}(N, -)$, proving its left-exactness.

Exercise 3.16. Let R be a ring. Let M and N be R-modules.

(1) If N and M are finite, then so is $M \otimes_R N$.
(2) If N and M are finitely presented, then so is $M \otimes_R N$.

EXERCISE 3.17. An abelian group N is called an (A, B)-*bimodule* if it is both an A-module and a B-module, and the actions $A \to End(M)$ and $B \to End(M)$ are compatible in the sense that $(ax)b = a(xb)$ for all $a \in A, b \in B, x \in N$. Usually we denote it as ${}_AN_B$. For A-module M, B-module P and (A, B)-bimodule N, the modules $(M \otimes_A N) \otimes_B P$ and $M \otimes_A (N \otimes_B P)$ can both be given (A, B)-bimodule structure, and moreover

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

4. Ext and projective modules

In this section we do a tiny bit of homological algebra. Given maps $a : M \to M'$ and $b : N \to N'$ of R-modules, we can pre-compose and post-compose homomorphisms by a and b. This leads to the following commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(M', N) \arrow[r, "b\circ-"'] \arrow[d, "-\circ a"'] & \mathrm{Hom}_R(M', N') \arrow[d, "-\circ a"] \\
\mathrm{Hom}_R(M, N) \arrow[r, "b\circ-"] & \mathrm{Hom}_R(M, N')
\end{tikzcd}$$

In fact, the maps in this diagram are R-module maps. Thus Hom_R defines an additive functor

$$\mathrm{Mod}_R^{\mathrm{opp}} \times \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_R, \quad (M, N) \longmapsto \mathrm{Hom}_R(M, N).$$

LEMMA 4.1. *Exactness and* Hom_R. *Let R be a ring.*

(1) *Let $0 \to M' \to M \to M''$ be a complex of R-modules. Then $0 \to M' \to M \to M''$ is exact if and only if*

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

is exact for all R-modules N.

(2) *Let $M' \to M \to M'' \to 0$ be a complex of R-modules. Then $M' \to M \to M'' \to 0$ is exact if and only if*

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

is exact for all R-modules N.

PROOF. Elementary; or, see Remark 3.15 □

DEFINITION 4.2. Let R be a ring. An R-module P is *projective* if and only if the functor $\mathrm{Hom}_R(P, -) : \mathrm{Mod}_R \to \mathrm{Mod}_R$ is an exact functor, i.e., takes any exact complex to an exact complex. Since $\mathrm{Hom}_R(P, -)$ is already left-exact, it is equivalent that for any surjection of R-modules $M \to M''$ the map $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'')$ is surjective (this requires a short argument).

DEFINITION 4.3. Let R be a ring. An R-module I is *injective* if and only if the functor $\mathrm{Hom}_R(-, I) : \mathrm{Mod}_R \to \mathrm{Mod}_R$ is an exact functor; equivalently, given an injection of R-modules $M' \to M$ the map $\mathrm{Hom}_R(M, I) \to \mathrm{Hom}_R(M', I)$ is surjective.

We now construct the Ext groups as the derived functors of Hom.

Lemma 4.4. *Let R be a ring. Let M be an R-module. There exists an exact complex*
$$\cdots \to F_2 \to F_1 \to F_0 \to M \to 0.$$
with F_i free R-modules.

Definition 4.5. Let R be a ring. Let M be an R-module.

(1) A (left) *resolution* $F_\bullet \to M$ of M is an exact complex
$$\cdots \to F_2 \to F_1 \to F_0 \to M \to 0$$
of R-modules.

(2) A *resolution of M by free R-modules* is a resolution $F_\bullet \to M$ where each F_i is a free R-module.

(3) A *resolution of M by finite free R-modules* is a resolution $F_\bullet \to M$ where each F_i is a finite free R-module.

We often use the notation $F_\bullet$ to denote a complex of R-modules
$$\cdots \to F_i \to F_{i-1} \to \ldots$$
In this case we often use d_i or $d_{F,i}$ to denote the map $F_i \to F_{i-1}$. In this section we are always going to assume that F_0 is the last nonzero term in the complex. The *ith homology group of the complex $F_\bullet$* is the group $H_i = \ker(d_{F,i})/\mathrm{im}(d_{F,i+1})$. A *map of complexes* $\alpha : F_\bullet \to G_\bullet$ is given by maps $\alpha_i : F_i \to G_i$ such that $\alpha_{i-1} \circ d_{F,i} = d_{G,i-1} \circ \alpha_i$. Such a map induces a map on homology $H_i(\alpha) : H_i(F_\bullet) \to H_i(G_\bullet)$. If $\alpha, \beta : F_\bullet \to G_\bullet$ are maps of complexes, then a *homotopy* between α and β is given by a collection of maps $h_i : F_i \to G_{i+1}$ such that $\alpha_i - \beta_i = d_{G,i+1} \circ h_i + h_{i-1} \circ d_{F,i}$.

We will use a very similar notation regarding complexes of the form $F^\bullet$ which look like
$$\cdots \to F^i \xrightarrow{d^i} F^{i+1} \to \ldots$$
There are maps of complexes, homotopies, etc. In this case we set $H^i(F^\bullet) = \ker(d^i)/\mathrm{im}(d^{i-1})$ and we call it the *ith cohomology group*.

Lemma 4.6. *Any two homotopic maps of complexes induce the same maps on (co)homology groups.*

Lemma 4.7. *Let R be a ring. Let $M \to N$ be a map of R-modules. Let $F_\bullet \to M$ be a resolution by free R-modules and let $N_\bullet \to N$ be an arbitrary resolution. Then*

(1) *there exists a map of complexes $F_\bullet \to N_\bullet$ inducing the given map*
$$M = \mathrm{coker}(F_1 \to F_0) \to \mathrm{coker}(N_1 \to N_0) = N$$

(2) *two maps $\alpha, \beta : F_\bullet \to N_\bullet$ inducing the same map $M \to N$ are homotopic.*

Proof. Proof of (1). Because F_0 is free we can find a map $F_0 \to N_0$ lifting the map $F_0 \to M \to N$. We obtain an induced map $F_1 \to F_0 \to N_0$ which ends up in the image of $N_1 \to N_0$. Since F_1 is free we may lift this to a map $F_1 \to N_1$. This in turn induces a map $F_2 \to F_1 \to N_1$ which maps to zero into N_0. Since $N_\bullet$ is exact we see that the image of this map is contained in the image of $N_2 \to N_1$. Hence we may lift to get a map $F_2 \to N_2$. Repeat.

Proof of (2). To show that α, β are homotopic it suffices to show the difference $\gamma = \alpha - \beta$ is homotopic to zero. Note that the image of $\gamma_0 : F_0 \to N_0$ is contained in the image of $N_1 \to N_0$. Hence we may lift γ_0 to a map $h_0 : F_0 \to N_1$. Consider the map $\gamma_1' = \gamma_1 - h_0 \circ d_{F,1}$. By our choice of h_0 we see that the image of γ_1' is contained in the kernel of $N_1 \to N_0$. Since $N_\bullet$ is exact we may lift γ_1' to a map $h_1 : F_1 \to N_2$. At this point we have $\gamma_1 = h_0 \circ d_{F,1} + d_{N,2} \circ h_1$. Repeat. □

At this point we are ready to define the groups $\mathrm{Ext}^i_R(M, N)$. Namely, choose a resolution $F_\bullet$ of M by free R-modules, see Lemma 4.4. Consider the (cohomological) complex

$$\mathrm{Hom}_R(F_\bullet, N) : \mathrm{Hom}_R(F_0, N) \to \mathrm{Hom}_R(F_1, N) \to \mathrm{Hom}_R(F_2, N) \to \ldots$$

We define $\mathrm{Ext}^i_R(M, N)$ for $i \geq 0$ to be the ith cohomology group of this complex[1]. For $i < 0$ we set $\mathrm{Ext}^i_R(M, N) = 0$. Before we continue we point out that

$$\mathrm{Ext}^0_R(M, N) = \ker(\mathrm{Hom}_R(F_0, N) \to \mathrm{Hom}_R(F_1, N)) = \mathrm{Hom}_R(M, N)$$

because we can apply part (1) of Lemma 4.1 to the exact sequence $F_1 \to F_0 \to M \to 0$. The following lemma explains in what sense this is well defined (and more generally gives the functorial properties of $\mathrm{Ext}^i(-, N)$).

Lemma 4.8. *Let R be a ring. Let M_1, M_2, N be R-modules. Suppose that $F_\bullet$ is a free resolution of the module M_1, and $G_\bullet$ is a free resolution of the module M_2. Let $\varphi : M_1 \to M_2$ be a module map. Let $\alpha : F_\bullet \to G_\bullet$ be a map of complexes inducing φ on $M_1 = \mathrm{coker}(d_{F,1}) \to M_2 = \mathrm{coker}(d_{G,1})$, see Lemma 4.7. Then the induced maps*

$$H^i(\alpha) : H^i(\mathrm{Hom}_R(G_\bullet, N)) \longrightarrow H^i(\mathrm{Hom}_R(F_\bullet, N))$$

are independent of the choice of α. If φ is an isomorphism, so are all the maps $H^i(\alpha)$. If $M_1 = M_2$, $F_\bullet = G_\bullet$, and φ is the identity, so are all the maps $H_i(\alpha)$.

Proof. Another map $\beta : F_\bullet \to G_\bullet$ inducing φ is homotopic to α by Lemma 4.7. Hence the maps $\mathrm{Hom}_R(G_\bullet, N) \to \mathrm{Hom}_R(F_\bullet, N)$ are homotopic. Hence the independence result follows from Lemma 4.6.

Suppose that φ is an isomorphism. Let $\psi : M_2 \to M_1$ be an inverse. Choose $\beta : G_\bullet \to F_\bullet$ be a map inducing $\psi : M_2 = \mathrm{coker}(d_{G,1}) \to M_1 = \mathrm{coker}(d_{F,1})$, see Lemma 4.7. Now consider the map $H^i(\beta) \circ H^i(\alpha) = H^i(\alpha \circ \beta)$. By the above the map $H^i(\alpha \circ \beta)$ is the *same* as the map $H^i(\mathrm{id}_{G_\bullet}) = \mathrm{id}$. Similarly for the composition $H^i(\beta) \circ H^i(\alpha)$. Hence $H^i(\alpha)$ and $H^i(\beta)$ are inverses of each other. □

Lemma 4.9. *Let R be a ring. Let M be an R-module. Let $0 \to N' \to N \to N'' \to 0$ be a short exact sequence. Then we get a long exact sequence*

$$\begin{aligned} 0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'') \\ \to \mathrm{Ext}^1_R(M, N') \to \mathrm{Ext}^1_R(M, N) \to \mathrm{Ext}^1_R(M, N'') \to \cdots \end{aligned}$$

Proof. Pick a free resolution $F_\bullet \to M$. Since each of the F_i are free we see that we get a short exact sequence of complexes

$$0 \to \mathrm{Hom}_R(F_\bullet, N') \to \mathrm{Hom}_R(F_\bullet, N) \to \mathrm{Hom}_R(F_\bullet, N'') \to 0$$

Thus we get the long exact sequence from the snake lemma applied to this. □

[1] At this point it would perhaps be more appropriate to say "an" in stead of "the" Ext-group.

Lemma 4.10. *Let R be a ring. Let N be an R-module. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Then we get a long exact sequence*

$$\begin{aligned} 0 &\to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N) \\ &\to \mathrm{Ext}^1_R(M'', N) \to \mathrm{Ext}^1_R(M, N) \to \mathrm{Ext}^1_R(M', N) \to \ldots \end{aligned}$$

Proof. Pick sets of generators $\{m'_{i'}\}_{i' \in I'}$ and $\{m''_{i''}\}_{i'' \in I''}$ of M' and M''. For each $i'' \in I''$ choose a lift $\tilde{m}''_{i''} \in M$ of the element $m''_{i''} \in M''$. Set $F' = \bigoplus_{i' \in I'} R$, $F'' = \bigoplus_{i'' \in I''} R$ and $F = F' \oplus F''$. Mapping the generators of these free modules to the corresponding chosen generators gives surjective R-module maps $F' \to M'$, $F'' \to M''$, and $F \to M$. We obtain a map of short exact sequences

$$\begin{array}{ccccccccc} 0 & \to & M' & \to & M & \to & M'' & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & F' & \to & F & \to & F'' & \to & 0 \end{array}$$

By the snake lemma we see that the sequence of kernels $0 \to K' \to K \to K'' \to 0$ is short exact sequence of R-modules. Hence we can continue this process indefinitely. In other words we obtain a short exact sequence of resolutions fitting into the diagram

$$\begin{array}{ccccccccc} 0 & \to & M' & \to & M & \to & M'' & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & F'_\bullet & \to & F_\bullet & \to & F''_\bullet & \to & 0 \end{array}$$

Because each of the sequences $0 \to F'_n \to F_n \to F''_n \to 0$ is split exact (by construction) we obtain a short exact sequence of complexes

$$0 \to \mathrm{Hom}_R(F''_\bullet, N) \to \mathrm{Hom}_R(F_\bullet, N) \to \mathrm{Hom}_R(F'_\bullet, N) \to 0$$

by applying the $\mathrm{Hom}_R(-, N)$ functor. Thus we get the long exact sequence from the snake lemma applied to this. $\square$

There is more that would usually be said here but that will not be needed in these notes. For instance, the same Ext groups can be computed using injective resolutions of N instead of free resolutions of M. Thus one obtains a collection of *bifunctors* $\mathrm{Ext}^i(-,-)$, covariant in the second variable, contravariant in the first. Moreover, the groups $\mathrm{Ext}^i(-,-)$ have a concrete interpretation in terms of (equivalence classes of) module extensions.

Lemma 4.11. *Let R be a ring. Let M, N be R-modules. Any $x \in R$ such that either $xN = 0$, or $xM = 0$ annihilates each of the modules $\mathrm{Ext}^i_R(M, N)$.*

Proof. Pick a free resolution $F_\bullet$ of M. Since $\mathrm{Ext}^i_R(M, N)$ is defined as the cohomology of the complex $\mathrm{Hom}_R(F_\bullet, N)$ the lemma is clear when $xN = 0$. If $xM = 0$, then we see that multiplication by x on $F_\bullet$ lifts the zero map on M. Hence by Lemma 4.8 we see that it induces the same map on Ext groups as the zero map. $\square$

Lemma 4.12. *Let R be a ring. Let P be an R-module. The following are equivalent*

(1) *P is projective,*
(2) *$\mathrm{Ext}^i_R(P, M) = 0$ for every R-module M and $i > 0$,*
(3) *$\mathrm{Ext}^1_R(P, M) = 0$ for every R-module M, and*
(4) *P is a direct summand of a free R-module.*

PROOF. Assume P is projective. Choose a surjection $\pi : F \to P$ where F is a free R-module. As P is projective there exists a $i \in \mathrm{Hom}_R(P, F)$ such that $i \circ \pi = \mathrm{id}_P$. In other words $F \cong \ker(\pi) \oplus i(P)$ and we see that P is a direct summand of F.

Conversely, assume that $P \oplus Q = F$ is a free R-module. Note that the free module $F = \bigoplus_{i\in I} R$ is projective as $\mathrm{Hom}_R(F, M) = \prod_{i\in I} M$ and the functor $M \mapsto \prod_{i\in I} M$ is exact. Then $\mathrm{Hom}_R(F, -) = \mathrm{Hom}_R(P, -) \times \mathrm{Hom}_R(Q, -)$ as functors, hence both P and Q are projective. Thus (1) and (4) are equivalent.

If F is free, then it is immediate from the construction that $\mathrm{Ext}^i(F, M) = 0$ for all $i > 0$: simply choose the resolution $F_\bullet \to F$ with $F_0 = F$ and $F_i = 0$ for $i > 0$. If P is a direct summand of F, then $\mathrm{Ext}^i(P, M)$ is a direct summand of $\mathrm{Ext}^i(F, M)$, and so it vanishes as well. Therefore (4) $\Rightarrow$ (2). The implication (2) $\Rightarrow$ (3) is obvious.

Finally, if (3) holds and $M \to M''$ is a surjection with kernel M', then the long exact sequence of Ext groups $\mathrm{Ext}^i(P, -)$ associated to the short exact sequence $0 \to M' \to M \to M'' \to 0$ gives an exact complex $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'') \to \mathrm{Ext}^1(P, M')$. The latter group vanishes by (3), so that $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$ is surjective and (1) holds. $\square$

5. Tor and flatness

Next we discuss the Tor groups, which do for the bifunctor $- \otimes_R -$ what the Ext functors do for $\mathrm{Hom}_R(-, -)$. Suppose that R is a ring and that M, N are two R-modules. Choose a resolution $F_\bullet$ of M by free R-modules. Consider the homological complex

$$F_\bullet \otimes_R N : \cdots \to F_2 \otimes_R N \to F_1 \otimes_R N \to F_0 \otimes_R N$$

We define $\mathrm{Tor}_i^R(M, N)$ to be the ith homology group of this complex. The following lemma explains in what sense this is well defined.

LEMMA 5.1. *Let R be a ring and let M be an R-module. Suppose that $0 \to N' \to N \to N'' \to 0$ is a short exact sequence of R-modules. There exists a long exact sequence*

$$\begin{gathered}\cdots \to \mathrm{Tor}_1^R(M, N') \to \mathrm{Tor}_1^R(M, N) \to \mathrm{Tor}_1^R(M, N'') \to \\ M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0\end{gathered}$$

PROOF. The proof of this is the same as the proof of Lemma 4.9. $\square$

It is obvious that one could proceed equally well by applying $M \otimes_R -$ to a free resolution of N, and that one obtains in this manner groups canonically isomorphic to $\mathrm{Tor}_i^R(N, M)$. Less obviously, the groups obtained in this manner are canonically the same as the ones obtained above; equivalently, $\mathrm{Tor}_i^R(M, N)$ and $\mathrm{Tor}_i^R(N, M)$ are canonically isomorphic. We now explain this.

Consider a homological double complex of R-modules

$$\begin{tikzcd}
\cdots \arrow[r, "d"] & A_{2,0} \arrow[r, "d"] & A_{1,0} \arrow[r, "d"] & A_{0,0} \\
\cdots \arrow[r, "d"] & A_{2,1} \arrow[r, "d"] \arrow[u, "\delta"] & A_{1,1} \arrow[r, "d"] \arrow[u, "\delta"] & A_{0,1} \arrow[u, "\delta"] \\
\cdots \arrow[r, "d"] & A_{2,2} \arrow[r, "d"] \arrow[u, "\delta"] & A_{1,2} \arrow[r, "d"] \arrow[u, "\delta"] & A_{0,2} \arrow[u, "\delta"] \\
& \vdots \arrow[u, "\delta"] & \vdots \arrow[u, "\delta"] & \vdots \arrow[u, "\delta"]
\end{tikzcd}$$

This means that $d_{i,j} : A_{i,j} \to A_{i-1,j}$ and $\delta_{i,j} : A_{i,j} \to A_{i,j-1}$ have the following properties

(1) Any composition of two $d_{i,j}$ is zero. In other words the rows of the double complex are complexes.
(2) Any composition of two $\delta_{i,j}$ is zero. In other words the columns of the double complex are complexes.
(3) For any pair (i, j) we have $\delta_{i-1,j} \circ d_{i,j} = d_{i,j-1} \circ \delta_{i,j}$. In other words, all the squares commute.

The correct thing to do is to associate a spectral sequence to any such double complex. However, for the current application we can get away with doing something slightly easier.

Namely, for the purposes of this section only, given a double complex $(A_{\bullet,\bullet}, d, \delta)$ set $R(A)_j = \mathrm{coker}(A_{1,j} \to A_{0,j})$ and $U(A)_i = \mathrm{coker}(A_{i,1} \to A_{i,0})$. (The letters R and U are meant to suggest Right and Up.) We endow $R(A)_\bullet$ with the structure of a complex using the maps δ. Similarly we endow $U(A)_\bullet$ with the structure of a complex using the maps d. In other words we obtain the following huge commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r, "d"] & U(A)_2 \arrow[r, "d"] & U(A)_1 \arrow[r, "d"] & U(A)_0 & \\
\cdots \arrow[r, "d"] & A_{2,0} \arrow[r, "d"] \arrow[u] & A_{1,0} \arrow[r, "d"] \arrow[u] & A_{0,0} \arrow[r] \arrow[u] & R(A)_0 \\
\cdots \arrow[r, "d"] & A_{2,1} \arrow[r, "d"] \arrow[u, "\delta"] & A_{1,1} \arrow[r, "d"] \arrow[u, "\delta"] & A_{0,1} \arrow[r] \arrow[u, "\delta"] & R(A)_1 \arrow[u, "\delta"] \\
\cdots \arrow[r, "d"] & A_{2,2} \arrow[r, "d"] \arrow[u, "\delta"] & A_{1,2} \arrow[r, "d"] \arrow[u, "\delta"] & A_{0,2} \arrow[r] \arrow[u, "\delta"] & R(A)_2 \arrow[u, "\delta"] \\
& \vdots \arrow[u, "\delta"] & \vdots \arrow[u, "\delta"] & \vdots \arrow[u, "\delta"] & \vdots \arrow[u, "\delta"]
\end{tikzcd}$$

(This is no longer a double complex of course.) It is clear what a morphism $\Phi : (A_{\bullet,\bullet}, d, \delta) \to (B_{\bullet,\bullet}, d, \delta)$ of double complexes is, and it is clear that this induces morphisms of complexes $R(\Phi) : R(A)_\bullet \to R(B)_\bullet$ and $U(\Phi) : U(A)_\bullet \to U(B)_\bullet$.

LEMMA 5.2. *Let $(A_{\bullet,\bullet}, d, \delta)$ be a double complex such that*

(1) *Each row $A_{\bullet,j}$ is a resolution of $R(A)_j$.*
(2) *Each column $A_{i,\bullet}$ is a resolution of $U(A)_i$.*

Then there are canonical isomorphisms

$$H_i(R(A)_\bullet) \cong H_i(U(A)_\bullet).$$

The isomorphisms are functorial with respect to morphisms of double complexes with the properties above.

PROOF. We will show that $H_i(R(A)_\bullet))$ and $H_i(U(A)_\bullet)$ are canonically isomorphic to a third group. Namely

$$\mathbf{H}_i(A) := \frac{\{(a_{i,0}, a_{i-1,1}, \dots, a_{0,i}) \mid d(a_{i,0}) = \delta(a_{i-1,1}), \dots, d(a_{1,i-1}) = \delta(a_{0,i})\}}{\{d(a_{i+1,0}) - \delta(a_{i,1}), d(a_{i,1}) - \delta(a_{i-1,2}), \dots, d(a_{1,i}) - \delta(a_{0,i+1})\}}$$

Here we use the notational convention that $a_{i,j}$ denotes an element of $A_{i,j}$. In other words, an element of $\mathbf{H}_i$ is represented by a zig-zag, represented as follows for $i = 2$

$$\begin{tikzcd}
a_{2,0} \arrow[r, mapsto] & d(a_{2,0}) = \delta(a_{1,1}) & \\
& a_{1,1} \arrow[u, mapsto] \arrow[r, mapsto] & d(a_{1,1}) = \delta(a_{0,2}) \\
& & a_{0,2} \arrow[u, mapsto]
\end{tikzcd}$$

Naturally, we divide out by “trivial” zig-zags, namely the submodule generated by elements of the form $(0, \dots, 0, -\delta(a_{t+1,t-i}), d(a_{t+1,t-i}), 0, \dots, 0)$. Note that there are canonical homomorphisms

$$\mathbf{H}_i(A) \to H_i(R(A)_\bullet), \quad (a_{i,0}, a_{i-1,1}, \dots, a_{0,i}) \mapsto \text{class of image of } a_{0,i}$$

and

$$\mathbf{H}_i(A) \to H_i(U(A)_\bullet), \quad (a_{i,0}, a_{i-1,1}, \dots, a_{0,i}) \mapsto \text{class of image of } a_{i,0}$$

First we show that these maps are surjective. Suppose that $\overline{r} \in H_i(R(A)_\bullet)$. Let $r \in R(A)_i$ be a cocycle representing the class of $\overline{r}$. Let $a_{0,i} \in A_{0,i}$ be an element which maps to r. Because $\delta(r) = 0$, we see that $\delta(a_{0,i})$ is in the image of d. Hence there exists an element $a_{1,i-1} \in A_{1,i-1}$ such that $d(a_{1,i-1}) = \delta(a_{0,i})$. This in turn implies that $\delta(a_{1,i-1})$ is in the kernel of d (because $d(\delta(a_{1,i-1})) = \delta(d(a_{1,i-1})) = \delta(\delta(a_{0,i})) = 0$. By exactness of the rows we find an element $a_{2,i-2}$ such that $d(a_{2,i-2}) = \delta(a_{1,i-1})$. And so on until a full zig-zag is found. Of course surjectivity of $\mathbf{H}_i \to H_i(U(A))$ is shown similarly.

To prove injectivity we argue in exactly the same way. Namely, suppose we are given a zig-zag $(a_{i,0}, a_{i-1,1}, \dots, a_{0,i})$ which maps to zero in $H_i(R(A)_\bullet)$. This means that $a_{0,i}$ maps to an element of $\mathrm{coker}(A_{i,1} \to A_{i,0})$ which is in the image of $\delta : \mathrm{coker}(A_{i+1,1} \to A_{i+1,0}) \to \mathrm{coker}(A_{i,1} \to A_{i,0})$. In other words, $a_{0,i}$ is in the image of $\delta \oplus d : A_{0,i+1} \oplus A_{1,i} \to A_{0,i}$. From the definition of trivial zig-zags we see that we may modify our zig-zag by a trivial one and assume that $a_{0,i} = 0$. This immediately implies that $d(a_{1,i-1}) = 0$. As the rows are exact this implies that $a_{1,i-1}$ is in the image of $d : A_{2,i-1} \to A_{1,i-1}$. Thus we may modify our zig-zag once again by a trivial zig-zag and assume that our zig-zag looks like $(a_{i,0}, a_{i-1,1}, \ldots, a_{2,i-2}, 0, 0)$. Continuing like this we obtain the desired injectivity.

If $\Phi : (A_{\bullet,\bullet}, d, \delta) \to (B_{\bullet,\bullet}, d, \delta)$ is a morphism of double complexes both of which satisfy the conditions of the lemma, then we clearly obtain a commutative diagram

$$\begin{tikzcd}
H_i(U(A)_\bullet) \arrow[d] & \mathbf{H}_i(A) \arrow[l] \arrow[r] \arrow[d] & H_i(R(A)_\bullet) \arrow[d] \\
H_i(U(B)_\bullet) & \mathbf{H}_i(B) \arrow[l] \arrow[r] & H_i(R(B)_\bullet)
\end{tikzcd}$$

This proves the functoriality. □

Remark 5.3. The isomorphism constructed above is the "correct" one only up to signs. A good part of homological algebra is concerned with choosing signs for various maps and showing commutativity of diagrams with intervention of suitable signs.

Lemma 5.4. *Let R be a ring. For any $i \geq 0$ the functors $\mathrm{Mod}_R \times \mathrm{Mod}_R \to \mathrm{Mod}_R$, $(M, N) \mapsto \mathrm{Tor}_i^R(M, N)$ and $(M, N) \mapsto \mathrm{Tor}_i^R(N, M)$ are canonically isomorphic.*

Proof. Let $F_\bullet$ be a free resolution of the module M and let $G_\bullet$ be a free resolution of the module N. Consider the double complex $(A_{i,j}, d, \delta)$ defined as follows:

(1) set $A_{i,j} = F_i \otimes_R G_j$,
(2) set $d_{i,j} : F_i \otimes_R G_j \to F_{i-1} \otimes G_j$ equal to $d_{F,i} \otimes \mathrm{id}$, and
(3) set $\delta_{i,j} : F_i \otimes_R G_j \to F_i \otimes G_{j-1}$ equal to $\mathrm{id} \otimes d_{G,j}$.

Since each G_j is free, and hence flat we see that each row of the double complex is exact except in homological degree 0. Since each F_i is free and hence flat we see that each column of the double complex is exact except in homological degree 0. Hence the double complex satisfies the conditions of Lemma 5.2.

To see what the lemma says we compute $R(A)_\bullet$ and $U(A)_\bullet$. Namely,

$$\begin{aligned}
R(A)_i &= \mathrm{coker}(A_{1,i} \to A_{0,i}) \\
&= \mathrm{coker}(F_1 \otimes_R G_i \to F_0 \otimes_R G_i) \\
&= \mathrm{coker}(F_1 \to F_0) \otimes_R G_i \\
&= M \otimes_R G_i
\end{aligned}$$

In fact these isomorphisms are compatible with the differentials δ and we see that $R(A)_\bullet = M \otimes_R G_\bullet$ as homological complexes. In exactly the same way we see that

$U(A)_\bullet = F_\bullet \otimes_R N$. We get

$$\begin{aligned}
\mathrm{Tor}_i^R(M,N) &= H_i(F_\bullet \otimes_R N) \\
&= H_i(U(A)_\bullet) \\
&= H_i(R(A)_\bullet) \\
&= H_i(M \otimes_R G_\bullet) \\
&= H_i(G_\bullet \otimes_R M) \\
&= \mathrm{Tor}_i^R(N,M)
\end{aligned}$$

Here the third equality is Lemma 5.2, and the fifth equality uses the isomorphism $V \otimes W = W \otimes V$ of the tensor product.

Functoriality: Suppose that we have R-modules M_ν, N_ν, $\nu = 1,2$. Let $\varphi : M_1 \to M_2$ and $\psi : N_1 \to N_2$ be morphisms of R-modules. Suppose that we have free resolutions $F_{\nu,\bullet}$ for M_ν and free resolutions $G_{\nu,\bullet}$ for N_ν. By Lemma 4.7 we may choose maps of complexes $\alpha : F_{1,\bullet} \to F_{2,\bullet}$ and $\beta : G_{1,\bullet} \to G_{2,\bullet}$ compatible with φ and ψ. We claim that the pair (α, β) induces a morphism of double complexes

$$\alpha \otimes \beta : F_{1,\bullet} \otimes_R G_{1,\bullet} \longrightarrow F_{2,\bullet} \otimes_R G_{2,\bullet}$$

This is a straightforward check using the rule that $F_{1,i} \otimes_R G_{1,j} \to F_{2,i} \otimes_R G_{2,j}$ is given by $\alpha_i \otimes \beta_j$ where α_i, resp. β_j is the degree i, resp. j component of α, resp. β. The reader also readily verifies that the induced maps $R(F_{1,\bullet} \otimes_R G_{1,\bullet})_\bullet \to R(F_{2,\bullet} \otimes_R G_{2,\bullet})_\bullet$ agrees with the map $M_1 \otimes_R G_{1,\bullet} \to M_2 \otimes_R G_{2,\bullet}$ induced by $\varphi \otimes \beta$. Similarly for the map induced on the $U(-)_\bullet$ complexes. Thus the statement on functoriality follows from the statement on functoriality in Lemma 5.2. □

Definition 5.5. Let R be a ring.

(1) An R-module M is called *flat* if whenever $N_1 \to N_2 \to N_3$ is an exact sequence of R-modules the sequence $M \otimes_R N_1 \to M \otimes_R N_2 \to M \otimes_R N_3$ is exact as well.
(2) A ring map $R \to S$ is called *flat* if S is flat as an R-module.

It is not hard to check that the R-module M is flat if and only if the functor $- \otimes_R M$ takes injective maps to injective maps. Here is an example of how you can use the flatness condition.

Lemma 5.6. *Let R be a ring. Let $I, J \subset R$ be ideals. Let M be a flat R-module. Then $IM \cap JM = (I \cap J)M$.*

Proof. Consider the exact sequence $0 \to I \cap J \to R \to R/I \oplus R/J$. Tensoring with the flat module M we obtain an exact sequence

$$0 \to (I \cap J) \otimes_R M \to M \to M/IM \oplus M/JM$$

Since the kernel of $M \to M/IM \oplus M/JM$ is equal to $IM \cap JM$ we conclude. □

Exercise 5.7. Suppose that M is flat over R, and that $R \to R'$ is a ring map. Then $M \otimes_R R'$ is flat over R'.

Exercise 5.8. Let R be a ring. Let $\{M_i, \varphi_{ii'}\}$ be a directed system of flat R-modules. Then $\mathrm{colim}_i M_i$ is a flat R-module.

Lemma 5.9. *Let M be an R-module. The following are equivalent:*

(1) *M is flat over R.*

(2) *for every injection of* R*-modules* $K \subset N$ *the map* $K \otimes_R M \to N \otimes_R M$ *is injective.*
(3) *for every ideal* $I \subset R$ *the map* $I \otimes_R M \to R \otimes_R M = M$ *is injective.*
(4) *for every finitely generated ideal* $I \subset R$ *the map* $I \otimes_R M \to R \otimes_R M = M$ *is injective.*

PROOF. The implications (1) $\Leftrightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are all easy. Thus we prove (4) implies (2).

Assume $K \subset N$ is an inclusion of R-modules and let $x \in \ker(K \otimes_R M \to N \otimes_R M)$. We have to show that x is zero. The R-module K is the union of its finite R-submodules; hence, $K \otimes_R M$ is the colimit of R-modules of the form $K_i \otimes_R M$ where K_i runs over all finite R-submodules of K (because tensor product commutes with colimits). Thus, for some i our x comes from an element $x_i \in K_i \otimes_R M$. Thus we may assume that K is a finite R-module. By a similar argument we may then assume that N is finite. (Consider finite R-submodules of N that contain K, which are a *directed* system, so that Lemma 2.6 applies.)

Write $N = R^{\oplus n}/L$ and $K = L'/L$ for some $L \subset L' \subset R^{\oplus n}$. It suffices to prove that the canonical maps $L \otimes_R M \to M^{\oplus n}$ and $L' \otimes_R M \to M^{\oplus n}$ are injective, for then $K \otimes_R M = (L' \otimes_R M)/(L \otimes_R M) \to M^{\oplus n}/(L \otimes_R M)$ is injective too.

Thus it suffices to show that $L \otimes_R M \to M^{\oplus n}$ is injective when $L \subset R^{\oplus n}$ is any R-submodule. We do this by induction on n. The base case $n = 1$ is the case where I is an ideal. We reduce to the case where I is a finitely generated ideal by exactly the same argument as two paragraphs previous, but this case is given to us by (4).

For the induction step assume $n > 1$ and set $L' = L \cap (R \oplus 0^{\oplus n-1})$. Then $L'' = L/L'$ is a submodule of $R^{\oplus n-1}$. We obtain a diagram

$$\begin{tikzcd}
 & L' \otimes_R M \arrow[r] \arrow[d] & L \otimes_R M \arrow[r] \arrow[d] & L'' \otimes_R M \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M \arrow[r] & M^{\oplus n} \arrow[r] & M^{\oplus n-1} \arrow[r] & 0
\end{tikzcd}$$

By induction hypothesis and the base case the left and right vertical arrows are injective. The rows are exact. It follows that the middle vertical arrow is injective too. $\square$

LEMMA 5.10. *Let* R *be a ring. Let* M *be an* R*-module. The following are equivalent:*

(1) *The module* M *is flat over* R.
(2) *For all* $i > 0$ *the functor* $\mathrm{Tor}_i^R(M, -)$ *is zero.*
(3) *The functor* $\mathrm{Tor}_1^R(M, -)$ *is zero.*
(4) *For all ideals* $I \subset R$ *we have* $\mathrm{Tor}_1^R(M, R/I) = 0$.
(5) *For all finitely generated ideals* $I \subset R$ *we have* $\mathrm{Tor}_1^R(M, R/I) = 0$.

PROOF. Suppose M is flat. Let N be an R-module. Let $F_\bullet$ be a free resolution of N. Then $F_\bullet \otimes_R M$ is a resolution of $N \otimes_R M$, by flatness of M. This proves that the groups $\mathrm{Tor}_i^R(N, M)$ all vanish. Now (2) follows from Lemma 5.4.

It now suffices to show that the last condition implies that M is flat. Let $I \subset R$ be an ideal. Consider the short exact sequence $0 \to I \to R \to R/I \to 0$. Apply

Lemma 5.1. We get an exact sequence

$$\mathrm{Tor}_1^R(M, R/I) \to M \otimes_R I \to M \otimes_R R \to M \otimes_R R/I \to 0$$

Since obviously $M \otimes_R R = M$ we conclude that the last hypothesis implies that $M \otimes_R I \to M$ is injective for every finitely generated ideal I. Thus M is flat by Lemma 5.9. □

Remark 5.11. The proof of Lemma 5.10 actually shows that

$$\mathrm{Tor}_1^R(M, R/I) = \ker(I \otimes_R M \to M).$$

We close this section with a few useful lemmas.

Lemma 5.12. *Let R be a ring. Any projective R-module is flat.*

Proof. Let P be a projective R-module. By Lemma 4.12 we can write $F = P \oplus Q$ for some R-modules F, Q with F free. If $N \to N'$ is any injection, then $F \otimes_R N \to F \otimes_R N'$ is injective, and therefore so is $P \otimes_R N \to P \otimes_R N'$. □

Lemma 5.13. *Suppose that R is a ring, $0 \to N' \to N \to N'' \to 0$ a short exact sequence, and M an R-module. If N'' is flat then $M \otimes_R N' \to M \otimes_R N$ is injective, i.e., the sequence*

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

is a short exact sequence.

Proof. Immediate from the vanishing of the functor $\mathrm{Tor}_1^R(-, N'')$. Alternately, let $R^I \to N$ be a surjection from a free module onto N, with kernel K. The result follows from the snake lemma applied to the diagram

$$\begin{tikzcd}
& M'' \otimes_R K \arrow[r] \arrow[d] & M' \otimes_R K \arrow[r] \arrow[d] & M \otimes_R K \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M'' \otimes_R R^I \arrow[r] & M' \otimes_R R^I \arrow[r] & M \otimes_R R^I \arrow[r] & 0.
\end{tikzcd}$$

□

Lemma 5.14. *Suppose that $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules. If M' and M'' are flat so is M. If M and M'' are flat so is M'.*

Proof. We will use the criterion of Lemma 5.9(3). Consider an ideal $I \subset R$. Consider the diagram

$$\begin{tikzcd}
& M' \otimes_R I \arrow[r] \arrow[d] & M \otimes_R I \arrow[r] \arrow[d] & M'' \otimes_R I \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

with exact rows. The snake lemma immediately proves the first assertion. The second follows because if M'' is flat then the upper left horizontal arrow is injective by Lemma 5.13. □

Elementary results

6. Localization

DEFINITION 6.1. Let R be a ring, S a subset of R. We say S is a *multiplicative subset of* R is $1 \in S$ and S is closed under multiplication, i.e., $s, s' \in S \Rightarrow ss' \in S$.

Given a ring A and a multiplicative subset S, we define a relation on $A \times S$ as follows:

$$(x, s) \sim (y, t) \Leftrightarrow \exists u \in S \text{ such that } (xt - ys)u = 0$$

It is easily checked that this is an equivalence relation. Let x/s (or $\frac{x}{s}$) be the equivalence class of (x, s) and $S^{-1}A$ be the set of all equivalence classes. Define addition and multiplication in $S^{-1}A$ as follows:

$$x/s + y/t = (xt + ys)/st, \quad x/s \cdot y/t = xy/st$$

One can check that $S^{-1}A$ becomes a ring under these operations.

DEFINITION 6.2. This ring is called the *localization of* A *with respect to* S.

We have a natural ring map from A to its localization $S^{-1}A$,

$$A \longrightarrow S^{-1}A, \quad x \longmapsto x/1$$

which is sometimes called the *localization map*. The localization map is injective if and only if S contains no zerodivisors. The localization of a ring has the following universal property.

PROPOSITION 6.3. *Let $f : A \to B$ be a ring map that sends every element in S to a unit of B. Then there is a unique homomorphism $g : S^{-1}A \to B$ such that the following diagram commutes.*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr] & & B \\ & S^{-1}A \arrow[ur, "g"'] & \end{tikzcd}$$

LEMMA 6.4. *The localization $S^{-1}A$ is the zero ring if and only if $0 \in S$.*

PROOF. $1/1 = 0/1$ in $S^{-1}A$ iff there exists $u \in S$ such that $u \cdot 1 = 0$. $\square$

The notion of localization of a ring can be generalized to the localization of a module. Let A be a ring, S a multiplicative subset of A and M an A-module. We define a relation on $M \times S$ as follows

$$(m, s) \sim (n, t) \Leftrightarrow \exists u \in S \text{ such that } (mt - ns)u = 0$$

This is clearly an equivalence relation. Denote by m/s (or $\frac{m}{s}$) be the equivalence class of (m, s) and $S^{-1}M$ be the set of all equivalence classes. Define the addition and scalar multiplication as follows

$$m/s + n/t = (mt + ns)/st, \quad m/s \cdot n/t = mn/st$$

It is clear that this makes $S^{-1}M$ an $S^{-1}A$ module. The construction is functorial, in the sense that if $f : M \to N$ is an R-module homomorphism then there is an associated $S^{-1}R$-module map $S^{-1}M \to S^{-1}N$ sending $m/s \mapsto f(m)/s$.

Definition 6.5. The $S^{-1}A$-module $S^{-1}M$ is called the *localization* of M at S.

Exercise 6.6. Let $S \subset R$ be a multiplicative subset and let M, N be $S^{-1}R$-modules. Then the natural map $M \otimes_R N \to M \otimes_{S^{-1}R} N$ is an isomorphism.

Note that there is an A-module map $M \to S^{-1}M$, $m \mapsto m/1$ which is sometimes called the *localization map*. It satisfies the following universal property.

Lemma 6.7. *Let R be a ring. Let $S \subset R$ a multiplicative subset. Let M, N be R-modules. Assume all the elements of S act as automorphisms on N. Then the canonical map*

$$\mathrm{Hom}_R(S^{-1}M, N) \longrightarrow \mathrm{Hom}_R(M, N)$$

induced by the localization map, is an isomorphism.

Example 6.8. Let A be a ring and let M be an A-module. Here are some important examples of localizations.

(1) Given $\mathfrak{p}$ a prime ideal of A consider $S = A \setminus \mathfrak{p}$. It is immediately checked that S is a multiplicative set. In this case we denote $A_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$ the localization of A and M with respect to S respectively. These are called the *localization of A, resp. M at $\mathfrak{p}$*.
(2) Let $f \in A$. Consider $S = \{1, f, f^2, \dots\}$. This is clearly a multiplicative subset of A. In this case we denote A_f (resp. M_f) the localization $S^{-1}A$ (resp. $S^{-1}M$). This is called the *localization of A, resp. M with respect to f*. Note that $A_f = 0$ if and only if f is nilpotent in A.
(3) Let $S = \{f \in A \mid f \text{ is not a zerodivisor in } A\}$. This is a multiplicative subset of A. In this case the ring $Q(A) = S^{-1}A$ is called either the *total quotient ring*, or the *total ring of fractions* of A.

Localization is exact.

Proposition 6.9. *Let $L \xrightarrow{u} M \xrightarrow{v} N$ is an exact sequence of R-modules. Then $S^{-1}L \to S^{-1}M \to S^{-1}N$ is also exact.*

Proof. This is almost immediate from the definitions. □

Lemma 6.10. *Localization respects quotients, i.e. if N is a submodule of M, then $S^{-1}(M/N) \simeq (S^{-1}M)/(S^{-1}N)$.*

Proof. From the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

we have

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0$$

by Proposition 6.9. □

If, in the preceding Corollary, we take $N = I$ and $M = A$ for an ideal I of A, we see that $S^{-1}A/S^{-1}I \simeq S^{-1}(A/I)$ as A-modules, but indeed this is also an isomorphism of rings.

Lemma 6.11. *If S and S' are multiplicative sets of A, then it is clear that*

$$SS' = \{ss' : s \in S,\ s' \in S'\}$$

is also a multiplicative set of A. Let $\overline{S}$ be the image of S in $S'^{-1}A$, then $(SS')^{-1}A$ is isomorphic to $\overline{S}^{-1}(S'^{-1}A)$.

Proof. Omitted. □

Lemma 6.12. *Let R be a ring. Let M be a finitely presented R-module. Let N be an R-module. Then for a multiplicative subset S of R we have*

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

Proof. The second equality follows from Lemma 6.7. Choose a presentation

$$R^m \to R^n \to M \to 0.$$

By Lemma 4.1 this gives an exact sequence

$$0 \to \operatorname{Hom}_R(M, N) \to N^n \to N^m.$$

Inverting S and using Proposition 6.9 we get an exact sequence

$$0 \to S^{-1}\operatorname{Hom}_R(M, N) \to (S^{-1}N)^n \to (S^{-1}N)^m.$$

On the other hand if we first localize the presentation with respect to S and then apply $\operatorname{Hom}_{S^{-1}R}(-, S^{-1}N)$ we get the exact sequence

$$0 \to \operatorname{Hom}_R(S^{-1}M, S^{-1}N) \to (S^{-1}N)^n \to (S^{-1}N)^m$$

in which the right-hand map is the same as the one above. □

Exercise 6.13. Let R be a ring. Let $S \subset R$ be a multiplicative subset. Let M be an R-module. Then

$$S^{-1}M = \operatorname{colim}_{f \in S} M_f$$

where the partial ordering on S is given by $f \geq f' \Leftrightarrow f = f'f''$ for some $f'' \in R$ in which case the map $M_{f'} \to M_f$ is given by $m/(f')^e \mapsto m(f'')^e/f^e$.

7. Nakayama's lemma and other elementary results

Elementary properties of ideals.

Lemma 7.1. *Let R be a ring, I and J two ideals and $\mathfrak{p}$ a prime ideal containing the product IJ. Then $\mathfrak{p}$ contains I or J.*

Proof. Assume the contrary and take $x \in I \setminus \mathfrak{p}$ and $y \in J \setminus \mathfrak{p}$. Their product is an element of $IJ \subset \mathfrak{p}$, which contradicts the assumption that $\mathfrak{p}$ was prime. □

Lemma 7.2 (Prime avoidance). *Let R be a ring. Let $I_i \subset R$, $i = 1, \ldots, r$, and $J \subset R$ be ideals. Assume*

1. *$J \subset \bigcup I_i$, and*
2. *all but possibly two of I_i are prime ideals.*

Then $J \subset I_i$ for some i.

Proof. The result is true for $r = 1$. If $r = 2$, suppose not; i.e., suppose there exist $x, y \in J$ with $x \notin I_1$ and $y \notin I_2$. By (1) we have $x \in I_2$ and $y \in I_1$. Then the element $x + y$ cannot be in I_1 (since that would mean $x + y - y \in I_1$) and it also cannot be in I_2. Contradiction.

For $r \geq 3$, assume the result holds for $r - 1$. After renumbering we may assume that I_r is prime. We may also assume that there are no inclusions among the I_i. If $J \subset \bigcup_{i=1}^{r-1} I_i$ we conclude by induction. Otherwise we can pick $x \in J \setminus \bigcup_{i=1}^{r-1} I_i$. We have $x \in I_r$ by (1). If $JI_1 \ldots I_{r-1} \subset I_r$ then $J \subset I_r$ (by Lemma 7.1) and we conclude. Otherwise pick $y \in JI_1 \ldots I_{r-1}$, $y \notin I_r$. Then $x + y$ contradicts (1). □

Lemma 7.3 (Chinese remainder). *Let R be a ring.*

1. *If $I_1, \ldots, I_r$ are ideals such that $I_a + I_b = R$ when $a \neq b$, then $I_1 \cap \cdots \cap I_r = I_1 I_2 \ldots I_r$ and $R/(I_1 I_2 \ldots I_r) \cong R/I_1 \times \cdots \times R/I_r$.*
2. *If $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are pairwise distinct maximal ideals then $\mathfrak{m}_a + \mathfrak{m}_b = R$ for $a \neq b$ and the above applies.*

Proof. We first observe that $I_1 \cdots I_{r-1} + I_r = R$. This is because

$$(I_1 + I_r) \cdots (I_{r-1} + I_r) \subset I_1 \cdots I_{r-1} + I_r$$

and the left-hand side certainly contains 1.

We also claim that $I \cap J = IJ$ whenever $I + J = R$: Write $1 = x + y$ with $x \in I$ and $y \in J$. Now if $z \in I \cap J$ then $z = zx + zy \in IJ$, so $I \cap J \subset IJ$. The reverse inclusion is clear.

Now it follows by induction that $I_1 \cap \cdots \cap I_r = I_1 \ldots I_r$: apply the previous paragraph with $I = I_r$ and $J = I_1 \cdots I_{r-1}$, and induct.

For the isomorphism $R/(I_1 I_2 \ldots I_r) \cong R/I_1 \times \cdots \times R/I_r$, injectivity is equivalent to what we just proved. As for surjectivity, the first paragraph of the proof implies that we may write $1 = x + y$ with $y \in I_r$ and $x \in I_1 \cap \cdots \cap I_{r-1}$. Then $x = 1 - y \in R$ maps to $(0, \ldots, 0, 1)$ in $R/I_1 \times \cdots \times R/I_r$. □

Definition 7.4. A *local ring* is a ring with exactly one maximal ideal. The maximal ideal is often denoted $\mathfrak{m}_R$ in this case. We often say "let $(R, \mathfrak{m}, \kappa)$ be a local ring" to indicate that R is local, $\mathfrak{m}$ is its unique maximal ideal and $\kappa = R/\mathfrak{m}$ is its residue field. A *local homomorphism of local rings* is a ring map $\varphi : R \to S$ such that R and S are local rings and such that $\varphi(\mathfrak{m}_R) \subset \mathfrak{m}_S$. If it is given that R and S are local rings, then the phrase "*local ring map $\varphi : R \to S$*" means that φ is a local homomorphism of local rings.

Example 7.5. A field is a local ring. Any ring map between fields is a local homomorphism of local rings.

Lemma 7.6. *Let R be a ring. The following are equivalent:*

1. *R is a local ring,*
2. *R has a maximal ideal $\mathfrak{m}$ and every element of $R \setminus \mathfrak{m}$ is a unit.*

Proof. Let R be a ring, and $\mathfrak{m}$ a maximal ideal. If $x \in R \setminus \mathfrak{m}$, and x is not a unit then there is a maximal ideal $\mathfrak{m}'$ containing x. Hence R has at least two maximal ideals. Conversely, if $\mathfrak{m}'$ is another maximal ideal, then choose $x \in \mathfrak{m}'$, $x \notin \mathfrak{m}$. Clearly x is not a unit. □

EXERCISE 7.7. The localization $R_{\mathfrak{p}}$ of a ring R at a prime $\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Namely, the quotient $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is the fraction field of the domain $R/\mathfrak{p}$ and every element of $R_{\mathfrak{p}}$ which is not contained in $\mathfrak{p}R_{\mathfrak{p}}$ is invertible.

Linear algebra.

LEMMA 7.8. *Let R be a ring. Let $n \geq m$. Let A be an $n \times m$ matrix with coefficients in R. Let $J \subset R$ be the ideal generated by the $m \times m$ minors of A. Then for any $f \in J$ there exists a $m \times n$ matrix B such that $BA = f1_{m\times m}$.*

PROOF. It suffices to prove the claim when f is an $m \times m$ minor of A. Let $I \subset \{1, \ldots, n\}$ be a subset of size m, and let A_I be the matrix whose rows are the rows of A with indices in I. Note that $A_I = E_I A$ for an $m \times n$ matrix (namely the matrix of the map $R^n \to R^m$ by projection onto the coordinates in I). Then take $B = \mathrm{adj}(A_I)E_I$ where adj denotes the adjugate matrix. □

LEMMA 7.9 (Cayley–Hamilton theorem). *Let R be a ring. Let $A = (a_{ij})$ be an $n\times n$ matrix with coefficients in R. Let $P(x) \in R[x]$ be the characteristic polynomial of A (defined as $\det(x\mathrm{id}_{n\times n} - A)$). Then $P(A) = 0$ in $\mathrm{Mat}(n \times n, R)$.*

PROOF. We reduce the question to the well-known Cayley–Hamilton theorem from linear algebra in several steps:

(1) If $\phi : S \to R$ is a ring morphism and b_{ij} are inverse images of the a_{ij} under this map, then it suffices to show the statement for S and (b_{ij}) since ϕ is a ring morphism.
(2) If $\psi : R \hookrightarrow S$ is an injective ring morphism, it clearly suffices to show the result for S and the a_{ij} considered as elements of S.
(3) Thus we may first reduce to the case $R = \mathbf{Z}[X_{ij}]$, $a_{ij} = X_{ij}$ of a polynomial ring and then further to the case $R = \mathbf{Q}(X_{ij})$ where we may finally apply the classical Cayley–Hamilton over a field.

□

LEMMA 7.10 (The determinantal trick). *Let R be a ring and M a finite R-module. Let $\varphi : M \to M$ be an endomorphism. Then there exists a monic polynomial $P = t^n + a_1t^{n-1} + \cdots + a_n \in R[T]$ such that $P(\varphi) = 0$ as an endomorphism of M.*

Moreover, if $\varphi(M) \subset IM$ for an ideal $I \subset R$, then one can take $a_j \in I^j$.

PROOF. If no ideal I is specified as in the last sentence of the statement, take $I = R$. Choose a surjective R-module map $R^{\oplus n} \to M$, given by $(a_1, \ldots, a_n) \mapsto \sum a_i x_i$ for some generators $x_i \in M$. Choose $(a_{i1}, \ldots, a_{in}) \in I^{\oplus n}$ such that $\varphi(x_i) = \sum a_{ij}x_j$. In other words the diagram

$$\begin{tikzcd} R^{\oplus n} \arrow[r] \arrow[d, "A"'] & M \arrow[d, "\varphi"] \\ I^{\oplus n} \arrow[r] & M \end{tikzcd}$$

is commutative where $A = (a_{ij})$. By Lemma 7.9 the polynomial $P(t) = \det(t\mathrm{id}_{n\times n} - A)$ has all the desired properties. □

As a fun example application we prove the following surprising lemma.

LEMMA 7.11. *Let R be a ring. Let M be a finite R-module. Let $\varphi : M \to M$ be a surjective R-module map. Then φ is an isomorphism.*

PROOF. Think of M as a finite $R[x]$-module with x acting via φ. By our assumption that φ is surjective we have $(x) \cdot M = M$. Hence we may apply Lemma 7.10 to M as an $R[x]$-module, with $I = (x)$ and $\varphi = \mathrm{id}_M$. We conclude that $(1 + a_1 + \cdots + a_n)\mathrm{id}_M = 0$ with $a_j \in (x)$. If $m \in \ker(\varphi)$ then $a_j \cdot m = 0$, and applying $(1 + a_1 + \cdots + a_n)\mathrm{id}_M$ to m gives $m = 0$. □

REMARK 7.12. The lemma can also be proved in a completely elementary way, by induction on the minimal number of generators of M. In the case of one generator, so that $M \cong R/I$ for some I, we replace R by R/I so that $M = R$. Then φ must be multiplication by a unit.

In the general case where M has $n > 1$ generators, choose $M' \subset M$ so that M' and M/M' both have fewer than n generators. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d, "\varphi|_{M'}"] & M \arrow[r] \arrow[d, "\varphi"] & M/M' \arrow[r] \arrow[d, "\varphi \bmod M'"] & 0 \\ 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M/M' \arrow[r] & 0,. \end{tikzcd}$$

The right-hand vertical map is surjective, so by induction is an isomorphism. The snake lemma then implies that the left-hand vertical map is surjective, so is also an isomorphism. Another application of the snake lemma implies that the middle map is an isomorphism too.

Nakayama's Lemma.

We quote from [**Mat70**]: "This simple but important lemma is due to T. Nakayama, G. Azumaya and W. Krull. Priority is obscure, and although it is usually called the Lemma of Nakayama, late Prof. Nakayama did not like the name."

DEFINITION 7.13. The *Jacobson radical* of R is $\mathrm{rad}(R) = \bigcap_{\mathfrak{m} \subset R} \mathfrak{m}$ the intersection of all the maximal ideals of R.

There are a variety of forms of Nakayama's lemma, and we list just a few.

LEMMA 7.14 (Nakayama's lemma). *Let R be a ring, let M be a* finite *R-module, and let $I \subset R$ be an ideal.*

(1) *If $M/IM = 0$ then there exists $f \in 1 + I$ such that $fM = 0$, so that in particular $M_f = 0$.*
(2) *If $M/IM = 0$ and $I \subset \mathrm{rad}(R)$, then $M = 0$.*
(3) *If $x_1, \ldots, x_n \in M$ generate M/IM, then there exists an $f \in 1 + I$ such that $x_1, \ldots, x_n$ generate M_f over R_f.*
(4) *If $x_1, \ldots, x_n \in M$ generate M/IM and $I \subset \mathrm{rad}(R)$, then M is generated by $x_1, \ldots, x_n$.*

REMARK 7.15. In applications of (1) and (3), if $I = \mathfrak{p}$ is a prime ideal then $M_{\mathfrak{p}}$ is a localization of M_f by Lemma 6.11, and so the same conclusions apply to $M_{\mathfrak{p}}$.

In applications of (2) and (4), if R is a local ring then I may be any proper ideal of R.

PROOF. For (1), apply Lemma 7.10 to the identity map $M \to M$ to obtain monic $P(T) \in R[T]$ (with all non-leading coefficients in I) such that $P(\mathrm{Id}_M)\cdot M = 0$. Take $f = P(1)$.

An element of $1 + \mathrm{rad}(R)$ is not contained in any maximal ideal of R, hence is invertible, so that (1) implies (2).

Applying (1) to $N = M/(x_1, \ldots, x_n)$ gives (3), and applying (2) to $N = M/(x_1, \ldots, x_n)$ gives (4). □

The following variant, in which M is no longer assumed to be finite, but instead I is assumed to be nilpotent, often also goes under the name of Nakayama's lemma.

LEMMA 7.16. *Let R be a ring, let M be an R-module, and let $I \subset R$ be a* nilpotent *ideal.*

(1) *If $IM = M$ then $M = 0$.*
(2) *If $g\colon N \to M$ is a module map, I is nilpotent, and $\overline{g}\colon N/IN \to M/IM$ is surjective, then $N \to M$ is surjective.*

PROOF. The first part holds because if $M = IM$ then $M = I^n M$ for all $n \geq 0$ and I being nilpotent means $I^n = 0$ for some $n \gg 0$. The second part holds by applying the first part to $\mathrm{coker}(g)$. □

The spectrum of a ring

8. The spectrum of a ring (as a topological space)

DEFINITION 8.1. Let R be a ring.

(1) The *spectrum* of R is the set of prime ideals of R. It is usually denoted $\mathrm{Spec}(R)$.
(2) Given a subset $T \subset R$ we let $V(T) \subset \mathrm{Spec}(R)$ be the set of primes containing T, i.e., $V(T) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \forall f \in T, f \in \mathfrak{p}\}$.
(3) Given an element $f \in R$ we let $D(f) \subset \mathrm{Spec}(R)$ be the set of primes not containing f.

LEMMA 8.2. *Let R be a ring.*

(1) *The spectrum of a ring R is empty if and only if R is the zero ring.*
(2) *Every nonzero ring has a maximal ideal.*
(3) *Every nonzero ring has a minimal prime ideal.*
(4) *Given an ideal $I \subset R$ and a prime ideal $I \subset \mathfrak{p}$ there exists a prime $I \subset \mathfrak{q} \subset \mathfrak{p}$ such that $\mathfrak{q}$ is minimal over I.*

PROOF. (2) is a standard Zorn's lemma argument. (4) also follows from Zorn's lemma: given a totally ordered chain of prime ideals lying between I and $\mathfrak{p}$, one just has to check that the intersection remains prime. Now (3) is a special case of (4), and (1) is a consequence of either (2) or (3). $\square$

DEFINITION 8.3. The *radical* of an ideal $I \subset R$, denoted $\sqrt{I}$, is $\{x \in R : x^n \in I \text{ for } n \gg 0\}$. The radical can be checked to be an ideal. For example, $\sqrt{(0)}$ is the set of nilpotent elements in R.

It is easy to see that if I is an ideal then $V(I) = V(\sqrt{I})$, and that if $T \subset R$ is a set then $V(T) = V((T))$ (where (T) is the ideal generated by T), so that the sets of the form $V(T)$ are actually all of the form $V(I)$ with I a radical ideal.

LEMMA 8.4. *Given an ideal I of R we have $\sqrt{I} = \bigcap_{I \subset \mathfrak{p}} \mathfrak{p}$.*

PROOF. The inclusion $\subset$ is clear. For the reverse, replacing R with R/I we may suppose that $I = 0$. Suppose that $f \in \bigcap \mathfrak{p}$, the intersection taken over all primes of R. The preimage of any prime $\mathfrak{P}$ of R_f under the map $R \to R_f$ is a prime of R, and so by hypothesis contains f. Thus $f/1 \in \mathfrak{P}$. But this is a unit in R_f, and so is not contained in any prime, a contradiction. It follows that R_f has no prime ideals. By Lemma 8.2 we find $R_f = 0$, and then Lemma 6.4 implies that f is nilpotent. $\square$

LEMMA 8.5. *Let R be a ring. The subsets $V(T)$ from Definition 8.1 form the closed subsets of a topology on* $\mathrm{Spec}(R)$. *Moreover, the sets $D(f)$ are open and form a basis for this topology. Specifically, we have the following.*

(1) *If I is an ideal then $V(I) = \emptyset$ if and only if I is the unit ideal.*
(2) *If I, J are ideals of R then $V(I) \cup V(J) = V(I \cap J)$.*
(3) *If $(I_a)_{a \in A}$ is a set of ideals of R then $\cap_{a\in A} V(I_a) = V(\cup_{a\in A} I_a)$.*
(4) *If $f \in R$, then $D(f) \amalg V(f) = \mathrm{Spec}(R)$.*
(5) *If $f \in R$ then $D(f) = \emptyset$ if and only if f is nilpotent.*
(6) *If $I \subset R$ is an ideal, and $\mathfrak{p}$ is a prime of R with $\mathfrak{p} \notin V(I)$, then there exists an $f \in R$ such that $\mathfrak{p} \in D(f)$, and $D(f) \cap V(I) = \emptyset$.*
(7) *If $f, g \in R$, then $D(fg) = D(f) \cap D(g)$.*
(8) *If $f_i \in R$ for $i \in I$, then $\bigcup_{i\in I} D(f_i)$ is the complement of $V(\{f_i\}_{i\in I})$ in* $\mathrm{Spec}(R)$.

Proof. Elementary. Note that (5) makes use of Lemma 8.4. □

Definition 8.6. Let R be a ring. The topology on $\mathrm{Spec}(R)$ whose closed sets are the sets $V(T)$ is called the *Zariski* topology. The open subsets $D(f)$ are called the *standard opens* of $\mathrm{Spec}(R)$.

Lemma 8.7. *Let R be a ring. The space* $\mathrm{Spec}(R)$ *is quasi-compact.*

Proof. It suffices to prove that any covering of $\mathrm{Spec}(R)$ by standard opens can be refined by a finite covering. Thus suppose that $\mathrm{Spec}(R) = \cup D(f_i)$ for a set of elements $\{f_i\}_{i\in I}$ of R. This means that $\cap V(f_i) = \emptyset$. According to Lemma 8.5 this means that $V(\{f_i\}) = \emptyset$. According to the same lemma this means that the ideal generated by the f_i is the unit ideal of R. This means that we can write 1 as a *finite* sum: $1 = \sum_{i\in J} r_i f_i$ with $J \subset I$ finite. And then it follows that $\mathrm{Spec}(R) = \cup_{i\in J} D(f_i)$. □

Lemma 8.8. *Suppose that $\varphi : R \to R'$ is a ring homomorphism. The induced map*

$$\mathrm{Spec}(\varphi) : \mathrm{Spec}(R') \longrightarrow \mathrm{Spec}(R), \quad \mathfrak{p}' \longmapsto \varphi^{-1}(\mathfrak{p}')$$

is continuous for the Zariski topologies. In fact, for any element $f \in R$ we have $\mathrm{Spec}(\varphi)^{-1}(D(f)) = D(\varphi(f))$.

Proof. It is elementary that $\mathfrak{p} := \varphi^{-1}(\mathfrak{p}')$ is indeed a prime ideal of R. The last assertion of the lemma follows directly from the definitions, and implies the first. □

If $\varphi' : R' \to R''$ is a second ring homomorphism then the composition

$$\mathrm{Spec}(R'') \longrightarrow \mathrm{Spec}(R') \longrightarrow \mathrm{Spec}(R)$$

equals $\mathrm{Spec}(\varphi' \circ \varphi)$. In other words, Spec is a contravariant functor from the category of rings to the category of topological spaces.

Lemma 8.9. *Let R be a ring. Let $S \subset R$ be a multiplicative subset. The map $R \to S^{-1}R$ induces via the functoriality of* Spec *a homeomorphism*

$$\mathrm{Spec}(S^{-1}R) \longrightarrow \{\mathfrak{p} \in \mathrm{Spec}(R) \mid S \cap \mathfrak{p} = \emptyset\}$$

where the topology on the right hand side is that induced from the Zariski topology on $\mathrm{Spec}(R)$. *The inverse map is given by $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$.*

Proof. Denote the right hand side of the arrow of the lemma by D. Choose a prime $\mathfrak{p}' \subset S^{-1}R$ and let $\mathfrak{p}$ the inverse image of $\mathfrak{p}'$ in R. It is easy to see that $S^{-1}\mathfrak{p} = \mathfrak{p}'$. Since $\mathfrak{p}'$ does not contain 1 we see that $\mathfrak{p}$ does not contain any element of S. Hence $\mathfrak{p} \in D$ and we see that the image is contained in D.

Let $\mathfrak{p} \in D$. By assumption the image $\overline{S}$ does not contain 0. By Lemma 6.4, the ring $\overline{S}^{-1}(R/\mathfrak{p})$ is not the zero ring. We see $S^{-1}R/S^{-1}\mathfrak{p} = \overline{S}^{-1}(R/\mathfrak{p})$ is a domain, and hence $S^{-1}\mathfrak{p}$ is a prime. The equality of rings also shows that the inverse image of $S^{-1}\mathfrak{p}$ in R is equal to $\mathfrak{p}$, because $R/\mathfrak{p} \to \overline{S}^{-1}(R/\mathfrak{p})$ is injective. This proves that the map $\mathrm{Spec}(S^{-1}R) \to \mathrm{Spec}(R)$ is bijective onto D with inverse as given. It is continuous by Lemma 8.8.

Finally, let $D(g) \subset \mathrm{Spec}(S^{-1}R)$ be a standard open. Write $g = h/s$ for some $h \in R$ and $s \in S$. Since g and $h/1$ differ by a unit we have $D(g) = D(h/1)$ in $\mathrm{Spec}(S^{-1}R)$. Hence by Lemma 8.8 and the bijectivity above the image of $D(g) = D(h/1)$ is $D \cap D(h)$. This proves the map is open as well. □

We stress the point that the preimage of $\mathfrak{p} \cdot S^{-1}R$ in R is $\mathfrak{p}$ again.

LEMMA 8.10. *Let R be a ring. Let $f \in R$. The map $R \to R_f$ induces via the functoriality of* Spec *a homeomorphism*

$$\mathrm{Spec}(R_f) \longrightarrow D(f) \subset \mathrm{Spec}(R).$$

The inverse is given by $\mathfrak{p} \mapsto \mathfrak{p} \cdot R_f$.

PROOF. This is a special case of Lemma 8.9. □

It is not the case that every "affine open" of a spectrum is a standard open. See Example 9.4.

LEMMA 8.11. *Let R be a ring. Let $I \subset R$ be an ideal. The map $R \to R/I$ induces via the functoriality of* Spec *a homeomorphism*

$$\mathrm{Spec}(R/I) \longrightarrow V(I) \subset \mathrm{Spec}(R).$$

The inverse is given by $\mathfrak{p} \mapsto \mathfrak{p}/I$.

PROOF. It is immediate that the image is contained in $V(I)$. On the other hand, if $\mathfrak{p} \in V(I)$ then $\mathfrak{p} \supset I$ and we may consider the ideal $\mathfrak{p}/I \subset R/I$. Since $(R/I)/(\mathfrak{p}/I) = R/\mathfrak{p}$ is a domain we see that $\mathfrak{p}/I$ is a prime ideal. From this it is immediately clear that the image of $D(f + I)$ is $D(f) \cap V(I)$, and hence the map is a homeomorphism. □

REMARK 8.12. It follows from Lemma 8.11 that if $\varphi : R \to S$ is a map of rings and $I \subset R$ is an ideal, then the diagram

$$\begin{tikzcd} \mathrm{Spec}(S/IS) \arrow[r] \arrow[d] & \mathrm{Spec}(S) \arrow[d] \\ \mathrm{Spec}(R/I) \arrow[r] & \mathrm{Spec}(R) \end{tikzcd}$$

is cartesian, i.e., is a fibre product diagram of topological spaces.[2] To see this, we use the fact that if $X \subset Z$ is any inclusion of topological spaces (so that the topology on X is the subspace topology from Z) and if $Y \to Z$ is any map, then $X \times_Z Y \hookrightarrow Y$ is a homeomorphism to the subspace of Y that maps to X. Since the primes of S/IS pull back in S precisely to the primes whose pullback to R contains I, this proves the claim.

[2]Readers already familiar with schemes will be aware that the given diagram is a fibre product of schemes, since $S/IS \cong S \otimes_R R/I$. This does not tautologically imply that it's a fibre product of the underlying topological spaces! Consider the fibre product $\mathrm{Spec}(\mathbf{C}) \times_{\mathrm{Spec}(\mathbf{R})} \mathrm{Spec}(\mathbf{C})$.

Similarly if $T \subset R$ is a multiplicative subset then

$$\begin{array}{ccc} \mathrm{Spec}(\varphi(T)^{-1}S) & \longrightarrow & \mathrm{Spec}(S) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(T^{-1}R) & \longrightarrow & \mathrm{Spec}(R) \end{array}$$

is Cartesian by Lemma 8.9. Taking $I = \mathfrak{p}$ and $T = R \setminus \mathfrak{p}$ we get a diagram

$$\begin{array}{ccccc} \mathrm{Spec}(\kappa(\mathfrak{p}) \otimes_R S) = \mathrm{Spec}(S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}) & \longrightarrow & \mathrm{Spec}(S_\mathfrak{p}) & \longrightarrow & \mathrm{Spec}(S) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(\kappa(\mathfrak{p})) = \mathrm{Spec}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}) & \longrightarrow & \mathrm{Spec}(R_\mathfrak{p}) & \longrightarrow & \mathrm{Spec}(R) \end{array}$$

such that the whole diagram is cartesian. $\mathrm{Spec}(\kappa(\mathfrak{p}))$ in the bottom-left consists of a single point, which maps to $\mathfrak{p} \in \mathrm{Spec}(R)$ under the horizontal arrows on the bottom row. Thus $\mathrm{Spec}(\kappa(\mathfrak{p}) \otimes_R S)$ bijects via the top row with the fibre of $\mathrm{Spec}(\varphi)$ above $\mathfrak{p}$. In particular we get the following lemma.

LEMMA 8.13. *Let $\varphi : R \to S$ be a ring map. Let $\mathfrak{p}$ be a prime of R. The following are equivalent*

(1) *$\mathfrak{p}$ is in the image of $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$,*
(2) *$S \otimes_R \kappa(\mathfrak{p}) \neq 0$,*
(3) *$\mathfrak{p} = \varphi^{-1}(\mathfrak{p}S)$.*

PROOF. We have already seen the equivalence of the first two in Remark 8.12. The last is just a reformulation of this. Indeed, it is easy to see that (1) implies (3). Conversely if $\varphi^{-1}(\mathfrak{p}S) = \mathfrak{p}$ then $1 \notin \mathfrak{p}S_\mathfrak{p}$ and so (2) holds. $\square$

LEMMA 8.14. *Let $\varphi : R \to S$ be a ring map. The following are equivalent:*

(1) *The map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective.*
(2) *For any ideal $I \subset R$ the inverse image of $\sqrt{IS}$ in R is equal to $\sqrt{I}$.*
(3) *For every prime $\mathfrak{p}$ of R the inverse image of $\mathfrak{p}S$ in R is $\mathfrak{p}$.*

In this case the same is true after any base change: Given a ring map $R \to R'$ the ring map $R' \to R' \otimes_R S$ has the equivalent properties (1), (2), (3) also.

PROOF. The equivalence of (1) and (3) is straightforward from Lemma 8.13, and the implication (2) $\Rightarrow$ (3) is immediate. Assume (1). If $\mathfrak{p} \subset R$ contains I and $\mathfrak{q} \subset S$ pulls back to $\mathfrak{p} \subset R$, then $\sqrt{IS} \subset \mathfrak{q}$, so the inverse image of $\sqrt{IS}$ is contained in $\mathfrak{p}$. This shows that the inverse image of $\sqrt{IS}$ is contained in $\sqrt{I}$, and the reverse is trivial.

For the last part let $R \to R'$ be a ring map, and $\mathfrak{p}' \subset R'$ a prime ideal lying over the prime $\mathfrak{p}$ of R. Then

$$(R' \otimes_R S) \otimes_{R'} \kappa(\mathfrak{p}') = S \otimes_R \kappa(\mathfrak{p}) \otimes_{\kappa(\mathfrak{p})} \kappa(\mathfrak{p}')$$

is not zero as $S \otimes_R \kappa(\mathfrak{p})$ is not zero by assumption and $\kappa(\mathfrak{p}) \to \kappa(\mathfrak{p}')$ is an extension of fields. Then $\mathfrak{p}'$ is in the image of $\mathrm{Spec}(R' \otimes_R S) \to \mathrm{Spec}(R')$ by Lemma 8.13. $\square$

EXERCISE 8.15. If $R \hookrightarrow S$ is an injection of rings, then the image of $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ contains every minimal prime of $\mathrm{Spec}(R)$. (Hint: localize $R \hookrightarrow S$ at a minimal prime of R.)

9. Examples of spectra of rings

In this section we put some examples of spectra.

EXAMPLE 9.1. In this example we describe $X = \mathrm{Spec}(\mathbf{Z}[x]/(x^2-4))$. Let $\mathfrak{p}$ be an arbitrary prime in X. Let $\phi : \mathbf{Z} \to \mathbf{Z}[x]/(x^2-4)$ be the natural ring map. Then, $\phi^{-1}(\mathfrak{p})$ is a prime in $\mathbf{Z}$. If $\phi^{-1}(\mathfrak{p}) = (2)$, then since $\mathfrak{p}$ contains 2, it corresponds to a prime ideal in $\mathbf{Z}[x]/(x^2-4, 2) \cong (\mathbf{Z}/2\mathbf{Z})[x]/(x^2)$ via the map $\mathbf{Z}[x]/(x^2-4) \to \mathbf{Z}[x]/(x^2-4, 2)$. Any prime in $(\mathbf{Z}/2\mathbf{Z})[x]/(x^2)$ corresponds to a prime in $(\mathbf{Z}/2\mathbf{Z})[x]$ containing (x^2). Such primes will then contain x. Since $(\mathbf{Z}/2\mathbf{Z}) \cong (\mathbf{Z}/2\mathbf{Z})[x]/(x)$ is a field, (x) is a maximal ideal. Since any prime contains (x) and (x) is maximal, the ring contains only one prime (x). Thus, in this case, $\mathfrak{p} = (2, x)$. Now, if $\phi^{-1}(\mathfrak{p}) = (q)$ for $q > 2$, then since $\mathfrak{p}$ contains q, it corresponds to a prime ideal in $\mathbf{Z}[x]/(x^2-4, q) \cong (\mathbf{Z}/q\mathbf{Z})[x]/(x^2-4)$ via the map $\mathbf{Z}[x]/(x^2-4) \to \mathbf{Z}[x]/(x^2-4, q)$. Any prime in $(\mathbf{Z}/q\mathbf{Z})[x]/(x^2-4)$ corresponds to a prime in $(\mathbf{Z}/q\mathbf{Z})[x]$ containing $(x^2-4) = (x-2)(x+2)$. Hence, these primes must contain either $x-2$ or $x+2$. Since $(\mathbf{Z}/q\mathbf{Z})[x]$ is a PID, all nonzero primes are maximal, and so there are precisely 2 primes in $(\mathbf{Z}/q\mathbf{Z})[x]$ containing $(x-2)(x+2)$, namely $(x-2)$ and $(x+2)$. In conclusion, there exist two primes $(q, x-2)$ and $(q, x+2)$ since $2 \neq -2 \in \mathbf{Z}/(q)$. Finally, we treat the case where $\phi^{-1}(\mathfrak{p}) = (0)$. Notice that $\mathfrak{p}$ corresponds to a prime ideal in $\mathbf{Z}[x]$ that contains $(x^2-4) = (x-2)(x+2)$. Hence, $\mathfrak{p}$ contains either $(x-2)$ or $(x+2)$. Hence, $\mathfrak{p}$ corresponds to a prime in $\mathbf{Z}[x]/(x-2)$ or one in $\mathbf{Z}[x]/(x+2)$ that intersects $\mathbf{Z}$ only at 0, by assumption. Since $\mathbf{Z}[x]/(x-2) \cong \mathbf{Z}$ and $\mathbf{Z}[x]/(x+2) \cong \mathbf{Z}$, this means that $\mathfrak{p}$ must correspond to 0 in one of these rings. Thus, $\mathfrak{p} = (x-2)$ or $\mathfrak{p} = (x+2)$ in the original ring.

EXAMPLE 9.2. In this example we describe $X = \mathrm{Spec}(\mathbf{Z}[x])$. Fix $\mathfrak{p} \in X$. Let $\phi : \mathbf{Z} \to \mathbf{Z}[x]$ and notice that $\phi^{-1}(\mathfrak{p}) \in \mathrm{Spec}(\mathbf{Z})$. If $\phi^{-1}(\mathfrak{p}) = (q)$ for q a prime number $q > 0$, then $\mathfrak{p}$ corresponds to a prime in $(\mathbf{Z}/(q))[x]$, which must be generated by a polynomial that is irreducible in $(\mathbf{Z}/(q))[x]$. If we choose a representative of this polynomial with minimal degree, then it will also be irreducible in $\mathbf{Z}[x]$. Hence, in this case $\mathfrak{p} = (q, f_q)$ where f_q is an irreducible polynomial in $\mathbf{Z}[x]$ that is irreducible when viewed in $(\mathbf{Z}/(q)[x])$. Now, assume that $\phi^{-1}(\mathfrak{p}) = (0)$. In this case, $\mathfrak{p}$ must be generated by nonconstant polynomials which, since $\mathfrak{p}$ is prime, may be assumed to be irreducible in $\mathbf{Z}[x]$. By Gauss' lemma, these polynomials are also irreducible in $\mathbf{Q}[x]$. Since $\mathbf{Q}[x]$ is a Euclidean domain, if there are at least two distinct irreducibles f, g generating $\mathfrak{p}$, then $1 = af + bg$ for $a, b \in \mathbf{Q}[x]$. Multiplying through by a common denominator, we see that $m = \bar{a}f + \bar{b}g$ for $\bar{a}, \bar{b} \in \mathbf{Z}[x]$ and nonzero $m \in \mathbf{Z}$. This is a contradiction. Hence, $\mathfrak{p}$ is generated by one irreducible polynomial in $\mathbf{Z}[x]$.

EXAMPLE 9.3. In this example we describe $X = \mathrm{Spec}(k[x, y])$ when k is an arbitrary field. Clearly (0) is prime, and any principal ideal generated by an irreducible polynomial will also be a prime since $k[x, y]$ is a unique factorization domain. Now assume $\mathfrak{p}$ is an element of X that is not principal. Since $k[x, y]$ is a Noetherian UFD, the prime ideal $\mathfrak{p}$ can be generated by a finite number of irreducible polynomials $(f_1, \ldots, f_n)$. Now, I claim that if f, g are irreducible polynomials in $k[x, y]$ that are not associates, then $(f, g) \cap k[x] \neq 0$. To do this, it is enough to show that f and g are relatively prime when viewed in $k(x)[y]$. In this case, $k(x)[y]$ is a Euclidean domain, so by applying the Euclidean algorithm and clearing denominators, we obtain $p = af + bg$ for $p, a, b \in k[x]$. Thus, assume this is not the case, that is, that some nonunit $h \in k(x)[y]$ divides both f and g. Then, by Gauss's lemma, for some $a, b \in k(x)$ we have $ah|f$ and $bh|g$ for $ah, bh \in k[x]$ since $Q(k[x]) = k(x)$. By irreducibility, $ah = f$ and $bh = g$ (since $h \notin k(x)$). So, back in $k(x)[y]$, f, g are associates, as $\frac{a}{b}g = f$. Since $k(x) = Q(k[x])$, we can write $g = \frac{r}{s}f$ for elements $r, s \in k[x]$ sharing no common factors. This implies that $sg = rf$ in $k[x, y]$ and so s must divide f since $k[x, y]$ is a UFD. Hence, $s = 1$ or $s = f$. If $s = f$, then $r = g$, implying $f, g \in k[x]$ and thus must be units in $k(x)$ and relatively prime in $k(x)[y]$, contradicting our hypothesis. If $s = 1$, then $g = rf$, another contradiction. Thus, we must have f, g relatively prime in $k(x)[y]$, a Euclidean domain. Thus, we have reduced to the case $\mathfrak{p}$ contains some irreducible polynomial $p \in k[x] \subset k[x, y]$. By the above, $\mathfrak{p}$ corresponds to a prime in the ring $k[x, y]/(p) = k(\alpha)[y]$, where α is an element algebraic over k with minimum polynomial p. This is a PID, and so any prime ideal corresponds to (0) or an irreducible polynomial in $k(\alpha)[y]$. Thus, $\mathfrak{p}$ is of the form (p) or (p, f) where f is a polynomial in $k[x, y]$ that is irreducible in the quotient $k[x, y]/(p)$.

Example 9.4. Consider the ring

$$R = \{f \in \mathbf{Q}[z] \text{ with } f(0) = f(1)\}.$$

Consider the map

$$\varphi : \mathbf{Q}[A, B] \to R$$

defined by $\varphi(A) = z^2 - z$ and $\varphi(B) = z^3 - z^2$. It is easily checked that $(A^3 - B^2 + AB) \subset \ker(\varphi)$ and that $A^3 - B^2 + AB$ is irreducible. Assume that φ is surjective; then since R is an integral domain (it is a subring of an integral domain), $\ker(\phi)$ must be a prime ideal of $\mathbf{Q}[A, B]$. The prime ideals which contain $(A^3 - B^2 + AB)$ are $(A^3 - B^2 + AB)$ itself and any maximal ideal (f, g) with $f, g \in \mathbf{Q}[A, B]$ such that f is irreducible mod g. But R is not a field, so the kernel must be $(A^3 - B^2 + AB)$; hence φ gives an isomorphism $R \to \mathbf{Q}[A, B]/(A^3 - B^2 + AB)$.

To see that φ is surjective, we must express any $f \in R$ as a $\mathbf{Q}$-coefficient polynomial in $A(z) = z^2 - z$ and $B(z) = z^3 - z^2$. Note the relation $zA(z) = B(z)$. Let $a = f(0) = f(1)$. Then $z(z-1)$ must divide $f(z) - a$, so we can write $f(z) = z(z-1)g(z) + a = A(z)g(z) + a$. If $\deg(g) < 2$, then $h(z) = c_1 z + c_0$ and $f(z) = A(z)(c_1 z + c_0) + a = c_1 B(z) + c_0 A(z) + a$, so we are done. If $\deg(g) \geq 2$, then by the polynomial division algorithm, we can write $g(z) = A(z)h(z) + b_1 z + b_0$ ($\deg(h) \leq \deg(g) - 2$), so $f(z) = A(z)^2 h(z) + b_1 B(z) + b_0 A(z)$. Applying division to $h(z)$ and iterating, we obtain an expression for $f(z)$ as a polynomial in $A(z)$ and $B(z)$; hence φ is surjective.

Now let $a \in \mathbf{Q}$, $a \neq 0, \frac{1}{2}, 1$ and consider

$$R_a = \{f \in \mathbf{Q}[z, \frac{1}{z-a}] \text{ with } f(0) = f(1)\}.$$

This is a finitely generated $\mathbf{Q}$-algebra as well: it is easy to check that the functions $z^2 - z$, $z^3 - z$, and $\frac{a^2-a}{z-a} + z$ generate R_a as an $\mathbf{Q}$-algebra. We have the following inclusions:

$$R \subset R_a \subset \mathbf{Q}[z, \frac{1}{z-a}], \quad R \subset \mathbf{Q}[z] \subset \mathbf{Q}[z, \frac{1}{z-a}].$$

Recall (Lemma 8.9) that for a ring T and a multiplicative subset $S \subset T$, the ring map $T \to S^{-1}T$ induces a map on spectra $\mathrm{Spec}(S^{-1}T) \to \mathrm{Spec}(T)$ which is a homeomorphism onto the subset

$$\{\mathfrak{p} \in \mathrm{Spec}(T) \mid S \cap \mathfrak{p} = \emptyset\} \subset \mathrm{Spec}(T).$$

When $S = \{1, f, f^2, \dots\}$ for some $f \in T$, this is the open set $D(f) \subset T$. We now verify a corresponding property for the ring map $R \to R_a$: we will show that the map $\theta : \mathrm{Spec}(R_a) \to \mathrm{Spec}(R)$ induced by inclusion $R \subset R_a$ is a homeomorphism onto an open subset of $\mathrm{Spec}(R)$ by verifying that θ is an injective local homeomorphism. We do so with respect to an open cover of $\mathrm{Spec}(R_a)$ by two distinguished opens, as we now describe. For any $r \in \mathbf{Q}$, let $\mathrm{ev}_r : R \to \mathbf{Q}$ be the homomorphism given by evaluation at r. Note that for $r = 0$ and $r = 1-a$, this can be extended to a homomorphism $\mathrm{ev}'_r : R_a \to \mathbf{Q}$ (the latter because $\frac{1}{z-a}$ is well-defined at $z = 1-a$, since $a \neq \frac{1}{2}$). However, ev_a does not extend to R_a. Write $\mathfrak{m}_r = \ker(\mathrm{ev}_r)$. We have

$$\begin{aligned} \mathfrak{m}_0 &= (z^2 - z, z^3 - z), \\ \mathfrak{m}_a &= ((z-1+a)(z-a), (z^2-1+a)(z-a)), \text{ and} \\ \mathfrak{m}_{1-a} &= ((z-1+a)(z-a), (z-1+a)(z^2-a)). \end{aligned}$$

To verify this, note that the right-hand sides are clearly contained in the left-hand sides. Then check that the right-hand sides are maximal ideals by writing the generators in terms of A and B, and viewing R as $\mathbf{Q}[A,B]/(A^3 - B^2 + AB)$. Note that $\mathfrak{m}_a$ is not in the image of θ: we have

$$(z^2-z)^2(z-a)(\frac{a^2-a}{z-a} + z) = (z^2-z)^2(a^2-a) + (z^2-z)^2(z-a)z$$

The left hand side is in $\mathfrak{m}_a R_a$ because $(z^2-z)(z-a)$ is in $\mathfrak{m}_a$ and because $(z^2 - z)(\frac{a^2-a}{z-a} + z)$ is in R_a. Similarly the element $(z^2-z)^2(z-a)z$ is in $\mathfrak{m}_a R_a$ because (z^2-z) is in R_a and $(z^2-z)(z-a)$ is in $\mathfrak{m}_a$. As $a \notin \{0,1\}$ we conclude that $(z^2-z)^2 \in \mathfrak{m}_a R_a$. Hence no ideal I of R_a can satisfy $I \cap R = \mathfrak{m}_a$, as such an I would have to contain $(z^2-z)^2$, which is in R but not in $\mathfrak{m}_a$. The distinguished open set $D((z-1+a)(z-a)) \subset \mathrm{Spec}(R)$ is equal to the complement of the closed set $\{\mathfrak{m}_a, \mathfrak{m}_{1-a}\}$. Then check that $R_{(z-1+a)(z-a)} = (R_a)_{(z-1+a)(z-a)}$; calling this localized ring R', then, it follows that the map $R \to R'$ factors as $R \to R_a \to R'$. By Lemma 8.9, then, these maps express $\mathrm{Spec}(R') \subset \mathrm{Spec}(R_a)$ and $\mathrm{Spec}(R') \subset \mathrm{Spec}(R)$ as open subsets; hence $\theta : \mathrm{Spec}(R_a) \to \mathrm{Spec}(R)$, when restricted to $D((z-1+a)(z-a))$, is a homeomorphism onto an open subset. Similarly, θ restricted to $D((z^2+z+2a-2)(z-a)) \subset \mathrm{Spec}(R_a)$ is a homeomorphism onto the open subset $D((z^2+z+2a-2)(z-a)) \subset \mathrm{Spec}(R)$. Depending on whether $z^2+z+2a-2$ is irreducible or not over $\mathbf{Q}$, this former distinguished open set has complement equal to one or two closed points along with the closed point $\mathfrak{m}_a$. Furthermore, the ideal in R_a generated by the elements $(z^2+z+2a-a)(z-a)$ and $(z-1+a)(z-a)$ is all of R_a, so these two distinguished open sets cover $\mathrm{Spec}(R_a)$. Hence in order to show that θ is a homeomorphism onto $\mathrm{Spec}(R) - \{\mathfrak{m}_a\}$, it suffices to show that these one or two points can never equal $\mathfrak{m}_{1-a}$. And this is indeed the case, since $1-a$ is a root of $z^2+z+2a-2$ if and only of $a = 0$ or $a = 1$, both of which do not occur.

Despite this homeomorphism which mimics the behavior of a localization at an element of R, while $\mathbf{Q}[z, \frac{1}{z-a}]$ is the localization of $\mathbf{Q}[z]$ at the maximal ideal $(z-a)$, the ring R_a is *not* a localization of R: Any localization $S^{-1}R$ results in more units than the original ring R. The units of R are $\mathbf{Q}^\times$, the units of $\mathbf{Q}$. In fact, it is easy to see that the units of R_a are $\mathbf{Q}^*$. Namely, the units of $\mathbf{Q}[z, \frac{1}{z-a}]$ are $c(z-a)^n$ for $c \in \mathbf{Q}^*$ and $n \in \mathbf{Z}$ and it is clear that these are in R_a only if $n = 0$. Hence R_a has no more units than R does, and thus cannot be a localization of R.

We used the fact that $a \neq 0, 1$ to ensure that $\frac{1}{z-a}$ makes sense at $z = 0, 1$. We used the fact that $a \neq 1/2$ in a few places: (1) In order to be able to talk about the kernel of ev_{1-a} on R_a, which ensures that $\mathfrak{m}_{1-a}$ is a point of R_a (i.e., that R_a is missing just one point of R). (2) At the end in order to conclude that $(z-a)^{k+\ell}$ can only be in R for $k = \ell = 0$; indeed, if $a = 1/2$, then this is in R as long as $k + \ell$ is even. Hence there would indeed be more units in R_a than in R, and R_a could possibly be a localization of R.

10. Glueing

In this section we show that given an open covering

$$\mathrm{Spec}(R) = \bigcup\nolimits_{i=1}^{n} D(f_i)$$

by standard opens, and given an element $h_i \in R_{f_i}$ for each i such that $h_i = h_j$ as elements of $R_{f_i f_j}$ then there exists a unique $h \in R$ such that the image of h in R_{f_i} is h_i. This result can be interpreted in two ways:

(1) The rule $D(f) \mapsto R_f$ is a sheaf of rings on the standard opens.
(2) If we think of elements of R_f as the "algebraic" or "regular" functions on $D(f)$, then these glue as would continuous, resp. differentiable functions on a topological, resp. differentiable manifold.

The following lemma is what we want to prove.

Lemma 10.1. *Let R be a ring, and let $f_1, f_2, \ldots f_n \in R$ generate the unit ideal in R. Then the following sequence is exact:*

$$0 \longrightarrow R \longrightarrow \bigoplus\nolimits_i R_{f_i} \longrightarrow \bigoplus\nolimits_{i,j} R_{f_i f_j}$$

where the maps $\alpha : R \longrightarrow \bigoplus_i R_{f_i}$ and $\beta : \bigoplus_i R_{f_i} \longrightarrow \bigoplus_{i,j} R_{f_i f_j}$ are defined as

$$\alpha(x) = \left(\frac{x}{1}, \ldots, \frac{x}{1}\right) \text{ and } \beta\left(\frac{x_1}{f_1^{r_1}}, \ldots, \frac{x_n}{f_n^{r_n}}\right) = \left(\frac{x_i}{f_i^{r_i}} - \frac{x_j}{f_j^{r_j}} \text{ in } R_{f_i f_j}\right).$$

Proof. We first show that α is injective, and then that the image of α equals the kernel of β. Assume there exists $x \in R$ such that $\alpha(x) = (0, \ldots, 0)$. Then $\frac{x}{1} = 0$ in R_{f_i} for all i. This means, for all i, there exists a number n_i such that

$$f_i^{n_i} x = 0$$

Since the f_i generate R, we can pick a_i so

$$1 = \sum\nolimits_{i=1}^{n} a_i f_i$$

Then for all $M \geq \sum n_i$, we have

$$x = \left(\sum a_i f_i\right)^M x = 0$$

since each term has a factor of at least $f_i^{n_i}$ for some i. Thus, if $\alpha(x) = 0$, $x = 0$ and α is injective.

The image of α is evidently in the kernel of β, and it remains only to verify, assuming

$$\beta\left(\frac{x_1}{f_1^{r_1}}, \ldots, \frac{x_n}{f_n^{r_n}}\right) = 0,$$

that there exists $x \in R$ so that for all i,

$$\frac{x}{1} = \frac{x_i}{f_i^{r_i}}.$$

For all pairs i, j, there exists an n_{ij} such that

$$f_i^{n_{ij}} f_j^{n_{ij}} (f_j^{r_j} x_i - f_i^{r_i} x_j) = 0.$$

Replacing $x_i/f_i^{r_i}$ with $(x_i f_i^N)/(f_i^{r_i+N})$ for $N \gg 0$, we may assume without loss of generality that $f_j^{r_j} x_i = f_i^{r_i} x_j$ for all i, j.

Since $(f_1, \ldots, f_n) = 1$, the $f_i^{r_i}$'s also generate the unit ideal, and so we may write $1 = \sum_i a_i f_i^{r_i}$ for some elements $a_i \in R$. We claim that $x := \sum_i a_i x_i$ is the desired element. Calculating

$$x f_j^{r_j} = \sum_i a_i x_i f_j^{r_j} = \sum_i a_i f_i^{r_i} x_j = x_j$$

we indeed have $x = x_j/f_j^{r_j}$ in R_{f_j}. $\square$

As a first application of these results we describe the open and closed subsets of a spectrum in terms of the idempotents of the ring. In particular this characterizes the connected components of $\mathrm{Spec}(R)$ provided that there are finitely many components. The characterization when there are infinitely many components is more subtle.

LEMMA 10.2. *Let R be a ring. For each $U \subset \mathrm{Spec}(R)$ which is open and closed there exists a unique idempotent $e \in R$ such that $U = D(e)$. This induces a 1-1 correspondence between open and closed subsets $U \subset \mathrm{Spec}(R)$ and idempotents $e \in R$.*

PROOF. Since U is closed it is quasi-compact by Lemma 8.7, and similarly for its complement. Write $U = \bigcup_{i=1}^n D(f_i)$ as a finite union of standard opens. Similarly, write $\mathrm{Spec}(R) \setminus U = \bigcup_{j=1}^m D(g_j)$ as a finite union of standard opens.

Lemma 10.1 applied to the elements $1 \in R_{f_i}$ for all i and $0 \in R_{g_j}$ for all j shows that there exists a unique element $e \in R$ such that $e = 1$ in R_{f_i} for all i and $e = 0$ in R_{g_j} for all j. Note that e^2 has exactly the same property; thus $e^2 = e$ (uniqueness) and e is idempotent.

For each prime $\mathfrak{p}$ of R, the image of e in the field $\kappa(\mathfrak{p})$ (or indeed the image of any idempotent) is idempotent and hence is either 0 or 1, evidently depending on whether e is or is not in $\mathfrak{p}$. On the other hand the image of e in $\kappa(\mathfrak{p})$ is 1 if and only if $\mathfrak{p} \in U$: use the fact that $R_\mathfrak{p}$ is a localization of R_{f_i} (resp. R_{g_j}) if $\mathfrak{p} \in D(f_i)$ (resp. $D(g_j)$). This shows $U = D(e)$.

If e is an idempotent, then so is $1 - e$, and the equation $e(1 - e) = 0$ quickly implies that $\mathrm{Spec}(R) = D(e) \coprod D(1 - e)$. In particular $D(e)$ is both closed and open.

It remains to show that if e' is another idempotent such that $D(e') = D(e)$ then $e' = e$. By the observation in the last paragraph we have $e - e' = 0$ in $\kappa(\mathfrak{p})$ for all $\mathfrak{p}$. Hence $e - e' \in \bigcap \mathfrak{p}$ is nilpotent. But two idempotents whose difference is nilpotent must be equal: consider $e - e'$ raised to a sufficiently large odd power and note that all terms except the first and last will cancel out. $\square$

LEMMA 10.3.

(1) *Let R_1 and R_2 be rings. The spectrum of $R = R_1 \times R_2$ is the disjoint union of the spectrum of R_1 and the spectrum of R_2. More precisely, the maps $R \to R_1$, $(x, y) \mapsto x$ and $R \to R_2$, $(x, y) \mapsto y$ induce continuous maps $\mathrm{Spec}(R_1) \to \mathrm{Spec}(R)$ and $\mathrm{Spec}(R_2) \to \mathrm{Spec}(R)$, and The induced map*
$$\mathrm{Spec}(R_1) \amalg \mathrm{Spec}(R_2) \longrightarrow \mathrm{Spec}(R)$$
is a homeomorphism.

(2) *Conversely, if R is a ring and $\mathrm{Spec}(R) = U \amalg V$ with both U and V open, then $R \cong R_1 \times R_2$ with $U \cong \mathrm{Spec}(R_1)$ and $V \cong \mathrm{Spec}(R_2)$ via the maps in (1). Moreover, both R_1 and R_2 are localizations as well as quotients of the ring R.*

PROOF. If $R = R_1 \times R_2$, observe that R_1 is the localization of R at $(1, 0)$, and the projection $(x, y) \mapsto x$ is the localization map. Similarly for R_2. Thus part (1) follows from Lemma 8.10.

By Lemma 10.2 we have $U = D(e)$ for some idempotent e, and evidently also $V = D(1 - e)$. By Lemma 10.1 we see that $R \cong R_e \times R_{1-e}$ (since clearly $R_{e(1-e)} = 0$ so the glueing condition is trivial; of course it is trivial to prove the product decomposition directly in this case). The lemma follows. $\square$

11. Local properties of modules

In this section we set down a number of standard results of the form: if something is true for all members of a standard open covering then it is true. In fact, it often suffices to check things on the level of local rings as in the following lemma.

LEMMA 11.1. *Let R be a ring, and suppose that $f_1, \ldots, f_n$ is a finite list of elements such that $\bigcup D(f_i) = \mathrm{Spec}(R)$ (or in other words $(f_1, \ldots, f_n) = R$).*

(1) *For an element x of an R-module M the following are equivalent.*
   (a) *$x = 0$,*
   (b) *x maps to zero in M_{f_i} for all i,*
   (c) *x maps to zero in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$,*
   (d) *x maps to zero in $M_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R.*
   In other words, the map $M \to \prod_{\mathfrak{m}} M_{\mathfrak{m}}$ is injective.
(2) *Given an R-module M the following are equivalent.*
   (a) *M is zero,*
   (b) *M_{f_i} is zero for all i,*
   (c) *$M_{\mathfrak{p}}$ is zero for all $\mathfrak{p} \in \mathrm{Spec}(R)$,*
   (d) *$M_{\mathfrak{m}}$ is zero for all maximal ideals $\mathfrak{m}$ of R.*
(3) *Given a complex $M' \to M \to M''$ of R-modules the following are equivalent.*
   (a) *$M' \to M \to M''$ is exact,*
   (b) *$M'_{f_i} \to M_{f_i} \to M''_{f_i}$ is exact for all i,*
   (c) *$M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}}$ is exact for every prime $\mathfrak{p}$ of R,*
   (d) *$M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to M''_{\mathfrak{m}}$ is exact for every maximal ideal $\mathfrak{m}$ of R.*

(4) *Given a map $g : M \to M'$ of R-modules and for each property $P \in$ {injective, surjective, bijective} the following are equivalent*
 (a) *g has P,*
 (b) *$g_i : M_{f_i} \to M'_{f_i}$ has P for all i,*
 (c) *$g_\mathfrak{p} : M_\mathfrak{p} \to M'_\mathfrak{p}$ has P for all primes $\mathfrak{p}$ of R,*
 (d) *$g_\mathfrak{m} : M_\mathfrak{m} \to M'_\mathfrak{m}$ has P for all maximal ideals $\mathfrak{m}$ of R.*

PROOF. In each case the implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) are immediate using the exactness of localizations, so we must only check that (d) implies (a).

Let $x \in M$ as in (1). Let $I = \{f \in R \mid fx = 0\}$. It is easy to see that I is an ideal (it is the annihilator of x). Condition (1)(d) means that for all maximal ideals $\mathfrak{m}$ there exists an $f \in R \setminus \mathfrak{m}$ such that $fx = 0$. In other words, $V(I)$ does not contain a closed point. By Lemma 8.5 we see I is the unit ideal. Hence x is zero, i.e., (1)(a) holds. This proves (1).

Part (2) follows by applying (1) to all elements of M simultaneously.

Proof of (3). Let H be the cohomology of the sequence, i.e., $H = \ker(M_2 \to M_3)/\mathrm{im}(M_1 \to M_2)$. By Proposition 6.9 we have that $H_\mathfrak{p}$ is the cohomology of the sequence $M_{1,\mathfrak{p}} \to M_{2,\mathfrak{p}} \to M_{3,\mathfrak{p}}$. Hence (3) is a consequence of (2).

Parts (4) for "injective" and "surjective" are special cases of (3), and for "bijective" follows formally on combining the other two. $\square$

Our finiteness conditions are also local.

LEMMA 11.2. *Let R be a ring. Let M be an R-module. Suppose that $f_1, \ldots, f_n$ is a finite list of elements of R such that $\bigcup D(f_i) = \mathrm{Spec}(R)$ in other words $(f_1, \ldots, f_n) = R$.*
 (1) *If each M_{f_i} is a finite R_{f_i}-module, then M is a finite R-module.*
 (2) *If each M_{f_i} is a finitely presented R_{f_i}-module, then M is a finitely presented R-module.*

PROOF. (1) For each i take a finite generating set X_i of M_{f_i}. Clearing denominators, we may assume that the elements of X_i are in the image of the localization map $M \to M_{f_i}$, so we take a finite set Y_i of preimages of the elements of X_i in M. Let Y be the union of these sets. Consider the obvious R-linear map $R^Y \to M$ sending the basis element e_y to y. By assumption the cokernel of this map is trivial after localizing at each f_i, so the cokernel is trivial by Lemma 11.1(4).

(2) From the previous part, we have a short exact sequence

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

Since localization is an exact functor and M_{f_i} is finitely presented we see that K_{f_i} is finite for all i by Lemma 1.3. By (1) this implies that K is a finite R-module and therefore M is finitely presented. $\square$

EXERCISE 11.3. In the setting of Lemma 11.2, let S be an R-algebra.
 (1) If each S_{f_i} is a finite type R-algebra, so is S.
 (2) If each S_{f_i} is of finite presentation over R, so is S. (Use Exercise 1.5.)

Flatness is local

LEMMA 11.4. *Let R be a ring. Let $S \subset R$ be a multiplicative subset.*

(1) *The localization $S^{-1}R$ is a flat R-algebra.*
(2) *If M is an $S^{-1}R$-module, then M is a flat R-module if and only if M is a flat $S^{-1}R$-module.*

Proof. (1) is a restatement of the exactness of localization, while (2) is a restatement of Exercise 6.6. □

Lemma 11.5. *Let $R \to A$ be a ring map, and write φ for the corresponding map $\operatorname{Spec}(A) \to \operatorname{Spec}(R)$. Suppose that $g_1, \ldots, g_m$ generate the unit ideal of A. Let M be an A-module. Then the following are equivalent.*

(1) *M is a flat R-module,*
(2) *M_{g_i} is a flat R-module for $i = 1, \ldots, m$,*
(3) *$M_{\mathfrak{p}}$ is a flat $R_{\varphi(\mathfrak{p})}$-module for all primes $\mathfrak{p}$ of A,*
(4) *$M_{\mathfrak{m}}$ is a flat $R_{\varphi(\mathfrak{m})}$-module for all maximal ideals $\mathfrak{m}$ of A.*

This is applicable in particular with $R = A$ and φ the identity map.

Proof. The implications (1) ⇒ (2) ⇒ (3) ⇒ (4) are easy using Lemma 11.4.

Suppose that (4) holds. Let $N \to N'$ be an injective map of R-modules. We have to show the map $N \otimes_R M \to N' \otimes_R M$ is injective. Let K be its kernel. We can think of this as a map of A-modules. The localization $(N \otimes_R M)_{\mathfrak{m}} \to (N' \otimes_R M)_{\mathfrak{m}}$ is the same as

$$N_{\varphi(\mathfrak{m})} \otimes_{R_{\varphi(\mathfrak{m})}} M_{\mathfrak{m}} \to (N')_{\varphi(\mathfrak{m})} \otimes_{R_{\varphi(\mathfrak{m})}} M_{\mathfrak{m}}.$$

But this is injective because localization at $\varphi(\mathfrak{m})$ is exact and $M_{\mathfrak{m}}$ is flat. Hence $K_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$, and $K = 0$ by Lemma 11.1(4). □

Finite projective is finite locally free

Definition 11.6. Let R be a ring and M an R-module.

(1) We say that M is *locally free* if we can cover $\operatorname{Spec}(R)$ by standard opens $D(f_i)$, $i \in I$ such that M_{f_i} is a free R_{f_i}-module for all $i \in I$.
(2) We say that M is *finite locally free* if we can choose the covering such that each M_{f_i} is finite free.
(3) We say that M is *finite locally free of rank r* if we can choose the covering such that each M_{f_i} is isomorhic to $R_{f_i}^{\oplus r}$.

Note that a finite locally free R-module is automatically finitely presented by Lemma 11.2.

Lemma 11.7. *Let R be a ring and let M be an R-module. The following are equivalent*

(1) *M is finite projective,*
(2) *M is finite locally free (equivalently, finite and locally free),*
(3) *M is finitely presented and for all primes $\mathfrak{p}$ of R the localization $M_{\mathfrak{p}}$ is free,*
(4) *M is finitely presented and for all maximal ideals $\mathfrak{m}$ of R the localization $M_{\mathfrak{m}}$ is free, and*
(5) *M is finitely presented and R-flat.*

Proof. Assume (1), so we can write $K \oplus M \cong R^{\oplus n}$. So K is a direct summand of R^n and thus finitely generated. This shows $M = R^{\oplus n}/K$ is finitely presented. Considering Lemma 5.12 we see that (1) ⇒ (5).

The implications (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) are clear (the latter using that flatness can be checked locally, Lemma 11.5).

Suppose that M satisfies (2). Let us check (1). We have to show that $\mathrm{Hom}_R(M, -)$ is exact. Let $0 \to N'' \to N \to N' \to 0$ be a short exact sequence of R-module. We want to show that $0 \to \mathrm{Hom}_R(M, N'') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N') \to 0$ is exact. As M is finite locally free there exists a covering $\mathrm{Spec}(R) = \bigcup D(f_i)$ such that M_{f_i} is finite free. By Lemma 6.12 and the observation that M is finitely presented we see that

$$0 \to \mathrm{Hom}_R(M, N'')_{f_i} \to \mathrm{Hom}_R(M, N)_{f_i} \to \mathrm{Hom}_R(M, N')_{f_i} \to 0$$

is equal to $0 \to \mathrm{Hom}_{R_{f_i}}(M_{f_i}, N''_{f_i}) \to \mathrm{Hom}_{R_{f_i}}(M_{f_i}, N_{f_i}) \to \mathrm{Hom}_{R_{f_i}}(M_{f_i}, N'_{f_i}) \to 0$ which is exact as M_{f_i} is free and as the localization $0 \to N''_{f_i} \to N_{f_i} \to N'_{f_i} \to 0$ is exact (as localization is exact). We conclude that $0 \to \mathrm{Hom}_R(M, N'') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N') \to 0$ is exact by Lemma 11.1.

Finally we check that (5) implies (2). Pick any prime $\mathfrak{p}$ and $x_1, \ldots, x_r \in M$ which map to a basis of $M \otimes_R \kappa(\mathfrak{p})$. By Nakayama's Lemma 7.14 these elements generate M_g for some $g \in R$, $g \notin \mathfrak{p}$. The corresponding surjection $\varphi : R_g^{\oplus r} \to M_g$ has the following two properties: (a) $\ker(\varphi)$ is a finite R_g-module (see Lemma 1.3) and (b) $\ker(\varphi) \otimes \kappa(\mathfrak{p}) = 0$ by flatness of M_g over R_g (see Lemma 5.13). Hence by Nakayama's lemma again there exists a $g' \in R_g$, $g' \notin \mathfrak{p}R_g$ such that $\ker(\varphi)_{g'} = 0$. In other words, $\mathfrak{p} \in D(gg')$ in $M_{gg'}$ is free. $\square$

Reducedness is local

DEFINITION 11.8. A ring R is *reduced* is it has no nonzero nilpotent elements.

LEMMA 11.9. *If the ring R is reduced then so is any localization of R. Consequently, if $\mathrm{Spec}(R) = \bigcup_{i=1}^n D(f_i)$ then the following are equivalent:*

(1) *R is reduced,*
(2) *R_{f_i} is reduced for all i,*
(3) *$R_{\mathfrak{p}}$ is reduced for all prime ideals $\mathfrak{p}$ of R,*
(4) *$R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$ of R.*

PROOF. For the first statement, let $S \subset R$ be a multiplicative subset, and suppose that $x^n = 0$ in $S^{-1}R$ for some $x \in R$. Then there exists $s \in S$ such that $sx^n = 0$ in R; then $(sx)^n = 0$, and $sx = 0$ because R is reduced. It follows that $x = 0$ in $S^{-1}R$.

The first statement already gives the implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4). Suppose that $R_{\mathfrak{m}}$ is reduced. If $x \in R$ is nilpotent, then $x = 0$ in $R_{\mathfrak{m}}$ for all $\mathfrak{m}$, and so $x = 0$ by Lemma 11.1(1). This shows that (4) implies (1). $\square$

12. Irreducible components of spectra

We show that irreducible components of the spectrum of a ring correspond to the minimal primes in the ring, and describe the local rings at minimal primes.

DEFINITION 12.1. Let X be a topological space.

(1) We say X is *irreducible*, if X is not empty, and whenever $X = Z_1 \cup Z_2$ with Z_i closed, we have $X = Z_1$ or $X = Z_2$.
(2) We say $Z \subset X$ is an *irreducible component* of X if Z is a maximal irreducible subset of X.

An irreducible space is obviously connected.

EXERCISE 12.2. Let X be a topological space. Any irreducible component of X is closed, and X is the union of its irreducible components.

A singleton is irreducible. Thus if $x \in X$ is a point then the closure $\overline{\{x\}}$ is an irreducible closed subset of X.

LEMMA 12.3. *Let R be a ring.*

(1) *For a prime $\mathfrak{p} \subset R$ the closure of $\{\mathfrak{p}\}$ in the Zariski topology is $V(\mathfrak{p})$.*
(2) *The irreducible closed subsets of* $\text{Spec}(R)$ *are exactly the subsets $V(\mathfrak{p})$, with $\mathfrak{p} \subset R$ a prime.*
(3) *The irreducible components of* $\text{Spec}(R)$ *are exactly the subsets $V(\mathfrak{p})$, with $\mathfrak{p} \subset R$ a minimal prime.*

PROOF. To show (2), let $V(I) \subset \text{Spec}(R)$ with I a radical ideal. If I is not prime, then choose $a, b \in R$, $a, b \notin I$ with $ab \in I$. In this case $V(I, a) \cup V(I, b) = V(I)$. If we had $V(I, a) = V(I)$ then $\sqrt{(I, a)} = \sqrt{I} = I$ since I is radical, and so $a \in I$. Thus $V(I, a) \neq V(I)$. Similarly $V(I, b) \neq V(I)$. Hence $V(I)$ is not irreducible. □

In other words, this lemma shows that every irreducible closed subset of $\text{Spec}(R)$ is of the form $V(\mathfrak{p})$ for some prime $\mathfrak{p}$. Since $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$ we see that each irreducible closed subset has a unique generic point in the sense of the following definition.

DEFINITION 12.4. Let X be a topological space. Let $Z \subset X$ be an irreducible closed subset. A *generic point* of Z is a point $\xi \in Z$ such that $Z = \overline{\{\xi\}}$.

A topological space with the property that every irreducible closed subset has a unique generic point is called a sober space.

We now consider the local rings $R_{\mathfrak{p}}$ at minimal primes $\mathfrak{p}$ of a ring R.

LEMMA 12.5. *Let $\mathfrak{p}$ be a minimal prime of a ring R. Every element of $\mathfrak{p}$ is a zerodivisor. Every element of the maximal ideal of $R_{\mathfrak{p}}$ is nilpotent. If R is reduced then $R_{\mathfrak{p}}$ is a field.*

PROOF. If $\mathfrak{p}$ is a minimal prime of R then $\mathfrak{p}R_{\mathfrak{p}}$ is the only prime of $R_{\mathfrak{p}}$, hence is the radical of $R_{\mathfrak{p}}$. This gives the second statement. If $x \in \mathfrak{p}$ is nonzero and $n > 0$ is minimal such that $x^n = 0$ in $R_{\mathfrak{p}}$, then there exists $s \in R \setminus \mathfrak{p}$ such that $sx^n = 0$. By the minimality of n we have $sx^{n-1} \neq 0$, so that x is a zerodivisor. This gives the first statement. If R is reduced, then so is $R_{\mathfrak{p}}$ by Lemma 11.9. Then $\mathfrak{p}R_{\mathfrak{p}} = 0$ and so $R_{\mathfrak{p}}$ is a field. □

LEMMA 12.6. *Let R be a reduced ring. Then*

(1) *R is a subring of a product of fields,*
(2) *$R \to \prod_{\mathfrak{p} \text{ minimal}} R_{\mathfrak{p}}$ is an embedding into a product of fields,*
(3) *$\bigcup_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$ is the set of zerodivisors of R.*

PROOF. By Lemma 12.5 each of the rings $R_{\mathfrak{p}}$ is a field. In particular, the kernel of the ring map $R \to R_{\mathfrak{p}}$ is $\mathfrak{p}$. By Lemma 8.5 we have $\bigcap_{\mathfrak{p}} \mathfrak{p} = (0)$. Hence (2) and (1) are true. If $xy = 0$ and $y \neq 0$, then $y \notin \mathfrak{p}$ for some minimal prime $\mathfrak{p}$. Hence $x \in \mathfrak{p}$. Thus every zerodivisor of R is contained in $\bigcup_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$. The converse is the first statement of Lemma 12.5. □

The total ring of fractions $Q(R)$ of a ring R was introduced in Example 6.8.

LEMMA 12.7. *Let R be a ring. If $f \in R$ is such that R_f is a local ring, with maximal ideal $\mathfrak{p}R_f$ for $\mathfrak{p} \in \operatorname{Spec}(R)$, then $R_f \cong R_{\mathfrak{p}}$.*

PROOF. Since $f \notin \mathfrak{p}$ there is a natural map $R_f \to R_{\mathfrak{p}}$. Since R_f is a local ring with maximal ideal $\mathfrak{p}R_f$, every element of $R \setminus \mathfrak{p}$ is already invertible in R_f, and the map $R_f \to R_{\mathfrak{p}}$ is an isomorphism. ☐

LEMMA 12.8. *Let R be a ring. Assume that R has finitely many minimal primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$, and that $\mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_t$ is the set of zerodivisors of R. Then the total ring of fractions $Q(R)$ is equal to $R_{\mathfrak{q}_1} \times \cdots \times R_{\mathfrak{q}_t}$.*

PROOF. For any nonminimal prime $\mathfrak{p} \subset R$ we see that $\mathfrak{p} \not\subset \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_t$ by prime avoidance (Lemma 7.2). Hence $\operatorname{Spec}(Q(R)) = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$ (as subsets of $\operatorname{Spec}(R)$, see Lemma 8.9). Therefore $\operatorname{Spec}(Q(R))$ is a finite discrete set and it follows that $Q(R) = A_1 \times \cdots \times A_t$ with $\operatorname{Spec}(A_i) = \{\mathfrak{q}_i\}$, see Lemma 10.3. Moreover A_i is a local ring, and a localization of R, and so $A_i \cong R_{\mathfrak{q}_i}$ by Lemma 12.7. Finally, note that the isomorphism $Q(R) \cong R_{\mathfrak{q}_1} \times \cdots \times R_{\mathfrak{q}_t}$ that we have constructed is precisely the product of the natural maps $Q(R) \to R_{\mathfrak{q}_i}$ (which exist since any nonzerodivisor is contained in $R \setminus \mathfrak{q}_i$). ☐

13. Images of ring maps of finite presentation

In this section we prove some results on the topology of maps $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ induced by ring maps $R \to S$, mainly Chevalley's Theorem.

LEMMA 13.1. *Let $U \subset \operatorname{Spec}(R)$ be open. The following are equivalent:*

(1) *U is quasi-compact,*
(2) *U is a finite union of standard opens, and*
(3) *there exists a finitely generated ideal $I \subset R$ such that $X \setminus V(I) = U$.*

PROOF. Since each standard open is quasi-compact (because $D(f) \subset \operatorname{Spec}(R)$ is homeomorphic to $\operatorname{Spec}(R_f)$, which is quasi-compact by Lemma 8.7), the equivalence between (1), (2), (3) is straightforward. ☐

DEFINITION 13.2. Let X be a topological space. Let $E \subset X$ be a subset of X. We say E is *constructible* in X if E is a finite union of subsets of the form $U \cap V^c$ where $U, V \subset X$ are open and quasicompact in X.

EXERCISE 13.3. The collection of constructible sets is closed under finite intersections, finite unions and complements.

LEMMA 13.4. *Let X be a subspace of* $\operatorname{Spec}(R)$*. Suppose that either:*

(1) *X is open in* $\operatorname{Spec}(R)$*, or else*
(2) *the complement of X is a quasi-compact open.*

Then the image in $\operatorname{Spec}(R)$ *of any constructible subspace of X is constructible.*

PROOF. If $U, V \subset X$ are quasi-compact opens, we need to prove that $U \cap V^c$ is constructible in $\operatorname{Spec}(R)$. Although the complement should by definition be taken in X, in fact it may be taken in $\operatorname{Spec}(R)$ instead, since the complement of V in X is just the intersection of X with the complement of V in $\operatorname{Spec}(R)$. To show that $U \cap V^c$ is constructible we need to prove that U (and V) are constructible in $\mathrm{Spec}(R)$. If X is open, this is immediate: U is itself a quasi-compact open in $\mathrm{Spec}(R)$.

In case (2), write $U = X \cap U'$ with U' open in $\mathrm{Spec}(R)$. Choose an open cover $U' = \cup_i U_i'$ by quasi-compact opens (this is possible because $\mathrm{Spec}(R)$ has a quasi-compact basis). Then $U = \cup_i X \cap U_i'$, and the quasi-compactness of U in X means that U is the union of finitely many of the $X \cap U_i'$. Since X by hypothesis is the complement of a quasi-compact open, this realizes U as a constructible subset of $\mathrm{Spec}(R)$. $\square$

We note the following two special cases.

Lemma 13.5. *Let R be a ring. Let f be an element of R. Let $S = R_f$. Then the image of a constructible subset of $\mathrm{Spec}(S)$ is constructible in $\mathrm{Spec}(R)$.*

Lemma 13.6. *Let R be a ring. Let I be a finitely generated ideal of R. Let $S = R/I$. Then the image of a constructible of $\mathrm{Spec}(S)$ is constructible in $\mathrm{Spec}(R)$.*

Lemma 13.7. *Let R be a ring. The map $\mathrm{Spec}(R[x]) \to \mathrm{Spec}(R)$ is open, and the image of any standard open is a quasi-compact open.*

Proof. It suffices to show that the image of a standard open $D(f)$, $f \in R[x]$ is quasi-compact open. By Lemma 8.13, a prime $\mathfrak{p} \subset R$ is in the image of $D(f) = \mathrm{Spec}(R[x]_f) \to \mathrm{Spec}(R)$ if and only if $R[x]_f \otimes_R \kappa(\mathfrak{p}) = \kappa(\mathfrak{p})[x]_{\overline{f}}$ is not the zero ring. This is exactly the condition that f does not map to zero in $\kappa(\mathfrak{p})[x]$. Hence we see: if $f = a_d x^d + \cdots + a_0$, then the image of $D(f)$ is $D(a_d) \cup \cdots \cup D(a_0)$. $\square$

We prove a property of characteristic polynomials which will be used below.

Lemma 13.8. *Let $R \to A$ be a ring homomorphism. Assume $A \cong R^{\oplus n}$ as an R-module. Let $f \in A$. The multiplication map $m_f : A \to A$ is R-linear and hence has a characteristic polynomial $P(T) = T^n + r_{n-1}T^{n-1} + \cdots + r_0 \in R[T]$. For any prime $\mathfrak{p} \in \mathrm{Spec}(R)$, f acts nilpotently on $A \otimes_R \kappa(\mathfrak{p})$ if and only if $\mathfrak{p} \in V(r_0, \ldots, r_{n-1})$.*

Proof. Immediate once we observe that the characteristic polynomial $\bar{P}(T) \in \kappa(\mathfrak{p})[T]$ of the multiplication map $m_{\bar{f}} : A \otimes_R \kappa(\mathfrak{p}) \to A \otimes_R \kappa(\mathfrak{p})$ which multiplies elements of $A \otimes_R \kappa(\mathfrak{p})$ by $\bar{f}$, the image of f viewed in $\kappa(\mathfrak{p})$, is just the image of $P(T)$ in $\kappa(\mathfrak{p})[T]$. $\square$

Lemma 13.9. *Let R be a ring. Let $f, g \in R[x]$ be polynomials. Assume the leading coefficient of g is a unit of R. There exist elements $r_i \in R$, $i = 1 \ldots, n$ such that the image of $D(f) \cap V(g)$ in $\mathrm{Spec}(R)$ is $\bigcup_{i=1,\ldots,n} D(r_i)$.*

Proof. Write $g = ux^d + a_{d-1}x^{d-1} + \cdots + a_0$, where d is the degree of g, and hence $u \in R^\times$. Consider the ring $A = R[x]/(g)$. It is, as an R-module, finite free with basis the images of $1, x, \ldots, x^{d-1}$. Consider multiplication by (the image of) f on A. This is an R-module map. Hence we can let $P(T) \in R[T]$ be the characteristic polynomial of this map. Write $P(T) = T^d + r_{d-1}T^{d-1} + \cdots + r_0$. We claim that $r_0, \ldots, r_{d-1}$ have the desired property. By Lemma 13.8 we have that

$$\mathfrak{p} \in V(r_0, \ldots, r_{d-1}) \Leftrightarrow f \text{ is nilpotent in } A \otimes_R \kappa(\mathfrak{p}) = \kappa(\mathfrak{p})[x]/(\overline{g}).$$

The image of $D(f) \cap V(g)$ in $\mathrm{Spec}(R)$ is the image of the map $(R[x]/(g))_{\overline{f}} \to \mathrm{Spec}(R)$. A prime $\mathfrak{p} \subset R$ lies in the image of this map if and only if

$$(R[x]/(g))_{\overline{f}} \otimes_R \kappa(\mathfrak{p}) \cong (\kappa(\mathfrak{p})[x]/(\overline{g}))_{\overline{f}} \neq 0.$$

Since $\kappa(\mathfrak{p})[x]/(\overline{g})$ is nonzero, this is the case if and only if the image of f is not nilpotent in $\kappa(\mathfrak{p})[x]/(\overline{g})$. By the first paragraph, this image is exactly the complement of $V(r_0, \ldots, r_{d-1})$. $\square$

THEOREM 13.10 (Chevalley's Theorem). *Suppose that $R \to S$ is of finite presentation. The image of a constructible subset of* $\mathrm{Spec}(S)$ *in* $\mathrm{Spec}(R)$ *is constructible.*

PROOF. Write $S = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. We may factor $R \to S$ as $R \to R[x_1] \to R[x_1, x_2] \to \cdots \to R[x_1, \ldots, x_n] \to S$ and by Lemma 13.6 we reduce to the case $S = R[x]$. By Lemma 13.1 suffices to show that if $T = (\bigcup_{i=1\ldots n} D(f_i)) \cap V(g_1, \ldots, g_m)$ for $f_i, g_j \in R[x]$ then the image in $\mathrm{Spec}(R)$ is constructible. Since finite unions of constructible sets are constructible, it suffices to deal with the case $n = 1$, i.e., when $T = D(f) \cap V(g_1, \ldots, g_m)$.

Note that if $c \in R$, then we have

$$\mathrm{Spec}(R) = V(c) \amalg D(c) = \mathrm{Spec}(R/(c)) \amalg \mathrm{Spec}(R_c),$$

and correspondingly $\mathrm{Spec}(R[x]) = V(c) \amalg D(c) = \mathrm{Spec}(R/(c)[x]) \amalg \mathrm{Spec}(R_c[x]))$. The intersection of $T = D(f) \cap V(g_1, \ldots, g_m)$ with each part still has the same shape, with f, g_i replaced by their images in $R/(c)[x]$, respectively $R_c[x]$. Note that the image of T in $\mathrm{Spec}(R)$ is the union of the image of $T \cap V(c)$ and $T \cap D(c)$. Using Lemmas 13.5 and 13.6, the result for R, f, and $g_1, \ldots, g_m$ follows from the result for R_c and R/c and the (images) of the same polynomials.

We are going to use induction on m and (for each m) on the total of the degrees of the nonzero g_i. The base case $m = 0$ is Lemma 13.7. Suppose without loss of generality that g_1 has the lowest degree among the g_i's, and let c be its leading coefficient. The result for R/c and the images of f and the g_i's holds by induction, since the image of g_1 either is 0 or is nonzero but has lower degree in R/c than in R. Next consider R_c. If $m > 1$, let g_2' be the remainder in R_c of the division of g_2 by g_1 (whose leading coefficient in R_c is invertible). Then $(g_1, \ldots, g_m) = (g_1, g_2', \ldots, g_m)$ and either $g_2' = 0$ or else the latter list has lower total degree, and the result again holds by induction. If instead $m = 1$, we are reduced to the case of $D(f) \cap V(g)$ where the leading coefficient of g is invertible, which is covered by Lemma 13.9. $\square$

14. Jacobson rings and the Nullstellensatz

Let R be a ring. The closed points of $\mathrm{Spec}(R)$ are the maximal ideals of R.

DEFINITION 14.1. Let R be a ring. We say that R is a *Jacobson ring* if every radical ideal I is the intersection of the maximal ideals containing it.

EXAMPLE 14.2. Any field is Jacobson. The ring $\mathbf{Z}$ is Jacobson.

LEMMA 14.3. *Let R be a ring. The following are equivalent:*

1. *R is Jacobson,*
2. *Each prime of R is the intersection of the maximal ideals that contain it,*
3. *Every domain admitting a surjection from R has trivial Jacobson radical.*

PROOF. (1) and (2) are equivalent because every radical ideal is an intersection of primes. (3) is effectively a restatement of (2). $\square$

DEFINITION 14.4. Let X be a topological space. We say that X is *Jacobson* if any nonempty subset $U \cap Z \subset X$ with U open and Z closed contains a closed point of X; equivalently, $Z \cap X_0$ is dense in Z for every closed subset $Z \subset X$, where X_0 be the set of closed points of X.

LEMMA 14.5. *A ring R is Jacobson if and only if* $\mathrm{Spec}(R)$ *is Jacobson.*

PROOF. Suppose R is Jacobson. Let $Z = V(I)$ be a closed subset of $\mathrm{Spec}(R)$, so that without loss of generality we may assume I is a radical ideal. We must show that if $D(f)$ is a standard open such that $D(f) \cap V(I)$ is nonempty, then $D(f) \cap V(I)$ contains a closed point. Since $D(f) \cap V(I)$ is nonempty, $f \notin I$. Since R is Jacobson and I is radical there is a maximal ideal $\mathfrak{m} \subset R$ containing I and not containing f, and this is exactly the closed point that we need.

Conversely, suppose that $\mathrm{Spec}(R)$ is Jacobson. Let $I \subset R$ be a radical ideal. Let $J = \cap_{I \subset \mathfrak{m}} \mathfrak{m}$ be the intersection of the maximal ideals containing I. Clearly J is radical, $V(J) \subset V(I)$, and $V(J)$ is the smallest closed subset of $V(I)$ containing all the closed points of $V(I)$. By assumption we see that $V(J) = V(I)$. But Lemma 8.5 shows there is a bijection between Zariski closed sets and radical ideals, hence $I = J$ as desired. $\square$

LEMMA 14.6. *Any finite type inclusion of rings $R \hookrightarrow K$ with K a field is of finite presentation.*

PROOF. Note that by hypothesis R is a domain. Write $K = R[x_1, \ldots, x_n]/\mathfrak{m}$ with $\mathfrak{m}$ a maximal ideal (not necessarily finitely generated). We claim that there exists $c \in R \setminus \{0\}$ such that $\mathfrak{m}_c := \mathfrak{m} \cdot R_c[x_1, \ldots, x_n]$ is finitely generated. Admitting this claim for now, the map $R_c \to R_c[x_1, \ldots, x_n]/\mathfrak{m}_c \cong K_c \cong K$ is of finite finite presentation. But $R \to R_c$ is also of finite presentation, because $R_c \cong R[x]/(xc-1)$, so the composite $R \to R_c \to K$ is of finite presentation.

It remains to check the claim. Choose any total ordering on the monomials in $x_1, \ldots, x_n$ that is compatible with divisibility (e.g. the lexicographic ordering will do). Let S be the set of monomials that occur as leading terms in $\mathfrak{m}$. The subset $T \subset S$ consisting of elements that are minimal with respect to divisibility is finite (in any infinite list of monomials, one must divide another). Choose for each $t \in T$ an element $g_t \in \mathfrak{m}$ with leading term t, and let c be the product of the leading coefficients of the g_t's. In $R_c[x_1, \ldots, x_n]$ it is possible to carry out division by the g_t's, and it follows that $\mathfrak{m} \cdot R_c[x_1, \ldots, x_n]$ is generated by the g_t's. $\square$

LEMMA 14.7. *Suppose that R is a Jacobson ring. If $\psi : R \to S$ map of finite type then the induced map* $\mathrm{Spec}(\psi) : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ *takes closed points to closed points.*

PROOF. If $\mathfrak{m} \subset S$ is a maximal ideal, we can replace ψ with the composite map $R \to S \to S/\mathfrak{m}$ and reduce to the case where $S = K$ is a field. Replacing R with $R/\ker(\psi)$ we then reduce to the case where ψ is injective. By Lemma 14.6 the map $\psi : R \hookrightarrow K$ has finite presentation. By Chevalley's Theorem (Theorem 13.10) the image of $\mathrm{Spec}(\psi) : \mathrm{Spec}(K) \to \mathrm{Spec}(R)$ is constructible. Since $\mathrm{Spec}(K)$ is a single point, so is this image. Any nonempty constructible subset of a Jacobson space must contain a closed point of the space (cf. Definition 14.4). Therefore the image of $\mathrm{Spec}(\psi)$ is a closed point of $\mathrm{Spec}(R)$. $\square$

THEOREM 14.8. *Let R be a Jacobson ring and let $\psi : R \to S$ be a ring map of finite type. Then:*

(1) *The ring S is Jacobson.*
(2) *For a maximal ideal $\mathfrak{m}' \subset S$ lying over $\mathfrak{m} \subset R$, the field extension $\kappa(\mathfrak{m}) \subset \kappa(\mathfrak{m}')$ is finite.*

PROOF. If we factor $R \to S$ into two maps $R \to S' \to S$ both of finite type, it is clear that it suffices to prove the theorem for $R \to S'$ and $R \to S$ separately. It therefore suffices to prove the lemma in the cases $S = R[x]$ and $S = R/I$. The case $S = R/I$ is obvious (cf. Lemma 14.3(2)), so we can assume $S = R[x]$.

Let $R[x] \to A$ be a surjective map with A a domain. By Lemma 14.3, to show that $R[x]$ is Jacobson it is enough to show for each nonzero element $f \in A$ that there is a maximal ideal of A not containing f.

Let $\mathfrak{m}'$ be a maximal ideal of the nonzero ring A_f. Consider the composite map $R \to R[x] \to A \to A_f$, and suppose that $\mathfrak{m}'$ pulls back to $\mathfrak{m}$ and $\mathfrak{p}$ in R and A respectively, with $f \notin \mathfrak{p}$. The map $R \to A_f$ is of finite type, so by Lemma 14.7 we see that $\mathfrak{m}$ is indeed a maximal ideal of R. Write k for the field $R/\mathfrak{m}$.

The map $R[x] \to A$ induces a surjection $\alpha : k[x] \to A/\mathfrak{p}$. We distinguish two cases. We distinguish two cases. If α is not an isomorphism, then $A/\mathfrak{p}$ is a field. (Any domain that is a nontrivial quotient of a polynomial ring in one variable over a field is a field.) We deduce that $\mathfrak{p}$ is a maximal ideal of A, evidently not containing f. Otherwise α is an isomorphism. The ring $k[x]$ is Jacobson (easy), so $A/\mathfrak{p}$ has a maximal ideal that does not contain the image of f. The preimage in A of such a maximal ideal is what we want. This proves (1).

For (2), let $\mathfrak{m}' \subset R[x]$ be a maximal ideal pulling back to $\mathfrak{m} \subset R$. Write k for the field $R/\mathfrak{m}$. We see that $S/\mathfrak{m}' \cong k[x]/\overline{\mathfrak{m}}'$ where $\overline{\mathfrak{m}}' = \mathfrak{m}'/\mathfrak{m}$. Then certainly $S/\mathfrak{m}'$ is a finite extension of k. □

As a special case of Theorem 14.8 we have the following.

THEOREM 14.9 (Hilbert Nullstellensatz). *Let k be a field.*

(1) *For any maximal ideal $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ the field extension $k \subset \kappa(\mathfrak{m})$ is finite.*
(2) *Any radical ideal $I \subset k[x_1, \ldots, x_n]$ is the intersection of maximal ideals containing it.*

Chain conditions

15. Noetherian rings

A ring R is *Noetherian* if any ideal of R is finitely generated. This is clearly equivalent to the ascending chain condition for ideals of R.

LEMMA 15.1. *Any finitely generated ring over a Noetherian ring is Noetherian. Any localization of a Noetherian ring is Noetherian.*

PROOF. The statement on localizations follows from the fact that any ideal $J \subset S^{-1}R$ is of the form $I \cdot S^{-1}R$. Any quotient R/I of a Noetherian ring R is Noetherian because any ideal $\overline{J} \subset R/I$ is of the form J/I for some ideal $I \subset J \subset R$. Thus it suffices to show that if R is Noetherian so is $R[X]$. Suppose $J_1 \subset J_2 \subset \ldots$ is an ascending chain of ideals in $R[X]$. Consider the ideals $I_{i,d}$ defined as the ideal of elements of R which occur as leading coefficients of degree d polynomials in J_i. Clearly $I_{i,d} \subset I_{i',d'}$ whenever $i \leq i'$ and $d \leq d'$. By the ascending chain condition in R there are at most finitely many distinct ideals among all of the $I_{i,d}$. (Hint: Any infinite set of elements of $\mathbf{N} \times \mathbf{N}$ contains an increasing infinite sequence.) Take i_0 so large that $I_{i,d} = I_{i_0,d}$ for all $i \geq i_0$ and all d. Suppose $f \in J_i$ for some $i \geq i_0$. By induction on the degree $d = \deg(f)$ we show that $f \in J_{i_0}$. Namely, there exists a $g \in J_{i_0}$ whose degree is d and which has the same leading coefficient as f. By induction $f - g \in J_{i_0}$ and we win. $\square$

EXERCISE 15.2. If R is a Noetherian ring, then so is the formal power series ring $R[[x_1, \ldots, x_n]]$.

LEMMA 15.3. *Any finite type algebra over a field is Noetherian. Any finite type algebra over* $\mathbf{Z}$ *is Noetherian.*

PROOF. This is immediate from Lemma 15.1 and the fact that fields are Noetherian rings and that $\mathbf{Z}$ is Noetherian ring (because it is a principal ideal domain). $\square$

LEMMA 15.4. *Let R be a Noetherian ring.*

(1) *Any finite R-module is of finite presentation.*
(2) *Any submodule of a finite R-module is finite.*
(3) *The ascending chain condition holds for submodules of a finite R-module.*
(4) *Any finite type R-algebra is an algebra of finite presentation over R.*

PROOF. We first show that any submodule N of a finite R-module M is finite. We do this by induction on the number of generators of M. If this number is 1, then $N = J/I \subset M = R/I$ for some ideals $I \subset J \subset R$. Thus the definition of Noetherian implies the result. If the number of generators of M is greater than 1, then we can find a short exact sequence $0 \to M' \to M \to M'' \to 0$ where M' and M'' have fewer generators. Note that setting $N' = M' \cap N$ and $N'' = \mathrm{im}(N \to M'')$ gives a similar short exact sequence for N. Hence the result follows from the induction hypothesis and Lemma 1.3(3).

To show that M is finitely presented just apply the previous result to the kernel of a presentation $R^n \to M$.

The equivalence of (2) and (3) is an easy exercise. To see (4) note that any ideal of $R[x_1, \ldots, x_n]$ is finitely generated by Lemma 15.1. $\square$

Definition 15.5. A topological space is called *Noetherian* if the descending chain condition holds for closed subsets of X.

Lemma 15.6. *Let X be a Noetherian topological space. The space X has finitely many irreducible components.*

Proof. Consider the set of closed subsets of X which do not have finitely many irreducible components, which (if nonempty) must have a minimal element by the Noetherian hypothesis. $\square$

Lemma 15.7. *If R is a Noetherian ring then* $\mathrm{Spec}(R)$ *is a Noetherian topological space.*

Proof. This is because any closed subset of $\mathrm{Spec}(R)$ is uniquely of the form $V(I)$ with I a radical ideal, see Lemma 8.5. And this correspondence is inclusion reversing. Thus the result follows from the definitions. $\square$

Lemma 15.8. *If R is a Noetherian ring then* $\mathrm{Spec}(R)$ *has finitely many irreducible components. In other words R has finitely many minimal primes.*

Proof. By Lemma 15.7 and Lemma 15.6 we see there are finitely many irreducible components. By Lemma 12.3 these correspond to minimal primes of R. $\square$

Lemma 15.9 (Artin-Rees). *Suppose that R is Noetherian, $I \subset R$ an ideal. Let $N \subset M$ be finite R-modules. There exists a constant $c > 0$ such that $I^n M \cap N = I^{n-c}(I^c M \cap N)$ for all $n \geq c$.*

Proof. Consider the ring $S = R \oplus I \oplus I^2 \oplus \cdots = \bigoplus_{n \geq 0} I^n$. Convention: $I^0 = R$. Multiplication maps $I^n \times I^m$ into I^{n+m} by multiplication in R. Note that if $I = (f_1, \ldots, f_t)$ then S is a quotient of the Noetherian ring $R[X_1, \ldots, X_t]$. The map just sends the monomial $X_1^{e_1} \ldots X_t^{e_t}$ to $f_1^{e_1} \ldots f_t^{e_t}$. Thus S is Noetherian. Similarly, consider the module $M \oplus IM \oplus I^2 M \oplus \cdots = \bigoplus_{n \geq 0} I^n M$. This is a finitely generated S-module. Namely, if $x_1, \ldots, x_r$ generate M over R, then they also generate $\bigoplus_{n \geq 0} I^n M$ over S. Next, consider the submodule $\bigoplus_{n \geq 0} I^n M \cap N$. This is an S-submodule, as is easily verified. By Lemma 15.4 it is finitely generated as an S-module, say by $\xi_j \in \bigoplus_{n \geq 0} I^n M \cap N$, $j = 1, \ldots, s$. We may assume by decomposing each ξ_j into its homogeneous pieces that each $\xi_j \in I^{d_j} M \cap N$ for some d_j. Set $c = \max\{d_j\}$. Then for all $n \geq c$ every element in $I^n M \cap N$ is of the form $\sum h_j \xi_j$ with $h_j \in I^{n-d_j}$. The lemma now follows from this and the trivial observation that $I^{n-d_j}(I^{d_j} M \cap N) \subset I^{n-c}(I^c M \cap N)$. $\square$

Lemma 15.10 (Krull's intersection theorem). *Let R be a Noetherian local ring. Let $I \subset R$ be a proper ideal. Let M be a finite R-module. Then $\bigcap_{n \geq 0} I^n M = 0$.*

Proof. Let $N = \bigcap_{n \geq 0} I^n M$. Then $N = I^n M \cap N$ for all $n \geq 0$. By the Artin-Rees Lemma 15.9 we see that $N = I^n M \cap N \subset IN$ for some suitably large n. By Nakayama's Lemma 7.14 we see that $N = 0$. $\square$

Exercise 15.11. Let R be a Noetherian ring. Let M, N be finite R-modules. Then $\text{Ext}^i_R(M, N)$ and $\text{Tor}^R_i(M, N)$ are finite R-modules for all i. (Hint: show that modules F_i of Lemma 4.4 may be taken to be finite free.)

16. Length

Definition 16.1. Let R be a ring. For any R-module M we define the *length* of M over R by the formula

$$\text{length}_R(M) = \sup\{n \mid \exists\, 0 = M_0 \subset M_1 \subset \cdots \subset M_n = M,\ M_i \neq M_{i+1}\}.$$

In other words it is the supremum of the lengths of chains of submodules. There is an obvious notion of when a chain of submodules is a refinement of another. This gives a partial ordering on the collection of all chains of submodules, with the smallest chain having the shape $0 = M_0 \subset M_1 = M$ if M is not zero. We note the obvious fact that if the length of M is finite, then every chain can be refined to a maximal chain. But it is not as obvious that all maximal chains have the same length (as we will see later).

Lemma 16.2. *Let R be a ring. Let M be an R-module. If* $\text{length}_R(M) < \infty$ *then M is a finite R-module.*

Proof. Omitted. Note that the converse to this lemma is very false! $\square$

Lemma 16.3. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of modules over R then the length of M is the sum of the lengths of M' and M''.*

Proof. Given filtrations of M' and M'' of lengths n', n'' it is easy to make a corresponding filtration of M of length $n' + n''$. Thus we see that $\text{length}_R M \geq \text{length}_R M' + \text{length}_R M''$. Conversely, given a filtration $M_0 \subset M_1 \subset \cdots \subset M_n$ of M consider the induced filtrations $M_i' = M_i \cap M'$ and $M_i'' = \text{im}(M_i \to M'')$. Let n' (resp. n'') be the number of steps in the filtration $\{M_i'\}$ (resp. $\{M_i''\}$). If $M_i' = M_{i+1}'$ and $M_i'' = M_{i+1}''$ then $M_i = M_{i+1}$. Hence we conclude that $n' + n'' \geq n$. $\square$

Lemma 16.4. *Let $R \to S$ be a ring map. Let M be an S-module. We always have* $\text{length}_R(M) \geq \text{length}_S(M)$. *If $R \to S$ is surjective then equality holds.*

Proof. A filtration of M by S-submodules gives rise a filtration of M by R-submodules. This proves the inequality. And if $R \to S$ is surjective, then any R-submodule of M is automatically an S-submodule. Hence equality in this case. $\square$

Lemma 16.5. *Let R be a ring with maximal ideal $\mathfrak{m}$. Suppose that M is an R-module with $\mathfrak{m}M = 0$. Then the length of M as an R-module agrees with the dimension of M as a $R/\mathfrak{m}$ vector space. The length is finite if and only if M is a finite R-module.*

Proof. The first part is a special case of Lemma 16.4. Thus the length is finite if and only if M has a finite basis as a $R/\mathfrak{m}$-vector space if and only if M has a finite set of generators as an R-module. $\square$

Lemma 16.6. *Let R be a ring with finitely generated maximal ideal $\mathfrak{m}$. (For example R Noetherian.) Suppose that M is a finite R-module with $\mathfrak{m}^n M = 0$ for some n. Then* $\text{length}_R(M) < \infty$.

Proof. Consider the filtration $0 = \mathfrak{m}^n M \subset \mathfrak{m}^{n-1} M \subset \cdots \subset \mathfrak{m} M \subset M$. All of the subquotients are finitely generated R-modules to which Lemma 16.5 applies. We conclude by additivity, see Lemma 16.3. □

Definition 16.7. Let R be a ring. Let M be an R-module. We say M is *simple* if $M \neq 0$ and every submodule of M is either equal to M or to 0.

Lemma 16.8. *Let R be a ring. Let M be an R-module. The following are equivalent:*

(1) *M is simple,*
(2) $\text{length}_R(M) = 1$, *and*
(3) *$M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset R$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of R. The equivalence of the first two assertions is tautological, and Lemma 16.5 immediately gives (3) implies (2). To see that (2) implies (3), note that any simple M has $M = R \cdot x$ for any non-zero $x \in R$, so that $M \cong R/I$ for I the annihilator of x. If I were not maximal, then M would have the nontrivial submodule $\mathfrak{m}/I$ for any maximal ideal $\mathfrak{m}$ containing I. □

Lemma 16.9. *Let R be a ring. Suppose that*

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$$

is a maximal chain of submodules with $M_i \neq M_{i-1}$, $i = 1, \ldots, n$. Then

(1) $n = \text{length}_R(M)$ *(in particular M has finite length),*
(2) *each M_i/M_{i-1} is simple,*
(3) *each M_i/M_{i-1} is of the form $R/\mathfrak{m}_i$ for some maximal ideal $\mathfrak{m}_i$,*
(4) *given a maximal ideal $\mathfrak{m} \subset R$ we have*

$$\#\{i \mid \mathfrak{m}_i = \mathfrak{m}\} = \text{length}_{R_\mathfrak{m}}(M_\mathfrak{m}).$$

Proof. If M_i/M_{i-1} is not simple then we can refine the filtration and the filtration is not maximal. Thus we see that M_i/M_{i-1} is simple. By Lemma 16.8 the modules M_i/M_{i-1} have length 1 and are of the form $R/\mathfrak{m}_i$ for some maximal ideals $\mathfrak{m}_i$. By additivity of length, Lemma 16.3, we see $n = \text{length}_R(M)$ is finite. Since localization is exact, we see that

$$0 = (M_0)_\mathfrak{m} \subset (M_1)_\mathfrak{m} \subset (M_2)_\mathfrak{m} \subset \cdots \subset (M_n)_\mathfrak{m} = M_\mathfrak{m}$$

is a filtration of $M_\mathfrak{m}$ with successive quotients $(M_i/M_{i-1})_\mathfrak{m}$. Thus the last statement follows directly from the fact that given maximal ideals $\mathfrak{m}$, $\mathfrak{m}'$ of R we have

$$(R/\mathfrak{m}')_\mathfrak{m} \cong \begin{cases} 0 & \text{if } \mathfrak{m} \neq \mathfrak{m}', \\ R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m} & \text{if } \mathfrak{m} = \mathfrak{m}' \end{cases}$$

□

Lemma 16.10. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be an R-module. If M has finite length n then $\mathfrak{m}^n M = 0$.*

Proof. Indeed, if R is any ring (not necessarily local) and $n_\mathfrak{m} := \#\{i \mid \mathfrak{m}_i = \mathfrak{m}\}$ as in Lemma 16.9, then an easy argument shows that $\prod_\mathfrak{m} \mathfrak{m}^{n_\mathfrak{m}} \cdot M = 0$: use the fact that if $M_i/M_{i-1} \cong R/\mathfrak{m}$ then $\mathfrak{m} \cdot M_i \subset M_{i-1}$. □

17. Artinian rings

Artinian rings, and especially local Artinian rings, play an important role in algebraic geometry, for example in deformation theory.

Definition 17.1. A ring R is *Artinian* if it satisfies the descending chain condition for ideals.

Lemma 17.2. *Suppose R is a finite dimensional algebra over a field. Then R is Artinian.*

Proof. The descending chain condition for ideals obviously holds. $\square$

Lemma 17.3.

(1) *If R is Artinian then R has only finitely many maximal ideals.*
(2) *Any localization of an Artinian ring is Artinian.*

Proof. (1) Suppose that $\mathfrak{m}_i$, $i = 1, 2, 3, \ldots$ are maximal ideals. Then $\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supset \ldots$ is an infinite descending sequence (because by the Chinese remainder theorem all the maps $R \to \oplus_{i=1}^n R/\mathfrak{m}_i$ are surjective).

(2) Just as the corresponding statement for Noetherian rings, this follows because any ideal of $S^{-1}R$ is of the form $I \cdot S^{-1}R$. $\square$

Lemma 17.4. *Let R be Artinian. The radical* $\mathrm{rad}(R)$ *of R is a nilpotent ideal.*

Proof. Denote the radical I. Note that $I \supset I^2 \supset I^3 \supset \ldots$ is a descending sequence. Thus $I^n = I^{n+1}$ for some n. We wish to show that $I^n = 0$, so consider $J = \mathrm{Ann}(I^n) = \{x \in R \mid xI^n = 0\}$. We have to show $J = R$. If not, choose an ideal $J' \neq J$, $J \subset J'$ minimal (possible by the Artinian property), so that J'/J is simple. (In particular J'/J is finite.) By construction $I^n \cdot (J'/J) \cong I^n J' \neq 0$. Since J'/J is simple the only other possibility is $I^n \cdot (J'/J) = J'/J$. By Nakayama's Lemma 7.14(2), we have $J' = J$. Contradiction. $\square$

Lemma 17.5. *Any ring with finitely many maximal ideals and radical consisting of nilpotent elements (so in particular any Artinian ring) is the product of its localizations at its maximal ideals. Also, all primes of such a ring are maximal.*

Proof. Let R be a ring as in the statement, with finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Let $\mathfrak{p}$ be a prime ideal of R. Since every prime contains every nilpotent element of R we see $\mathfrak{p} \supset \mathrm{rad}(R) \supset \mathfrak{m}_1 \ldots \mathfrak{m}_n$. Hence $\mathfrak{p} \supset \mathfrak{m}_i$ for some i, and so $\mathfrak{p} = \mathfrak{m}_i$. This gives the last part of the statement.

In particular the topological space $\mathrm{Spec}(R)$ is discrete, and it follows from Lemma 10.2 and Lemma 10.3(2) that there exists an idempotent e_i for each i such that $\{\mathfrak{m}_i\} = D(e_i)$ and such that $R \cong \prod_i R_{e_i}$. By Lemma 12.7 we have $R_{\mathfrak{m}_i} \cong R_{e_i}$ and the result follows. $\square$

We have the following two important characterizations of Artinian rings.

Lemma 17.6. *Let R be a ring.*

(1) *The ring R is Artinian if and only if it is of finite length as a module over itself.*
(2) *The ring R is Artinian if and only if it is Noetherian, and every prime ideal of R is maximal.*

Proof. (1) The "if" direction is obvious. For the reverse, Lemma 11.1(2)(d) and the exactness of localization imply that $\mathrm{length}_R(R) \leq \sum_{\mathfrak{m}} \mathrm{length}_{R_{\mathfrak{m}}}(R_{\mathfrak{m}})$. By Lemma 17.3(2) we are reduced to the case where R is an Artinian local ring.

Let $\mathfrak{m}$ be the maximal ideal of R. The quotient $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ must be a finite-dimensional $R/\mathfrak{m}$-vector space (else it contains an infinite decreasing chain of subspaces, which pull back to an infinite decreasing chain of ideals of R), hence of finite length as an R-module by Lemma 16.5. The result follows from Lemma 16.3 together with the fact that $\mathfrak{m}^n = 0$ for $n \gg 0$ (Lemma 17.4).

(2) If R is Artinian then it is of finite length over itself by (1), and this implies that R satisfies the increasing chain condition as well. Every prime ideal of R is maximal by Lemma 17.5.

Conversely, suppose that R is Noetherian. If all prime ideals of R are maximal, then all prime ideals of R are also minimal, and by Lemma 15.7 the ring R has finitely many maximal ideals $\mathfrak{m}_i$. We want to show that R is of finite length over itself, and now by the same reduction as in (1) we may assume that R is local.

Since $\mathfrak{m}$ is the only prime ideal of R, we have $\mathfrak{m} = \sqrt{(0)}$, and so $\mathfrak{m}$ is nilpotent (it consists of nilpotent elements and is finitely generated). We conclude by Lemma 16.6. $\square$

Supports and associated primes

18. Supports

We start with some very basic definitions and lemmas.

Definition 18.1. Let R be a ring and let M be an R-module. The *support of* M is the set

$$\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_\mathfrak{p} \neq 0\}$$

Remark 18.2. If M is a finite R-module, then $M_\mathfrak{p} \neq 0$ if and only if $M_\mathfrak{p} \neq \mathfrak{p}M_\mathfrak{p}$ by Lemma 7.14(2), so that that $\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M \otimes_R \kappa(\mathfrak{p}) \neq 0\}$.

Lemma 18.3. *Let R be a ring. Let M be an R-module. Then*

$$M = (0) \Leftrightarrow \operatorname{Supp}(M) = \emptyset.$$

Proof. Actually, Lemma 11.1 even shows that $\operatorname{Supp}(M)$ always contains a maximal ideal if M is not zero. $\square$

Definition 18.4. Let R be a ring. Let M be an R-module.

(1) Given an element $m \in M$ the *annihilator of* m is the ideal

$$\operatorname{Ann}_R(m) = \operatorname{Ann}(m) = \{f \in R \mid fm = 0\}.$$

(2) The *annihilator of* M is the ideal

$$\operatorname{Ann}_R(M) = \operatorname{Ann}(M) = \{f \in R \mid fm = 0 \ \forall m \in M\}.$$

Lemma 18.5. *Let R be a ring and let M be an R-module. We have* $\operatorname{Supp}(M) \subset V(\operatorname{Ann}(M))$. *If M is finite, then equality holds; in particular* $\operatorname{Supp}(M)$ *is closed.*

Proof. Suppose $\mathfrak{p} \in \operatorname{Supp}(M)$, so that $M_\mathfrak{p} \neq 0$. In particular $M_f \neq 0$ for all $f \in S \setminus \mathfrak{p}$. But if $f \in \operatorname{Ann}(M)$ then $M_f = 0$, hence $\operatorname{Ann}(M) \subset \mathfrak{p}$.

Conversely, suppose that M is finite and that $\mathfrak{p} \notin \operatorname{Supp}(M)$. Then $M_\mathfrak{p} = 0$. Let $x_1, \ldots, x_r \in M$ be generators. For each i there exists $f_i \in R \setminus \mathfrak{p}$ such that $f_i x_i = 0$. Then the product $f = f_1 \cdots f_r$ is also not in $\mathfrak{p}$, and $fM = 0$. $\square$

Corollary 18.6. *The support of R/I-module (regarded as an R-module) is contained in $V(I)$, and the support of R/I is precisely $V(I)$.*

Lemma 18.7. *Let R be a ring and let M be an R-module.*

(1) *If M is finite then the support of M/IM is* $\operatorname{Supp}(M) \cap V(I)$.
(2) *If $N \subset M$, then* $\operatorname{Supp}(N) \subset \operatorname{Supp}(M)$.
(3) *If Q is a quotient module of M then* $\operatorname{Supp}(Q) \subset \operatorname{Supp}(M)$.
(4) *If $0 \to N \to M \to Q \to 0$ is a short exact sequence then* $\operatorname{Supp}(M) = \operatorname{Supp}(Q) \cup \operatorname{Supp}(N)$.

PROOF. The functors $M \mapsto M_{\mathfrak{p}}$ are exact. This immediately implies all but the first assertion. For the first assertion, the inclusion $\mathrm{Supp}(M/IM) \subset \mathrm{Supp}(M) \cap V(I)$ follows from (3) and Lemma 18.5. For the reverse we need to show that $M_{\mathfrak{p}} \neq 0$ and $I \subset \mathfrak{p}$ implies $(M/IM)_{\mathfrak{p}} = M_{\mathfrak{p}}/IM_{\mathfrak{p}} \neq 0$. This follows from Nakayama's Lemma 7.14(2). $\square$

EXERCISE 18.8. Let $R \to R'$ be a ring map and let M be a finite R-module. Then the support of $M \otimes_R R'$ consists of the fibres above the primes in the support of M.

EXERCISE 18.9. Let R be a ring and let M be an R-module. If M is a finitely presented R-module, then $\mathrm{Supp}(M)$ is a closed subset of $\mathrm{Spec}(R)$ whose complement is quasi-compact.

We now consider supports in the case where R is a Noetherian ring.

LEMMA 18.10. *Let R be a Noetherian ring, and let M be a finite R-module. There exists a filtration by R-submodules*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that each quotient M_i/M_{i-1} is isomorphic to $R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$ of R.

PROOF. It suffices to do the case $M = R/I$ for some ideal I. Consider the set S of ideals J such that the lemma does not hold for the module R/J, and order it by inclusion. To arrive at a contradiction, assume that S is not empty. Because R is Noetherian, S has a maximal element J. By definition of S, the ideal J cannot be prime. Pick $a, b \in R$ such that $ab \in J$, but neither $a \in J$ nor $b \in J$. Consider the filtration $0 \subset aR/(J \cap aR) \subset R/J$. Note that $aR/(J \cap aR)$ is a quotient of $R/(J + bR)$ and the second quotient equals $R/(aR + J)$. Hence by maximality of J, each of these has a filtration as above and hence so does R/J. Contradiction. $\square$

LEMMA 18.11. *Let R, M, M_i, $\mathfrak{p}_i$ as in Lemma 18.10. Then* $\mathrm{Supp}(M) = \bigcup V(\mathfrak{p}_i)$. *In particular $\mathfrak{p}_i \in \mathrm{Supp}(M)$, and the minimal elements of the set $\{\mathfrak{p}_i\}$ are the minimal elements of* $\mathrm{Supp}(M)$.

PROOF. This follows from Lemmas 18.5 and 18.7. $\square$

EXERCISE 18.12. Suppose that R is a Noetherian ring. Let M be a nonzero finite R-module. Then M has finite length over R if and only if M is supported on the closed points of $\mathrm{Spec}(R)$.

LEMMA 18.13. *Let R be a Noetherian ring. Let $I \subset R$ be an ideal. Let M be a finite R-module. Then $I^n M = 0$ for some $n \geq 0$ if and only if* $\mathrm{Supp}(M) \subset V(I)$.

PROOF. It is clear (e.g. from Lemma 18.5) that $I^n M = 0$ for some $n \geq 0$ implies $\mathrm{Supp}(M) \subset V(I)$. Suppose that $\mathrm{Supp}(M) \subset V(I)$. Choose a filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ as in Lemma 18.10. Each of the primes $\mathfrak{p}_i$ is contained in $V(I)$ by Lemma 18.11. Hence $I \subset \mathfrak{p}_i$ and I annihilates M_i/M_{i-1}. Hence I^n annihilates M. $\square$

19. Associated primes

Here is the standard definition. (For non-Noetherian rings and non-finite modules it may be more appropriate to use a slightly different definition.)

DEFINITION 19.1. Let R be a ring. Let M be an R-module. A prime $\mathfrak{p}$ of R is *associated* to M if there exists an injection $R/\mathfrak{p} \hookrightarrow M$; equivalently, there is an element $m \in M$ whose annihilator is $\mathfrak{p}$ (namely any nonzero element of the image of $R/\mathfrak{p} \hookrightarrow M$). The set of all such primes is denoted $\mathrm{Ass}_R(M)$ or $\mathrm{Ass}(M)$.

LEMMA 19.2. *Let R be a ring. Let M be an R-module. Then* $\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$.

PROOF. If $R/\mathfrak{p} \hookrightarrow M$ then $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \mathrm{Frac}(R/\mathfrak{p}) \hookrightarrow M_\mathfrak{p}$. □

LEMMA 19.3. *Let R be a ring. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then* $\mathrm{Ass}(M') \subset \mathrm{Ass}(M)$ *and* $\mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.

PROOF. Suppose that $f\colon R/\mathfrak{p} \hookrightarrow M$. If $M' \cap \mathrm{im}(f) = 0$ then $R/\mathfrak{p} \hookrightarrow M''$. Otherwise there is a nonzero element of $M' \cap \mathrm{im}(f)$; but every nonzero element of $\mathrm{im}(f)$ has annihilator $\mathfrak{p}$. □

LEMMA 19.4. *Let R be a ring, and M an R-module. Suppose there exists a filtration by R-submodules*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that each quotient M_i/M_{i-1} is isomorphic to $R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$ of R. Then $\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

PROOF. By Lemma 19.3 we reduce immediately to the case $M = R/\mathfrak{p}$, in which every nonzero element has annihilator $\mathfrak{p}$. □

LEMMA 19.5. *Let R be a Noetherian ring. Let M be a finite R-module. Then* $\mathrm{Ass}(M)$ *is finite.*

PROOF. Immediate from Lemma 19.4 and Lemma 18.10. □

LEMMA 19.6. *Let R be a Noetherian ring. Let M be an R-module. Then*

$$M = (0) \Leftrightarrow \mathrm{Ass}(M) = \emptyset.$$

PROOF. If $M = (0)$, then $\mathrm{Ass}(M) = \emptyset$ by definition. If $M \neq 0$, pick any nonzero finitely generated submodule $M' \subset M$, for example a submodule generated by a single nonzero element. For any filtration of M' as in Lemma 18.10 we have $R/\mathfrak{p}_1 \hookrightarrow M' \hookrightarrow M$, so that $\mathfrak{p}_1 \in \mathrm{Ass}(M)$. □

PROPOSITION 19.7. *Let R be a Noetherian ring. Let M be a finite R-module. The following sets of primes are the same:*

1. *The minimal primes in the support of M.*
2. *The minimal primes in* $\mathrm{Ass}(M)$.
3. *For any filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$ with $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ the minimal primes of the set $\{\mathfrak{p}_i\}$.*

Proof. Choose a filtration as in (3). In Lemma 18.11 we have seen that the sets in (1) and (3) are equal.

Let $\mathfrak{p}$ be a minimal element of the set $\{\mathfrak{p}_i\}$. Let i be minimal such that $\mathfrak{p} = \mathfrak{p}_i$. Pick $m \in M_i$, $m \notin M_{i-1}$. The annihilator of m is contained in $\mathfrak{p}_i = \mathfrak{p}$ and contains $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_i$. By our choice of i and $\mathfrak{p}$ we have $\mathfrak{p}_j \not\subset \mathfrak{p}$ for $j < i$ and hence we have $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_{i-1} \not\subset \mathfrak{p}_i$. Pick $f \in \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_{i-1}$, $f \notin \mathfrak{p}$. Then fm has annihilator $\mathfrak{p}$. In this way we see that $\mathfrak{p}$ is an associated prime of M. By Lemma 19.2 we have $\text{Ass}(M) \subset \text{Supp}(M)$ and hence $\mathfrak{p}$ is minimal in $\text{Ass}(M)$. Thus the set of primes in (1) is contained in the set of primes of (2).

That the set of primes in (2) is contained in the set of primes of (1) follows formally from the reverse inclusion together with the fact that $\text{Ass}(M) \subset \text{Supp}(M)$. $\square$

Lemma 19.8. *Let R be a Noetherian ring. Let M be an R-module. Any $\mathfrak{p} \in \text{Supp}(M)$ which is minimal among the elements of $\text{Supp}(M)$ is an element of $\text{Ass}(M)$.*

Proof. If M is a finite R-module, then this is a consequence of Proposition 19.7. In general write $M = \bigcup M_\lambda$ as the union of its finite submodules, and use that $\text{Supp}(M) = \bigcup \text{Supp}(M_\lambda)$ and $\text{Ass}(M) = \bigcup \text{Ass}(M_\lambda)$. $\square$

Example 19.9. If R is a Noetherian ring and $I \subset R$ is an ideal, then Proposition 19.7 shows that the minimal primes in $\text{Ass}(R/I)$ are exactly the minimal primes in $\text{Supp}(R/I)$. But by Lemma 18.5 this support is exactly $V(I)$. We conclude in this case that the minimal elements of $\text{Ass}(R/I)$ are exactly (the generic points of) the irreducible components of $\text{Spec}(R/I)$.

Regarding non-minimal elements of $\text{Ass}(M)$, we make the following definition.

Definition 19.10. Let R be a ring. Let M be an R-module.

(1) The associated primes of M which are not minimal among the associated primes of M are called the *embedded associated primes* of M.
(2) The *embedded primes of* R are the embedded associated primes of R as an R-module.

Example 19.11. Let k be a field, and consider the ideal $I = (xy, x^2)$ in $R = k[x, y]$. We have $V(I) = V(\sqrt{I}) = V(x)$, so that (x) is the unique minimal associated prime of R/I. But the annihilator of $x \in R/I$ is the ideal $\mathfrak{m} = (x, y)$, so that $\mathfrak{m} \in \text{Ass}(R/I)$ is an embedded associated prime. This reflects the fact that R/I has some nilpotence that is concentrated at the origin rather than living on the whole component $\{x = 0\}$.

We record two lemmas for future use.

Lemma 19.12. *Let R be a Noetherian ring. Let M be an R-module. The union $\bigcup_{\mathfrak{q} \in \text{Ass}(M)} \mathfrak{q}$ is the set of elements of R which are zerodivisors on M.*

Proof. Any element in any associated prime clearly is a zerodivisor on M. Conversely, suppose $x \in R$ is a zerodivisor on M. Consider the submodule $N = \{m \in M \mid xm = 0\}$. Since N is not zero it has an associated prime $\mathfrak{q}$ by Lemma 19.6. Then $x \in \mathfrak{q}$ and $\mathfrak{q}$ is an associated prime of M by Lemma 19.3. $\square$

Lemma 19.13. *Let R be a Noetherian ring and $I \subset R$ an ideal. Let M be a finite R-module. The following are equivalent:*

(1) *Every $x \in I$ is a zerodivisor on M.*
(2) *We have $I \subset \mathfrak{q}$ for some $\mathfrak{q} \in \text{Ass}(M)$.*

Proof. The implication (2) $\Rightarrow$ (1) is immediate from Lemma 19.12. The reverse implication also follows directly from Lemma 19.12 combined with Lemmas 19.5 and 7.2. $\square$

Lemma 19.14. *Let R be a ring. Let M be an R-module. If R is Noetherian the map*
$$M \longrightarrow \prod\nolimits_{\mathfrak{p} \in \text{Ass}(M)} M_{\mathfrak{p}}$$
is injective.

Proof. Let $x \in M$ be an element of the kernel of the map. Then if $\mathfrak{p}$ is an associated prime of $Rx \subset M$ we see on the one hand that $\mathfrak{p} \in \text{Ass}(M)$ and on the other hand that $(Rx)_{\mathfrak{p}} \subset M_{\mathfrak{p}}$ is not zero. This contradiction shows that $\text{Ass}(Rx) = \emptyset$. Hence $Rx = 0$ by Lemma 19.6. $\square$

Finally we record (mostly as exercises) some functorial properties of the set of associated primes.

Exercise 19.15. Let $\varphi : R \to S$ be a ring map. Let M be an S-module. Then the image of $\text{Ass}_S(M)$ in $\text{Spec}(R)$ is contained in $\text{Ass}_R(M)$.

Exercise 19.16. Let $\varphi : R \to S$ be a ring map. Let M be an S-module. Then the image of $\text{Ass}_S(M)$ in $\text{Spec}(R)$ need not equal $\text{Ass}_R(M)$. For example, consider the ring map $R = k \to S = k[x_1, x_2, x_3, \ldots]/(x_i^2)$ and $M = S$. Then $\text{Ass}_R(M)$ is not empty, but $\text{Ass}_S(S)$ is empty.

Proposition 19.17. *Let $\varphi : R \to S$ be a ring map. Let M be an S-module. If S is Noetherian, then the image of $\text{Ass}_S(M)$ in $\text{Spec}(R)$ is $\text{Ass}_R(M)$.*

Proof. We have already seen in Exercise 19.15 that $\text{Spec}(\varphi)(\text{Ass}_S(M)) \subset \text{Ass}_R(M)$. For the converse, choose a prime $\mathfrak{p} \in \text{Ass}_R(M)$. Let $m \in M$ be an element such that the annihilator of m in R is $\mathfrak{p}$. Let I be the annihilator of m in S. Then $R/\mathfrak{p} \subset S/I$ is injective, hence by Exercise 8.15 there exists a prime $\mathfrak{q} \subset S$ containing I and lying over $\mathfrak{p}$. One can further arrange that $\mathfrak{q}/I$ is a minimal prime of S/I. By Lemma 19.12 and Lemma 12.5 we see that $\mathfrak{q}$ is an associated prime of S/I. Since $S/I \hookrightarrow M$ it is also an associated prime of M. $\square$

Exercise 19.18. Let R be a ring. Let I be an ideal. Let M be an R/I-module. Via the canonical injection $\text{Spec}(R/I) \to \text{Spec}(R)$ we have $\text{Ass}_{R/I}(M) = \text{Ass}_R(M)$.

Exercise 19.19. Let R be a ring. Let M be an R-module. Let $\mathfrak{p} \subset R$ be a prime.

(1) If $\mathfrak{p} \in \text{Ass}(M)$ then $\mathfrak{p}R_{\mathfrak{p}} \in \text{Ass}(M_{\mathfrak{p}})$.
(2) If $\mathfrak{p}$ is finitely generated then the converse holds as well.

Exercise 19.20. Let R be a ring. Let M be an R-module. Let $S \subset R$ be a multiplicative subset. Via the canonical injection $\text{Spec}(S^{-1}R) \to \text{Spec}(R)$ we have

(1) $\text{Ass}_R(S^{-1}M) = \text{Ass}_{S^{-1}R}(S^{-1}M)$,
(2) $\text{Ass}_R(M) \cap \text{Spec}(S^{-1}R) \subset \text{Ass}_R(S^{-1}M)$, and
(3) if R is Noetherian this inclusion is an equality.

Going up and going down

20. Going down for flat ring maps

Definition 20.1. Let $\varphi : R \to S$ be a ring map.

(1) We say a $\varphi : R \to S$ satisfies *going up* if given primes $\mathfrak{p} \subset \mathfrak{p}'$ in R and a prime $\mathfrak{q}$ in S lying over $\mathfrak{p}$ there exists a prime $\mathfrak{q}'$ of S such that (a) $\mathfrak{q} \subset \mathfrak{q}'$, and (b) $\mathfrak{q}'$ lies over $\mathfrak{p}'$.
(2) We say a $\varphi : R \to S$ satisfies *going down* if given primes $\mathfrak{p} \subset \mathfrak{p}'$ in R and a prime $\mathfrak{q}'$ in S lying over $\mathfrak{p}'$ there exists a prime $\mathfrak{q}$ of S such that (a) $\mathfrak{q} \subset \mathfrak{q}'$, and (b) $\mathfrak{q}$ lies over $\mathfrak{p}$.

As a first example, we prove in this section that flat ring maps satisfy going down. We begin with a brief discussion of faithful flatness.

Definition 20.2.

(1) An R-module M is called *faithfully flat* if the complex of R-modules $N_1 \to N_2 \to N_3$ is exact if and only if the sequence $M \otimes_R N_1 \to M \otimes_R N_2 \to M \otimes_R N_3$ is exact.
(2) A ring map $R \to S$ is called *faithfully flat* if S is faithfully flat as an R-module.

To get used to the definition, we give two easy exercises on the interaction of flatness with base change.

Exercise 20.3. Let $R \to R'$ be a faithfully flat ring map. Let M be a module over R, and set $M' = R' \otimes_R M$. Then M is flat over R if and only if M' is flat over R'.

Exercise 20.4. Let R be a ring. Let $S \to S'$ be a faithfully flat map of R-algebras. Let M be a module over S, and set $M' = S' \otimes_S M$. Then M is flat over R if and only if M' is flat over R.

We now establish some standard properties of faithfully flat maps.

Lemma 20.5. *Let R be a ring. Let M be an R-module. The following are equivalent.*

(1) *M is faithfully flat, and*
(2) *M is flat and for all R-module homomorphisms $\alpha : N \to N'$ we have $\alpha = 0$ if and only if $\alpha \otimes \mathrm{id}_M = 0$.*

Proof. The flatness of M implies that $\ker(\alpha \otimes \mathrm{id}_M) = \ker(\alpha) \otimes_R M$. If M is faithfully flat, then $0 \to \ker(\alpha) \to N \to 0$ is exact if and only if the same holds after tensoring with M. This proves (1) implies (2).

For the reverse, let $N_1 \to N_2 \to N_3$ be a complex with cohomology H, and assume the complex $N_1 \otimes_R M \to N_2 \otimes_R M \to N_3 \otimes_R M$ is exact. Then apply (2) with $\alpha = \mathrm{id}_H$, noting that $\alpha \otimes \mathrm{id}_M = 0$ because $- \otimes_R M$ is exact. □

Lemma 20.6. *Let M be a flat R-module. The following are equivalent:*
1. *M is faithfully flat,*
2. *for all $\mathfrak{p} \in \mathrm{Spec}(R)$ the tensor product $M \otimes_R \kappa(\mathfrak{p})$ is nonzero, and*
3. *for all maximal ideals $\mathfrak{m}$ of R the tensor product $M \otimes_R \kappa(\mathfrak{m}) = M/\mathfrak{m}M$ is nonzero.*

Proof. Assume M faithfully flat. Since $R \to \kappa(\mathfrak{p})$ is not zero we deduce that $M \to M \otimes_R \kappa(\mathfrak{p})$ is not zero, see Lemma 20.5.

Conversely assume that M is flat and that $M/\mathfrak{m}M$ is never zero. Suppose that $N_1 \to N_2 \to N_3$ is a complex and suppose that $N_1 \otimes_R M \to N_2 \otimes_R M \to N_3 \otimes_R M$ is exact. Let H be the cohomology of the complex, so $H = \ker(N_2 \to N_3)/\mathrm{im}(N_1 \to N_2)$. By flatness we see that $H \otimes_R M = 0$. Take $x \in H$ and let $I = \{f \in R \mid fx = 0\}$ be its annihilator. Since $R/I \subset H$ we get $M/IM \subset H \otimes_R M = 0$ by flatness of M. If $I \neq R$ we may choose a maximal ideal $I \subset \mathfrak{m} \subset R$. This immediately gives a contradiction. □

Lemma 20.7. *Let $R \to S$ be a flat ring map. The following are equivalent:*
1. *$R \to S$ is faithfully flat,*
2. *the induced map on* Spec *is surjective, and*
3. *any closed point $x \in \mathrm{Spec}(R)$ is in the image of the map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$.*

Proof. This follows quickly from Lemma 20.6, because we saw in Remark 8.12 that $\mathfrak{p}$ is in the image if and only if the ring $S \otimes_R \kappa(\mathfrak{p})$ is nonzero. □

Corollary 20.8. *A flat local ring homomorphism of local rings is faithfully flat.*

Lemma 20.9 (Going down for flat maps). *Let $R \to S$ be flat. Let $\mathfrak{p} \subset \mathfrak{p}'$ be primes of R. Let $\mathfrak{q}' \subset S$ be a prime of S mapping to $\mathfrak{p}'$. Then there exists a prime $\mathfrak{q} \subset \mathfrak{q}'$ mapping to $\mathfrak{p}$.*

Proof. The local ring map $R_{\mathfrak{p}'} \to S_{\mathfrak{q}'}$ is flat: the composition $R \to S \to S_{\mathfrak{q}'}$ is flat, and then apply Lemma 11.4(2). By Corollary 20.8 this map is faithfully flat. By Lemma 20.7 there is a prime of $S_{\mathfrak{q}'}$ mapping to $\mathfrak{p}R_{\mathfrak{p}'}$. The inverse image of this prime in S does the job. □

21. Finite and integral ring extensions

Definition 21.1. Let $\varphi : R \to S$ be a ring map.
1. An element $s \in S$ is *integral over R* if there exists a monic polynomial $P(x) \in R[x]$ such that $P^\varphi(s) = 0$, where $P^\varphi(x) \in S[x]$ is the image of P under $\varphi : R[x] \to S[x]$.
2. The ring map φ is *integral* if every $s \in S$ is integral over R.

We sometimes abuse notation and omit the superscript on P^φ(x).

Lemma 21.2. *Let $\varphi : R \to S$ be a ring map. Let $y \in S$. If there exists a finite R-submodule M of S such that $1 \in M$ and $yM \subset M$, then y is integral over R.*

Proof. Let $x_1 = 1 \in M$ and $x_i \in M$, $i = 2, \ldots, n$ be a finite set of elements generating M as an R-module. Write $yx_i = \sum \varphi(a_{ij})x_j$ for some $a_{ij} \in R$. Let $P(T) \in R[T]$ be the characteristic polynomial of the $n \times n$ matrix $A = (a_{ij})$. By Lemma 7.9 we see $P(A) = 0$. Then $P^\varphi(y) \cdot x_i = 0$ for all i. Taking $i = 1$ gives $P^\varphi(y) = 0$. $\square$

Lemma 21.3. *A finite ring extension is integral.*

Proof. Let $R \to S$ be finite. Let $y \in S$. Apply Lemma 21.2 to $M = S$ to see that y is integral over R. $\square$

Lemma 21.4. *Let $\varphi : R \to S$ be a ring map. Let $s_1, \ldots, s_n$ be a finite set of elements of S. Then s_i is integral over R for all $i = 1, \ldots, n$ if and only if there exists an R-subalgebra $S' \subset S$ finite over R containing all of the s_i.*

Proof. If each s_i is integral, then the subalgebra generated by $\varphi(R)$ and the s_i is finite over R. Namely, if s_i satisfies a monic equation of degree d_i over R, then this subalgebra is generated as an R-module by the elements $s_1^{e_1} \ldots s_n^{e_n}$ with $0 \leq e_i \leq d_i - 1$. Conversely, suppose given a finite R-subalgebra S' containing all the s_i. Then all of the s_i are integral by Lemma 21.3. $\square$

Lemma 21.5. *Let $R \to S$ be a ring map. The following are equivalent*

1. *$R \to S$ is finite,*
2. *$R \to S$ is integral and of finite type, and*
3. *there exist $x_1, \ldots, x_n \in S$ which generate S as an algebra over R such that each x_i is integral over R.*

Proof. Clear from Lemma 21.4. $\square$

Lemma 21.6. *Let $R \to S$ be a ring homomorphism. The set*

$$S' = \{s \in S \mid s \text{ is integral over } R\}$$

is an R-subalgebra of S.

Proof. This is clear from Lemmas 21.4 and 21.3. $\square$

Definition 21.7. Let $R \to S$ be a ring map. The ring $S' \subset S$ of elements integral over R, see Lemma 21.6, is called the *integral closure* of R in S. If $R \subset S$ we say that R is *integrally closed* in S if $R = S'$.

In particular, we see that $R \to S$ is integral if and only if the integral closure of R in S is all of S.

Exercise 21.8. Integral closure commutes with localization: If $A \to B$ is a ring map, and $S \subset A$ is a multiplicative subset, then the integral closure of $S^{-1}A$ in $S^{-1}B$ is $S^{-1}B'$, where $B' \subset B$ is the integral closure of A in B.

Lemma 21.9. *Let $R \to S$ and $R \to R'$ be ring maps. Set $S' = R' \otimes_R S$.*

1. *If $R \to S$ is integral so is $R' \to S'$.*
2. *If $R \to S$ is finite so is $R' \to S'$.*

Proof. Part (2) is trivial. We prove (1). Let $s_i \in S$ be generators for S over R. Each of these satisfies a monic polynomial equation P_i over R. Hence the elements $1 \otimes s_i \in S'$ generate S' over R' and satisfy the corresponding polynomial P_i' over R'. Since these elements generate S' over R' we see e.g. by Lemma 21.6 that S' is integral over R'. $\square$

The basic philosophy in this section is that many properties of finite maps also hold for integral maps, and are often proved by reducing to the finite case.

LEMMA 21.10. *Suppose that $R \to S$ and $S \to T$ are integral ring maps. Then $R \to T$ is integral.*

PROOF. Let $t \in T$. Let $P(x) \in S[x]$ be a monic polynomial such that $P(t) = 0$. Apply Lemma 21.4 to the finite set of coefficients of P. Hence t is integral over some subalgebra $S' \subset S$ finite over R. Apply Lemma 21.4 again to find a subalgebra $T' \subset T$ finite over S' and containing t. Lemma 1.8 applied to $R \to S' \to T'$ shows that T' is finite over R. The integrality of t over R now follows from Lemma 21.3. $\square$

LEMMA 21.11. *Suppose that $R \to S$ is an integral ring extension with $R \subset S$. Then $\varphi : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective.*

PROOF. If R is local with maximal ideal $\mathfrak{m}$ and the inclusion $R \to S$ is finite, then the closed point $\mathfrak{m}$ is in the image of φ: this is equivalent to the statement $\mathfrak{m}S \neq S$, which is immediate from Nakayama's Lemma 7.14(2). We now reduce to this case.

In general let $\mathfrak{p} \subset R$ be a prime ideal. We have to show $\mathfrak{p}S_{\mathfrak{p}} \neq S_{\mathfrak{p}}$, see Lemma 8.13. The localization $R_{\mathfrak{p}} \to S_{\mathfrak{p}}$ is injective (as localization is exact) and integral by Exercise 21.8 or Lemma 21.9. Hence we may replace R, S by $R_{\mathfrak{p}}$, $S_{\mathfrak{p}}$ and we may assume R is local with maximal ideal $\mathfrak{m}$ and it suffices to show that $\mathfrak{m}S \neq S$. Suppose $1 = \sum f_i s_i$ with $f_i \in \mathfrak{m}$ and $s_i \in S$ in order to get a contradiction. Let $R \subset S' \subset S$ be such that $R \to S'$ is finite and $s_i \in S'$ for all i, see Lemma 21.4. The equation $1 = \sum f_i s_i$ implies that the finite R-module S' satisfies $S' = \mathfrak{m}S'$. This contradicts the first paragraph. $\square$

LEMMA 21.12 (Going up for integral ring maps). *Let $R \to S$ be a ring map such that S is integral over R. Let $\mathfrak{p} \subset \mathfrak{p}' \subset R$ be primes. Let $\mathfrak{q}$ be a prime of S mapping to $\mathfrak{p}$. Then there exists a prime $\mathfrak{q}'$ with $\mathfrak{q} \subset \mathfrak{q}'$ mapping to $\mathfrak{p}'$.*

PROOF. We may replace R by $R/\mathfrak{p}$ and S by $S/\mathfrak{q}$. This reduces us to the situation of having an integral extension of domains $R \subset S$ and a prime $\mathfrak{p}' \subset R$. By Lemma 21.11 we are done. $\square$

EXERCISE 21.13. Let $\varphi : R \to S$ be a ring map. Let $x \in S$. The following are equivalent:

(1) x is integral over R, and
(2) for every prime ideal $\mathfrak{p} \subset R$ the element $x \in S_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$.

EXERCISE 21.14. Let $R \to S$ be a ring map. Let $f_1, \ldots, f_n \in R$ generate the unit ideal.

(1) If each $R_{f_i} \to S_{f_i}$ is integral, so is $R \to S$.
(2) If each $R_{f_i} \to S_{f_i}$ is finite, so is $R \to S$.

EXERCISE 21.15. Let R be a ring. Let K be a field. If $R \subset K$ and K is integral over R, then R is a field and K is an algebraic extension. If $R \subset K$ and K is finite over R, then R is a field and K is a finite algebraic extension.

22. Normal rings

We first introduce the notion of a normal domain, and then we introduce the (very general) notion of a normal ring.

Definition 22.1. A domain R is called *normal* if it is integrally closed in its field of fractions.

Example 22.2. Let k be a ring. The domain $R = k[x, y]/(y^3 - x^2)$ is not normal because the element $x/y \in Q(R)$ is integral (it is a root of the polynomial $t^2 - y$) but not contained in R.

Definition 22.3. Let R be a domain.

(1) An element g of the fraction field of R is called *almost integral over R* if there exists an element $r \in R$, $r \neq 0$ such that $rg^n \in R$ for all $n \geq 0$.
(2) The domain R is called *completely normal* if every almost integral element of the fraction field of R is contained in R.

The following lemma shows that a Noetherian domain is normal if and only if it is completely normal.

Lemma 22.4. *Let R be a domain with fraction field K. If $u, v \in K$ are almost integral over R, then so are $u+v$ and uv. Any element $g \in K$ which is integral over R is almost integral over R. If R is Noetherian then the converse holds as well.*

Proof. If $ru^n \in R$ for all $n \geq 0$ and $v^n r' \in R$ for all $n \geq 0$, then $(uv)^n rr'$ and $(u+v)^n rr'$ are in R for all $n \geq 0$. Hence the first assertion. Suppose $g \in K$ is integral over R. In this case there exists an $d > 0$ such that the ring $R[g]$ is generated by $1, g, \ldots, g^d$ as an R-module. Let $r \in R$ be a common denominator of the elements $1, g, \ldots, g^d \in K$. It is follows that $rR[g] \subset R$, and hence g is almost integral over R.

Suppose R is Noetherian and $g \in K$ is almost integral over R. Let $r \in R$, $r \neq 0$ be as in the definition. Then $R[g] \subset \frac{1}{r}R$ as an R-module. Since R is Noetherian this implies that $R[g]$ is finite over R. Hence g is integral over R, see Lemma 21.3. $\square$

Lemma 22.5. *Any localization of a normal domain is normal.*

Proof. Let R be a normal domain, and let $S \subset R$ be a multiplicative subset. Suppose g is an element of the fraction field of R which is integral over $S^{-1}R$. Let $P = x^d + \sum_{j<d} a_j x^j$ be a polynomial with $a_i \in S^{-1}R$ such that $P(g) = 0$. Choose $s \in S$ such that $sa_i \in R$ for all i. Then sg satisfies the monic polynomial $x^d + \sum_{j<d} s^{d-j} a_j x^j$ which has coefficients $s^{d-j}a_j$ in R. Hence $sg \in R$ because R is normal. Hence $g \in S^{-1}R$. $\square$

Lemma 22.6. *A principal ideal domain is normal.*

Proof. Let R be a principal ideal domain. Let $g = a/b$ be an element of the fraction field of R integral over R. Because R is a principal ideal domain we may divide out a common factor of a and b and assume $(a, b) = R$. In this case, any equation $(a/b)^n + r_{n-1}(a/b)^{n-1} + \cdots + r_0 = 0$ with $r_i \in R$ would imply $a^n \in (b)$. This contradicts $(a, b) = R$ unless b is a unit in R. $\square$

Lemma 22.7. *Let R be a domain with fraction field K. Suppose $f = \sum \alpha_i x^i$ is an element of $K[x]$.*

(1) *If f is integral over $R[x]$ then all α_i are integral over R, and*
(2) *If f is almost integral over $R[x]$ then all α_i are almost integral over R.*

Proof. We first prove the second statement. Write $f = \alpha_0 + \alpha_1 x + \cdots + \alpha_r x^r$ with $\alpha_r \neq 0$. By assumption there exists $h = b_0 + b_1 x + \cdots + b_s x^s \in R[x]$, $b_s \neq 0$ such that $f^n h \in R[x]$ for all $n \geq 0$. This implies that $b_s \alpha_r^n \in R$ for all $n \geq 0$. Hence α_r is almost integral over R. Since the set of almost integral elements form a subring (Lemma 22.4) we deduce that $f - \alpha_r x^r = \alpha_0 + \alpha_1 x + \cdots + \alpha_{r-1} x^{r-1}$ is almost integral over $R[x]$. By induction on r we win.

In order to prove the first statement we will use absolute Noetherian reduction. Namely, write $\alpha_i = a_i/b_i$ and let $P(t) = t^d + \sum_{j<d} f_j t^j$ be a polynomial with coefficients $f_j \in R[x]$ such that $P(f) = 0$. Let $f_j = \sum f_{ji} x^i$. Consider the subring $R_0 \subset R$ generated over $\mathbf{Z}$ by the finite list of elements a_i, b_i, f_{ji} of R. It is a domain; let K_0 be its field of fractions. Since R_0 is a finite type $\mathbf{Z}$-algebra it is Noetherian, see Lemma 15.3. It is still the case that $f \in K_0[x]$ is integral over $R_0[x]$, because all the identities in R among the elements a_i, b_i, f_{ji} also hold in R_0. By Lemma 22.4 the element f is almost integral over $R_0[x]$. By the second statement of the lemma, the elements α_i are almost integral over R_0. And since R_0 is Noetherian, they are integral over R_0, see Lemma 22.4. Of course, then they are integral over R. $\square$

Lemma 22.8. *Let R be a normal domain. Then $R[x]$ is a normal domain.*

Proof. The result is true if R is a field K because $K[x]$ is a euclidean domain and hence a principal ideal domain and hence normal by Lemma 22.6. Let g be an element of the fraction field of $R[x]$ which is integral over $R[x]$. Because g is integral over $K[x]$ where K is the fraction field of R we may write $g = \alpha_d x^d + \alpha_{d-1} x^{d-1} + \cdots + \alpha_0$ with $\alpha_i \in K$. By Lemma 22.7 the elements α_i are integral over R and hence are in R. $\square$

Lemma 22.9. *Let R be a domain. The following are equivalent:*

(1) *The domain R is a normal domain,*
(2) *for every prime $\mathfrak{p} \subset R$ the local ring $R_{\mathfrak{p}}$ is a normal domain, and*
(3) *for every maximal ideal $\mathfrak{m}$ the ring $R_{\mathfrak{m}}$ is a normal domain.*

Proof. This follows easily from the fact that for any domain R we have

$$R = \bigcap\nolimits_{\mathfrak{m}} R_{\mathfrak{m}}$$

inside the fraction field of R. Namely, if g is an element of the right hand side then the ideal $I = \{x \in R \mid xg \in R\}$ is not contained in any maximal ideal $\mathfrak{m}$, whence $I = R$. $\square$

Lemma 22.9 shows that the following definition is compatible with Definition 22.1. (It is the definition from EGA – see [**DG67**, IV, 5.13.5 and 0, 4.1.4].)

Definition 22.10. A ring R is called *normal* if for every prime $\mathfrak{p} \subset R$ the localization $R_{\mathfrak{p}}$ is a normal domain (see Definition 22.1).

Note that a normal ring is a reduced ring, as R is a subring of the product of its localizations at all primes (see for example Lemma 11.1).

Lemma 22.11. *Let R be a normal ring. Then $R[x]$ is a normal ring.*

Proof. Let $\mathfrak{q}$ be a prime of $R[x]$. Set $\mathfrak{p} = R \cap \mathfrak{q}$. Then we see that $R_{\mathfrak{p}}[x]$ is a normal domain by Lemma 22.8. Hence $(R[x])_{\mathfrak{q}}$ is a normal domain by Lemma 22.5. □

Lemma 22.12. *Let R be a ring. Assume R is reduced and has finitely many minimal primes. Then the following are equivalent:*

(1) *R is a normal ring,*
(2) *R is integrally closed in its total ring of fractions, and*
(3) *R is a finite product of normal domains.*

Proof. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ be the minimal primes of R. By Lemmas 12.6 and 12.8 we have $Q(R) = R_{\mathfrak{q}_1} \times \cdots \times R_{\mathfrak{q}_t}$, and by Lemma 12.5 each factor is a field. Denote $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ the ith idempotent of $Q(R)$.

If R is integrally closed in $Q(R)$, then it contains in particular the idempotents e_i, and we see that R is a product of t domains (see Section 10). Hence it is clear that R is a finite product of normal domains.

Suppose R is normal. Each prime $\mathfrak{p}$ of R contains exactly one minimal prime, since $R_{\mathfrak{p}}$ is a domain. The irreducible components $V(\mathfrak{q}_i)$ of $\mathrm{Spec}(R)$ are therefore pairwise disjoint, hence both open and closed, and it follows from Lemma 10.2 that R contains the idempotents e_i. We conclude that R is a product of t domains as before. Each of these t domains is normal by Lemma 22.9 and the assumption that R is a normal ring. Hence it follows that R is a finite product of normal domains.

We omit the verification that (3) implies (1) and (2). □

Exercise 22.13. If R is a Noetherian normal domain, then so is $R[[x]]$.

Exercise 22.14. A localization of a normal ring is a normal ring.

Valuation rings

Definition 22.15. Let A be a domain. We say that A is a *valuation ring* if for each x in the field of fractions $Q(A)$, either $x \in A$ or $x^{-1} \in A$ or both.

Lemma 22.16. *A valuation ring is either a field or a local domain.*

Proof. If A is not a field then there is a nonzero maximal ideal $\mathfrak{m}$. If $\mathfrak{m}'$ is a second maximal ideal, then choose $x, y \in A$ with $x \in \mathfrak{m}$, $y \notin \mathfrak{m}$, $x \notin \mathfrak{m}'$, and $y \in \mathfrak{m}'$ (see Lemma 7.2). Then neither $x/y \in A$ nor $y/x \in A$, a contradiction. Thus we see that A is a local ring. □

Valuation rings are an important class of normal rings.

Lemma 22.17. *Let A be a valuation ring. Then A is a normal domain.*

Proof. Suppose x is in the field of fractions of A and integral over A, say $x^d + \sum_{i<d} a_i x^i = 0$. Either $x \in A$ (and we're done) or $x^{-1} \in A$. In the second case we see that $x = -\sum a_i x^{i-d} \in A$ as well. □

We mention a few more basic properties of valuation rings. The following exercises are elementary.

Exercise 22.18. Let A be a valuation ring with field of fractions K. Set $\Gamma = K^\times / A^\times$ (with group law written additively). For $\gamma, \gamma' \in \Gamma$ define $\gamma \geq \gamma'$ if and only if $\gamma - \gamma'$ is in the image of $A \setminus \{0\} \to \Gamma$. Then $(\Gamma, \geq)$ is a totally ordered abelian group.

Definition 22.19. Let A be a valuation ring.

(1) The totally ordered abelian group $(\Gamma, \geq)$ of Lemma 22.18 is called the *value group* of the valuation ring A.
(2) The map $v : A - \{0\} \to \Gamma$ and also $v : K^* \to \Gamma$ is called the *valuation* associated to A.
(3) The valuation ring A is called a *discrete valuation ring* if $\Gamma \cong \mathbf{Z}$.

Exercise 22.20. Let $(\Gamma, \geq)$ be a totally ordered abelian group. Let K be a field. Let $v : K^\times \to \Gamma$ be a homomorphism of abelian groups such that $v(a+b) \geq \min(v(a), v(b))$ for $a, b \in K$ with $a, b, a+b$ not zero. Then

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

is a valuation ring with value group $\mathrm{im}(v) \subset \Gamma$, with maximal ideal

$$\mathfrak{m} = \{x \in K \mid x = 0 \text{ or } v(x) > 0\}$$

and with group of units

$$A^\times = \{x \in K^* \mid v(x) = 0\}.$$

Let $(\Gamma, \geq)$ be a totally ordered abelian group. An *ideal of* Γ is a subset $I \subset \Gamma$ such that all elements of I are ≥ 0 and $\gamma \in I$, $\gamma' \geq \gamma$ implies $\gamma' \in I$. We say that such an ideal is *prime* if $\gamma + \gamma' \in I, \gamma, \gamma' \geq 0 \Rightarrow \gamma \in I$ or $\gamma' \in I$.

Exercise 22.21. Let A be a valuation ring. Ideals in A are in one-to-one correspondence with ideals of Γ. This bijection is inclusion preserving, and maps prime ideals to prime ideals.

Lemma 22.22. *A valuation ring is Noetherian if and only if it is a discrete valuation ring or a field.*

Proof. Suppose A is a discrete valuation ring with valuation $v : A \setminus \{0\} \to \mathbf{Z}$ normalized so that $\mathrm{im}(v) \subset \mathbf{Z}_{\geq 0}$. By Exercise 22.21 the ideals of A are the subsets $I_n = \{0\} \cup v^{-1}(\mathbf{Z}_{\geq n})$. It is clear that any element $x \in A$ with $v(x) = n$ generates I_n. Hence A is a PID so certainly Noetherian.

Suppose A is a Noetherian valuation ring with value group Γ. By Lemma 22.21 we see the ascending chain condition holds for ideals in Γ. We may assume A is not a field, i.e., there is a $\gamma \in \Gamma$ with $\gamma > 0$. Applying the ascending chain condition to the subsets $\gamma + \Gamma_{\geq 0}$ with $\gamma > 0$ we see there exists a smallest element γ_0 which is bigger than 0. Let $\gamma \in \Gamma$ be an element $\gamma > 0$. Consider the sequence of elements γ, $\gamma - \gamma_0$, $\gamma - 2\gamma_0$, etc. By the ascending chain condition these cannot all be > 0. Let $\gamma - n\gamma_0$ be the last one ≥ 0. By minimality of γ_0 we see that $0 = \gamma - n\gamma_0$. Hence Γ is a cyclic group as desired. □

23. Going down for integral over normal

We first play around a little bit with the notion of elements integral over an ideal, and then we prove the theorem referred to in the section title.

Definition 23.1. Let $\varphi : R \to S$ be a ring map. Let $I \subset R$ be an ideal. We say an element $g \in S$ is *integral over I* if there exists a monic polynomial $P = x^d + \sum_{j<d} a_j x^j$ with coefficients $a_j \in I^{d-j}$ such that $P^\varphi(g) = 0$ in S.

This is mostly used when $\varphi = \mathrm{id}_R : R \to R$. In this case the set I' of elements integral over I is called the *integral closure of* I. We will see that I' is an ideal of R (and of course $I \subset I'$).

LEMMA 23.2. *Let $\varphi : R \to S$ be a ring map. Let $I \subset R$ be an ideal. Let $A = \sum I^n t^n \subset R[t]$ be the subring of the polynomial ring generated by $R \oplus It \subset R[t]$. An element $s \in S$ is integral over I if and only if the element $st \in S[t]$ is integral over A.*

PROOF. Suppose that s is integral over I, say via $P = x^d + \sum_{j<d} a_j x^j$ with $a_j \in I^{d-j}$. The we immediately find a polynomial $Q = x^d + \sum_{j<d}(a_j t^{d-j})x^j$ with coefficients in A which proves that st is integral over A.

Suppose st is integral over A. Let $P = x^d + \sum_{j<d} a_j x^j$ be a monic polynomial with coefficients in A such that $P^\varphi(st) = 0$. Let $a'_j \in A$ be part of a_i of degree $d-j$ in t, in other words $a'_j = a''_j t^{d-j}$ with $a''_j \in I^{d-j}$. For degree reasons we still have $(st)^d + \sum_{j<d} \varphi(a''_j) t^{d-j} (st)^j = 0$. Hence we see that s is integral over I. $\square$

LEMMA 23.3. *Let $\varphi : R \to S$ be a ring map. Let $I \subset R$ be an ideal. The set of elements of S which are integral over I form a R-submodule of S. Furthermore, if $s \in S$ is integral over R, and s' is integral over I, then ss' is integral over I.*

PROOF. Closure under addition is clear by the characterization of Lemma 23.2. Any element $s \in S$ which is integral over R corresponds to the degree 0 element s of $S[x]$ which is integral over A (because $R \subset A$). Hence we see that multiplication by s on $S[x]$ preserves the property of being integral over A, by Lemma 21.6. $\square$

LEMMA 23.4. *Suppose $\varphi : R \to S$ is integral. Suppose $I \subset R$ is an ideal. Then every element of IS is integral over I.*

PROOF. Immediate from Lemma 23.3. $\square$

LEMMA 23.5. *Let K be a field. If the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ divides the polynomial $x^m + b_{m-1}x^{m-1} + \cdots + b_0$ in $K[x]$ then*

(1) *$a_0, \ldots, a_{n-1}$ are integral over any subring R_0 of K containing the elements $b_0, \ldots, b_{m-1}$, and*
(2) *each a_i lies in $\sqrt{(b_0, \ldots, b_{m-1})R}$ for any subring $R \subset K$ containing the elements $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1}$.*

PROOF. Let L/K be a field extension such that we can write $x^m + b_{m-1}x^{m-1} + \cdots + b_0 = \prod_{i=1}^m (x - \beta_i)$ with $\beta_i \in L$. Each β_i is integral over R_0. Since each a_i is a homogeneous polynomial in $\beta_1, \ldots, \beta_m$ we deduce the same for the a_i (use Lemma 21.6).

Choose $c_0, \ldots, c_{m-n-1} \in K$ such that

$$x^m + b_{m-1}x^{m-1} + \cdots + b_0 = \\ (x^n + a_{n-1}x^{n-1} + \cdots + a_0)(x^{m-n} + c_{m-n-1}x^{m-n-1} + \cdots + c_0).$$

By part (1) the elements c_i are integral over R. Consider the integral extension

$$R \subset R' = R[c_0, \ldots, c_{m-n-1}] \subset K$$

By Lemmas 21.11 and 8.14(2) we see that $R \cap \sqrt{(b_0, \ldots, b_{m-1})R'} = \sqrt{(b_0, \ldots, b_{m-1})R}$. Thus we may replace R by R' and assume $c_i \in R$. Dividing out the radical

$\sqrt{(b_0, \ldots, b_{m-1})}$ we get a reduced ring $\overline{R}$. We have to show that the images $\overline{a_i} \in \overline{R}$ are zero. And in $\overline{R}[x]$ we have the relation

$$x^m = x^m + \overline{b_{m-1}}x^{m-1} + \cdots + \overline{b_0} =$$
$$(x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0})(x^{m-n} + \overline{c_{m-n-1}}x^{m-n-1} + \cdots + \overline{c_0}).$$

It is easy to see that this implies $\overline{a_i} = 0$ for all i. For example one can see this by localizing at all the minimal primes, see Lemma 12.6. $\square$

LEMMA 23.6. *Let $R \subset S$ be an inclusion of domains. Assume R is normal. Let $g \in S$ be integral over R. Then the minimal polynomial of g has coefficients in R.*

PROOF. Let $P = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ be a polynomial with coefficients in R such that $P(g) = 0$. Let $Q = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be the minimal polynomial for g over the fraction field K of R. Then Q divides P in $K[x]$. By Lemma 23.5 we see the a_i are integral over R. Since R is normal this means they are in R. $\square$

PROPOSITION 23.7. *Let $R \subset S$ be an inclusion of domains. Assume R is normal and S integral over R. Let $\mathfrak{p} \subset \mathfrak{p}' \subset R$ be primes. Let $\mathfrak{q}'$ be a prime of S with $\mathfrak{p}' = R \cap \mathfrak{q}'$. Then there exists a prime $\mathfrak{q}$ with $\mathfrak{q} \subset \mathfrak{q}'$ such that $\mathfrak{p} = R \cap \mathfrak{q}$. In other words: the going down property holds for $R \to S$, see Definition 20.1.*

PROOF. Let $\mathfrak{p}$, $\mathfrak{p}'$ and $\mathfrak{q}'$ be as in the statement. We have to show there is a prime $\mathfrak{q}$, with $\mathfrak{q} \subset \mathfrak{q}'$ and $R \cap \mathfrak{q} = \mathfrak{p}$. This is the same as finding a prime of $S_{\mathfrak{q}'}$ mapping to $\mathfrak{p}$. According to Lemma 8.13 we have to show that $\mathfrak{p}S_{\mathfrak{q}'} \cap R = \mathfrak{p}$. Pick $z \in \mathfrak{p}S_{\mathfrak{q}'} \cap R$. We may write $z = y/g$ with $y \in \mathfrak{p}S$ and $g \in S$, $g \notin \mathfrak{q}'$. Written differently we have $zg = y$.

By Lemma 23.4 there exists a monic polynomial $P = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ with $b_i \in \mathfrak{p}$ such that $P(y) = 0$.

By Lemma 23.6 the minimal polynomial of g over K has coefficients in R. Write it as $Q = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Note that not all a_i, $i = n-1, \ldots, 0$ are in $\mathfrak{p}$ since that would imply $g^n = -\sum_{j<n} a_j g^j \in \mathfrak{p}S \subset \mathfrak{p}'S \subset \mathfrak{q}'$ which is a contradiction.

Since $y = zg$ we see immediately from the above that $Q' = x^n + za_{n-1}x^{n-1} + \cdots + z^n a_0$ is the minimal polynomial for y. Hence Q' divides P and by Lemma 23.5 we see that $z^j a_{n-j} \in \sqrt{(b_0, \ldots, b_{m-1})} \subset \mathfrak{p}$, $j = 1, \ldots, n$. Because not all a_i, $i = n-1, \ldots, 0$ are in $\mathfrak{p}$ we conclude $z \in \mathfrak{p}$ as desired. $\square$

Dimension theory I

24. Noetherian graded rings

In this section and the two sections that follow we will develop the basics of dimension theory. For this we need to begin with a discussion of Noetherian graded rings.

A *graded ring* will be for us a ring S endowed with a direct sum decomposition $S = \bigoplus_{d \geq 0} S_d$ such that $S_d \cdot S_e \subset S_{d+e}$. Note that we do not allow nonzero elements in negative degrees. The *irrelevant ideal* is the ideal $S_+ = \bigoplus_{d>0} S_d$. A *graded module* will be an S-module M endowed with a direct sum decomposition $M = \bigoplus_{n \in \mathbf{Z}} M_n$ such that $S_d \cdot M_e \subset M_{d+e}$. Note that for modules we do allow nonzero elements in negative degrees. We think of S as a graded S-module by setting $S_{-k} = (0)$ for $k > 0$. An element x (resp. f) of M (resp. S) is called *homogeneous* if $x \in M_d$ (resp. $f \in S_d$) for some d. A *map of graded S-modules* is a map of S-modules $\varphi : M \to M'$ such that $\varphi(M_d) \subset M'_d$. We do not allow maps to shift degrees.

Example 24.1. The standard example of a graded ring is a polynomial ring $R[x_1, \ldots, x_n]$ graded by degree, with $R = S_0$ the subring of constants.

At this point there are the notions of graded ideal, graded quotient ring, graded submodule, graded quotient module, graded tensor product, etc. We leave it to the reader to find the relevant definitions, and lemmas. For example: A short exact sequence of graded modules is short exact in every degree.

Exercise 24.2. Let S be a graded ring. A set of homogeneous elements $f_i \in S_+$ generates S as an algebra over S_0 if and only if they generate S_+ as an ideal of S.

Exercise 24.3. A graded ring S is Noetherian if and only if S_0 is Noetherian and S_+ is finitely generated as an ideal of S.

Lemma 24.4. *If M is a finitely generated graded S-module, and if S is finitely generated over S_0, then each M_n is a finite S_0-module.*

Proof. Suppose the generators of M are m_i and the generators of S are f_i. By taking homogeneous components we may assume that the m_i and the f_i are homogeneous and we may assume $f_i \in S_+$. In this case it is clear that each M_n is generated over S_0 by the "monomials" $\prod f_i^{e_i} m_j$ whose degree is n. $\square$

Definition 24.5. Let A be an abelian group. We say that a function $f : n \mapsto f(n) \in A$ defined for all sufficiently large integers n is a *numerical polynomial* if there exist $r \geq 0$ and elements $a_0, \ldots, a_r \in A$ such that

$$f(n) = \sum\nolimits_{i=0}^{r} \binom{n}{i} a_i$$

for all $n \gg 0$.

The reason for using the binomial coefficients is the elementary fact that any polynomial $P \in \mathbf{Q}[T]$ all of whose values at integer points are integers, is equal to a sum $P(T) = \sum a_i \binom{T}{i}$ with $a_i \in \mathbf{Z}$. Note that in particular the expressions $\binom{T+1}{i+1}$ are of this form.

Lemma 24.6. *If $A \to A'$ is a homomorphism of abelian groups and if $f : n \mapsto f(n) \in A$ is a numerical polynomial, then so is the composition.*

Proof. This is immediate from the definitions. $\square$

Lemma 24.7. *Suppose that $f : n \mapsto f(n) \in A$ is defined for all n sufficiently large and suppose that $n \mapsto f(n) - f(n-1)$ is a numerical polynomial. Then f is a numerical polynomial.*

Proof. Let $f(n) - f(n-1) = \sum_{i=0}^{r} \binom{n}{i} a_i$ for all $n \gg 0$. Set $g(n) = f(n) - \sum_{i=0}^{r} \binom{n+1}{i+1} a_i$. Then $g(n) - g(n-1) = 0$ for all $n \gg 0$. Hence g is eventually constant, say equal to a_{-1}. We leave it to the reader to show that $a_{-1} + \sum_{i=0}^{r} \binom{n+1}{i+1} a_i$ has the required shape. $\square$

Before proceeding further, we recall that there is a group $K'_0(R)$ associated to any ring R that has the following properties:

(1) For every finite R-module M there is given an element $[M]$ in $K'_0(R)$,
(2) for every short exact sequence $0 \to M' \to M \to M'' \to 0$ we have the relation $[M] = [M'] + [M'']$,
(3) the group $K'_0(R)$ is generated by the elements $[M]$, and
(4) all relations in $K'_0(R)$ are $\mathbf{Z}$-linear combinations of the relations coming from exact sequences as above.

The actual construction is a bit annoying for set-theoretic reasons (one has to take care that the collection of all finitely generated R-modules is a proper class). However, this problem can be overcome by taking as set of generators of the group $K'_0(R)$ the elements $[R^n/K]$ where n ranges over all integers and K ranges over all submodules $K \subset R^n$. The generators for the subgroup of relations imposed on these elements will be the relations coming from short exact sequences whose terms are of the form R^n/K. The element $[M]$ is defined by choosing n and K such that $M \cong R^n/K$ and putting $[M] = [R^n/K]$. Details are left to the reader.

Example 24.8. If R is an Artinian local ring then the length function defines a natural abelian group isomorphism $\text{length}_R : K'_0(R) \cong \mathbf{Z}$.

Proof. The length of any finite R-module is finite, because it is the quotient of R^n which has finite length by Lemma 17.6. The length function is additive in short exact sequences, see Lemma 16.3, and so defines a homomorphism $K'_0(R) \to \mathbf{Z}$. But the group $K'_0(R)$ is generated by $[R/\mathfrak{m}]$ (cf. Lemma 16.9), which has length 1, and so the homomorphism is an isomorphism. $\square$

Proposition 24.9. *Suppose that S is a Noetherian graded ring and M a finite graded S-module. Consider the function*

$$\mathbf{Z} \longrightarrow K'_0(S_0), \quad n \longmapsto [M_n]$$

see Lemma 24.4. If S_+ is generated by elements of degree 1, then this function is a numerical polynomial.

PROOF. We prove this by induction on the minimal number of generators of S_1. If this number is 0, then $M_n = 0$ for all $n \gg 0$ and the result holds. To prove the induction step, let $x \in S_1$ be one of a minimal set of generators, so that the induction hypothesis applies to the graded ring $S/(x)$.

Let $\overline{M} = M/xM$, so that the result holds for $\overline{M}$ by induction. Note that the map $x : M \to M$ is *not* a map of graded S-modules, since it does not map M_d into M_d. Namely, for each d we have the following short exact sequence of S_0-modules

$$M_d \xrightarrow{x} M_{d+1} \to \overline{M}_{d+1} \to 0.$$

If multiplication by x were injective on M we would have $[M_{d+1}] - [M_d] = [\overline{M}_{d+1}]$, and the result would follow from Lemma 24.7. It therefore suffices to explain how to reduce to the case where multiplication by x is injective.

First we show the result holds if x is nilpotent on M. This we do by induction on the minimal integer r such that $x^r M = 0$. If $r = 1$, then M is a module over S/xS and the result holds (by the first induction hypothesis). If $r > 1$, then we can find a short exact sequence $0 \to M' \to M \to M'' \to 0$ such that the integers r', r'' are strictly smaller than r. Thus we know the result for M'' and M'. Hence we get the result for M because of the relation $[M_d] = [M'_d] + [M''_d]$ in $K'_0(S_0)$.

If x is not nilpotent on M, let $M' \subset M$ be the largest submodule on which x is nilpotent. Considering the exact sequence $0 \to M' \to M \to M/M' \to 0$ we see again it suffices to prove the result for M/M'. But multiplication by x is injective on M/M', and so we are done. □

EXERCISE 24.10. If S is still Noetherian but S is not generated in degree 1, then the function associated to a graded S-module is a periodic polynomial (i.e., it is a numerical polynomial on the congruence classes of integers modulo n for some n).

EXAMPLE 24.11. Suppose that S_0 is an Artinian local ring. Combining Proposition 24.9 with Example 24.8 and Lemma 24.6 we see that any finitely generated graded S-module gives rise to an integer-valued numerical polynomial $n \mapsto \text{length}_{S_0}(M_n)$.

LEMMA 24.12. *Let k be a field. Suppose that $I \subset k[X_1, \ldots, X_d]$ is a nonzero graded ideal. Let $M = k[X_1, \ldots, X_d]/I$. Then the numerical polynomial $n \mapsto \dim_k(M_n)$ (see Example 24.11) has degree $< d - 1$ (or is zero if $d = 1$).*

PROOF. The numerical polynomial associated to the graded module $k[X_1, \ldots, X_n]$ is $n \mapsto \binom{n-1+d}{d-1}$. For any nonzero homogeneous $f \in I$ of degree e and any degree $n \gg e$ we have $I_n \supset f \cdot k[X_1, \ldots, X_d]_{n-e}$ and hence $\dim_k(I_n) \geq \binom{n-e-1+d}{d-1}$. Hence $\dim_k(M_n) \leq \binom{n-1+d}{d-1} - \binom{n-e-1+d}{d-1}$. We win because the last expression has degree $< d - 1$ (or is zero if $d = 1$). □

25. Hilbert polynomials

In all of this section $(R, \mathfrak{m}, \kappa)$ is a Noetherian local ring. We develop some theory on Hilbert functions of modules in this section. Let M be a finite R-module. We define the *Hilbert function* of M to be the function

$$\varphi_M : n \longmapsto \text{length}_R(\mathfrak{m}^n M/\mathfrak{m}^{n+1} M)$$

defined for all integers $n \geq 0$. Another important invariant is the function

$$\chi_M : n \longmapsto \text{length}_R(M/\mathfrak{m}^{n+1}M)$$

defined for all integers $n \geq 0$. There is a variant of this construction which uses an ideal of definition.

Definition 25.1. Let $(R, \mathfrak{m})$ be a local Noetherian ring. An ideal satisfying any of the following equivalent conditions:

- $\sqrt{I} = \mathfrak{m}$,
- $V(I) = \{\mathfrak{m}\}$,
- $\mathfrak{m}^r \subset I \subset \mathfrak{m}$ for some r

is called an *ideal of definition of R.*

Let $I \subset R$ be an ideal of definition. Any finite R-module annihilated by a power of I therefore has finite length (Lemma 16.6) and it makes sense to define

$$\varphi_{I,M}(n) = \text{length}_R(I^nM/I^{n+1}M) \quad \text{and} \quad \chi_{I,M}(n) = \text{length}_R(M/I^{n+1}M)$$

for all $n \geq 0$.

Proposition 25.2. *Let R be a Noetherian local ring. Let M be a finite R-module. Let $I \subset R$ be an ideal of definition. The Hilbert function $\varphi_{I,M}$ and the function $\chi_{I,M}$ are numerical polynomials.*

Proof. Consider the graded ring $S = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots = \bigoplus_{d \geq 0} I^d/I^{d+1}$. Consider the graded S-module $N = M/IM \oplus IM/I^2M \oplus \cdots = \bigoplus_{d \geq 0} I^dM/I^{d+1}M$. This pair (S, N) satisfies the hypotheses of Proposition 24.9. Hence the result for $\varphi_{I,M}$ follows from that proposition and Example 24.8. The result for $\chi_{I,M}$ follows from this and Lemma 24.7. ☐

Definition 25.3. Let R be a Noetherian local ring. Let M be a finite R-module. The *Hilbert polynomial* of M over R is the element $P(t) \in \mathbf{Q}[t]$ such that $P(n) = \varphi_M(n)$ for $n \gg 0$.

By Proposition 25.2 we see that the Hilbert polynomial exists. We remark that because $\chi_M(n) \leq \chi_{I,M}(n) \leq \chi_M((r+1)n)$, the degrees of χ_M and $\chi_{I,M}$ are the same for any ideal of definition I, and therefore the same holds for $\varphi_M, \varphi_{I,M}$.

Definition 25.4. Let R be a local Noetherian ring and M a finite R-module. We denote $d(M)$ the element of $\{-\infty, 0, 1, 2, \ldots\}$ defined as follows:

(1) If $M = 0$ we set $d(M) = -\infty$,
(2) if $M \neq 0$ then $d(M)$ is the degree of the numerical polynomial χ_M.

If $\mathfrak{m}^nM \neq 0$ for all n, then since $\varphi_M(n) = \chi_M(n) - \chi_M(n-1)$ we see that $d(M)$ is the degree $+1$ of the Hilbert polynomial of M.

In the rest of this section we establish some technical results that will be used in the next section.

Lemma 25.5. *Suppose that $M' \subset M$ are finite R-modules with finite length quotient. Then there exist constants c_1, c_2 such that for all $n \geq c_2$ we have*

$$c_1 + \chi_{I,M'}(n - c_2) \leq \chi_{I,M}(n) \leq c_1 + \chi_{I,M'}(n)$$

Proof. Since M/M' has finite length there is a $c_2 \geq 0$ such that $I^{c_2}M \subset M'$. Let $c_1 = \text{length}_R(M/M')$. For $n \geq c_2$ we have

$$\begin{aligned} \chi_{I,M}(n) &= \text{length}_R(M/I^{n+1}M) \\ &= c_1 + \text{length}_R(M'/I^{n+1}M) \\ &\leq c_1 + \text{length}_R(M'/I^{n+1}M') \\ &= c_1 + \chi_{I,M'}(n) \end{aligned}$$

On the other hand, since $I^{c_2}M \subset M'$, we have $I^nM \subset I^{n-c_2}M'$ for $n \geq c_2$. Thus for $n \geq c_2$ we get

$$\begin{aligned} \chi_{I,M}(n) &= \text{length}_R(M/I^{n+1}M) \\ &= c_1 + \text{length}_R(M'/I^{n+1}M) \\ &\geq c_1 + \text{length}_R(M'/I^{n+1-c_2}M') \\ &= c_1 + \chi_{I,M'}(n - c_2) \end{aligned}$$

which finishes the proof. □

Lemma 25.6. *Let R be a Noetherian local ring. Let $I \subset R$ be an ideal of definition. Let M be a finite R-module which does not have finite length. If $M' \subset M$ is a submodule with finite colength, then $\chi_{I,M}$, $\chi_{I,M'}$ are numerical polynomials with the same degree and leading coefficient. In particular $\chi_{I,M} - \chi_{I,M'}$ is a polynomial of lower degree.*

Proof. Follows from Lemma 25.5 by elementary considerations. □

Lemma 25.7. *Suppose that $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of finite R-modules. Then there exists a submodule $N \subset M'$ with finite colength l and $c \geq 0$ such that*

$$\chi_{I,M}(n) = \chi_{I,M''}(n) + \chi_{I,N}(n - c) + l$$

for all $n \geq c$.

Proof. Note that $M/I^nM \to M''/I^nM''$ is surjective with kernel $M'/M' \cap I^nM$. By the Artin-Rees Lemma 15.9 there exists a constant c such that $M' \cap I^nM = I^{n-c}(M' \cap I^cM)$ for all $n \geq c$. Denote $N = M' \cap I^cM$. Note that $I^cM' \subset N \subset M'$. Hence $\text{length}_R(M'/M' \cap I^nM) = \text{length}_R(M'/N) + \text{length}_R(N/I^{n-c}N)$ for $n \geq c$. From the short exact sequence

$$0 \to M'/M' \cap I^nM \to M/I^nM \to M''/I^nM'' \to 0$$

and additivity of lengths (Lemma 16.3) we obtain the equality

$$\chi_{I,M}(n-1) = \chi_{I,M''}(n-1) + \chi_{I,N}(n-c-1) + \text{length}_R(M'/N)$$

for $n \geq c$. □

Lemma 25.8. *Let R be a Noetherian local ring. Let $I \subset R$ be an ideal of definition. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finite R-modules. Then*

1. *if M' does not have finite length, then $\chi_{I,M} - \chi_{I,M''} - \chi_{I,M'}$ is a numerical polynomial of degree less than the degree of $\chi_{I,M'}$,*
2. $\max\{\deg(\chi_{I,M'}), \deg(\chi_{I,M''})\} = \deg(\chi_{I,M})$, *and*
3. $\max\{d(M'), d(M'')\} = d(M)$,

Proof. Part (1) straightforwardly combines Lemmas 25.7 and 25.6. (The latter is to be applied to the inclusion $N \subset M'$ with N as in Lemma 25.7).

Note that the leading coefficients of $\chi_{I,M'}$ and $\chi_{I,M''}$ are nonnegative. Thus the degree of $\chi_{I,M'} + \chi_{I,M''}$ is equal to the maximum of the degrees. Thus if M' does not have finite length, then (2) follows from (1). If M' does have finite length, then $I^nM \cap M' = 0$ for all $n \gg 0$ by Artin-Rees (Lemma 15.9). Thus $M/I^nM \to M''/I^nM''$ is a surjection with kernel M' for $n \gg 0$ and we see that $\chi_{I,M}(n) - \chi_{I,M''}(n) = \text{length}(M')$ for all $n \gg 0$. Thus (2) holds in this case also.

Part (3) is by definition equivalent to (2) except if one of M, M', or M'' is zero. These special cases are trivial. ☐

26. Dimensions of local Noetherian rings

Definition 26.1. The *Krull dimension* of the ring R is the Krull dimension of the topological space $\text{Spec}(R)$, i.e., the supremum of the lengths of the chains of irreducible closed subsets of $\text{Spec}(R)$). In other words it is the supremum of the integers $n \geq 0$ such that there exists a chain of prime ideals of length n:

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n, \quad \mathfrak{p}_i \neq \mathfrak{p}_{i+1}.$$

Definition 26.2. The *height* of a prime ideal $\mathfrak{p}$ of a ring R is the dimension of the local ring $R_{\mathfrak{p}}$.

If R is a Noetherian local ring, our goal is to show that the invariant $d(R)$ defined in Definition 25.4 coincides with $\dim(R)$. Here is a warm up lemma.

Lemma 26.3. *Let R be a Noetherian local ring. Then* $\dim(R) = 0 \Leftrightarrow d(R) = 0$.

Proof. This is a consequence of Lemma 17.6: $d(R) = 0$ if and only if R has finite length as an R-module if and only if every prime ideal of R is maximal if and only if $\dim(R) = 0$. ☐

Proposition 26.4. *Let R be a local Noetherian ring. Let $d \geq 0$ be an integer. The following are equivalent:*

1. $\dim(R) = d$,
2. $d(R) = d$,
3. *there exists an ideal of definition generated by d elements, and no ideal of definition is generated by fewer than d elements.*

In particular R is finite-dimensional.

Proof. We will prove the proposition by induction on d. The base case $d = 0$ is given by Lemma 26.3, so we may assume that $d > 0$. Denote the minimal number of generators for an ideal of definition of R by $d'(R)$. We will prove that the inequalities $\dim(R) \geq d'(R) \geq d(R) \geq \dim(R)$, and hence they are all equal.

First, assume that $\dim(R) = d$. Let $\mathfrak{p}_i$ be the minimal primes of R. According to Lemma 15.8 there are finitely many, so we can find $x \in \mathfrak{m}$, $x \notin \mathfrak{p}_i$ by Lemma 7.2. Note that every maximal chain of primes starts with some $\mathfrak{p}_i$, hence the dimension of R/xR is at most $d-1$. By induction there are $x_2, \ldots, x_d$ which generate an ideal of definition in R/xR. Hence R has an ideal of definition generated by (at most) d elements.

Assume $d'(R) = d$. Let $I = (x_1, \ldots, x_d)$ be an ideal of definition. Note that I^n/I^{n+1} is a quotient of a direct sum of $\binom{d+n-1}{d-1}$ copies R/I via multiplication by all degree n monomials in $x_1, \ldots, x_n$. Hence $\text{length}_R(I^n/I^{n+1})$ is bounded by a polynomial of degree $d-1$. Thus $d(R) \leq d$.

Assume $d(R) = d$. Consider a chain of primes $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_e$, with all inclusions strict. Write $\mathfrak{p} = \mathfrak{p}_0$. We want to show $e \leq d$. This is certainly true if $e = 1$, so assume $e \geq 2$. Pick some ideal of definition $I \subset R$. Lemma 25.8(2) implies, via the exact sequence $0 \to \mathfrak{p} \to R \to R/\mathfrak{p} \to 0$, that $d(R/\mathfrak{p}) \leq d$. Also, Lemma 26.3 gives $d(R/\mathfrak{p}) \neq 0$. Pick $x \in \mathfrak{p}_1$, $x \notin \mathfrak{p}$. Consider the short exact sequence

$$0 \to R/\mathfrak{p} \xrightarrow{x} R/\mathfrak{p} \to R/(xR + \mathfrak{p}) \to 0.$$

Lemma 25.8(1) implies that $\chi_{I,R/\mathfrak{p}} - \chi_{I,R/\mathfrak{p}} - \chi_{I,R/(xR+\mathfrak{p})} = -\chi_{I,R/(xR+\mathfrak{p})}$ has degree less than d. In other words, $d(R/(xR+\mathfrak{p})) \leq d-1$, and hence $\dim(R/(xR+\mathfrak{p})) \leq d-1$, by induction. Now $R/(xR+\mathfrak{p})$ has the chain of prime ideals $\mathfrak{p}_1/(xR+\mathfrak{p}) \subset \cdots \subset \mathfrak{p}_e/(xR+\mathfrak{p})$ which gives $e-1 \leq d-1$. Since we started with an arbitrary chain of primes this proves that $\dim(R) \leq d(R)$. □

Let $(R, \mathfrak{m})$ be a Noetherian local ring. From the above it is clear that $\mathfrak{m}$ cannot be generated by fewer than $\dim(R)$ elements. By Nakayama's Lemma 7.14 the minimal number of generators of $\mathfrak{m}$ equals $\dim_{\kappa(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$. Hence we have the following fundamental inequality

$$\dim(R) \leq \dim_{\kappa(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2.$$

It turns out that the rings where equality holds have a lot of good properties. They are called regular local rings.

Definition 26.5. Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d.

(1) A *system of parameters of* R is a sequence of elements $x_1, \ldots, x_d \in \mathfrak{m}$ which generates an ideal of definition of R,
(2) if there exist $x_1, \ldots, x_d \in \mathfrak{m}$ such that $\mathfrak{m} = (x_1, \ldots, x_d)$ then we call R a *regular local ring* and $x_1, \ldots, x_d$ a *regular system of parameters.*

Lemma 26.6. *Suppose that R is a Noetherian local ring and $x \in \mathfrak{m}$ an element of its maximal ideal. Then $\dim R \leq \dim R/xR + 1$. If x is not contained in any of the minimal primes of R (for example, if x is not a zerodivisor) then equality holds.*

Proof. If $x_1, \ldots, x_{\dim R/xR} \in R$ map to elements of R/xR which generate an ideal of definition for R/xR, then $x, x_1, \ldots, x_{\dim R/xR}$ generate an ideal of definition for R. Hence the inequality by Proposition 26.4. On the other hand, if x is not contained in any minimal prime of R, then the chains of primes in R/xR all give rise to chains in R which are at least one step away from being maximal. □

Lemma 26.7. *Let R be a Noetherian local ring, M a finite R-module, and $f \in \mathfrak{m}$ an element of the maximal ideal of R. Then*

$$\dim(\text{Supp}(M/fM)) \leq \dim(\text{Supp}(M)) \leq \dim(\text{Supp}(M/fM)) + 1$$

If f is not in any of the minimal primes of the support of M (for example if f is not a zerodivisor on M), then equality holds for the right-hand inequality.

Proof. (The parenthetical statement follows from Lemma 19.12.) The first inequality follows from $\text{Supp}(M/fM) \subset \text{Supp}(M)$, see Lemma 18.7. For the second inequality, note that $\text{Supp}(M/fM) = \text{Supp}(M) \cap V(f)$, see Lemma 18.7. It follows, for example by Lemma 18.11 and elementary properties of dimension, that it suffices to show $\dim V(\mathfrak{p}) \leq \dim(V(\mathfrak{p}) \cap V(f)) + 1$ for primes $\mathfrak{p}$ of R. This is a consequence of Lemma 26.6. Finally, if f is not contained in any minimal prime of the support of M, then the chains of primes in $\mathrm{Supp}(M/fM)$ all give rise to chains in $\mathrm{Supp}(M)$ which are at least one step away from being maximal. □

The following exercises are applications of the lemmas and proposition above.

Exercise 26.8. Let R be a Noetherian ring. Let $f_1, \ldots, f_r \in R$.

(1) If $\mathfrak{p}$ is minimal over $(f_1, \ldots, f_r)$ then the height of $\mathfrak{p}$ is $\leq r$.
(2) If $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(R)$ and $\mathfrak{q}$ is minimal over $(\mathfrak{p}, f_1, \ldots, f_r)$, then every chain of primes between $\mathfrak{p}$ and $\mathfrak{q}$ has length at most r.

The case $r = 1$ in the above is often called *Krull's Hauptidealsatz*.

Exercise 26.9. Let $(R, \mathfrak{m})$ be a Noetherian local ring. Suppose $x_1, \ldots, x_d \in \mathfrak{m}$ generate an ideal of definition and $d = \dim(R)$. Then $\dim(R/(x_1, \ldots, x_i)) = d - i$ for all $i = 1, \ldots, d$.

Exercise 26.10. Let R be a Noetherian local ring. Let M be a finite R-module. Then $d(M) = \dim(\mathrm{Supp}(M))$. (Hint: use that $d(M) = \max\{d(R/\mathfrak{p}_i)\}$ where the primes $\mathfrak{p}_i$ are as in Lemma 18.10.)

Exercise 26.11. Let R be a Noetherian ring. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finite R-modules. Then $\mathrm{Supp}(M')$, $\mathrm{Supp}(M'')$, and $\mathrm{Supp}(M)$ are closed (Lemma 18.5) and so

$$\max\{\dim(\mathrm{Supp}(M')), \dim(\mathrm{Supp}(M''))\} = \dim(\mathrm{Supp}(M)).$$

27. Transcendence

We digress briefly to review the basic results of transcendence theory for fields.

Definition 27.1. Let $k \subset K$ be a field extension.

(1) A collection of elements $\{x_i\}_{i \in I}$ of K is called *algebraically independent* over k if the map
$$k[X_i; i \in I] \longrightarrow K$$
which maps X_i to x_i is injective.
(2) The field of fractions of a polynomial ring $k[x_i; i \in I]$ is denoted $k(x_i; i \in I)$.
(3) A *purely transcendental extension* of k is any field extension $k \subset K$ isomorphic to the field of fractions of a polynomial ring over k.
(4) A *transcendence basis* of K/k is a collection of elements $\{x_i\}_{i \in I}$ which are algebraically independent over k and such that the extension $k(x_i; i \in I) \subset K$ is algebraic.

Lemma 27.2. *Let E/F be a field extension. A transcendence basis of E over F exists. Any two transcendence bases have the same cardinality.*

Proof. Let A be an algebraically independent subset of E. Let G be a subset of E containing A that generates E/F. We claim we can find a transcendence basis B such that $A \subset B \subset G$. To prove this consider the collection of algebraically independent subsets $\mathcal{B}$ whose members are subsets of G that contain A. Define a partial ordering on $\mathcal{B}$ using inclusion. Then $\mathcal{B}$ contains at least one element

A. The union of the elements of a totally ordered subset T of $\mathcal{B}$ is an algebraically independent subset of E over F since any algebraic dependence relation would have occurred in one of the elements of T (since polynomials only involve finitely many variables). The union also contains A and is contained in G. By Zorn's lemma, there is a maximal element $B \in \mathcal{B}$. Now we claim E is algebraic over $F(B)$. This is because if it wasn't then there would be an element $f \in G$ transcendental over $F(B)$ since $E(G) = F$. Then $B \cup \{f\}$ wold be algebraically independent contradicting the maximality of B. Thus B is our transcendence basis.

Let B and B' be two transcendence bases. Without loss of generality, we can assume that $|B'| \leq |B|$. Now we divide the proof into two cases: the first case is that B is an infinite set. Then for each $\alpha \in B'$, there is a finite set B_α such that α is algebraic over $E(B_\alpha)$ since any algebraic dependence relation only uses finitely many indeterminates. Then we define $B^* = \bigcup_{\alpha \in B'} B_\alpha$. By construction, $B^* \subset B$, but we claim that in fact the two sets are equal. To see this, suppose that they are not equal, say there is an element $\beta \in B \setminus B^*$. We know β is algebraic over $E(B')$ which is algebraic over $E(B^*)$. Therefore β is algebraic over $E(B^*)$, a contradiction. So $|B| \leq |\bigcup_{\alpha \in B'} B_\alpha|$. Now if B' is finite, then so is B so we can assume B' is infinite; this means

$$|B| \leq |\bigcup_{\alpha \in B'} B_\alpha| = |B'|$$

because each B_α is finite and B' is infinite. Therefore in the infinite case, $|B| = |B'|$.

Now we need to look at the case where B is finite. In this case, B' is also finite, so suppose $B = \{\alpha_1, \dots, \alpha_n\}$ and $B' = \{\beta_1, \dots, \beta_m\}$ with $m \leq n$. We perform induction on m: if $m = 0$ then E/F is algebraic so $B = \emptyset$ so $n = 0$. If $m > 0$, there is an irreducible polynomial $f \in E[x, y_1, \dots, y_n]$ such that $f(\beta_1, \alpha_1, \dots, \alpha_n) = 0$ and such that x occurs in f. Since β_1 is not algebraic over F, f must involve some y_i so without loss of generality, assume f uses y_1. Let $B^* = \{\beta_1, \alpha_2, \dots, \alpha_n\}$. We claim that B^* is a basis for E/F. To prove this claim, we see that we have a tower of algebraic extensions

$$E/F(B^*, \alpha_1)/F(B^*)$$

since α_1 is algebraic over $F(B^*)$. Now we claim that B^* (counting multiplicity of elements) is algebraically independent over E because if it weren't, then there would be an irreducible $g \in E[x, y_2, \dots, y_n]$ such that $g(\beta_1, \alpha_2, \dots, \alpha_n) = 0$ which must involve x making β_1 algebraic over $E(\alpha_2, \dots, \alpha_n)$ which would make α_1 algebraic over $E(\alpha_2, \dots, \alpha_n)$ which is impossible. So this means that $\{\alpha_2, \dots, \alpha_n\}$ and $\{\beta_2, \dots, \beta_m\}$ are bases for E over $F(\beta_1)$ which means by induction, $m = n$. □

DEFINITION 27.3. Let $k \subset K$ be a field extension. The *transcendence degree* of K over k is the cardinality of a transcendence basis of K over k. It is denoted $\mathrm{trdeg}_k(K)$. If $R \subset S$ are domains we may write $\mathrm{trdeg}_R(S)$ for $\mathrm{trdeg}_{Q(R)}(Q(S))$.

LEMMA 27.4. *Let $k \subset K \subset L$ be field extensions. Then*

$$\mathrm{trdeg}_k(L) = \mathrm{trdeg}_K(L) + \mathrm{trdeg}_k(K).$$

PROOF. Choose a transcendence basis $A \subset K$ of K over k. Choose a transcendence basis $B \subset L$ of L over K. Then it is straightforward to see that $A \cup B$ is a transcendence basis of L over k. □

28. The dimension formula

We begin this section with a collection of easy results relating dimensions of rings when there are maps between them.

LEMMA 28.1. *Suppose $R \to S$ is a ring map satisfying either going up, see Definition 20.1, or going down see Definition 20.1. Assume in addition that* $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ *is surjective. Then* $\dim(R) \leq \dim(S)$.

PROOF. Assume going up. Take any chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_e$ of prime ideals in R. By surjectivity we may choose a prime $\mathfrak{q}_0$ mapping to $\mathfrak{p}_0$. By going up we may extend this to a chain of length e of primes $\mathfrak{q}_i$ lying over $\mathfrak{p}_i$. Thus $\dim(S) \geq \dim(R)$. The case of going down is exactly the same. □

LEMMA 28.2. *Let k be a field. Let S be a k-algebra.*

(1) *If S finite dimensional over k and a domain, then S is a field.*
(2) *If S is integral over k and a domain, then S is a field.*
(3) *If S is integral over k then every prime of S is a maximal ideal.*

PROOF. Part (2) evidently implies both (1) and (3). Let S be integral over k and assume S is a domain, Take any nonzero $s \in S$. Then $P(s) = 0$ for some polynomial with coefficients in k. Since S is a domain we may assume $P(0) \neq 0$. If $P(x) = a_n x^n + \cdots + a_1 x + a_0$ then $-a_0^{-1}(a_n s^{n-1} + \cdots + a_1)$ is an inverse of s in S. □

LEMMA 28.3. *Suppose that $R \to S$ is a ring map such that S is integral over R. Then* $\dim(R) \geq \dim(S)$.

PROOF. If $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(S)$ are distinct primes having the same image in $\mathrm{Spec}(R)$, then neither $\mathfrak{q} \subset \mathfrak{q}'$ nor $\mathfrak{q}' \subset \mathfrak{q}$. Indeed, let $\mathfrak{p} \subset R$ be the image. By Remark 8.12 the primes $\mathfrak{q}, \mathfrak{q}'$ correspond to prime ideals in $S \otimes_R \kappa(\mathfrak{p})$. Then the claim follows from Lemma 28.2.

Now the lemma follows by taking a chain of distinct primes of maximal length in S and pulling it back to R. □

LEMMA 28.4. *Suppose $R \subset S$ and S integral over R. Then* $\dim(R) = \dim(S)$.

PROOF. This is a combination of Lemmas 21.11, 21.12, 28.1, and 28.3. □

DEFINITION 28.5. Suppose that $R \to S$ is a ring map. Let $\mathfrak{q} \subset S$ be a prime lying over the prime $\mathfrak{p}$ of R. The *local ring of the fibre at* $\mathfrak{q}$ is the local ring

$$S_{\mathfrak{q}}/\mathfrak{p}S_{\mathfrak{q}} = (S/\mathfrak{p}S)_{\mathfrak{q}} = (S \otimes_R \kappa(\mathfrak{p}))_{\mathfrak{q}}$$

LEMMA 28.6. *Let $R \to S$ be a homomorphism of Noetherian rings. Let $\mathfrak{q} \subset S$ be a prime lying over the prime $\mathfrak{p}$. Then*

$$\dim(S_{\mathfrak{q}}) \leq \dim(R_{\mathfrak{p}}) + \dim(S_{\mathfrak{q}}/\mathfrak{p}S_{\mathfrak{q}}).$$

If moreover the going down property holds for $R \to S$ (for example if $R \to S$ is flat, see Lemma 20.9) then equality holds.

PROOF. We use the characterization of dimension of Proposition 26.4. Let $x_1, \ldots, x_d$ be elements of $\mathfrak{p}$ generating an ideal of definition of $R_{\mathfrak{p}}$ with $d = \dim(R_{\mathfrak{p}})$. Let $y_1, \ldots, y_e$ be elements of $\mathfrak{q}$ generating an ideal of definition of $S_{\mathfrak{q}}/\mathfrak{p}S_{\mathfrak{q}}$ with $e = \dim(S_{\mathfrak{q}}/\mathfrak{p}S_{\mathfrak{q}})$. It is clear that $S_{\mathfrak{q}}/(x_1, \ldots, x_d, y_1, \ldots, y_e)$ has a nilpotent maximal ideal. Hence $x_1, \ldots, x_d, y_1, \ldots, y_e$ generate an ideal of definition if $S_{\mathfrak{q}}$. This gives the first part.

To get equality in the second part, choose a chain of primes $\mathfrak{p}S \subset \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_e = \mathfrak{q}$ with $e = \dim(S_{\mathfrak{q}}/\mathfrak{p}S_{\mathfrak{q}})$. On the other hand, choose a chain of primes $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d = \mathfrak{p}$ with $d = \dim(R_{\mathfrak{p}})$. By the going down theorem we may choose $\mathfrak{q}_{-1} \subset \mathfrak{q}_0$ lying over $\mathfrak{p}_{d-1}$. And then we may choose $\mathfrak{q}_{-2} \subset \mathfrak{q}_{d-1}$ lying over $\mathfrak{p}_{d-2}$. Inductively we keep going until we get a chain $\mathfrak{q}_{-d} \subset \cdots \subset \mathfrak{q}_e$ of length $e + d$. □

EXERCISE 28.7. Let $R \to S$ be a local homomorphism of local Noetherian rings. Assume

(1) R is regular,
(2) $S/\mathfrak{m}_R S$ is regular, and
(3) $R \to S$ is flat.

Then S is regular.

DEFINITION 28.8.

(1) A ring R is said to be *catenary* if for any pair of prime ideals $\mathfrak{p} \subset \mathfrak{q}$, all maximal chains of primes $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_e = \mathfrak{q}$ have the same (finite) length.
(2) A ring R is said to be *universally catenary* if R is Noetherian and every R algebra of finite type is catenary.

LEMMA 28.9. *Any quotient of a (universally) catenary ring is (universally) catenary.*

PROOF. Let A be a ring and let $I \subset A$ be an ideal. The description of $\mathrm{Spec}(A/I)$ in Lemma 8.11 shows that if A is catenary, then so is A/I. If $A/I \to B$ is of finite type, then $A \to B$ is of finite type. Hence if A is universally catenary, then B is catenary. Combined with the Hilbert basis theorem (Lemma 15.1) this proves the lemma. □

By Lemma 28.9, universally catenary just means that R is Noetherian and that each polynomial algebra $R[x_1, \ldots, x_n]$ is catenary.

The main result of this section is the following.

LEMMA 28.10 (The dimension formula). *Let $R \subset S$ be a finite type inclusion of rings. Assume that R is Noetherian and that S is a domain. Let $\mathfrak{q}$ be a prime of S lying over the prime $\mathfrak{p}$ of R. Then we have*

$$\mathrm{height}(\mathfrak{q}) \leq \mathrm{height}(\mathfrak{p}) + \mathrm{trdeg}_R(S) - \mathrm{trdeg}_{\kappa(\mathfrak{p})}\kappa(\mathfrak{q}).$$

If R is universally catenary then equality holds.

PROOF. Suppose that $R \subset S' \subset S$ is a finitely generated R-subalgebra of S. In this case set $\mathfrak{q}' = S' \cap \mathfrak{q}$. The lemma for the ring maps $R \to S'$ and $S' \to S$ implies the lemma for $R \to S$ by additivity of transcendence degree in towers of fields (Lemma 27.4). Hence we can use induction on the number of generators of S over R and reduce to the case where S is generated by one element over R. Write k for the fraction field $Q(R/\mathfrak{p})$.

Case I: $S = R[x]$ is a polynomial algebra over R. In this case we have $\mathrm{trdeg}_R(S) = 1$. Also $R \to S$ is flat and hence

$$\dim(S_{\mathfrak{q}}) = \dim(R_{\mathfrak{p}}) + \dim(S_{\mathfrak{q}}/\mathfrak{p}S_{\mathfrak{q}})$$

by Lemma 28.6. Note that $S_{\mathfrak q}/\mathfrak p S_{\mathfrak q} \cong k[x]_{\mathfrak q}$ has dimension at most 1. Let $\mathfrak r = \mathfrak p S$. Then $\text{trdeg}_{\kappa(\mathfrak p)}\kappa(\mathfrak q) = 1$ is equivalent to $\mathfrak q = \mathfrak r$, and implies that $S_{\mathfrak q}/\mathfrak p S_{\mathfrak q} \cong k(x)$ has dimension 0. In the same vein $\text{trdeg}_{\kappa(\mathfrak p)}\kappa(\mathfrak q) = 0$ is equivalent to having a strict inclusion $\mathfrak r \subset \mathfrak q$, which implies that $\dim(S_{\mathfrak q}/\mathfrak p S_{\mathfrak q}) = 1$. Thus we are done with case I with equality in every instance.

Case II: $S = R[x]/\mathfrak n$ with $\mathfrak n \neq 0$. In this case we have $\text{trdeg}_R(S) = 0$. Denote $\mathfrak q' \subset R[x]$ the prime corresponding to $\mathfrak q$. Thus we have

$$S_{\mathfrak q} = (R[x])_{\mathfrak q'}/\mathfrak n(R[x])_{\mathfrak q'}$$

By the previous case we have $\dim((R[x])_{\mathfrak q'}) = \dim(R_{\mathfrak p}) + 1 - \text{trdeg}_{\kappa(\mathfrak p)}\kappa(\mathfrak q)$. Since $\mathfrak n \neq 0$ we see that the dimension of $S_{\mathfrak q}$ decreases by at least one, see Lemma 26.6, which proves the inequality of the lemma. To see the equality in case R is universally catenary note that $\mathfrak n \subset R[x]$ is a height one prime as $\mathfrak n \cap R = 0$ and so it corresponds to a nonzero prime in $Q(R)[x]$. Hence any maximal chain of primes in $R[x]_{\mathfrak q'}/\mathfrak n$ corresponds to a maximal chain of primes with length 1 greater between $\mathfrak q'$ and (0) in $R[x]$. If R is universally catenary these all have the same length equal to the height of $\mathfrak q'$. This proves that $\dim(R[x]_{\mathfrak q'}/\mathfrak n) = \dim(R[x]_{\mathfrak q'}) - 1$ as desired. $\square$

Exercise 28.11. Let R be a Noetherian domain. Then $\dim R[x_1, \ldots, x_n] = \dim R + n$.

The following lemma says that generically finite maps tend to be quasi-finite in codimension 1.

Lemma 28.12. *Let $A \to B$ be a ring map. Assume*

1. *$A \subset B$ is an extension of domains.*
2. *A is Noetherian,*
3. *$A \to B$ is of finite type, and*
4. *the extension $Q(A) \subset Q(B)$ is finite.*

Let $\mathfrak p \subset A$ be a prime of height 1. Then there are at most finitely many primes of B lying over $\mathfrak p$ and they all have height 1.

Proof. By the dimension formula (Lemma 28.10) for any prime $\mathfrak q$ lying over $\mathfrak p$ we have

$$\dim(B_{\mathfrak q}) \leq \dim(A_{\mathfrak p}) - \text{trdeg}_{\kappa(\mathfrak p)}\kappa(\mathfrak q).$$

As the domain $B_{\mathfrak q}$ has at least 2 prime ideals we see that $\dim(B_{\mathfrak q}) \geq 1$. We conclude that $\dim(B_{\mathfrak q}) = 1$ and that the extension $\kappa(\mathfrak p) \subset \kappa(\mathfrak q)$ is algebraic. Any ring between $\kappa(\mathfrak p)$ and $\kappa(\mathfrak q)$ is a field, and so $\mathfrak q$ defines a closed point of the fibre $\text{Spec}(B \otimes_A \kappa(\mathfrak p))$. Since $B \otimes_A \kappa(\mathfrak p)$ is a Noetherian ring the fibre $\text{Spec}(B \otimes_A \kappa(\mathfrak p))$ is a Noetherian topological space, see Lemma 15.7. A Noetherian topological space consisting of closed points is finite, see for example Lemma 15.6. $\square$

29. Noether normalization

In this section we prove variants of the Noether normalization lemma. As a first step we prove the following.

Lemma 29.1. *Let k be a field. Let $S = k[x_1, \ldots, x_n]/I$ for some ideal I. If $I \neq 0$, then there exist $y_1, \ldots, y_{n-1} \in k[x_1, \ldots, x_n]$ such that S is finite over $k[y_1, \ldots, y_{n-1}]$. Moreover we may choose y_i to be in the $\mathbf{Z}$-subalgebra of $k[x_1, \ldots, x_n]$ generated by $x_1, \ldots, x_n$.*

PROOF. Pick $f \in I$, $f \neq 0$. It suffices to show the lemma for $k[x_1, \ldots, x_n]/(f)$ since S is a quotient of that ring. We will take $y_i = x_i - x_n^{e_i}$, $i = 1, \ldots, n-1$ for suitable integers e_i. When does this work? It suffices to show that $\overline{x_n} \in k[x_1, \ldots, x_n]/(f)$ is integral over the ring $k[y_1, \ldots, y_{n-1}]$. An equation for $\overline{x_n}$ over this ring is

$$f(y_1 + x_n^{e_1}, \ldots, y_{n-1} + x_n^{e_{n-1}}, x_n) = 0.$$

Hence we are done if we can show there exists integers e_i such that the leading coefficient with respect to x_n of the equation above is a nonzero element of k. Note that the leading term in x_n of

$$(y_1 + x_n^{e_1})^{\nu_1} \ldots (y_{n-1} + x_n^{e_{n-1}})^{\nu_{n-1}} x_n^{\nu_n} \quad \text{is} \quad x_n^{e_1\nu_1 + \cdots + e_{n-1}\nu_{n-1} + \nu_n}.$$

So what we want can be achieved by choosing $e_1, \ldots, e_{n-1}, e_n$ with $e_n = 1$ so that the numbers $\sum_i e_i \nu_i$ are all distinct as one varies over the multi-degrees $(\nu_1, \ldots, \nu_n)$ of nonzero terms of f. This is certainly possible, e.g. take $e_i = b^{n-i}$ for any integer b greater than the total degree of f. $\square$

LEMMA 29.2. *Let k be a field. Let $S = k[x_1, \ldots, x_n]/I$ for some ideal I. There exist $r \geq 0$, and $y_1, \ldots, y_r \in k[x_1, \ldots, x_n]$ such that (a) the map $k[y_1, \ldots, y_r] \to S$ is injective, and (b) the map $k[y_1, \ldots, y_r] \to S$ is finite. In this case the integer r is the dimension of S. Moreover we may choose y_i to be in the $\mathbf{Z}$-subalgebra of $k[x_1, \ldots, x_n]$ generated by $x_1, \ldots, x_n$.*

PROOF. By induction on n, with $n = 0$ being trivial. If $I = 0$, then take $r = n$ and $y_i = x_i$. If $I \neq 0$, then choose $y_1, \ldots, y_{n-1}$ as in Lemma 29.1. Let $S' \subset S$ be the subring generated by the images of the y_i. By induction we can choose r and $z_1, \ldots, z_r \in k[y_1, \ldots, y_{n-1}]$ such that (a), (b) hold for $k[z_1, \ldots, z_r] \to S'$. Since $S' \to S$ is injective and finite we see (a), (b) hold for $k[z_1, \ldots, z_r] \to S$. The assertion about dimension follows from Lemma 28.4. $\square$

LEMMA 29.3. *Let $R \to S$ be an injective finite type map of domains. Then there exists an integer d and factorization*

$$R \to R[y_1, \ldots, y_d] \to S' \to S$$

by injective maps such that S' is finite over $R[y_1, \ldots, y_d]$ and such that $S'_f \cong S_f$ for some nonzero $f \in R$.

PROOF. Pick $x_1, \ldots, x_n \in S$ which generate S over R. Let $K = Q(R)$ and $S_K = S \otimes_R K$. By Lemma 29.2 we can find $y_1, \ldots, y_d \in S$ such that $K[y_1, \ldots, y_d] \to S_K$ is a finite injective map. Moreover we may pick the y_j in the $\mathbf{Z}$-algebra generated by $x_1, \ldots, x_n$, ensuring $y_i \in S$ for all i.

As a finite ring map is integral (see Lemma 21.3) we can find monic $P_i \in K[y_1, \ldots, y_d][T]$ such that $P_i(x_i) = 0$ in S_K. Let $f \in R$ be a nonzero element such that $fP_i \in R[y_1, \ldots, y_d][T]$ for all i. Set $x'_i = fx_i$ and note that x'_i is integral over $R[y_1, \ldots, y_d]$ as we have $Q_i(x'_i) = 0$ where $Q_i = f^{\deg_T(P_i)} P_i(T/f)$ which is a monic polynomial in T with coefficients in $R[y_1, \ldots, y_d]$ by our choice of f.

Let $S' \subset S$ be the subalgebra generated by $y_1, \ldots, y_d$ and $x'_1, \ldots, x'_n$. Then $R[y_1, \ldots, y_n] \subset S'$ is finite by Lemma 21.5, and by construction $S'_f \cong S_f$. $\square$

As an application of Noether normalization, we prove a version of the generic flatness theorem, which says that a finite type algebra over a domain becomes flat after inverting a single element of the domain.

Lemma 29.4 (Generic flatness). *Let $R \to S$ be a ring map. Let M be an S-module. Assume*

(1) *R is Noetherian,*
(2) *R is a domain,*
(3) *$R \to S$ is of finite type, and*
(4) *M is a finite S-module.*

Then there exists a nonzero $f \in R$ such that M_f is a free R_f-module.

Proof. Let K be the fraction field of R. Set $S_K = K \otimes_R S$. This is an algebra of finite type over K. We will argue by induction on $d = \dim(S_K)$ (which is finite, see e.g. Exercise 28.11). Fix $d \geq 0$. Assume we know that the lemma holds in all cases where $\dim(S_K) < d$.

Suppose given $R \to S$ and M as in the lemma with $\dim(S_K) = d$. By Lemma 18.10 there exists a filtration $0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ so that M_i/M_{i-1} is isomorphic to $S/\mathfrak{q}$ for some prime $\mathfrak{q}$ of S. Note that $\dim((S/\mathfrak{q})_K) \leq \dim(S_K)$. Also, note that an extension of free modules is free. Thus we may assume $M = S$ and that S is a domain of finite type over R.

If $R \to S$ has a nontrivial kernel, then take a nonzero $f \in R$ in this kernel. In this case $S_f = 0$ and the lemma holds. (This is really the case $d = -1$ and the start of the induction.) Hence we may assume that $R \to S$ is a finite type extension of Noetherian domains.

Apply Lemma 29.3 and replace R by R_f (with f as in the lemma) to get a factorization

$$R \subset R[y_1, \ldots, y_d] \subset S$$

where the second extension is finite. Note that $Q(R[y_1, \ldots, y_d]) \subset Q(S)$ is a finite extension of fields. Choose $z_1, \ldots, z_r \in S$ which form a basis for $Q(S)$ over $Q(R[y_1, \ldots, y_d])$. This gives a short exact sequence

$$0 \to R[y_1, \ldots, y_d]^{\oplus r} \xrightarrow{(z_1, \ldots, z_r)} S \to N \to 0$$

By construction N is a finite $R[y_1, \ldots, y_d]$-module whose support does not contain the generic point (0) of $\mathrm{Spec}(R[y_1, \ldots, y_d])$. By Lemma 18.5 there exists a nonzero $g \in R[y_1, \ldots, y_d]$ such that g annihilates N, so we may view N as a finite module over $S' = R[y_1, \ldots, y_d]/(g)$. Since $\dim(S'_K) < d$ by induction there exists a nonzero $f \in R$ such that N_f is a free R_f-module. Since $(R[y_1, \ldots, y_d])_f \cong R_f[y_1, \ldots, y_d]$ is free also we conclude by the already mentioned fact that an extension of free modules is free. $\square$

There are other (stronger) versions of the above result, including versions in which R is merely reduced (rather than a Noetherian domain).

Regularity

30. Depth

In this section we develop some basic properties of regular sequences.

Definition 30.1. Let R be a ring. Let M be an R-module. A sequence of elements $f_1, \ldots, f_r$ of R is called an *M-regular sequence* if the following conditions hold:

(1) f_i is a nonzerodivisor on $M/(f_1, \ldots, f_{i-1})M$ for each $i = 1, \ldots, r$, and
(2) the module $M/(f_1, \ldots, f_r)M$ is not zero.

If I is an ideal of R and $f_1, \ldots, f_r \in I$ then we call $f_1, \ldots, f_r$ a *M-regular sequence in I*. If $M = R$, we call $f_1, \ldots, f_r$ simply a *regular sequence* (in I).

Please pay attention to the fact that the definition depends on the order of the elements $f_1, \ldots, f_r$ (see examples below).

Example 30.2. Let k be a field. In the ring $k[x, y, z]$ the sequence $x, y(1 - x), z(1 - x)$ is regular but the sequence $y(1 - x), z(1 - x), x$ is not.

Example 30.3. Let k be a field. Consider the ring $k[x, y, w_0, w_1, w_2, \ldots]/I$ where I is generated by yw_i, $i = 0, 1, 2, \ldots$ and $w_i - xw_{i+1}$, $i = 0, 1, 2, \ldots$. The sequence x, y is regular, but y is a zerodivisor. Moreover you can localize at the maximal ideal (x, y, w_i) and still get an example.

On the other hand, regular sequences in local Noetherian rings are better-behaved.

Lemma 30.4. *Let R be a local Noetherian ring. Let M be a finite R-module. Let $x_1, \ldots, x_c$ be an M-regular sequence. Then any permutation of the x_i is a regular sequence as well.*

Proof. First we do the case $c = 2$. Let K be the kernel of $x_2 : M \to M$. Consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "x_1"] \arrow[d, "x_2"] & M \arrow[r] \arrow[d, "x_2"] & M/x_1M \arrow[r] \arrow[d, "x_2"] & 0 \\
0 \arrow[r] & M \arrow[r, "x_1"] & M \arrow[r] & M/x_1M \arrow[r] & 0
\end{tikzcd}$$

Since the right-hand vertical map has trivial kernel, the snake lemma implies that $x_1 : K \to K$ is an isomorphism, so that $K = 0$ by Nakayama's Lemma 7.14, and that $x_1 : M/x_2M \to M/x_2M$ is injective. This is exactly what we need to show.

For the general case, observe that any permutation is a composition of transpositions of adjacent indices. Hence it suffices to prove that

$$x_1, \ldots, x_{i-2}, x_i, x_{i-1}, x_{i+1}, \ldots, x_c$$

is an M-regular sequence. This follows from the case we just did applied to the module $M/(x_1, \ldots, x_{i-2})$ and the length 2 regular sequence x_{i-1}, x_i. $\square$

EXERCISE 30.5. If $x_1, \ldots, x_r$ is an M-regular sequence, then so is $x_1^{a_1}, \ldots, x_r^{a_r}$ for any integers $a_i \geq 1$. (Hint: show that $x_1, \ldots, x_{r-1}, x_r^{a_r}$ is an M-regular sequence, and use Lemma 30.4.

LEMMA 30.6. *Let R, S be local rings. Let $R \to S$ be a flat local ring homomorphism. Let $x_1, \ldots, x_r$ be a sequence in R. Let M be an R-module. The following are equivalent*

(1) *$x_1, \ldots, x_r$ is an M-regular sequence in R, and*
(2) *the images of $x_1, \ldots, x_r$ in S form a $M \otimes_R S$-regular sequence.*

PROOF. This is so because $R \to S$ is faithfully flat by Lemma 20.8. $\square$

Here is our definition of depth.

DEFINITION 30.7. Let R be a ring, and $I \subset R$ an ideal. Let M be a finite R-module. The *I-depth* of M, denoted $\text{depth}_I(M)$, is defined as follows:

(1) if $IM \neq M$, then $\text{depth}_I(M)$ is the supremum in $\{0, 1, 2, \ldots, \infty\}$ of the lengths of M-regular sequences in I,
(2) if $IM = M$ we set $\text{depth}_I(M) = \infty$.

If $(R, \mathfrak{m})$ is local we call $\text{depth}_{\mathfrak{m}}(M)$ simply the *depth* of M.

For practical purposes it turns out to be convenient to set the depth of the 0 module equal to $+\infty$ (cf. Lemma 30.9 for example). Note that if $I = R$, then $\text{depth}_I(M) = \infty$ for all finite R-modules M.

LEMMA 30.8. *Let R be a Noetherian local ring. Let M be a nonzero finite R-module. Then* $\dim(\text{Supp}(M)) \geq \text{depth}(M)$. *In particular* $\text{depth}(M)$ *is finite.*

PROOF. We induct on $\dim \text{Supp}(M)$. If $\text{Supp}(M)$ has dimension 0, it must be equal to $\{\mathfrak{m}\}$. By Proposition 19.7 we have $\mathfrak{m} \in \text{Ass}(M)$. Then every $x \in \mathfrak{m}$ is a zerodivisor on M by Lemma 19.13, and $\text{depth}(M) = 0$.

Suppose $\dim \text{Supp}(M) > 0$. If $\text{depth}(M) = 0$ we are done. Otherwise let f be an element of the maximal ideal of R and a nonzerodivisor on M. Then $\dim(\text{Supp}(M)) - 1 = \dim(\text{Supp}(M/fM)) \geq \text{depth}(M/fM)$, by Lemma 26.7 and induction. The supremum of the right-hand side as f varies is $\text{depth}(M) - 1$ and we are done. $\square$

LEMMA 30.9. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finite R-module. Then* $\text{depth}(M)$ *is equal to the smallest integer i such that* $\text{Ext}^i_R(R/\mathfrak{m}, M)$ *is nonzero.*

PROOF. If $M = 0$ then both quantities are $+\infty$. Suppose M is nonzero. Let $\delta(M)$ denote the depth of M and let $i(M)$ denote the smallest integer i such that $\text{Ext}^i_R(R/\mathfrak{m}, M)$ is nonzero. We will see in a moment that $i(M) < \infty$. We have $\delta(M) = 0$ if and only if $i(M) = 0$: $\mathfrak{m} \in \text{Ass}(M)$ by definition means that $i(M) = 0$, while by Lemma 19.13 it is also the same as $\delta(M) = 0$. Hence if $\delta(M)$ or $i(M)$ is positive, then we may choose $x \in \mathfrak{m}$ such that (a) x is a nonzerodivisor on M, and (b) $\text{depth}(M/xM) = \delta(M) - 1$. Consider the long exact sequence of Ext-groups associated to the short exact sequence $0 \to M \to M \to M/xM \to 0$ by Lemma 4.9:

$$\begin{aligned}0 &\to \text{Hom}_R(\kappa, M) \to \text{Hom}_R(\kappa, M) \to \text{Hom}_R(\kappa, M/xM)\\ &\to \text{Ext}^1_R(\kappa, M) \to \text{Ext}^1_R(\kappa, M) \to \text{Ext}^1_R(\kappa, M/xM) \to \ldots\end{aligned}$$

Since $x \in \mathfrak{m}$ all the maps $\text{Ext}^i_R(\kappa, M) \to \text{Ext}^i_R(\kappa, M)$ are zero, see Lemma 4.11. Thus it is clear that $i(M/xM) = i(M) - 1$. Induction on $\delta(M)$ finishes the proof. □

LEMMA 30.10. *Let R be a local Noetherian ring. Let $0 \to N' \to N \to N'' \to 0$ be a short exact sequence of finite R-modules.*

(1) $\text{depth}(N) \geq \min\{\text{depth}(N'), \text{depth}(N'')\}$
(2) $\text{depth}(N'') \geq \min\{\text{depth}(N), \text{depth}(N') - 1\}$
(3) $\text{depth}(N') \geq \min\{\text{depth}(N), \text{depth}(N'') + 1\}$

PROOF. Use the characterization of depth using the Ext groups $\text{Ext}^i(\kappa, N)$, see Lemma 30.9, and use the long exact cohomology sequence

$$\begin{aligned}0 &\to \text{Hom}_R(\kappa, N') \to \text{Hom}_R(\kappa, N) \to \text{Hom}_R(\kappa, N'')\\ &\to \text{Ext}^1_R(\kappa, N') \to \text{Ext}^1_R(\kappa, N) \to \text{Ext}^1_R(\kappa, N'') \to \ldots\end{aligned}$$

from Lemma 4.9. □

LEMMA 30.11. *Let R be a local Noetherian ring and M a nonzero finite R-module.*

(1) *If $x \in \mathfrak{m}$ is a nonzerodivisor on M, then* $\text{depth}(M/xM) = \text{depth}(M) - 1$.
(2) *Any M-regular sequence $x_1, \ldots, x_r$ can be extended to an M-regular sequence of length* $\text{depth}(M)$.

PROOF. Part (2) is a formal consequence of part (1). Let $x \in R$ be as in (1). By the short exact sequence $0 \to M \to M \to M/xM \to 0$ and Lemma 30.10 we see that the depth drops by at most 1. On the other hand, if $x_1, \ldots, x_r \in \mathfrak{m}$ is a regular sequence for M/xM, then $x, x_1, \ldots, x_r$ is a regular sequence for M. Hence we see that the depth drops by at least 1. □

LEMMA 30.12. *Let $(R, \mathfrak{m})$ be a local Noetherian ring and M a finite R-module. Let $x \in \mathfrak{m}$, $\mathfrak{p} \in \text{Ass}(M)$, and $\mathfrak{q}$ minimal over $\mathfrak{p} + (x)$. Then $\mathfrak{q} \in \text{Ass}(M/x^nM)$ for some $n \geq 1$.*

PROOF. Pick a submodule $N \subset M$ with $N \cong R/\mathfrak{p}$. By the Artin-Rees lemma (Lemma 15.9) we can pick $n > 0$ such that $N \cap x^nM \subset xN$. Let $\overline{N} = N/(N \cap x^nM)$, so that $\overline{N} \hookrightarrow M/x^nM$ but also there is a surjection $\overline{N} \to N/xN = R/(\mathfrak{p} + (x))$. The prime $\mathfrak{q}$ is in the support of $\overline{N}$ as $\overline{N}$ surjects onto $R/\mathfrak{p} + (x)$. Since $\overline{N}$ is annihilated by x^n and $\mathfrak{p}$ we see that $\mathfrak{q}$ is minimal among the primes in the support of $\overline{N}$. Thus $\mathfrak{q}$ is an associated prime of M/x^nM, see Lemmas 19.8 and 19.3. □

LEMMA 30.13. *Let $(R, \mathfrak{m})$ be a local Noetherian ring and M a finite R-module. For $\mathfrak{p} \in \text{Ass}(M)$ we have $\dim(R/\mathfrak{p}) \geq \text{depth}(M)$.*

PROOF. If $\mathfrak{m} \in \text{Ass}(M)$ then there is a nonzero element $x \in M$ which is annihilated by all elements of $\mathfrak{m}$. Thus $\text{depth}(M) = 0$. In particular the lemma holds in this case.

If $\operatorname{depth}(M) = 1$, then by the first paragraph we find that $\mathfrak{m} \not\in \operatorname{Ass}(M)$. Hence $\dim(R/\mathfrak{p}) \geq 1$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$ and the lemma is true in this case as well.

We will prove the lemma in general by induction on $\operatorname{depth}(M)$ which we may and do assume to be greater than 1. Pick $x \in \mathfrak{m}$ which is a nonzerodivisor on M. Since x is a nonzerodivisor on M we have $\operatorname{depth}(M/x^n M) = \operatorname{depth}(M) - 1$ by Lemma 30.11. Fix $\mathfrak{p} \in \operatorname{Ass}(M)$. By Lemma 26.6 we have $\dim(R/\mathfrak{p} + (x)) = \dim(R/\mathfrak{p}) - 1$. Thus there exists a prime $\mathfrak{q}$ minimal over $\mathfrak{p} + (x)$ with $\dim(R/\mathfrak{q}) = \dim(R/\mathfrak{p}) - 1$. By Lemma 30.12 there exists $n > 0$ such that $\mathfrak{q} \in \operatorname{Ass}(M/x^n M)$. By induction we find $\dim(R/\mathfrak{q}) \geq \operatorname{depth}(M/x^n M)$ and we win. $\square$

31. Cohen–Macaulay modules

Definition 31.1. Let R be a Noetherian local ring. Let M be a finite R-module. We say M is *Cohen–Macaulay* if $\dim(\operatorname{Supp}(M)) = \operatorname{depth}(M)$.

Definition 31.2. A Noetherian local ring R is called *Cohen–Macaulay* if it is Cohen–Macaulay as a module over itself.

Throughout this section we will repeatedly use the observation that if R is a Noetherian local ring, M is a nonzero finite R-module, and $x \in \mathfrak{m}$ is a nonzerodivisor on M, then we have both $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$ (Lemma 30.11(1)) and $\dim(\operatorname{Supp}(M/xM)) = \dim(\operatorname{Supp}(M)) - 1$ (Lemma 26.7). For example we have the following.

Lemma 31.3. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finite R-module. Let $x \in \mathfrak{m}$ be a nonzerodivisor on M. Then M is Cohen–Macaulay if and only if M/xM is Cohen–Macaulay.*

A first goal will be to establish Proposition 31.7, which says that regular sequences for Cohen–Macaulay modules are characterized by cutting out a quotient of the correct dimension. We do this by a (perhaps nonstandard) sequence of elementary lemmas involving almost none of the earlier results on depth. Let us introduce some notation.

Definition 31.4. Let R be a local Noetherian ring. Let M be a Cohen–Macaulay module, and let $f_1, \ldots, f_d$ be an M-regular sequence with $d = \operatorname{depth}(M)$. We say that $g \in \mathfrak{m}$ is *good with respect to* $(M, f_1, \ldots, f_d)$ if $d > 0$ and for all $i = 0, 1, \ldots, d-1$ we have $\dim \operatorname{Supp}(M/(g, f_1, \ldots, f_i)M) = d - i - 1$.

Lemma 31.5. *Notation and assumptions as above. If g is good with respect to $(M, f_1, \ldots, f_d)$, then $g, f_1, \ldots, f_{d-1}$ is an M-regular sequence. Equivalently:*

1. *g is a nonzerodivisor on M, and*
2. *M/gM is Cohen–Macaulay with maximal regular sequence $f_1, \ldots, f_{d-1}$.*

Proof. We prove the lemma by induction on d. The case $d = 0$ is vacuous. If $d = 1$, then we only have to show that $g : M \to M$ is injective. Its kernel K has support a subset of $\{\mathfrak{m}\}$ because this support is contained in $\operatorname{Supp}(M) \cap V(g) = \operatorname{Supp}(M/gM)$ (Lemma 18.7(1)). Hence K has finite length. But $f_1 : K \to K$ is injective, which implies the length of the image is the length of K, and hence $f_1 K = K$. By Nakayama's Lemma 7.14 this implies $K = 0$.

If $d > 1$, then g is good for $(M/f_1M, f_2, \ldots, f_d)$, as is easily seen from the definition. By induction $g, f_2, \ldots, f_{d-1}$ is an M/f_1M-regular sequence, or equivalently $f_1, g, f_2, \ldots, f_{d-1}$ is an M-regular sequence. We conclude by Lemma 30.4. $\square$

LEMMA 31.6. *Let R be a Noetherian local ring and let M be a Cohen–Macaulay module over R. Suppose $g \in \mathfrak{m}$ is such that* $\dim(\text{Supp}(M/gM)) = \dim(\text{Supp}(M)) - 1$. *Then g is a nonzerodivisor on M.*

PROOF. Choose a M-regular sequence $f_1, \ldots, f_d$ with $d = \dim(\text{Supp}(M))$. If g is is good with respect to $(M, f_1, \ldots, f_d)$ we are done by Lemma 31.5. In particular the lemma holds if $d = 1$. This is the base case for an induction on d. (The case $d = 0$ does not occur.)

Assume $d > 1$. We claim that there exists $h \in R$ such that

(1) h is good with respect to $(M, f_1, \ldots, f_d)$, and
(2) $\dim(\text{Supp}(M/(h, g)M) = d - 2$.

To see this, let $\{\mathfrak{q}_j\}$ be the (finite) set of minimal primes of the closed sets $\text{Supp}(M/(f_1, \ldots, f_i)M)$ for $i = 0, \ldots, d-1$ and $\text{Supp}(M/gM)$. These spaces all have dimension at least 1, so none of the $\mathfrak{q}_j$ is equal to $\mathfrak{m}$. Hence we may find $h \in \mathfrak{m}$, $h \notin \mathfrak{q}_j$ by Lemma 7.2. Then h satisfies (1) and (2) by Lemma 26.7.

At this point we may apply Lemma 31.5 to conclude from (1) that M/hM is Cohen–Macaulay. By (2) we see that the pair $(M/hM, g)$ satisfies the induction hypothesis. Hence $g : M/hM \to M/hM$ is injective and h, g is a regular sequence on M. Therefore so also is g, h, and in particular g is a nonzerodivisor on M. $\square$

PROPOSITION 31.7. *Let R be a Noetherian local ring, with maximal ideal $\mathfrak{m}$. Let M be a Cohen–Macaulay module over R whose support has dimension d. Suppose that $g_1, \ldots, g_c$ are elements of $\mathfrak{m}$ such that* $\dim(\text{Supp}(M/(g_1, \ldots, g_c)M)) = d - c$. *Then $g_1, \ldots, g_c$ is an M-regular sequence, and can be extended to a maximal M-regular sequence.*

PROOF. We have $\dim(\text{Supp}(M/(g_1, \ldots, g_i)M)) = d - i$ for each i, an immediate consequence of Lemma 26.7 which tells us that the dimension drops by at most 1 each time. Thus we may successively apply Lemma 31.6 to the modules $M/(g_1, \ldots, g_i)$ and the element g_{i+1} to see that $g_1, \ldots, g_c$ is an M-regular sequence. Then $\text{depth}(M/(g_1, \ldots, g_c)) = d - c$ by Lemma 30.11, and so $g_1, \ldots, g_c$ can be extended to a maximal M-regular sequence. $\square$

EXERCISE 31.8. Let R be a Cohen–Macaulay local ring and $x_1, \ldots, x_r \in \mathfrak{m}$. Then the following are equivalent.

(1) $x_1, \ldots, x_r$ is part of a system of parameters for R,
(2) $x_1, \ldots, x_r$ is a regular sequence,
(3) $\text{height}(x_1, \ldots, x_i) = i$ for $1 \leq i \leq r$, and
(4) $\text{height}(x_1, \ldots, x_r) = r$.

Having proved Proposition 31.7 we continue the development of standard theory.

LEMMA 31.9. *Let $R \to S$ be a surjective homomorphism of Noetherian local rings. Let N be a finite S-module. Then N is Cohen–Macaulay as an S-module if and only if N is Cohen–Macaulay as an R-module.*

PROOF. The depths of N over R and S are the same, and similarly for the dimension of the support. $\square$

LEMMA 31.10. *Let R be a Noetherian local ring. Let M be a Cohen–Macaulay R-module.*

(1) *The associated primes of M are precisely the minimal primes of* $\text{Supp}(M)$.

(2) *We have* $\dim(R/\mathfrak{p}) = \dim(\mathrm{Supp}(M))$ *for all* $\mathfrak{p} \in \mathrm{Ass}(M)$.

In particular, M has no embedded associated primes.

Proof. We already know from Proposition 19.7 that the minimal primes in $\mathrm{Supp}(M)$ are all in $\mathrm{Ass}(M)$. Suppose $\mathfrak{p} \in \mathrm{Ass}(M)$. By Lemma 30.13 we have $\mathrm{depth}(M) \leq \dim(R/\mathfrak{p})$. Also $\dim(R/\mathfrak{p}) \leq \dim(\mathrm{Supp}(M))$ as $\mathfrak{p} \in \mathrm{Supp}(M)$ (Lemma 19.2). Thus we have equality in both inequalities as M is Cohen–Macaulay, giving (2). Finally, (2) implies that $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$, giving the other direction in (1). □

Recall that the set of zerodivisors on a module M over a Noetherian ring is exactly $\bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \mathfrak{q}$ (Lemma 19.12). If M is Cohen–Macaulay, Lemma 31.10 tells us that the associated primes of M are exactly the minimal primes of $\mathrm{Supp}(M)$. In that case, to produce a nonzerodivisor on M contained in some ideal J, it is necessary and sufficient by Lemma 7.2 to see that J is not contained in any minimal prime of $\mathrm{Supp}(M)$.

Definition 31.11. Let R be a Noetherian local ring. A finite module M over R is called a *maximal Cohen–Macaulay* module if $\mathrm{depth}(M) = \dim(R)$.

In other words, a maximal Cohen–Macaulay module over a Noetherian local ring is a finite module with the largest possible depth over that ring. An example is that if R is a local Cohen–Macaulay ring then $M = R$ is maximal Cohen–Macaulay.

Example 31.12. Let k be a field and take $R = k[[x,y]]/(x^2, xy)$. Then R is not Cohen–Macaulay (it has dimension 1 and depth 0), but $M = R/(x)$ has depth 1 and so is maximal Cohen–Macaulay.

Lemma 31.13. *Let R be a Noetherian local ring. Suppose that there exists a Cohen–Macaulay module M over R such that* $\mathrm{Supp}(M) = \mathrm{Spec}(R)$ *(e.g. suppose R is Cohen–Macaulay). Then:*

(1) *Any maximal chain of prime ideals in R has length* $\dim(R)$.
(2) *For a prime $\mathfrak{p} \subset R$ we have*
$$\dim(R) = \dim(R_{\mathfrak{p}}) + \dim(R/\mathfrak{p}),$$
and for any ideal $I \subset R$ we have
$$\dim(R) = \mathrm{height}(I) + \dim(R/I).$$

Proof. Part (2) is immediate from (1). We will prove (1) by induction on $\dim(R)$, the case $\dim(R) = 0$ being clear. Assume $\dim(R) > 0$. Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a maximal chain of primes, so that $n > 0$. Using prime avoidance (Lemma 7.2) choose any element $x \in \mathfrak{p}_1$ with x not in any of the minimal primes of R, and so that in particular x is not a zerodivisor on M. Then M/xM is Cohen–Macaulay over R/xR with support $\mathrm{Spec}(R/xR)$ (Lemmas 31.3, 31.9, and 18.7(1)). Moreover $\dim(R/xR) = \dim(R) - 1$ by Lemma 26.6.

After replacing x by x^n for some n we may assume that $\mathfrak{p}_1$ is an associated prime of M/xM, by Lemma 30.12. By Lemma 31.10 the prime $\mathfrak{p}_1/xR$ is minimal in R/xR. Thus the chain of prime ideals $\mathfrak{p}_1/xR \subset \cdots \subset \mathfrak{p}_n/xR$ is maximal in R/xR. By induction it has length $\dim(R) - 1$. □

Lemma 31.14. *Suppose R is a Noetherian local ring. Let M be a Cohen–Macaulay module over R.*

(1) *For any prime* $\mathfrak{p} \subset R$ *the module* $M_\mathfrak{p}$ *is Cohen–Macaulay over* $R_\mathfrak{p}$*.*
(2) *If* $M_\mathfrak{p} \neq 0$ *then* $\operatorname{depth}_\mathfrak{p}(M) = \operatorname{depth}_{R_\mathfrak{p}}(M_\mathfrak{p})$*.*

In particular if R *is Cohen–Macaulay then so is* $R_\mathfrak{p}$ *for every prime* $\mathfrak{p} \subset R$*.*

PROOF. The case $M_\mathfrak{p} = 0$ is trivial, so we may assume $M_\mathfrak{p} \neq 0$. Since localization is exact an M-regular sequence in $\mathfrak{p}$ is also an $M_\mathfrak{p}$-regular sequence. We therefore have the inequalities

$$\dim(\operatorname{Supp}(M_\mathfrak{p})) \geq \operatorname{depth}(M_\mathfrak{p}) \geq \operatorname{depth}_\mathfrak{p}(M)$$

and so to prove both parts it suffices to show that $\dim(\operatorname{Supp}(M_\mathfrak{p})) = \operatorname{depth}_\mathfrak{p}(M)$. We do this by induction on $\operatorname{depth}_\mathfrak{p}(M)$.

Suppose that $\operatorname{depth}_\mathfrak{p}(M) = 0$. Then $\mathfrak{p}$ must be contained in some minimal prime of $\operatorname{Supp}(M)$, by the argument preceding Definition 31.11. Since (by assumption) $\mathfrak{p}$ is in the support of M, it must itself be a minimal prime of $\operatorname{Supp}(M)$. Then $\operatorname{Supp}(M_\mathfrak{p}) = \operatorname{Supp}(M) \cap \operatorname{Spec}(R_\mathfrak{p}) = \{\mathfrak{p}R_\mathfrak{p}\}$ has dimension 0.

Now suppose that $\operatorname{depth}_\mathfrak{p}(M) > 0$. Take x an M-regular sequence of length 1 in $\mathfrak{p}$. The module M/xM is Cohen–Macaulay over R by Lemma 31.3, nonzero by construction, and evidently $\operatorname{depth}_\mathfrak{p}(M/xM) < \operatorname{depth}_\mathfrak{p}(M)$. So by induction we get

$$\dim(\operatorname{Supp}(M_\mathfrak{p}/xM_\mathfrak{p})) = \operatorname{depth}_\mathfrak{p}(M/xM).$$

Since x is $M_\mathfrak{p}$-regular the left-hand side is $\dim(\operatorname{Supp}(M_\mathfrak{p})) - 1$. Finally

$$\operatorname{depth}_\mathfrak{p}(M) \geq 1 + \operatorname{depth}_\mathfrak{p}(M/xM) = \dim(\operatorname{Supp}(M_\mathfrak{p}))$$

as desired. □

DEFINITION 31.15. Let R be a Noetherian ring. Let M be a finite R-module. We say M is *Cohen–Macaulay* if $M_\mathfrak{p}$ is a Cohen–Macaulay module over $R_\mathfrak{p}$ for all primes $\mathfrak{p}$ of R. We say that R is Cohen–Macaulay if it is a Cohen–Macaulay module over itself.

By Lemma 31.14 this is consistent with Definition 31.2, and moreover it suffices to check the Cohen–Macaulay condition in the maximal ideals of R.

LEMMA 31.16. *Let* $R \to S$ *be a flat ring map. Let* M *be an* R*-module and* $m \in M$*. Then* $\operatorname{Ann}_R(m)S = \operatorname{Ann}_S(m \otimes 1)$*. If* M *is a finite* R*-module, then* $\operatorname{Ann}_R(M)S = \operatorname{Ann}_S(M \otimes_R S)$*.*

PROOF. Set $I = \operatorname{Ann}_R(m)$. By definition there is an exact sequence $0 \to I \to R \to M$ where the map $R \to M$ sends f to fm. Using flatness we obtain an exact sequence $0 \to I \otimes_R S \to S \to M \otimes_R S$ which proves the first assertion. If $m_1, \ldots, m_n$ is a set of generators of M then $\operatorname{Ann}_R(M) = \bigcap \operatorname{Ann}_R(m_i)$. Similarly $\operatorname{Ann}_S(M \otimes_R S) = \bigcap \operatorname{Ann}_S(m_i \otimes 1)$. Set $I_i = \operatorname{Ann}_R(m_i)$. Then it suffices to show that $\bigcap_{i=1,\ldots,n}(I_i S) = (\bigcap_{i=1,\ldots,n} I_i)S$. This is Lemma 5.6. □

LEMMA 31.17. *Let* R *be a Noetherian ring. Let* M *be a Cohen–Macaulay module over* R*. Then* $M \otimes_R R[x_1, \ldots, x_n]$ *is a Cohen–Macaulay module over* $R[x_1, \ldots, x_n]$*.*

PROOF. By induction on the number of variables it suffices to prove this for $M[x] = M \otimes_R R[x]$ over $R[x]$. Let $\mathfrak{m} \subset R[x]$ be a maximal ideal, and let $\mathfrak{p} = R \cap \mathfrak{m}$. Let $f_1, \ldots, f_d$ be a $M_\mathfrak{p}$-regular sequence in the maximal ideal of $R_\mathfrak{p}$ of length $d = \dim(\operatorname{Supp}(M_\mathfrak{p}))$. Note that since $R[x]$ is flat over R the localization $R[x]_\mathfrak{m}$ is flat over

$R_{\mathfrak{p}}$. Hence, by Lemma 30.6, the sequence $f_1, \ldots, f_d$ is a $M[x]_{\mathfrak{m}}$-regular sequence of length d in $R[x]_{\mathfrak{m}}$. The quotient

$$Q = M[x]_{\mathfrak{m}}/(f_1, \ldots, f_d)M[x]_{\mathfrak{m}} = M_{\mathfrak{p}}/(f_1, \ldots, f_d)M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R[x]_{\mathfrak{m}}$$

has support equal to the primes lying over $\mathfrak{p}$ because $R_{\mathfrak{p}} \to R[x]_{\mathfrak{m}}$ is flat and the support of $M_{\mathfrak{p}}/(f_1, \ldots, f_d)M_{\mathfrak{p}}$ is equal to $\{\mathfrak{p}\}$ (details omitted; hint: follows from Lemmas 31.16 and 18.5). Hence the dimension is 1. To finish the proof it suffices to find an $f \in \mathfrak{m}$ which is a nonzerodivisor on Q. Since $\mathfrak{m}$ is a maximal ideal, we have $\mathfrak{m} \neq \mathfrak{p}[x]$. Hence we can find $f \in \mathfrak{m}$ which viewed as a polynomial in x has leading coefficient not in $\mathfrak{p}$. Such an f acts as a nonzerodivisor on

$$M_{\mathfrak{p}}/(f_1, \ldots, f_d)M_{\mathfrak{p}} \otimes_R R[x] = \bigoplus\nolimits_{n \geq 0} M_{\mathfrak{p}}/(f_1, \ldots, f_d)M_{\mathfrak{p}} \cdot x^n$$

and hence acts as a nonzerodivisor on Q. $\square$

Lemma 31.18. *If R is a Noetherian ring and there exists a Cohen–Macaulay R-module M with* $\mathrm{Supp}(M) = \mathrm{Spec}(R)$ *(for instance, if R is Cohen–Macaulay) then R is universally catenary.*

Proof. Since a polynomial algebra over R satisfies the same hypothesis, by Lemma 31.17, it suffices to show that R is catenary. Let $\mathfrak{p} \subset \mathfrak{q}$ be primes. Consider the localization $R_{\mathfrak{q}}$, noting that $\mathrm{Supp}(M_{\mathfrak{q}}) = \mathrm{Spec}(R_{\mathfrak{q}})$. It is an immediate consequence of Lemmas 31.13 and 31.14 that any maximal chain of prime ideals $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ has length $\dim(R_{\mathfrak{p}})$, and so (using Lemma 31.13 again) any maximal chain of primes between $\mathfrak{p}$ and $\mathfrak{q}$ has length $\dim(R_{\mathfrak{q}}) - \dim(R_{\mathfrak{p}})$. $\square$

Lemma 31.19. *Let R be a Noetherian local Cohen–Macaulay ring of dimension d. Let $0 \to K \to R^{\oplus n} \to M \to 0$ be an exact sequence of R-modules. Then either* $\mathrm{depth}(K) = \mathrm{depth}(M) + 1$ *or* $\mathrm{depth}(K) = \mathrm{depth}(M) = d$.

Proof. Lemma 30.10(3) tells us that $\mathrm{depth}(K) \geq \min\{d, \mathrm{depth}(M) + 1\} \geq \mathrm{depth}(M)$. If $\mathrm{depth}(K) = \mathrm{depth}(M)$ then evidently both must be d. On the other hand $\mathrm{depth}(M) \geq \min\{d, \mathrm{depth}(K) - 1\} \geq \mathrm{depth}(K) - 1$ by (2) of *loc. cit.*, so the only other possibility is that $\mathrm{depth}(K) = \mathrm{depth}(M) + 1$. $\square$

Lemma 31.20. *Let R be a local Noetherian Cohen–Macaulay ring of dimension d. Let M be a finite R module of depth e. There exists an exact complex*

$$0 \to K \to F_{d-e-1} \to \cdots \to F_0 \to M \to 0$$

with each F_i finite free and K maximal Cohen–Macaulay.

Proof. Immediate from the definition and Lemma 31.19. $\square$

Lemma 31.21. *Let $\varphi : A \to B$ be a map of local rings. Assume that B is Noetherian and Cohen–Macaulay and that $\mathfrak{m}_B = \sqrt{\varphi(\mathfrak{m}_A)B}$. Then there exists a sequence of elements $f_1, \ldots, f_{\dim(B)}$ in A such that $\varphi(f_1), \ldots, \varphi(f_{\dim(B)})$ is a regular sequence in B.*

Proof. By induction on $\dim(B)$ it suffices to prove: If $\dim(B) \geq 1$, then we can find an element f of A which maps to a nonzerodivisor in B. By Proposition 31.7 it suffices to find $f \in A$ whose image in B is not contained in any of the finitely many minimal primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of B. By the assumption that $\mathfrak{m}_B = \sqrt{\varphi(\mathfrak{m}_A)B}$ we see that $\mathfrak{m}_A \not\subset \varphi^{-1}(\mathfrak{q}_i)$. Hence we can find f by Lemma 7.2. $\square$

32. Regular local rings

We discuss some basic properties of regular local rings. One important fact is that all prime localizations of a regular local ring are regular, but this is fairly difficult and will not be proved until Section 37. Quite a bit of the material developed so far is geared towards a proof of this fact.

LEMMA 32.1. *Let R be a regular local ring with maximal ideal $\mathfrak{m}$. The graded ring $\bigoplus \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is isomorphic to the graded polynomial algebra $\kappa(\mathfrak{m})[X_1, \ldots, X_d]$.*

PROOF. Let $x_1, \ldots, x_d$ be a minimal set of generators for the maximal ideal $\mathfrak{m}$. By Definition 26.5 this implies that $\dim(R) = d$. Write $\kappa = \kappa(\mathfrak{m})$. There is a surjection $\kappa[X_1, \ldots, X_d] \to \bigoplus \mathfrak{m}^n/\mathfrak{m}^{n+1}$, which maps X_i to the class of x_i in $\mathfrak{m}/\mathfrak{m}^2$. Since $d(R) = d$ by Proposition 26.4 we know that the numerical polynomial $n \mapsto \dim_\kappa \mathfrak{m}^n/\mathfrak{m}^{n+1}$ has degree $d - 1$. By Lemma 24.12 we conclude that the surjection $\kappa[X_1, \ldots, X_d] \to \bigoplus \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an isomorphism. □

LEMMA 32.2. *Any regular local ring is a domain.*

PROOF. We will use that $\bigcap \mathfrak{m}^n = 0$ by Lemma 15.10. Let $f, g \in R$ such that $fg = 0$. Suppose that $f \in \mathfrak{m}^a$ and $g \in \mathfrak{m}^b$, with a, b maximal. Since $fg = 0 \in \mathfrak{m}^{a+b+1}$ we see from the result of Lemma 32.1 that either $f \in \mathfrak{m}^{a+1}$ or $g \in \mathfrak{m}^{b+1}$. Contradiction. □

LEMMA 32.3. *Let R be a regular local ring and let $x_1, \ldots, x_d$ be a minimal set of generators for the maximal ideal $\mathfrak{m}$. Then $x_1, \ldots, x_d$ is a regular sequence, and each $R/(x_1, \ldots, x_c)$ is a regular local ring of dimension $d - c$. In particular R is Cohen–Macaulay.*

PROOF. Note that R/x_1R is a Noetherian local ring of dimension $\geq d - 1$ by Lemma 26.6 with $x_2, \ldots, x_d$ generating the maximal ideal. Hence it is a regular local ring by definition. Since R is a domain by Lemma 32.2 x_1 is a nonzerodivisor. □

LEMMA 32.4. *Let R be a regular local ring. Let $I \subset R$ be an ideal such that R/I is a regular local ring as well. Then there exists a minimal set of generators $x_1, \ldots, x_d$ for the maximal ideal $\mathfrak{m}$ of R such that $I = (x_1, \ldots, x_c)$ for some $0 \leq c \leq d$.*

PROOF. Say $\dim(R) = d$ and $\dim(R/I) = d - c$. Denote $\overline{\mathfrak{m}} = \mathfrak{m}/I$ the maximal ideal of R/I. Let $\kappa = R/\mathfrak{m}$. We have

$$\dim_\kappa((I + \mathfrak{m}^2)/\mathfrak{m}^2) = \dim_\kappa(\mathfrak{m}/\mathfrak{m}^2) - \dim(\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2) = d - (d - c) = c$$

by the definition of a regular local ring. Hence we can choose $x_1, \ldots, x_c \in I$ whose images in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent and supplement with $x_{c+1}, \ldots, x_d$ to get a minimal system of generators of $\mathfrak{m}$. The induced map $R/(x_1, \ldots, x_c) \to R/I$ is a surjection between regular local rings of the same dimension (Lemma 32.3). It follows that the kernel is zero, i.e., $I = (x_1, \ldots, x_c)$. Namely, if not then we would have $\dim(R/I) < \dim(R/(x_1, \ldots, x_c))$ by Lemmas 32.2 and 26.6. □

LEMMA 32.5. *Let R be a Noetherian local ring. Let $x \in \mathfrak{m}$. Let M be a finite R-module such that x is a nonzerodivisor on M and M/xM is free over R/xR. Then M is free over R.*

Proof. Let $m_1, \ldots, m_r$ be elements of M which map to a R/xR-basis of M/xM. By Nakayama's Lemma 7.14 $m_1, \ldots, m_r$ generate M. If $\sum a_i m_i = 0$ is a relation, then $a_i \in xR$ for all i. Hence $a_i = b_i x$ for some $b_i \in R$. Hence the kernel K of $R^r \to M$ satisfies $xK = K$ and hence is zero by Nakayama's lemma. $\square$

Lemma 32.6. *Let R be a regular local ring. Any maximal Cohen–Macaulay module over R is free.*

Proof. A regular local ring of dimension 0 is a field, so the case $\dim(R) = 0$ is easy. Let M be a maximal Cohen–Macaulay module over R. Let $x \in \mathfrak{m}$ be part of a regular sequence generating $\mathfrak{m}$. Then x is a nonzerodivisor on M by Proposition 31.7, and M/xM is a maximal Cohen–Macaulay module over R/xR. By induction on $\dim(R)$ we see that M/xM is free. We win by Lemma 32.5. $\square$

Lemma 32.7. *Suppose R is a Noetherian local ring. Let $x \in \mathfrak{m}$ be a nonzerodivisor such that R/xR is a regular local ring. Then R is a regular local ring. More generally, if $x_1, \ldots, x_r$ is a regular sequence in R such that $R/(x_1, \ldots, x_r)$ is a regular local ring, then R is a regular local ring.*

Proof. This is true because x together with the lifts of a system of minimal generators of the maximal ideal of R/xR will give $\dim(R)$ generators of $\mathfrak{m}$. Use Lemma 26.6. The last statement follows from the first and induction. $\square$

Lemma 32.8. *Let $(R_i, \varphi_{ii'})$ be a directed system of local rings whose transition maps are local ring maps. If each R_i is a regular local ring and $R = \operatorname{colim} R_i$ is Noetherian, then R is a regular local ring.*

Proof. Let $\mathfrak{m} \subset R$ be the maximal ideal; it is the colimit of the maximal ideals $\mathfrak{m}_i \subset R_i$. We prove the lemma by induction on $d = \dim \mathfrak{m}/\mathfrak{m}^2$. If $d = 0$, then $R = R/\mathfrak{m}$ is a field and R is a regular local ring. If $d > 0$ pick an $x \in \mathfrak{m}$, $x \notin \mathfrak{m}^2$. For some i we can find an $x_i \in \mathfrak{m}_i$ mapping to x. Note that $R/xR = \operatorname{colim}_{i' \geq i} R_{i'}/x_i R_{i'}$ is a Noetherian local ring. By Lemma 32.3 we see that $R_{i'}/x_i R_{i'}$ is a regular local ring. Hence by induction we see that R/xR is a regular local ring. Since each R_i is a domain (Lemma 32.1) we see that R is a domain. Hence x is a nonzerodivisor and we conclude that R is a regular local ring by Lemma 32.7. $\square$

33. Krull-Akizuki

One application of Krull-Akizuki is to show that there are plenty of discrete valuation rings. More generally in this section we show how to construct discrete valuation rings dominating Noetherian local rings.

Lemma 33.1. *If $\varphi : R \to R'$ is a ring map that makes R' into a free R-module of rank 1, then φ is an isomorphism.*

Proof. It is obvious that φ must be injective. Write $R' = R \cdot u$. Then $1_{R'} = vu$ for some $v \in R$ and $u^2 = ru$ for some $r \in R$. Multiplying the latter by v gives $u \in R$, and φ is surjective. $\square$

Lemma 33.2 (Kollár). *Let $(R, \mathfrak{m})$ be a local Noetherian ring. Then exactly one of the following holds:*

(1) $(R, \mathfrak{m})$ *is Artinian,*
(2) $(R, \mathfrak{m})$ *is regular of dimension* 1*,*
(3) $\operatorname{depth}(R) \geq 2$*, or*

(4) *there exists a nonzero finite ring map $R \to R'$ which is not an isomorphism, whose kernel and cokernel are annihilated by a power of $\mathfrak{m}$, and such that $\mathfrak{m}$ is not an associated prime of R'.*

Proof. It is easy to see that (1), (2), (3) are mutually exclusive, and that (1) excludes (4). Let us also check that (2) and (3) exclude (4), so that at most one of (1)–(4) hold.

If R contains a nontrivial ideal annihilated by a power of $\mathfrak{m}$, then $\mathfrak{m} \in \mathrm{Ass}(R)$ and $\mathrm{depth}(R) = 0$; so if either (2) or (3) holds, any map as in (4) would have to be injective.

Suppose (2) holds and let $R \hookrightarrow R'$ be a finite map. If $\mathfrak{m} \notin \mathrm{Ass}_R(R')$, then R' is maximal Cohen–Macaulay as an R-module (the depth of R' as an R-module is nonzero because $\mathfrak{m} \notin \mathrm{Ass}_R(R')$, so the depth is 1, and the dimension of the support of R' in $\mathrm{Spec}(R)$ is obviously also 1). Hence it is free by Lemma 32.6. If R'/R is killed by a power of $\mathfrak{m}$ then $\mathrm{rank}_R R' = 1$. But then Lemma 33.1 says that the map $R \to R'$ is an isomorphism, and so there is no map as in (4).

Finally suppose (3) holds and let $R \hookrightarrow R'$ be a map as in (4). In particular the cokernel R'/R has depth 0. The long exact sequence of $\mathrm{Ext}^1(R/\mathfrak{m}, -)$ associated to the short exact sequence $0 \to R \to R' \to R'/R \to 0$, together with Lemma 30.9, shows that $\mathrm{depth}(R') = 0$, or equivalently $\mathfrak{m} \in \mathrm{Ass}_R(R')$, a contradiction.

Now we show that at least one of (1)–(4) holds. Observe that $(R, \mathfrak{m})$ is not Artinian if and only if $V(\mathfrak{m}) \subset \mathrm{Spec}(R)$ is nowhere dense. We assume this from now on.

Let $J \subset R$ be the largest ideal killed by a power of $\mathfrak{m}$. If $J \neq 0$ then $R \to R/J$ shows that $(R, \mathfrak{m})$ is as in (4).

Otherwise $J = 0$. In particular $\mathfrak{m}$ is not an associated prime of R and we see that there is a nonzerodivisor $x \in \mathfrak{m}$ by Lemma 19.13. If $\mathfrak{m}$ is not an associated prime of R/xR then $\mathrm{depth}(R) \geq 2$ by the same lemma. Thus we are left with the case when there is an $y \in R$, $y \notin xR$ such that $y\mathfrak{m} \subset xR$.

If $y\mathfrak{m} \subset x\mathfrak{m}$ then we can consider the map $\varphi : \mathfrak{m} \to \mathfrak{m}$, $f \mapsto yf/x$ (well defined as x is a nonzerodivisor). By the determinantal trick of Lemma 7.10 there exists a monic polynomial P with coefficients in R such that $P(\varphi) = 0$. We conclude that $P(y/x) \in \mathrm{Ann}_{R_x}\mathfrak{m}_x$. Since $\mathfrak{m} \notin \mathrm{Ass}(R)$, we have $\mathfrak{m}_x \notin \mathrm{Ass}(R_x)$, and so $\mathrm{Ann}_{R_x}\mathfrak{m}_x = 0$. Therefore $P(y/x) = 0$. Let $R' \subset R_x$ be the ring generated by R and y/x. Then $R \subset R'$ and R'/R is a finite R-module annihilated by a power of x. Since $\mathfrak{m} \notin \mathrm{Ass}(R_x)$ we see $\mathfrak{m} \notin \mathrm{Ass}(R')$. Thus R is as in (4).

Otherwise there is a $t \in \mathfrak{m}$ such that $yt = ux$ for some unit u of R. After replacing t by $u^{-1}t$ we get $yt = x$. In particular y is a nonzerodivisor. For any $t' \in \mathfrak{m}$ we have $yt' = xs$ for some $s \in R$. Thus $y(t' - st) = xs - xs = 0$. Since y is not a zero-divisor this implies that $t' = ts$ and so $\mathfrak{m} = (t)$. Thus $(R, \mathfrak{m})$ is regular of dimension 1. $\square$

Remark 33.3. If $(R, \mathfrak{m})$ is a local Noetherian domain such that (4) holds in the previous lemma, then R' is a domain with the same fraction field as R. Indeed, since R is a domain we have $R \subset R'$. Since $\mathfrak{m}$ is not an associated prime of R' there exists $x \in \mathfrak{m}$ which is a nonzerodivisor on R'. Then the rest of (4) gives $R_x = R'_x$. Since R_x is a domain and $R' \hookrightarrow R'_x$ we deduce that R' is a domain, and then the statement about the fraction fields is clear.

Lemma 33.4. *Let A be a ring. The following are equivalent.*

(1) *The ring A is a discrete valuation ring.*
(2) *The ring A is a valuation ring and Noetherian.*
(3) *The ring A is a regular local ring of dimension* 1*.*
(4) *The ring A is a Noetherian local domain with maximal ideal $\mathfrak{m}$ generated by a single nonzero element.*
(5) *The ring A is a Noetherian local normal domain of dimension* 1*.*

In this case if π is a generator of the maximal ideal of A, then every element of A can be uniquely written as $u\pi^n$, where $u \in A$ is a unit.

Proof. The equivalence of (1) and (2) is Lemma 22.22. Moreover, in the proof of Lemma 22.22 we saw that if A is a discrete valuation ring, then A is a PID, hence (3). Note that a regular local ring is a domain (see Lemma 32.2). Using this the equivalence of (3) and (4) follows from dimension theory, see Section 26.

Assume (3) and let π be a generator of the maximal ideal $\mathfrak{m}$. For all $n \geq 0$ we have $\dim_{A/\mathfrak{m}} \mathfrak{m}^n/\mathfrak{m}^{n+1} = 1$ because it is generated by π^n (and it cannot be zero). In particular $\mathfrak{m}^n = (\pi^n)$ and the graded ring $\bigoplus \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is isomorphic to the polynomial ring $A/\mathfrak{m}[T]$. For $x \in A \setminus \{0\}$ define $v(x) = \max\{n \mid x \in \mathfrak{m}^n\}$. In other words $x = u\pi^{v(x)}$ with $u \in A^*$. By the remarks above we have $v(xy) = v(x) + v(y)$ for all $x, y \in A \setminus \{0\}$. We extend this to the field of fractions K of A by setting $v(a/b) = v(a) - v(b)$ (well defined by multiplicativity shown above). Then it is clear that A is the set of elements of K which have valuation ≥ 0. Hence we see that A is a valuation ring by Lemma 22.20.

A valuation ring is a normal domain by Lemma 22.17. Hence we see that the equivalent conditions (1) – (3) imply (5). Assume (5). Suppose that $\mathfrak{m}$ cannot be generated by 1 element to get a contradiction. Then alternative (4) holds in Lemma 33.2. Let $A \to A'$ be such a map. By Remark 33.3 we have $Q(A) = Q(A')$. Since $A \to A'$ is finite it is integral (see Lemma 21.3). Since A is normal we get $A = A'$ a contradiction. $\square$

Definition 33.5. Let A be a discrete valuation ring. A *uniformizer* is an element $\pi \in A$ which generates the maximal ideal of A.

By Lemma 33.4 any two uniformizers of a discrete valuation ring are associates.

Lemma 33.6. *Let R be a Noetherian domain of dimension* 1*, with fraction field K. Let M be an R-submodule of $K^{\oplus r}$. For any nonzero $x \in R$ we have* $\text{length}_R(M/xM) < \infty$*.*

Proof. Since R has dimension 1 we see that x is contained in finitely many primes $\mathfrak{m}_i$, $i = 1, \ldots, n$, each maximal. The localization of any subquotient of M/xM at a prime $\mathfrak{p} \notin \{\mathfrak{m}_i\}$ is zero. From this it follows that $\text{length}_R(M/xM) \leq \sum_i \text{length}_{R_{\mathfrak{m}_i}} M_{\mathfrak{m}_i}/xM_{\mathfrak{m}_i}$, and we are therefore reduced to the case where R is local.

Consider $M \subset K^{\oplus r}$ as in the lemma. An easy dévissage reduces us to the case $r = 1$ and $M \neq 0$. If x is a unit then the result is true. Hence we may assume $x \in \mathfrak{m}$ the maximal ideal of R. Since x is not zero and R is a domain we have $\dim(R/xR) = 0$, and hence R/xR has finite length.

Suppose first that M is a finite R-module. In that case we can clear denominators and assume $M \subset R$. Since multiplication by x^i gives an isomorphism $M/xM \cong$

$x^iM/x^{i+1}M$, we see that

$$n \cdot \mathrm{length}_R(M/xM) = \mathrm{length}_R(M/x^nM)$$

and similarly with M replaced by R. The Artin-Rees Lemma (Lemma 15.9) gives $c > 0$ such that $x^nR \cap M = x^{n-c}(x^cR \cap M)$ for $n \gg 0$. Then

$$\begin{aligned} n \cdot \mathrm{length}_R(M/xM) &= \mathrm{length}_R(M/x^nM) \\ &= \mathrm{length}_R(M/(x^nR \cap M)) + \mathrm{length}_R((x^nR \cap M)/x^nM) \\ &\leq \mathrm{length}_R(R/x^nR) + \mathrm{length}_R(x^{n-c}(x^cR \cap M)/x^nM) \\ &= n \cdot \mathrm{length}_R(R/xR) + \mathrm{length}_R((x^cR \cap M)/x^cM. \end{aligned}$$

Dividing through by n and taking the limit as $n \to \infty$ gives $\mathrm{length}_R(M/xM) \leq \mathrm{length}_R(R/xR)$. In fact, the same argument applied to the inclusion $x^eR \subset M$ for some $e \gg 0$ shows that equality holds in this case.

Suppose now that M is not finite. Suppose that the length of M/xM is $\geq k$ for some natural number k. Then we can find

$$0 \subset N_0 \subset N_1 \subset N_2 \subset \ldots N_k \subset M/xM$$

with $N_i \neq N_{i+1}$ for $i = 0, \ldots k-1$. Choose an element $m_i \in M$ whose image in M/xM lies in N_i but not in N_{i-1} for $i = 1, \ldots, k$. Consider the finite R-module $M' \subset M$ generated by the m_i. Let $N_i' \subset M'/xM'$ be the inverse image of N_i under the map $M'/xM' \to M/xM$. It is clear that $N_i' \neq N_{i+1}'$ by our choice of m_i. Hence we see that $\mathrm{length}_R(M'/xM') \geq k$. By the finite case we conclude $k \leq \mathrm{length}_R(R/xR)$ as desired. $\square$

Here is an application.

Lemma 33.7 (Krull-Akizuki). *Let R be a Noetherian domain of dimension 1, with fraction field K. Let $K \subset L$ be a finite extension of fields. In this case any ring A with $R \subset A \subset L$ is Noetherian of dimension at most 1, and $\mathrm{length}_R(A/I) < \infty$ for any nonzero ideal $I \subset A$.*

Proof. To begin we may assume that L is the fraction field of A by replacing L by the fraction field of A if necessary. Let $I \subset A$ be a nonzero ideal. First observe that $I \cap R \neq 0$: if $r \in I$ is nonzero, then r is the root of some polynomial $p(t) \in K[t]$ with nonzero constant term. Clearing denominators we may assume that $p(t) \in R[t]$. Then $p(0)$ is a nonzero element of $I \cap R$.

Pick any nonzero $x \in I \cap R$. Then we get $I/xA \subset A/xA$. By Lemma 33.6 the R-module A/xA has finite length as an R-module. Hence A/I and I/xA have finite length as R-modules. The latter implies that I is finitely generated as an ideal in A. Finally, the observations that A/xA is Artinian for any $x \in R$, and that any $\mathfrak{p} \subset A$ contains an element of R, combined with Krull's Hauptidealsatz (Exercise 26.8 with $r = 1$), shows that the dimension of A is at most 1. $\square$

34. Serre's criterion for normality

We introduce the following properties of Noetherian rings.

Definition 34.1. Let R be a Noetherian ring. Let $k \geq 0$ be an integer.

(1) We say R has property (R_k) if for every prime $\mathfrak{p}$ of height $\leq k$ the local ring $R_{\mathfrak{p}}$ is regular. We also say that R is *regular in codimension* $\leq k$.

(2) We say R has property (S_k) if for every prime $\mathfrak{p}$ the local ring $R_\mathfrak{p}$ has depth at least $\min\{k, \dim(R_\mathfrak{p})\}$.
(3) Let M be a finite R-module. We say M has property (S_k) if for every prime $\mathfrak{p}$ the module $M_\mathfrak{p}$ has depth at least $\min\{k, \dim(\mathrm{Supp}(M_\mathfrak{p}))\}$.

Any Noetherian ring has property (S_0) (and so does any finite module over it). Our convention that $\dim(\emptyset) = -\infty$ guarantees that the zero module has property (S_k) for all k.

Remark 34.2. For a ring R, the property (S_k) is equivalent to: for every prime $\mathfrak{p}$ of height $\leq k$, the local ring $R_\mathfrak{p}$ is Cohen–Macaulay. This follows from Lemma 31.14(2) (note that $R_\mathfrak{p} \neq 0$ for all primes $\mathfrak{p}$).

Lemma 34.3. *Let R be a Noetherian ring. Let M be a finite R-module. The following are equivalent:*

(1) *M has no embedded associated prime, and*
(2) *M has property (S_1).*

Proof. Let $\mathfrak{p}$ be an embedded associated prime of M. Then there exists another associated prime $\mathfrak{q}$ of M such that $\mathfrak{p} \supset \mathfrak{q}$. In particular this implies that $\dim(\mathrm{Supp}(M_\mathfrak{p})) \geq 1$ (since $\mathfrak{q}$ is in the support as well). On the other hand $\mathfrak{p}R_\mathfrak{p}$ is associated to $M_\mathfrak{p}$ (Lemma 19.19) and hence $\mathrm{depth}(M_\mathfrak{p}) = 0$ (see Lemma 19.13). In other words (S_1) does not hold. Conversely, if (S_1) does not hold then there exists a prime $\mathfrak{p}$ such that $\dim(\mathrm{Supp}(M_\mathfrak{p})) \geq 1$ and $\mathrm{depth}(M_\mathfrak{p}) = 0$. Then we see (arguing backwards using the lemmas cited above) that $\mathfrak{p}$ is an embedded associated prime. $\square$

Lemma 34.4. *Let R be a Noetherian ring. The following are equivalent:*

(1) *R is reduced, and*
(2) *R has properties (R_0) and (S_1).*

Proof. Suppose that R is reduced. Then $R_\mathfrak{p}$ is a field for every minimal prime $\mathfrak{p}$ of R, according to Lemma 12.5. Hence we have (R_0). Let $\mathfrak{p}$ be a prime of height ≥ 1. Then $A = R_\mathfrak{p}$ is a reduced local ring of dimension ≥ 1. Hence its maximal ideal $\mathfrak{m}$ is not an associated prime since this would mean there exists a $x \in \mathfrak{m}$ with annihilator $\mathfrak{m}$ so $x^2 = 0$. Hence the depth of $A = R_\mathfrak{p}$ is at least one, by Lemma 19.12. This shows that (S_1) holds.

Conversely, assume that R satisfies (R_0) and (S_1). By Lemma 11.9 it is enough to prove that $R_\mathfrak{p}$ is reduced for all primes $\mathfrak{p} \subset R$. We prove this by induction on the height of $\mathfrak{p}$. If $\mathfrak{p}$ is a minimal prime of R, then $R_\mathfrak{p}$ is a field by (R_0), and hence is reduced. If $\mathfrak{p}$ is not minimal, then we see that $R_\mathfrak{p}$ has depth ≥ 1 by (S_1) and we conclude there exists an element $t \in \mathfrak{p}R_\mathfrak{p}$ such that $R_\mathfrak{p} \to R_\mathfrak{p}[1/t]$ is injective. Since $R_\mathfrak{p}[1/t] \to \prod_\mathfrak{q} R_\mathfrak{q}$ is injective where $\mathfrak{q}$ runs over all primes $t \notin \mathfrak{q} \subset \mathfrak{p}$ (cf. Lemma 11.1(1)), this implies that $R_\mathfrak{p}$ is a subring of localizations of R at primes of smaller height. Thus by induction on the height we conclude that $R_\mathfrak{p}$ is reduced. $\square$

Lemma 34.5 (Serre's criterion for normality). *Let R be a Noetherian ring. The following are equivalent:*

(1) *R is a normal ring, and*
(2) *R has properties (R_1) and (S_2).*

Proof. Proof of (1) $\Rightarrow$ (2). Assume R is normal, i.e., all localizations $R_\mathfrak{p}$ at primes are normal domains. In particular we see that R has (R_0) and (S_1) by Lemma 34.4. Hence it suffices to show that a local Noetherian normal domain R of dimension d has depth $\geq \min(2, d)$ and is regular if $d = 1$. The assertion if $d = 1$ follows from Lemma 33.4.

Let R be a local Noetherian normal domain with maximal ideal $\mathfrak{m}$ and dimension $d \geq 2$. Apply Lemma 33.2 to R. It is clear that R does not fall into cases (1) or (2) of the lemma. Let $R \to R'$ as in (4) of the lemma. Since R is a domain, Remark 33.3 we see that $R \subset R'$ are domains with the same fraction field. But finiteness of $R \subset R'$ implies every element of R' is integral over R (Lemma 21.3) and we conclude that $R = R'$ as R is normal. This means (4) does not happen. Thus we get the remaining possibility (3), i.e., $\text{depth}(R) \geq 2$ as desired.

Proof of (2) $\Rightarrow$ (1). Assume R satisfies (R_1) and (S_2). By Lemma 34.4 we conclude that R is reduced. Hence it suffices to show that if R is a reduced local Noetherian ring of dimension d satisfying (S_2) and (R_1) then R is a normal domain. We induct on d. If $d = 0$, the result is clear. If $d = 1$, then the result follows from Lemma 33.4.

Let R be a reduced local Noetherian ring with maximal ideal $\mathfrak{m}$ and dimension $d \geq 2$ which satisfies (R_1) and (S_2). By Lemma 22.12 it suffices to show that R is integrally closed in its total ring of fractions $Q(R)$. Pick $x \in Q(R)$ which is integral over R. Then $R' = R[x]$ is a finite ring extension of R (Lemma 21.5). Because $\dim(R_\mathfrak{p}) < d$ for every nonmaximal prime $\mathfrak{p} \subset R$ we have $R_\mathfrak{p}$ normal by induction, hence $R_\mathfrak{p} = R'_\mathfrak{p}$. Hence the support of R'/R is $\{\mathfrak{m}\}$. It follows that R'/R is annihilated by a power of $\mathfrak{m}$ (Lemma 18.13). Any $r \in \mathfrak{m}$ that is a nonzerodivisor on R is also a nonzerodivisor on $Q(R)$, hence on R', and therefore $\mathfrak{m} \notin \text{Ass}_R(R')$. By Lemma 33.2 and the assumption that the depth of R is $\geq 2 = \min(2, d)$ we must have $R' = R$ and the proof is complete. □

Lemma 34.6. *A regular ring is normal.*

Proof. Let R be a regular ring. By Lemma 34.5 it suffices to prove that R is (R_1) and (S_2). Property (R_1) is immediate. As a regular local ring is Cohen–Macaulay, see Lemma 32.3, it is also clear that R is (S_2). □

Dimension theory II

35. What makes a complex exact?

Some of this material can be found in the paper [**BE73**] by Buchsbaum and Eisenbud.

SITUATION 35.1. Here R is a ring, and we have a complex

$$0 \to R^{n_e} \xrightarrow{\varphi_e} R^{n_{e-1}} \xrightarrow{\varphi_{e-1}} \cdots \xrightarrow{\varphi_{i+1}} R^{n_i} \xrightarrow{\varphi_i} R^{n_{i-1}} \xrightarrow{\varphi_{i-1}} \cdots \xrightarrow{\varphi_1} R^{n_0}$$

In other words we require $\varphi_i \circ \varphi_{i+1} = 0$ for $i = 1, \ldots, e-1$.

LEMMA 35.2. *In Situation 35.1, suppose that for some i, some matrix coefficient of the map φ_i is invertible. Then the complex $0 \to R^{n_e} \to R^{n_{e-1}} \to \cdots \to R^{n_0}$ is isomorphic to the direct sum of a complex $0 \to R^{n_e} \to \cdots \to R^{n_i - 1} \to R^{n_{i-1} - 1} \to \cdots \to R^{n_0}$ and the complex $0 \to 0 \to \cdots \to R \to R \to 0 \to \cdots \to 0$ where the map $R \to R$ is the identity map.*

PROOF. The assumption means, after a change of basis of R^{n_i} and $R^{n_{i-1}}$ that the first basis vector of R^{n_i} is mapped via φ_i to the first basis vector of $R^{n_{i-1}}$. Let e_j denote the jth basis vector of R^{n_i} and f_k the kth basis vector of $R^{n_{i-1}}$. Write $\varphi_i(e_j) = \sum a_{jk} f_k$. So $a_{1k} = 0$ unless $k = 1$ and $a_{11} = 1$. Change basis on R^{n_i} again by setting $e'_j = e_j - a_{j1} e_1$ for $j > 1$. After this change of coordinates we have $a_{j1} = 0$ for $j > 1$. Note the image of $R^{n_{i+1}} \to R^{n_i}$ is contained in the subspace spanned by e_j, $j > 1$. Note also that $R^{n_{i-1}} \to R^{n_{i-2}}$ has to annihilate f_1 since it is in the image. These conditions and the shape of the matrix (a_{jk}) for φ_i imply the lemma. $\square$

Let us say that an acyclic complex of the form $\cdots \to 0 \to R \to R \to 0 \to \ldots$ is *trivial*. The lemma above says that any finite complex of finite free modules over a local ring is up to direct sums with trivial complexes the same as a complex all of whose maps have all matrix coefficients in the maximal ideal.

LEMMA 35.3. *In Situation 35.1, suppose that $0 \to R^{n_e} \to R^{n_{e-1}} \to \cdots \to R^{n_0}$ is an exact complex, and that R is a local Noetherian ring of depth 0 (e.g. R is an Artinian local ring). Then the complex is isomorphic to a direct sum of trivial complexes.*

PROOF. By hypothesis $\mathfrak{m} \in \mathrm{Ass}(R)$. We induct on the integer $\sum n_i$. Pick $x \in R$, $x \neq 0$, $\mathfrak{m}x = 0$. Pick a basis vector $e_i \in R^{n_e}$. Since xe_i is not mapped to zero by exactness of the complex we deduce that some matrix coefficient of the map $R^{n_e} \to R^{n_{e-1}}$ is not in $\mathfrak{m}$. Lemma 35.2 then allows us to decrease $\sum n_i$. $\square$

Below we define the rank of a map of finite free modules. This is just one possible definition of rank. It is just the definition that works in this section; there are others that may be more convenient in other settings.

DEFINITION 35.4. Let R be a ring. Suppose that $\varphi : R^m \to R^n$ is a map of finite free modules.

(1) The *rank* of φ is the size of the largest nonvanishing minor of the matrix of φ.
(2) We let $I(\varphi) \subset R$ be the ideal generated by the $r \times r$ minors of the matrix of φ, where r is the rank as defined above.

REMARK 35.5. We remark that localization can decrease the rank of a map. But if we localize R at a multiplicative set S such that $I(\varphi) \cdot S^{-1}R \neq 0$ then the rank of φ is unchanged. This always holds for example if $I(\varphi)$ contains a nonzerodivisor (and $0 \notin S$), or if $S^{-1}R = Q(R)$.

LEMMA 35.6. *In Situation 35.1, if the complex is isomorphic to a direct sum of trivial complexes then we have:*

(1) *for all* i, $1 \leq i \leq e$ *we have* $\text{rank}(\varphi_{i+1}) + \text{rank}(\varphi_i) = n_i$, *and*
(2) *each* $I(\varphi_i) = R$.

Conversely, if (1) and (2) hold then the complex is exact.

PROOF. For the first part, we may assume the complex is the direct sum of trivial complexes. Then for each i we can split the standard basis elements of R^{n_i} into those that map to a basis element of $R^{n_{i-1}}$ and those that are mapped to zero (and these are mapped onto by basis elements of $R^{n_{i+1}}$). Using descending induction starting with $i = e$ it is easy to prove that there are r_{i+1}-basis elements of R^{n_i} which are mapped to zero and r_i which are mapped to basis elements of $R^{n_{i-1}}$. From this the result follows. (Note that (2) holds tautologically when $r_i = 0$.)

For the converse, we reduce immediately to the case where R is local. Then the result follows by induction on $\sum_i n_i$ using Lemma 35.2. □

REMARK 35.7. Note that (1) holds in the previous lemma if and only if the maps φ_i have rank $r_i = n_i - n_{i+1} + \cdots + (-1)^{e-i-1}n_{e-1} + (-1)^{e-i}n_e$.

LEMMA 35.8 (Acyclicity lemma). *Let R be a local Noetherian ring. Let* $0 \to M_e \to M_{e-1} \to \cdots \to M_0$ *be a complex of finite R-modules. Assume* $\text{depth}(M_i) \geq i$. *Let i be the largest index such that the complex is not exact at M_i. If $i > 0$ then* $\ker(M_i \to M_{i-1})/\text{im}(M_{i+1} \to M_i)$ *has depth* ≥ 1.

PROOF. Let $H = \ker(M_i \to M_{i-1})/\text{im}(M_{i+1} \to M_i)$ be the homology group in question. We may break the complex into short exact sequences $0 \to M_e \to M_{e-1} \to K_{e-2} \to 0$, $0 \to K_j \to M_j \to K_{j-1} \to 0$, for $i+2 \leq j \leq e-2$, $0 \to K_{i+1} \to M_{i+1} \to B_i \to 0$, $0 \to K_i \to M_i \to M_{i-1}$, and $0 \to B_i \to K_i \to H \to 0$. We proceed up through these complexes to prove the statements about depths, repeatedly using Lemma 30.10. First of all, since $\text{depth}(M_e) \geq e$, and $\text{depth}(M_{e-1}) \geq e-1$ we deduce that $\text{depth}(K_{e-2}) \geq e-1$. At this point the sequences $0 \to K_j \to M_j \to K_{j-1} \to 0$ for $i+2 \leq j \leq e-2$ imply similarly that $\text{depth}(K_{j-1}) \geq j$ for $i+2 \leq j \leq e-2$. The sequence $0 \to K_{i+1} \to M_{i+1} \to B_i \to 0$ then shows that $\text{depth}(B_i) \geq i+1$. The sequence $0 \to K_i \to M_i \to M_{i-1}$ shows that $\text{depth}(K_i) \geq 1$ since M_i has depth $\geq i \geq 1$ by assumption. The sequence $0 \to B_i \to K_i \to H \to 0$ then implies the result. □

PROPOSITION 35.9. *In Situation 35.1, suppose R is a Noetherian ring. The complex is exact if and only if for all i, $1 \leq i \leq e$ the following two conditions are satisfied:*

(1) *we have* $\mathrm{rank}(\varphi_{i+1}) + \mathrm{rank}(\varphi_i) = n_i$, *and*
(2) $I(\varphi_i) = R$, *or* $I(\varphi_i)$ *contains a regular sequence of length* i.

PROOF. First assume the complex is exact. Let $\mathfrak{q} \in \mathrm{Ass}(R)$. (There is at least one such prime.) Note that the local ring $R_\mathfrak{q}$ has depth 0. Lemmas 35.3 and 35.6 together imply that $\mathrm{rank}((\varphi_{i+1})_\mathfrak{q}) + \mathrm{rank}((\varphi_i)_\mathfrak{q}) = n_i$ for all i, and that $I((\varphi_i)_\mathfrak{q}) = R_\mathfrak{q}$. The former implies that $\mathrm{rank}((\varphi_i)_\mathfrak{q}) = r_i$ as in Remark 35.7. Since the map $R \to \prod_{\mathfrak{q}\in\mathrm{Ass}(R)} R_\mathfrak{q}$ is injective, we deduce that $\mathrm{rank}(\varphi_i) = r_i$ as well. We deduce that (1) holds, and also (since the rank does not drop when we localize at $\mathfrak{q}$) that $I(\varphi_i) \cdot R_\mathfrak{q} = I((\varphi_i)_\mathfrak{q}) = R_\mathfrak{q}$. Thus none of the ideals $I(\varphi_i)$ is contained in $\mathfrak{q}$, and Lemma 19.13 implies that each $I(\varphi_i)$ contains a nonzerodivisor.

This already completes the case $e = 1$. If $e > 1$, choose a nonzerodivisor $x_i \in I(\varphi_i)$ and set $x = \prod_i x_i$. Since x is a nonzerodivisor it follows easily from the snake lemma that the complex $0 \to (R/xR)^{n_e} \to \cdots \to (R/xR)^{n_1}$ is still exact. By induction on e all the ideals $I(\varphi_i)/xR$ have a regular sequence of length $i-1$. This proves that $I(\varphi_i)$ contains a regular sequence of length i.

Conversely assume that conditions (1) and (2) are satisfied. Since (2) implies in particular that each $I(\varphi_i)$ contains a nonzerodivisor, the rank of each φ_i is stable under localization. Condition (2) is also preserved by localization. Since exactness is local, we are reduced to the case where R is local.

If any matrix coefficient of φ is not in $\mathfrak{m}$, then we apply Lemma 35.2 to write φ as the sum of $1 : R \to R$ and a map $\varphi' : R^{m-1} \to R^{n-1}$. It is easy to see that the lemma for φ' implies the lemma for φ. Thus we may assume from the outset that all the matrix coefficients of φ are in $\mathfrak{m}$.

We induct on $\dim(R)$, the case of dimension 0 being given by Lemma 35.6. Recall that $I(\varphi_i) \subset \mathfrak{m}$ for all i because of what was said in the first paragraph of the proof. Hence the assumption in particular implies that $\mathrm{depth}(R) \geq e$. By the induction hypothesis the complex is exact when localized at any nonmaximal prime of R. Thus $\ker(\varphi_i)/\mathrm{im}(\varphi_{i+1})$ has support $\{\mathfrak{m}\}$ and hence (if nonzero) depth 0. By Lemma 35.8 we see that the complex is exact. $\square$

36. Global dimension

The following lemma is often used to compare different projective resolutions of a given module.

LEMMA 36.1 (Schanuel's lemma). *Let R be a ring. Let M be an R-module. Suppose that $0 \to K \to P_1 \to M \to 0$ and $0 \to L \to P_2 \to M \to 0$ are two short exact sequences, with P_i projective. Then $K \oplus P_2 \cong L \oplus P_1$.*

PROOF. Consider the module N defined by the short exact sequence $0 \to N \to P_1 \oplus P_2 \to M \to 0$, where the last map is the sum of the two maps $P_i \to M$. It is easy to see that the projection $N \to P_1$ is surjective with kernel L, and that $N \to P_2$ is surjective with kernel K. Since P_i are projective we have $N \cong K \oplus P_2 \cong L \oplus P_1$. $\square$

DEFINITION 36.2. Let R be a ring. Let M be an R-module. We say M has *finite projective dimension* if it has a finite length resolution by projective R-modules. The minimal length of such a resolution is called the *projective dimension* of M.

It is clear that the projective dimension of M is 0 if and only if M is a projective module. The following lemma explains to what extent the projective dimension is independent of the choice of a projective resolution.

Lemma 36.3. *Let R be a ring. Suppose that M is an R-module of projective dimension d. Suppose that $F_e \to F_{e-1} \to \cdots \to F_0 \to M \to 0$ is exact with F_i projective and $e \geq d-1$. Then the kernel of $F_e \to F_{e-1}$ is projective (or the kernel of $F_0 \to M$ is projective in case $e = 0$).*

Proof. We prove this by induction on d. If $d = 0$, then M is projective. In this case there is a splitting $F_0 = \ker(F_0 \to M) \oplus M$, and hence $\ker(F_0 \to M)$ is projective. This finishes the proof if $e = 0$, and if $e > 0$, then replacing M by $\ker(F_0 \to M)$ we decrease e.

Next assume $d > 0$. Let $0 \to P_d \to P_{d-1} \to \cdots \to P_0 \to M \to 0$ be a minimal length finite resolution with P_i projective. According to Schanuel's Lemma 36.1 we have $P_0 \oplus \ker(F_0 \to M) \cong F_0 \oplus \ker(P_0 \to M)$. This proves the case $d = 1$, $e = 0$, because then the right hand side is $F_0 \oplus P_1$ which is projective. Hence now we may assume $e > 0$. The module $F_0 \oplus \ker(P_0 \to M)$ has the finite projective resolution

$$0 \to P_d \to P_{d-1} \to \cdots \to P_2 \to P_1 \oplus F_0 \to \ker(P_0 \to M) \oplus F_0 \to 0$$

of length $d-1$. By induction applied to the exact sequence

$$F_e \to F_{e-1} \to \cdots \to F_2 \to P_0 \oplus F_1 \to P_0 \oplus \ker(F_0 \to M) \to 0$$

of length $e-1$ we conclude $\ker(F_e \to F_{e-1})$ is projective (if $e \geq 2$) or that $\ker(F_1 \oplus P_0 \to F_0 \oplus P_0)$ is projective (if $e = 1$). This implies the lemma. $\square$

Lemma 36.4. *Let R be a Noetherian ring. Suppose that M is a finite R-module of projective dimension d. Then M has a resolution of length d by finite projective R-modules.*

Proof. Choose any resolution $F_{d-1} \to \cdots \to F_0 \to M$ by finite free R-modules and apply Lemma 36.3. $\square$

Lemma 36.5. *Let R be a ring. Let M be an R-module. Let $n \geq 0$. The following are equivalent*

(1) *M has projective dimension $\leq n$,*
(2) *$\mathrm{Ext}^i_R(M, N) = 0$ for all R-modules N and all $i \geq n+1$, and*
(3) *$\mathrm{Ext}^{n+1}_R(M, N) = 0$ for all R-modules N.*

Proof. Assume (1). Choose a free resolution $F_\bullet \to M$ of M. Denote $d_e : F_e \to F_{e-1}$. By Lemma 36.3 we see that $P_e = \ker(d_e)$ is projective for $e \geq n-1$. This implies that $F_e \cong P_e \oplus P_{e-1}$ for $e \geq n$ where d_e maps the summand P_{e-1} isomorphically to P_{e-1} in F_{e-1}. Hence, for any R-module N the complex $\mathrm{Hom}_R(F_\bullet, N)$ is split exact in degrees $\geq n+1$. Whence (2) holds. The implication (2) $\Rightarrow$ (3) is trivial.

Assume (3) holds. We induct on n. If $n = 0$ then M is projective by Lemma 4.12 and we see that (1) holds. If $n > 0$ choose a free R-module F and a surjection $F \to M$ with kernel K. By Lemma 4.10 and the vanishing of $\mathrm{Ext}^i_R(F, N)$ for all $i > 0$ by part (1) we see that $\mathrm{Ext}^n_R(K, N) = 0$ for all R-modules N. Hence by induction we see that K has projective dimension $\leq n-1$. Then M has projective dimension $\leq n$ as any finite projective resolution of K gives a projective resolution of length one more for M by adding F to the front. $\square$

LEMMA 36.6. *Let R be a ring. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules.*

(1) *If M has projective dimension $\leq n$ and M'' has projective dimension $\leq n+1$, then M' has projective dimension $\leq n$.*
(2) *If M' and M'' have projective dimension $\leq n$ then M has projective dimension $\leq n$.*
(3) *If M' has projective dimension $\leq n$ and M has projective dimension $\leq n+1$ then M'' has projective dimension $\leq n+1$.*

PROOF. Combine the characterization of projective dimension in Lemma 36.5 with the long exact sequence of Ext groups in Lemma 4.10. $\square$

DEFINITION 36.7. Let R be a ring. The ring R is said to have *finite global dimension* if there exists an integer n such that every R-module has a resolution by projective R-modules of length at most n. The minimal such n is then called the *global dimension* of R.

LEMMA 36.8. *Let R be a ring. Let M be an R-module. Let $S \subset R$ be a multiplicative subset.*

(1) *If M has projective dimension $\leq n$, then $S^{-1}M$ has projective dimension $\leq n$ over $S^{-1}R$.*
(2) *If R has finite global dimension $\leq n$, then $S^{-1}R$ has finite global dimension $\leq n$.*

PROOF. Let $0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$ be a projective resolution. As localization is exact, see Proposition 6.9, and as each $S^{-1}P_i$ is a projective $S^{-1}R$-module, we see that $0 \to S^{-1}P_n \to \cdots \to S^{-1}P_0 \to S^{-1}M \to 0$ is a projective resolution of $S^{-1}M$. This proves (1). Let M' be an $S^{-1}R$-module. Note that $M' = S^{-1}M'$. Hence we see that (2) follows from (1). $\square$

The argument in the proof of the following lemma can be found in the paper [**Aus55**] by Auslander.

LEMMA 36.9. *Let R be a ring. The following are equivalent*

(1) *R has finite global dimension $\leq n$,*
(2) *every finite R-module has projective dimension $\leq n$, and*
(3) *every cyclic R-module R/I has projective dimension $\leq n$.*

PROOF. It is clear that (1) $\Rightarrow$ (3). Assume (3). Since every finite R-module has a finite filtration by cyclic modules, we see that (2) follows by Lemma 36.6.

Assume (2). Let M be an arbitrary R-module. Choose a set $E \subset M$ of generators of M. Choose a well ordering on E. For $e \in E$ denote M_e the submodule of M generated by the elements $e' \in E$ with $e' \leq e$. Then $M = \bigcup_{e \in E} M_e$. Note that for each $e \in E$ the quotient

$$M_e / \bigcup\nolimits_{e' < e} M_{e'}$$

is either zero or generated by one element, hence has projective dimension $\leq n$. To finish the proof we claim that any time we have a well-ordered set E and a module $M = \bigcup_{e \in E} M_e$ such that the quotients $M_e / \bigcup_{e' < e} M_{e'}$ have projective dimension $\leq n$, then M has projective dimension $\leq n$.

We may prove this statement by induction on n. If $n = 0$, then for each $e \in E$ we may choose a splitting $M_e = \bigcup_{e' < e} M_{e'} \oplus P_e$ because $P_e = M_e / \bigcup_{e' < e} M_{e'}$ is projective. It follows by transfinite induction that $M = \bigoplus_{e \in E} P_e$. We conclude that M is projective because a direct sum of projective modules is projective.

If $n > 0$, then for $e \in E$ we denote F_e the free R-module on the set of elements of M_e. Then we have a system of short exact sequences

$$0 \to K_e \to F_e \to M_e \to 0$$

over the well-ordered set E. Note that the transition maps $F_{e'} \to F_e$ and $K_{e'} \to K_e$ are injective too. Set $F = \bigcup F_e$ and $K = \bigcup K_e$. Then

$$0 \to K_e / \bigcup\nolimits_{e' < e} K_{e'} \to F_e / \bigcup\nolimits_{e' < e} F_{e'} \to M_e / \bigcup\nolimits_{e' < e} M_{e'} \to 0$$

is a short exact sequence of R-modules too and $F_e / \bigcup_{e' < e} F_{e'}$ is the free R-module on the set of elements in M_e which are not contained in $\bigcup_{e' < e} M_{e'}$. Hence by Lemma 36.6 we see that the projective dimension of $K_e / \bigcup_{e' < e} K_{e'}$ is at most $n - 1$. By induction we conclude that K has projective dimension at most $n - 1$. Whence M has projective dimension at most n and we win. $\square$

37. Regular rings and global dimension

We can use the material on rings of finite global dimension to give another characterization of regular local rings.

PROPOSITION 37.1. *Let R be a regular local ring of dimension d. Every finite R-module M of depth e has a finite free resolution*

$$0 \to F_{d-e} \to \cdots \to F_0 \to M \to 0.$$

In particular a regular local ring has global dimension $\leq d$.

PROOF. The first part is clear in view of Lemma 32.6 and Lemma 31.20. The last part then follows from Lemma 36.9. $\square$

LEMMA 37.2. *Let R be a Noetherian ring. Then R has finite global dimension n if and only if for all maximal ideals $\mathfrak{m}$ of R the ring $R_{\mathfrak{m}}$ has finite global dimension $\leq n$, with equality for at least one $\mathfrak{m}$.*

PROOF. We saw, Lemma 36.8 that if R has finite global dimension n, then all the localizations $R_{\mathfrak{m}}$ have finite global dimension at most n. Conversely, suppose that all the $R_{\mathfrak{m}}$ have global dimension $\leq n$. Let M be a finite R-module. Let $0 \to K_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$ be a resolution with F_i finite free. Then K_n is a finite R-module. According to Lemma 36.3 and the assumption all the modules $K_n \otimes_R R_{\mathfrak{m}}$ are projective. Hence by Lemma 11.7 the module K_n is finite projective, and M has projective dimension $\leq n$. The result follows from Lemma 36.9. $\square$

LEMMA 37.3. *Suppose that R is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field κ. In this case the projective dimension of κ is $\geq \dim_\kappa \mathfrak{m}/\mathfrak{m}^2$.*

PROOF. Let $x_1, \ldots x_n$ be elements of $\mathfrak{m}$ whose images in $\mathfrak{m}/\mathfrak{m}^2$ form a basis. Consider the *Koszul complex* on $x_1, \ldots, x_n$. This is the complex

$$0 \to \wedge^n R^n \to \wedge^{n-1} R^n \to \wedge^{n-2} R^n \to \cdots \to \wedge^i R^n \to \cdots \to R^n \to R$$

with maps given by

$$e_{j_1} \wedge \cdots \wedge e_{j_i} \longmapsto \sum_{a=1}^{i} (-1)^{i+1} x_{j_a} e_{j_1} \wedge \cdots \wedge \hat{e}_{j_a} \wedge \cdots \wedge e_{j_i}$$

It is easy to see that this is a complex $K_\bullet(R, x_\bullet)$. Note that the cokernel of the last map of $K_\bullet(R, x_\bullet)$ is clearly κ.

Now, let $F_\bullet \to \kappa$ be any finite resolution by finite free R-modules (this exists by Lemmas 36.4 and 11.7). By Lemma 35.2 we may assume all the maps in the complex $F_\bullet$ have the property that $\text{im}(F_i \to F_{i-1}) \subset \mathfrak{m}F_{i-1}$, because removing a trivial summand from the resolution can at worst shorten the resolution. By Lemma 4.7 we can find a map of complexes $\alpha : K_\bullet(R, x_\bullet) \to F_\bullet$ inducing the identity on κ. We will prove by induction that the maps $\alpha_i : \wedge^i R^n = K_i(R, x_\bullet) \to F_i$ have the property that $\alpha_i \otimes \kappa : \wedge^i \kappa^n \to F_i \otimes \kappa$ are injective. This will prove the lemma since it clearly shows that $F_n \neq 0$.

The result is clear for $i = 0$ because the composition $R \xrightarrow{\alpha_0} F_0 \to \kappa$ is nonzero. Note that F_0 must have rank 1 since otherwise the map $F_1 \to F_0$ whose cokernel is a single copy of κ cannot have image contained in $\mathfrak{m}F_0$.

Next we check the case $i = 1$ as we feel that it is instructive; the reader can skip this as the induction step will deduce the $i = 1$ case from the case $i = 0$. We saw above that $F_0 = R$ and $F_1 \to F_0 = R$ has image $\mathfrak{m}$. We have a commutative diagram

$$\begin{array}{ccccccc} R^n & = & K_1(R, x_\bullet) & \to & K_0(R, x_\bullet) & = & R \\ & & \downarrow & & \downarrow & & \downarrow \\ & & F_1 & \to & F_0 & = & R \end{array}$$

where the rightmost vertical arrow is given by multiplication by a unit. Hence we see that the image of the composition $R^n \to F_1 \to F_0 = R$ is also equal to $\mathfrak{m}$. Thus the map $R^n \otimes \kappa \to F_1 \otimes \kappa$ has to be injective since $\dim_\kappa(\mathfrak{m}/\mathfrak{m}^2) = n$.

Let $i \geq 1$ and assume injectivity of $\alpha_j \otimes \kappa$ has been proved for all $j \leq i-1$. Consider the commutative diagram

$$\begin{array}{ccccccc} \wedge^i R^n & = & K_i(R, x_\bullet) & \to & K_{i-1}(R, x_\bullet) & = & \wedge^{i-1} R^n \\ & & \downarrow & & \downarrow & & \\ & & F_i & \to & F_{i-1} & & \end{array}$$

We know that $\wedge^{i-1}\kappa^n \to F_{i-1} \otimes \kappa$ is injective. This proves that $\wedge^{i-1}\kappa^n \otimes_\kappa \mathfrak{m}/\mathfrak{m}^2 \to F_{i-1} \otimes \mathfrak{m}/\mathfrak{m}^2$ is injective. Also, by our choice of the complex, F_i maps into $\mathfrak{m}F_{i-1}$, and similarly for the Koszul complex. Hence we get a commutative diagram

$$\begin{array}{ccc} \wedge^i \kappa^n & \to & \wedge^{i-1}\kappa^n \otimes \mathfrak{m}/\mathfrak{m}^2 \\ \downarrow & & \downarrow \\ F_i \otimes \kappa & \to & F_{i-1} \otimes \mathfrak{m}/\mathfrak{m}^2 \end{array}$$

At this point it suffices to verify the map $\wedge^i \kappa^n \to \wedge^{i-1}\kappa^n \otimes \mathfrak{m}/\mathfrak{m}^2$ is injective, which can be done by hand. $\square$

Lemma 37.4. *Let R be a Noetherian local ring. Suppose that the residue field κ has finite projective dimension n over R. In this case* $\dim(R) \geq n$.

Proof. Let $F_\bullet$ be a finite resolution of length n of κ by finite free R-modules (this exists by Lemmas 36.4 and 11.7). By Lemma 35.2 we may assume all the maps in the complex $F_\bullet$ have to property that $\mathrm{im}(F_i \to F_{i-1}) \subset \mathfrak{m}F_{i-1}$, because removing a trivial summand from the resolution can at worst shorten the resolution. By Proposition 35.9 we see that $\mathrm{depth}_{I(\varphi_n)}(R) \geq n$ since $I(\varphi_n)$ cannot equal R by our choice of the complex. Thus by Lemma 30.8 also $\dim(R) \geq n$. □

Proposition 37.5. *A Noetherian local ring whose residue field has finite projective dimension is a regular local ring. In particular a Noetherian local ring of finite global dimension is a regular local ring.*

Proof. By Lemmas 37.3 and 37.4 we see that $\dim(R) \geq \dim_\kappa(\mathfrak{m}/\mathfrak{m}^2)$. Thus the result follows immediately from Definition 26.5. □

Lemma 37.6. *A Noetherian local ring R is a regular local ring if and only if it has finite global dimension. In this case the global dimension of R is equal to $\dim(R)$, and $R_\mathfrak{p}$ is a regular local ring for all primes $\mathfrak{p}$.*

Proof. By Propositions 37.5 and 37.1 we see that a Noetherian local ring is a regular local ring if and only if it has finite global dimension. Furthermore, any localization $R_\mathfrak{p}$ has finite global dimension, see Lemma 36.8, and hence is a regular local ring.

The global dimension of R is at most $\dim(R)$ by Proposition 37.1, but on the other hand Lemmas 37.3 and 37.4 together show that κ has projective dimension exactly $\dim(R)$, and so equality holds. □

By Lemma 37.6 it makes sense to make the following definition, because it does not conflict with the earlier definition of a regular local ring.

Definition 37.7. A Noetherian ring R is said to be *regular* if all the localizations $R_\mathfrak{p}$ at primes are regular local rings.

It is enough to require the local rings at maximal ideals to be regular. Note that this is not the same as asking R to have finite global dimension, even assuming R is Noetherianbecause R need not have finite dimension. However, we do have the following.

Lemma 37.8. *Let R be a Noetherian ring. Then R has finite global dimension n if and only if R is regular with finite Krull dimension n.*

Proof. This is a reformulation of Lemma 37.2 in view of Lemma 37.6 and the discussion surrounding Definition 37.7. □

38. Auslander-Buchsbaum

Lemma 38.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finite R-module. If $x \in \mathfrak{m}$ is a nonzerodivisor on both R and M, then $\mathrm{pd}_R(M) = \mathrm{pd}_{R/xR}(M/xR)$.*

Proof. Let

$$0 \to R^{n_e} \to R^{n_{e-1}} \to \cdots \to R^{n_0} \to M \to 0$$

be a minimal finite free resolution, so $e = \mathrm{pd}_R(M)$ (cf. Lemma 36.4). By Lemma 35.2 we may assume all matrix coefficients of the maps in the complex are contained in the maximal ideal of R. Break the long exact sequence into short exact sequences

$$\begin{aligned} 0 \to R^{n_e} \to R^{n_{e-1}} \to K_{e-2} \to 0, \\ 0 \to K_{e-2} \to R^{n_{e-2}} \to K_{e-3} \to 0, \\ \ldots \\ 0 \to K_0 \to R^{n_0} \to M \to 0. \end{aligned}$$

Since $K_i \subset R^{n_i}$ we see that x is a nonzerodivisor on K_i for all i. Therefore $\mathrm{Tor}^1_R(R/x, K_i) = \ker(K_i \xrightarrow{x} K_i) = 0$ for all i, and similarly $\mathrm{Tor}^1_R(R/x, M) = 0$. It follows that each of the above short exact sequences remains exact after tensoring over R with R/xR. This implies that

$$0 \to (R/xR)^{n_e} \to (R/xR)^{n_{e-1}} \to \cdots \to (R/xR)^{n_0} \to M/xM \to 0$$

also remains exact. This gives $\mathrm{pd}_{R/xR}(M/xM) \leq \mathrm{pd}_R(M)$.

Conversely, let

$$F^\bullet : 0 \to (R/xR)^{n_e} \to (R/xR)^{n_{e-1}} \to \cdots \to (R/xR)^{n_0} \to M/xM \to 0$$

be a minimal finite free resolution, so now $e = \mathrm{pd}_{R/xR}(M/xM)$. Lift the resolution $F^\bullet$ to a complex (not *a priori* exact) of R-modules

$$G^\bullet : 0 \to R^{n_e} \to R^{n_{e-1}} \to \cdots \to R^{n_0} \to M \to 0$$

in any way (such a lift exists because the R^{n_i} are free and the maps $R^{n_i} \to (R/xR)^{n_i}$ are surjective). Let H^i be the ith homology of the complex $G^\bullet$. Since $F^\bullet$ is exact, the long exact sequence of homology associated to the short exact sequence of complexes

$$0 \to G^\bullet \xrightarrow{x} G^\bullet \to F^\bullet \to 0$$

shows that the map $H^i \xrightarrow{x} H^i$ is an isomorphism. By Nakayama's lemma 7.14 we conclude that $H^i = 0$ for all i and $G^\bullet$ is exact. Thus $G^\bullet$ is a projective resolution of M and we get the reverse inequality $\mathrm{pd}_R(M) \leq \mathrm{pd}_{R/xR}(M/xM)$. □

The following result can be found in [**AB57**].

Proposition 38.2. *Let R be a Noetherian local ring. Let M be a nonzero finite R-module which has finite projective dimension $\mathrm{pd}_R(M)$. Then we have*

$$\mathrm{depth}(R) = \mathrm{pd}_R(M) + \mathrm{depth}(M)$$

Proof. The case $\mathrm{pd}_R(M) = 0$ is trivial, for then M is free and $\mathrm{depth}(R) = \mathrm{depth}(M)$, so we assume throughout the remainder of the proof that $\mathrm{pd}_R(M) > 0$. Let

$$0 \to R^{n_e} \to R^{n_{e-1}} \to \cdots \to R^{n_0} \to M \to 0$$

be a minimal finite free resolution, so $e = \mathrm{pd}_R(M)$. By Lemma 35.2 we may assume all matrix coefficients of the maps in the complex are contained in the maximal ideal of R. By Proposition 35.9 we see that $\mathrm{depth}(R) \geq e$ (so in particular $\mathrm{depth}(R) > 0$).

We proceed by induction on $\mathrm{depth}(M)$. Suppose that $\mathrm{depth}(M) = 0$. In this case, breaking the long exact sequence into short exact sequences as in the proof of

Lemma 38.1 we see, using Lemma 30.10, that

$$\begin{aligned}
\text{depth}(K_{e-2}) &\geq \text{depth}(R) - 1, \\
\text{depth}(K_{e-3}) &\geq \text{depth}(R) - 2, \\
&\ldots, \\
\text{depth}(K_0) &\geq \text{depth}(R) - (e-1), \\
\text{depth}(M) &\geq \text{depth}(R) - e
\end{aligned}$$

and since $\text{depth}(M) = 0$ we conclude $\text{depth}(R) \leq e$. This finishes the proof of the case $\text{depth}(M) = 0$.

Induction step. Since by hypothesis $\text{depth}(M) > 0$ and $\text{depth}(R) > 0$, we have $\text{depth}(R \oplus M) > 0$ by Lemma 30.10 (for example) and we can find an $x \in \mathfrak{m}$ which is a nonzerodivisor on both R and M. Lemma 38.1 gives $\text{pd}_R(M) = \text{pd}_{R/xR}(M/xM)$. By Lemma 30.11 we have $\text{depth}(R/xR) = \text{depth}(R) - 1$ and $\text{depth}(M/xM) = \text{depth}(M) - 1$. Till now depths have all been depths as R modules, but we observe that $\text{depth}_R(M/xM) = \text{depth}_{R/xR}(M/xM)$ and similarly for R/xR. By induction hypothesis we see that the Auslander-Buchsbaum formula holds for M/xM over R/xR. Since the depths of both R/xR and M/xM have decreased by one and the projective dimension has not changed we conclude. □

39. Finite type algebras over fields

In this section we apply all the theory that we have developed so far in the case of finite type algebras over fields. Throughout this section let k be a field.

Lemma 39.1. *The polynomial ring $k[x_1, \ldots, x_n]$ has the following properties:*

(1) *The ring $k[x_1, \ldots, x_n]$ is universally catenary, Jacobson, regular, Cohen–Macaulay, and normal.*
(2) *Any maximal ideal $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ is generated by n elements.*
(3) *The dimension and global dimension of $k[x_1, \ldots, x_n]$ are both n.*

Proof. That $k[x_1, \ldots, x_n]$ is Jacobson follows directly from Theorem 14.8. Since k is Cohen–Macaulay, it follows from Lemma 31.17 that $k[x_1, \ldots, x_n]$ is Cohen–Macaulay and from Lemma 31.18 that it is universally catenary.

Every maximal ideal of $k[x_1, \ldots, x_n]$ has height n by Lemma 28.10, using Theorem 14.9 to see that the final term of the dimension formula vanishes. This shows that the dimension of $k[x_1, \ldots, x_n]$ is n. Once we have proved (2), it will follow that the localizations of $k[x_1, \ldots, x_n]$ at maximal ideals are regular, and hence $k[x_1, \ldots, x_n]$ is regular. Then the global dimension is computed by Lemma 37.8, and the ring is normal by Lemma 34.6.

It remains to prove (2). We proceed by induction on n, the case $n = 0$ being trivial and the case $n = 1$ being the standard fact that $k[x]$ is a PID. Write $R = k[x_1, \ldots, x_{n-1}]$. Let $\mathfrak{m} \subset R[x_n]$ be a maximal ideal. Since R is Jacobson, Lemma 14.7 tells us that $\mathfrak{q} := \mathfrak{m} \cap R$ is a maximal ideal of R. Since $R/\mathfrak{q}$, the case $n = 1$ tells us that $\mathfrak{m}/\mathfrak{q} \subset (R/\mathfrak{q})[x_n]$ is principal, generated by the image of some element $g \in R[x_n]$. Then $\mathfrak{m} = (\mathfrak{q}, g)$. Since $\mathfrak{q}$ is generated by $n - 1$ elements by induction, we conclude that n is generated by n elements. □

Definition 39.2. We say that the domain R is *equicodimensional* of dimension n if $\dim(R_\mathfrak{m}) = n$ for all maximal ideals $\mathfrak{m} \subset R$.

LEMMA 39.3. *Let S be a finite type k-algebra. Then:*

1. *S is universally catenary and Jacobson.*
2. *If S is an integral domain, let $K = Q(S)$ be the field of fractions of S. Then S is equicodimensional of dimension* $\text{trdeg}(K/k)$.

PROOF. The first part is an immediate corollary of Lemma 39.1, and the second is an immediate corollary of the dimension formula (Lemma 28.10) applied to $k \subset S$, using the Nullstellensatz (Theorem 14.9) to see that the final term of the dimension formula vanishes. ☐

DEFINITION 39.4. Let $x \in X$. The *Krull dimension of X at x* is defined as

$$\dim_x(X) = \min\{\dim(U), x \in U \subset X \text{ open}\}$$

the minimum of $\dim(U)$ where U runs over the open neighbourhoods of x in X.

LEMMA 39.5. *Suppose that the ring S is Noetherian and Jacobson, and that $S/\mathfrak{q}$ is equicodimensional for every minimal prime $\mathfrak{q} \subset S$ (for instance, S may be any finite type algebra over a field, by Lemma 39.3).*

Let $X = \text{Spec}(S)$. Let $\mathfrak{p} \subset S$ be a prime ideal and let $x \in X$ be the corresponding point. The following numbers are equal

1. $\dim_x(X)$,
2. $\max \dim(Z)$ *where the maximum is over those irreducible components Z of X passing through x, and*
3. $\min \dim(S_{\mathfrak{m}})$ *where the minimum is over maximal ideals $\mathfrak{m}$ with $\mathfrak{p} \subset \mathfrak{m}$.*

PROOF. Let $X = \bigcup_{i \in I} Z_i$ be the decomposition of X into its irreducible components, and let $\mathfrak{q}_i$ denote the minimal primes of S corresponding to the irreducible components Z_i. There are finitely many of them (see Lemmas 15.3 and 15.7). Let $I' = \{i \mid x \in Z_i\}$, and let $T = \bigcup_{i \notin I'} Z_i$. Then $U = X \setminus T$ is an open subset of X containing the point x. The number (2) is $\max_{i \in I'} \dim(Z_i)$. For any open $W \subset U$ with $x \in W$ the irreducible components of W are the irreducible sets $W_i = Z_i \cap W$ for $i \in I'$ and x is contained in each of these. Note that each W_i, $i \in I'$ contains a closed point because X is Jacobson, see Section 14. Since $W_i \subset Z_i$ we have $\dim(W_i) \leq \dim(Z_i)$. The existence of a closed point and the equicodimensionality of $S/\mathfrak{q}_i$ imply that there is a chain of irreducible closed subsets of length equal to $\dim(Z_i)$ in the open W_i. Thus $\dim(W_i) = \dim(Z_i)$ for any $i \in I'$. Hence $\dim(W)$ is equal to the number (2). This proves that (1) = (2).

Let $\mathfrak{m} \supset \mathfrak{p}$ be any maximal ideal containing $\mathfrak{p}$. Let $x_0 \in X$ be the corresponding point. First of all, x_0 is contained in all the irreducible components Z_i, $i \in I'$. For each i such that $x_0 \in Z_i$ (which is equivalent to $\mathfrak{m} \supset \mathfrak{q}_i$) we have a surjection

$$S_{\mathfrak{m}} \longrightarrow S_{\mathfrak{m}}/\mathfrak{q}_i S_{\mathfrak{m}} = (S/\mathfrak{q}_i)_{\mathfrak{m}}$$

Since the minimal primes of $S_{\mathfrak{m}}$ are in one-to-one correspondence with the irreducible components of $\text{Spec}(S)$ passing through $\mathfrak{m}$, the primes $\mathfrak{q}_i S_{\mathfrak{m}}$ so obtained exhaust the minimal primes of the Noetherian local ring $S_{\mathfrak{m}}$. We conclude, using equicodimensionality, that the dimension of $S_{\mathfrak{m}}$ is the maximum of the dimensions of the Z_i passing through x_0. To finish the proof of the lemma it suffices to show that we can choose x_0 such that $x_0 \in Z_i \Rightarrow i \in I'$. Because S is Jacobson (as we saw above) it is enough to show that $V(\mathfrak{p}) \setminus T$ (with T as above) is nonempty. And this is clear since it contains the point x (i.e. $\mathfrak{p}$). ☐

Lemma 39.6. *Let k be a field. Let S be a finite type k-algebra. Let $X = \mathrm{Spec}(S)$. Let $\mathfrak{m} \subset S$ be a maximal ideal and let $x \in X$ be the associated closed point. Then $\dim_x(X) = \dim(S_{\mathfrak{m}})$.*

Proof. This is a special case of Lemma 39.5. □

Lemma 39.7. *Let k be a field. Let S be a finite type k algebra. Let $X = \mathrm{Spec}(S)$. Let $\mathfrak{p} \subset S$ be a prime ideal, and let $x \in X$ be the corresponding point. Then we have*

$$\dim_x(X) = \dim(S_{\mathfrak{p}}) + \mathrm{trdeg}_k\ \kappa(\mathfrak{p}).$$

Proof. By Lemma 39.3(2) we know that $r = \mathrm{trdeg}_k\ \kappa(\mathfrak{p})$ is equal to the dimension of $V(\mathfrak{p})$. Therefore the right-hand side of the formula in the lemma is equal to the maximum of the lengths of the chains of prime ideals in S that include $\mathfrak{p}$. This is equal to $\dim_x(X)$ by the characterization of Lemma 39.5(2) together with the fact that $S/\mathfrak{q}$ is catenary and equicodimensional for any minimal prime $\mathfrak{q} \subset \mathfrak{q}$ (or indeed for any prime at all). □

Lemma 39.8. *Let k be a field. Let S be a finite type k algebra. Assume that S is Cohen–Macaulay. Then $\mathrm{Spec}(S) = \coprod T_d$ is a finite disjoint union of open and closed subsets T_d with T_d equidimensional of dimension d (i.e. all irreducible components have dimension d). Equivalently, S is a product of rings S_d, $d = 0, \ldots, \dim(S)$ such that every maximal ideal $\mathfrak{m}$ of S_d has height d.*

Proof. The equivalence of the two statements follows from Lemma 10.3. Since $\mathrm{Spec}(S)$ has a finite number of irreducible components (see Lemmas 15.3 and 15.7), we must show that any two irreducible components that meet have the same dimension. Suppose that Z, Z' are irreducible components that meet. Since $\mathrm{Spec}(S)$ is a Jacobson topological space the intersection of any two irreducible components contains a closed point if nonempty, see Lemma 14.5. Let $\mathfrak{m} \subset S$ be a maximal ideal corresponding to a closed point in $Z \cap Z'$. Since S is Cohen–Macaulay, every maximal chain of primes in $S_{\mathfrak{m}}$ has the same length equal to $\dim(S_{\mathfrak{m}})$, see Lemma 31.13. Hence, the dimension of the irreducible components passing through the point corresponding to $\mathfrak{m}$ all have dimension equal to $\dim(S_{\mathfrak{m}})$, by the equicodimensionality from Lemma 39.3. □

GNU Free Documentation License

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The **"Document"**, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as **"you"**. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A **"Modified Version"** of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A **"Secondary Section"** is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The **"Invariant Sections"** are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The **"Cover Texts"** are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A **"Transparent"** copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called **"Opaque"**.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The **"Title Page"** means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section **"Entitled XYZ"** means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as **"Acknowledgements"**, **"Dedications"**, **"Endorsements"**, or **"History"**.) To **"Preserve the Title"** of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright ©YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

History

This section was last updated in September 2016.

The Stacks Project, `http://stacks.math.columbia.edu`, is an open source textbook on algebraic stacks and the algebraic geometry that is needed to define them. The project was begun in 2005 and remains active as of 2016. The principal author is Johan de Jong.

This document is a Modified Version of the Stacks Project, created by David Savitt in 2016 by copying, rearranging, and modifying portions of the Stacks Project (largely from the chapter entitled "Commutative Algebra").

Bibliography

[AB57] Maurice Auslander and David A. Buchsbaum, *Homological dimension in local rings*, Trans. Amer. Math. Soc. **85** (1957), 390–405.

[Aus55] Maurice Auslander, *On the dimension of modules and algebras. III. Global dimension*, Nagoya Math. J. **9** (1955), 67–77.

[BE73] David Alvin Buchsbaum and David Eisenbud, *What makes a complex exact?*, J. Algebra **25** (1973), 259–268.

[DG67] Jean Dieudonné and Alexander Grothendieck, *Éléments de géométrie algébrique*, Inst. Hautes Études Sci. Publ. Math. **4, 8, 11, 17, 20, 24, 28, 32** (1961–1967).

[Mat70] Hideyuki Matsumura, *Commutative algebra*, W. A. Benjamin, Inc., 1970.