CHAPTER X

Noetherian Rings and Modules

This chapter may serve as an introduction to the methods of algebraic geometry rooted in commutative algebra and the theory of modules, mostly over a Noetherian ring.

§1. BASIC CRITERIA

Let A be a ring and M a module (i.e., a left A-module). We shall say that M is **Noetherian** if it satisfies any one of the following three conditions:

(1) Every submodule of M is finitely generated.

(2) Every ascending sequence of submodules of M,

$$M_1 \subset M_2 \subset M_3 \subset \cdots,$$

such that $M_i \neq M_{i+1}$ is finite.

(3) Every non-empty set S of submodules of M has a maximal element (i.e., a submodule M_0 such that for any element N of S which contains M_0 we have $N = M_0$).

We shall now prove that the above three conditions are equivalent.

(1) $\Rightarrow$ (2) Suppose we have an ascending sequence of submodules of M as above. Let N be the union of all the M_i ($i = 1, 2, \ldots$). Then N is finitely generated, say by elements $x_1, \ldots, x_r$, and each generator is in some M_i. Hence there exists an index j such that

$$x_1, \ldots, x_r \in M_j.$$

Then

$$\langle x_1, \ldots, x_r \rangle \subset M_j \subset N = \langle x_1, \ldots, x_r \rangle,$$

whence equality holds and our implication is proved.

(2) $\Rightarrow$ (3) Let N_0 be an element of S. If N_0 is not maximal, it is properly contained in a submodule N_1. If N_1 is not maximal, it is properly contained in a submodule N_2. Inductively, if we have found N_i which is not maximal, it is contained properly in a submodule N_{i+1}. In this way we could construct an infinite chain, which is impossible.

(3) $\Rightarrow$ (1) Let N be a submodule of M. Let $a_0 \in N$. If $N \neq \langle a_0 \rangle$, then there exists an element $a_1 \in N$ which does not lie in $\langle a_0 \rangle$. Proceeding inductively, we can find an ascending sequence of submodules of N, namely

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \cdots$$

where the inclusion each time is proper. The set of these submodules has a maximal element, say a submodule $\langle a_0, a_1, \ldots, a_r \rangle$, and it is then clear that this finitely generated submodule must be equal to N, as was to be shown.

Proposition 1.1. *Let M be a Noetherian A-module. Then every submodule and every factor module of M is Noetherian.*

Proof. Our assertion is clear for submodules (say from the first condition). For the factor module, let N be a submodule and $f: M \to M/N$ the canonical homomorphism. Let $\overline{M}_1 \subset \overline{M}_2 \subset \cdots$ be an ascending chain of submodules of M/N and let $M_i = f^{-1}(\overline{M}_i)$. Then $M_1 \subset M_2 \subset \cdots$ is an ascending chain of submodules of M, which must have a maximal element, say M_r, so that $M_i = M_r$ for $r \geqq i$. Then $f(M_i) = \overline{M}_i$ and our assertion follows.

Proposition 1.2. *Let M be a module, N a submodule. Assume that N and M/N are Noetherian. Then M is Noetherian.*

Proof. With every submodule L of M we associate the pair of modules

$$L \mapsto (L \cap N, (L + N)/N).$$

We contend: If $E \subset F$ are two submodules of M such that their associated pairs are equal, then $E = F$. To see this, let $x \in F$. By the hypothesis that $(E + N)/N = (F + N)/N$ there exist elements $u, v \in N$ and $y \in E$ such that $y + u = x + v$. Then

$$x - y = u - v \in F \cap N = E \cap N.$$

Since $y \in E$, it follows the $x \in E$ and our contention is proved. If we have an ascending sequence

$$E_1 \subset E_2 \subset \cdots$$

then the associated pairs form an ascending sequence of submodules of N and M/N respectively, and these sequences must stop. Hence our sequence $E_1 \subset E_2 \cdots$ also stops, by our preceding contention.

Propositions 1.1 and 1.2 may be summarized by saying that in an exact sequence $0 \to M' \to M \to M'' \to 0$, M is Noetherian if and only if M' and M'' are Noetherian.

Corollary 1.3. *Let M be a module, and let N, N' be submodules. If $M = N + N'$ and if both N, N' are Noetherian, then M is Noetherian. A finite direct sum of Noetherian modules is Noetherian.*

Proof. We first observe that the direct product $N \times N'$ is Noetherian since it contains N as a submodule whose factor module is isomorphic to N', and Proposition 1.2 applies. We have a surjective homomorphism

$$N \times N' \to M$$

such that the pair (x, x') with $x \in N$ and $x' \in N'$ maps on $x + x'$. By Proposition 1.1, it follows that M is Noetherian. Finite products (or sums) follow by induction.

A ring A is called **Noetherian** if it is Noetherian as a left module over itself. This means that every left ideal is finitely generated.

Proposition 1.4. *Let A be a Noetherian ring and let M be a finitely generated module. Then M is Noetherian.*

Proof. Let $x_1, \ldots, x_n$ be generators of M. There exists a homomorphism

$$f: A \times A \times \cdots \times A \to M$$

of the product of A with itself n times such that

$$f(a_1, \ldots, a_n) = a_1 x_1 + \cdots + a_n x_n.$$

This homomorphism is surjective. By the corollary of the preceding proposition, the product is Noetherian, and hence M is Noetherian by Proposition 1.1.

Proposition 1.5. *Let A be a ring which is Noetherian, and let $\varphi: A \to B$ be a surjective ring-homomorphism. Then B is Noetherian.*

Proof. Let $\mathfrak{b}_1 \subset \cdots \subset \mathfrak{b}_n \subset \cdots$ be an ascending chain of left ideals of B and let $\mathfrak{a}_i = \varphi^{-1}(\mathfrak{b}_i)$. Then the $\mathfrak{a}_i$ form an ascending chain of left ideals of A which must stop, say at $\mathfrak{a}_r$. Since $\varphi(\mathfrak{a}_i) = \mathfrak{b}_i$ for all i, our proposition is proved.

Proposition 1.6. *Let A be a commutative Noetherian ring, and let S be a multiplicative subset of A. Then $S^{-1}A$ is Noetherian.*

Proof. We leave the proof as an exercise.

Examples. In Chapter IV, we gave the fundamental examples of Noetherian rings, namely polynomial rings and rings of power series. The above propositions show how to construct other examples from these, by taking factor rings or modules, or submodules.

We have already mentioned that for applications to algebraic geometry, it is valuable to consider factor rings of type $k[X]/\mathfrak{a}$, where $\mathfrak{a}$ is an arbitrary ideal. For this and similar reasons, it has been found that the foundations should be laid in terms of modules, not just ideals or factor rings. Notably, we shall first see that the prime ideal associated with an irreducible algebraic set has an analogue in terms of modules. We shall also see that the decomposition of an algebraic set into irreducibles has a natural formulation in terms of modules, namely by expressing a submodule as an intersection or primary modules.

In §6 we shall apply some general notions to get the Hilbert polynomial of a module of finite length, and we shall make comments on how this can be interpreted in terms of geometric notions. Thus the present chapter is partly intended to provide a bridge between basic algebra and algebraic geometry.

§2. ASSOCIATED PRIMES

Throughout this section, we let A be a commutative ring. Modules and homomorphisms are A-modules and A-homomorphisms unless otherwise specified.

Proposition 2.1. *Let S be a multiplicative subset of A, and assume that S does not contain 0. Then there exists an ideal of A which is maximal in the set of ideals not intersecting S, and any such ideal is prime.*

Proof. The existence of such an ideal $\mathfrak{p}$ follows from Zorn's lemma (the set of ideals not meeting S is not empty, because it contains the zero ideal, and is clearly inductively ordered). Let $\mathfrak{p}$ be maximal in the set. Let $a, b \in A$, $ab \in \mathfrak{p}$, but $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. By hypothesis, the ideals $(a, \mathfrak{p})$ and $(b, \mathfrak{p})$ generated by a and $\mathfrak{p}$ (or b and $\mathfrak{p}$ respectively) meet S, and there exist therefore elements $s, s' \in S$, $c, c', x, x' \in A$, $p, p' \in \mathfrak{p}$ such that

$$s = ca + xp \quad \text{and} \quad s' = c'b + x'p'.$$

Multiplying these two expressions, we obtain

$$ss' = cc'ab + p''$$

with some $p'' \in \mathfrak{p}$, whence we see that ss' lies in $\mathfrak{p}$. This contradicts the fact that $\mathfrak{p}$ does not intersect S, and proves that $\mathfrak{p}$ is prime.

An element a of A is said to be **nilpotent** if there exists an integer $n \geqq 1$ such that $a^n = 0$.

Corollary 2.2. *An element a of A is nilpotent if and only if it lies in every prime ideal of A.*

Proof. If $a^n = 0$, then $a^n \in \mathfrak{p}$ for every prime $\mathfrak{p}$, and hence $a \in \mathfrak{p}$. If $a^n \neq 0$ for any positive integer n, we let S be the multiplicative subset of powers of a, namely $\{1, a, a^2, \ldots\}$, and find a prime ideal as in the proposition to prove the converse.

Let $\mathfrak{a}$ be an ideal of A. The **radical** of $\mathfrak{a}$ is the set of all $a \in A$ such that $a^n \in \mathfrak{a}$ for some integer $n \geqq 1$, (or equivalently, it is the set of elements $a \in A$ whose image in the factor ring $A/\mathfrak{a}$ is nilpotent). We observe that the radical of $\mathfrak{a}$ is an ideal, for if $a^n = 0$ and $b^m = 0$ then $(a + b)^k = 0$ if k is sufficiently large: In the binomial expansion, either a or b will appear with a power at least equal to n or m.

Corollary 2.3. *An element a of A lies in the radical of an ideal $\mathfrak{a}$ if and only if it lies in every prime ideal containing $\mathfrak{a}$.*

Proof. Corollary 2.3 is equivalent to Corollary 2.2 applied to the ring $A/\mathfrak{a}$.

We shall extend Corollary 2.2 to modules. We first make some remarks on localization. Let S be a multiplicative subset of A. If M is a module, we can define $S^{-1}M$ in the same way that we defined $S^{-1}A$. We consider equivalence classes of pairs (x, s) with $x \in M$ and $s \in S$, two pairs (x, s) and (x', s') being equivalent if there exists $s_1 \in S$ such that $s_1(s'x - sx') = 0$. We denote the equivalence class of (x, s) by x/s, and verify at once that the set of equivalence classes is an additive group (under the obvious operations). It is in fact an A-module, under the operation

$$(a, x/s) \mapsto ax/s.$$

We shall denote this module of equivalence classes by $S^{-1}M$. (We note that $S^{-1}M$ could also be viewed as an $S^{-1}A$-module.)

If $\mathfrak{p}$ is a prime ideal of A, and S is the complement of $\mathfrak{p}$ in A, then $S^{-1}M$ is also denoted by $M_{\mathfrak{p}}$.

It follows trivially from the definitions that if $N \to M$ is an injective homomorphism, then we have a natural injection $S^{-1}N \to S^{-1}M$. In other words, if N is a submodule of M, then $S^{-1}N$ can be viewed as a submodule of $S^{-1}M$. If $x \in N$ and $s \in S$, then the fraction x/s can be viewed as an element of $S^{-1}N$ or $S^{-1}M$. If $x/s = 0$ in $S^{-1}M$, then there exists $s_1 \in S$ such that $s_1 x = 0$, and this means that x/s is also 0 in $S^{-1}N$. Thus if $\mathfrak{p}$ is a prime ideal and N is a submodule of M, we have a natural inclusion of $N_{\mathfrak{p}}$ in $M_{\mathfrak{p}}$. We shall in fact identify $N_{\mathfrak{p}}$ as a submodule of $M_{\mathfrak{p}}$. In particular, we see that $M_{\mathfrak{p}}$ is the sum of its submodules $(Ax)_{\mathfrak{p}}$, for $x \in M$ (but of course not the direct sum).

Let $x \in M$. The **annihilator** $\mathfrak{a}$ of x is the ideal consisting of all elements $a \in A$ such that $ax = 0$. We have an isomorphism (of modules)

$$A/\mathfrak{a} \xrightarrow{\approx} Ax$$

under the map

$$a \to ax.$$

Lemma 2.4. *Let x be an element of a module M, and let $\mathfrak{a}$ be its annihilator. Let $\mathfrak{p}$ be a prime ideal of A. Then $(Ax)_{\mathfrak{p}} \neq 0$ if and only if $\mathfrak{p}$ contains $\mathfrak{a}$.*

Proof. The lemma is an immediate consequence of the definitions, and will be left to the reader.

Let a be an element of A. Let M be a module. The homomorphism

$$x \mapsto ax, \qquad x \in M$$

will be called the **principal homomorphism** associated with a, and will be denoted by a_M. We shall say that a_M is **locally nilpotent** if for each $x \in M$ there exists an integer $n(x) \geqq 1$ such that $a^{n(x)}x = 0$. This condition implies that for every finitely generated submodule N of M, there exists an integer $n \geqq 1$ such that $a^n N = 0$: We take for n the largest power of a annihilating a finite set of generators of N. Therefore, *if M is finitely generated, a_M is locally nilpotent if and only if it is nilpotent.*

Proposition 2.5. *Let M be a module, $a \in A$. Then a_M is locally nilpotent if and only if a lies in every prime ideal $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$.*

Proof. Assume that a_M is locally nilpotent. Let $\mathfrak{p}$ be a prime of A such that $M_{\mathfrak{p}} \neq 0$. Then there exists $x \in M$ such that $(Ax)_{\mathfrak{p}} \neq 0$. Let n be a positive integer such that $a^n x = 0$. Let $\mathfrak{a}$ be the annihilator of x. Then $a^n \in \mathfrak{a}$, and hence we can apply the lemma, and Corollary 4.3 to conclude that a lies in every prime $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$. Conversely, suppose a_M is not locally nilpotent, so there exists $x \in M$ such that $a^n x = 0$ for all $n \geqq 0$. Let $S = \{1, a, a^2, \ldots\}$, and using Proposition 2.1 let $\mathfrak{p}$ be a prime not intersecting S. Then $(Ax)_{\mathfrak{p}} \neq 0$, so $M_{\mathfrak{p}} \neq 0$ and $a \notin \mathfrak{p}$, as desired.

Let M be a module. A prime ideal $\mathfrak{p}$ of A will be said to be **associated** with M if there exists an element $x \in M$ such that $\mathfrak{p}$ is the annihilator of x. In particular, since $\mathfrak{p} \neq A$, we must have $x \neq 0$.

Proposition 2.6. *Let M be a module $\neq 0$. Let $\mathfrak{p}$ be a maximal element in the set of ideals which are annihilators of elements $x \in M, x \neq 0$. Then $\mathfrak{p}$ is prime.*

Proof. Let $\mathfrak{p}$ be the annihilator of the element $x \neq 0$. Then $\mathfrak{p} \neq A$. Let $a, b \in A$, $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$. Then $ax \neq 0$. But the ideal $(b, \mathfrak{p})$ annihilates ax, and contains $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, it follows that $b \in \mathfrak{p}$, and hence $\mathfrak{p}$ is prime.

Corollary 2.7. *If A is Noetherian and M is a module $\neq 0$, then there exists a prime associated with M.*

Proof. The set of ideals as in Proposition 2.6 is not empty since $M \neq 0$, and has a maximal element because A is Noetherian.

Corollary 2.8. *Assume that both A and M are Noetherian, $M \neq 0$. Then there exists a sequence of submodules*

$$M = M_1 \supset M_2 \supset \cdots \supset M_r = 0$$

such that each factor module M_i/M_{i+1} is isomorphic to $A/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$.

Proof. Consider the set of submodules having the property described in the corollary. It is not empty, since there exists an associated prime $\mathfrak{p}$ of M, and if $\mathfrak{p}$ is the annihilator of x, then $Ax \approx A/\mathfrak{p}$. Let N be a maximal element in the set. If $N \neq M$, then by the preceding argument applied to M/N, there exists a submodule N' of M containing N such that N'/N is isomorphic to $A/\mathfrak{p}$ for some $\mathfrak{p}$, and this contradicts the maximality of N.

Proposition 2.9. *Let A be Noetherian, and $a \in A$. Let M be a module. Then a_M is injective if and only if a does not lie in any associated prime of M.*

Proof. Assume that a_M is not injective, so that $ax = 0$ for some $x \in M$, $x \neq 0$. By Corollary 2.7, there exists an associated prime $\mathfrak{p}$ of Ax, and a is an element of $\mathfrak{p}$. Conversely, if a_M is injective, then a cannot lie in any associated prime because a does not annihilate any non-zero element of M.

Proposition 2.10. *Let A be Noetherian, and let M be a module. Let $a \in A$. The following conditions are equivalent:*

(i) *a_M is locally nilpotent.*

(ii) *a lies in every associated prime of M.*

(iii) *a lies in every prime $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$.*

If $\mathfrak{p}$ is a prime such that $M_{\mathfrak{p}} \neq 0$, then $\mathfrak{p}$ contains an associated prime of M.

Proof. The fact that (i) implies (ii) is obvious from the definitions, and does not need the hypothesis that A is Noetherian. Neither does the fact that (iii) implies (i), which has been proved in Proposition 2.5. We must therefore prove that (ii) implies (iii) which is actually implied by the last statement. The latter is proved as follows. Let $\mathfrak{p}$ be a prime such that $M_{\mathfrak{p}} \neq 0$. Then there exists $x \in M$ such that $(Ax)_{\mathfrak{p}} \neq 0$. By Corollary 2.7, there exists an associated prime $\mathfrak{q}$ of $(Ax)_{\mathfrak{p}}$ in A. Hence there exists an element y/s of $(Ax)_{\mathfrak{p}}$, with $y \in Ax$, $s \notin \mathfrak{p}$, and $y/s \neq 0$, such that $\mathfrak{q}$ is the annihilator of y/s. It follows that $\mathfrak{q} \subset \mathfrak{p}$, for otherwise, there exists $b \in \mathfrak{q}$, $b \notin \mathfrak{p}$, and $0 = by/s$, whence $y/s = 0$, contradiction. Let $b_1, \ldots, b_n$ be generators for $\mathfrak{q}$. For each i, there exists $s_i \in A$, $s_i \notin \mathfrak{p}$, such that $s_i b_i y = 0$ because $b_i y/s = 0$. Let $t = s_1 \cdots s_n$. Then it is trivially verified that $\mathfrak{q}$ is the annihilator of ty in A. Hence $\mathfrak{q} \subset \mathfrak{p}$, as desired.

Let us define the **support** of M by

$\operatorname{supp}(M)$ = set of primes $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$.

We also have the **annihilator** of M,

$$\operatorname{ann}(M) = \text{set of elements } a \in A \text{ such that } aM = 0.$$

We use the notation

$$\operatorname{ass}(M) = \text{set of associated primes of } M.$$

For any ideal $\mathfrak{a}$ we have its **radical**,

$$\operatorname{rad}(\mathfrak{a}) = \text{set of elements } a \in A \text{ such that } a^n \in \mathfrak{a} \text{ for some integer } n \geqq 1.$$

Then for *finitely generated* M, we can reformulate Proposition 2.10 by the following formula:

$$\operatorname{rad}(\operatorname{ann}(M)) = \bigcap_{\mathfrak{p} \in \operatorname{supp}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \operatorname{ass}(M)} \mathfrak{p}.$$

Corollary 2.11. *Let A be Noetherian, and let M be a module. The following conditions are equivalent:*

(i) *There exists only one associated prime of M.*

(ii) *We have $M \neq 0$, and for every $a \in A$, the homomorphism a_M is injective, or locally nilpotent.*

If these conditions are satisfied, then the set of elements $a \in A$ such that a_M is locally nilpotent is equal to the associated prime of M.

Proof. Immediate consequence of Propositions 2.9 and 2.10.

Proposition 2.12. *Let N be a submodule of M. Every associated prime of N is associated with M also. An associated prime of M is associated with N or with M/N.*

Proof. The first assertion is obvious. Let $\mathfrak{p}$ be an associated prime of M, and say $\mathfrak{p}$ is the annihilator of the element $x \neq 0$. If $Ax \cap N = 0$, then Ax is isomorphic to a submodule of M/N, and hence $\mathfrak{p}$ is associated with M/N. Suppose $Ax \cap N \neq 0$. Let $y = ax \in N$ with $a \in A$ and $y \neq 0$. Then $\mathfrak{p}$ annihilates y. We claim $\mathfrak{p} = \operatorname{ann}(y)$. Let $b \in A$ and $by = 0$. Then $ba \in \mathfrak{p}$ but $a \notin \mathfrak{p}$, so $b \in \mathfrak{p}$. Hence $\mathfrak{p}$ is the annihilator of y in A, and therefore is associated with N, as was to be shown.

§3. PRIMARY DECOMPOSITION

We continue to assume that A is a commutative ring, and that modules (resp. homomorphisms) are A-modules (resp. A-homomorphisms), unless otherwise specified.

Let M be a module. A submodule Q of M is said to be **primary** if $Q \neq M$, and if given $a \in A$, the homomorphism $a_{M/Q}$ is either injective or nilpotent. Viewing A as a module over itself, we see that an ideal $\mathfrak{q}$ is **primary** if and only if it satisfies the following condition:

Given $a, b \in A$, $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, then $b^n \in \mathfrak{q}$ for some $n \geqq 1$.

Let Q be primary. Let $\mathfrak{p}$ be the ideal of elements $a \in A$ such that $a_{M/Q}$ is nilpotent. Then $\mathfrak{p}$ is prime. Indeed, suppose that $a, b \in A$, $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$. Then $a_{M/Q}$ is injective, and consequently $a^n_{M/Q}$ is injective for all $n \geqq 1$. Since $(ab)_{M/Q}$ is nilpotent, it follows that $b_{M/Q}$ must be nilpotent, and hence that $b \in \mathfrak{p}$, proving that $\mathfrak{p}$ is prime. We shall call $\mathfrak{p}$ the prime **belonging** to Q, and also say that Q is $\mathfrak{p}$-primary.

We note the corresponding property for a primary module Q with prime $\mathfrak{p}$:

Let $b \in A$ and $x \in M$ be such that $bx \in Q$. If $x \notin Q$ then $b \in \mathfrak{p}$.

Examples. Let $\mathfrak{m}$ be a maximal ideal of A and let $\mathfrak{q}$ be an ideal of A such that $\mathfrak{m}^k \subset \mathfrak{q}$ for some positive integer k. Then $\mathfrak{q}$ is primary, and $\mathfrak{m}$ belongs to $\mathfrak{q}$. We leave the proof to the reader.

The above conclusion is not always true if $\mathfrak{m}$ is replaced by some prime ideal $\mathfrak{p}$. For instance, let R be a factorial ring with a prime element t. Let A be the subring of polynomials $f(X) \in R[X]$ such that

$$f(X) = a_0 + a_1 X + \dots$$

with a_1 divisible by t. Let $\mathfrak{p} = (tX, X^2, X^3)$. Then $\mathfrak{p}$ is prime but

$$\mathfrak{p}^2 = (t^2X^2, tX^3, X^4)$$

is not primary, as one sees because $X^2 \notin \mathfrak{p}^2$ but $t^k \notin \mathfrak{p}^2$ for all $k \geqq 1$, yet $t^2X^2 \in \mathfrak{p}^2$.

Proposition 3.1. *Let M be a module, and $Q_1, \dots, Q_r$ submodules which are $\mathfrak{p}$-primary for the same prime $\mathfrak{p}$. Then $Q_1 \cap \dots \cap Q_r$ is also $\mathfrak{p}$-primary.*

Proof. Let $Q = Q_1 \cap \dots \cap Q_r$. Let $a \in \mathfrak{p}$. Let n_i be such that $(a_{M/Q_i})^{n_i} = 0$ for each $i = 1, \dots, r$ and let n be the maximum of $n_1, \dots, n_r$. Then $a^n_{M/Q} = 0$, so that $a_{M/Q}$ is nilpotent. Conversely, suppose $a \notin \mathfrak{p}$. Let $x \in M$, $x \notin Q_j$ for some j. Then $a^n x \notin Q_j$ for all positive integers n, and consequently $a_{M/Q}$ is injective. This proves our proposition.

Let N be a submodule of M. When N is written as a finite intersection of primary submodules, say

$$N = Q_1 \cap \cdots \cap Q_r,$$

we shall call this a **primary decomposition** of N. Using Proposition 3.1, we see that by grouping the Q_i according to their primes, we can always obtain from a given primary decomposition another one such that the primes belonging to the primary ideals are all distinct. A primary decomposition as above such that the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ belonging to $Q_1, \ldots, Q_r$ respectively are distinct, and such that N cannot be expressed as an intersection of a proper subfamily of the primary ideals $\{Q_1, \ldots, Q_r\}$ will be said to be **reduced**. By deleting some of the primary modules appearing in a given decomposition, we see that if N admits some primary decomposition, then it admits a reduced one. We shall prove a result giving certain uniqueness properties of a reduced primary decomposition.

Let N be a submodule of M and let $x \mapsto \bar{x}$ be the canonical homomorphism. Let $\overline{Q}$ be a submodule of $\overline{M} = M/N$ and let Q be its inverse image in M. Then directly from the definition, one sees that $\overline{Q}$ is primary if and only if Q is primary; and if they are primary, then the prime belonging to Q is also the prime belonging to $\overline{Q}$. Furthermore, if $N = Q_1 \cap \ldots \cap Q_r$ is a primary decomposition of N in M, then

$$(0) = \overline{Q}_1 \cap \ldots \cap \overline{Q}_r$$

is a primary decomposition of (0) in $\overline{M}$, as the reader will verify at once from the definitions. In addition, the decomposition of N is reduced if and only if the decomposition of (0) is reduced since the primes belonging to one are the same as the primes belonging to the other.

Let $Q_1 \cap \cdots \cap Q_r = N$ be a reduced primary decomposition, and let $\mathfrak{p}_i$ belong to Q_i. If $\mathfrak{p}_i$ does not contain $\mathfrak{p}_j$ $(j \neq i)$ then we say that $\mathfrak{p}_i$ is **isolated**. The isolated primes are therefore those primes which are minimal in the set of primes belonging to the primary modules Q_i.

Theorem 3.2. *Let N be a submodule of M, and let*

$$N = Q_1 \cap \cdots \cap Q_r = Q'_1 \cap \cdots \cap Q'_s$$

be a reduced primary decomposition of N. Then $r = s$. The set of primes belonging to $Q_1, \ldots, Q_r$ and $Q'_1, \ldots, Q'_r$ is the same. If $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ is the set of isolated primes belonging to these decompositions, then $Q_i = Q'_i$ for $i = 1, \ldots, m$, in other words, the primary modules corresponding to isolated primes are uniquely determined.

Proof. The uniqueness of the number of terms in a reduced decomposition and the uniqueness of the family of primes belonging to the primary components will be a consequence of Theorem 3.5 below.

There remains to prove the uniqueness of the primary module belonging to an isolated prime, say $\mathfrak{p}_1$. By definition, for each $j = 2, \ldots, r$ there exists $a_j \in \mathfrak{p}_j$ and $a_j \notin \mathfrak{p}_1$. Let $a = a_2 \cdots a_r$ be the product. Then $a \in \mathfrak{p}_j$ for all $j > 1$, but $a \notin \mathfrak{p}_1$. We can find an integer $n \geqq 1$ such that $a^n_{M/Q_j} = 0$ for $j = 2, \ldots, r$. Let

$$N_1 = \text{set of } x \in M \text{ such that } a^n x \in N.$$

We contend that $Q_1 = N_1$. This will prove the desired uniqueness. Let $x \in Q_1$. Then $a^n x \in Q_1 \cap \cdots \cap Q_r = N$, so $x \in N_1$. Conversely, let $x \in N_1$, so that $a^n x \in N$, and in particular $a^n x \in Q_1$. Since $a \notin \mathfrak{p}_1$, we know by definition that a_{M/Q_1} is injective. Hence $x \in Q_1$, thereby proving our theorem.

Theorem 3.3. *Let M be a Noetherian module. Let N be a submodule of M. Then N admits a primary decomposition.*

Proof. We consider the set of submodules of M which do not admit a primary decomposition. If this set is not empty, then it has a maximal element because M is Noetherian. Let N be this maximal element. Then N is not primary, and there exists $a \in A$ such that $a_{M/N}$ is neither injective nor nilpotent. The increasing sequence of modules

$$\operatorname{Ker} a_{M/N} \subset \operatorname{Ker} a^2_{M/N} \subset \operatorname{Ker} a^3_{M/N} \subset \cdots$$

stops, say at $a^r_{M/N}$. Let $\varphi : M/N \to M/N$ be the endomorphism $\varphi = a^r_{M/N}$. Then $\operatorname{Ker} \varphi^2 = \operatorname{Ker} \varphi$. Hence $0 = \operatorname{Ker} \varphi \cap \operatorname{Im} \varphi$ in M/N, and neither the kernel nor the image of φ is 0. Taking the inverse image in M, we see that N is the intersection of two submodules of M, unequal to N. We conclude from the maximality of N that each one of these submodules admits a primary decomposition, and therefore that N admits one also, contradiction.

We shall conclude our discussion by relating the primes belonging to a primary decomposition with the associated primes discussed in the previous section.

Proposition 3.4. *Let A and M be Noetherian. A submodule Q of M is primary if and only if M/Q has exactly one associated prime $\mathfrak{p}$, and in that case, $\mathfrak{p}$ belongs to Q, i.e. Q is $\mathfrak{p}$-primary.*

Proof. Immediate consequence of the definitions, and Corollary 2.11.

Theorem 3.5. *Let A and M be Noetherian. The associated primes of M are precisely the primes which belong to the primary modules in a reduced primary decomposition of 0 in M. In particular, the set of associated primes of M is finite.*

Proof. Let

$$0 = Q_1 \cap \cdots \cap Q_r$$

be a reduced primary decomposition of 0 in M. We have an injective homomorphism

$$M \to \bigoplus_{i=1}^{r} M/Q_i.$$

By Proposition 2.12 and Proposition 3.4, we conclude that every associated prime of M belongs to some Q_i. Conversely, let $N = Q_2 \cap \cdots \cap Q_r$. Then $N \neq 0$ because our decomposition is reduced. We have

$$N = N/(N \cap Q_1) \approx (N + Q_1)/Q_1 \subset M/Q_1.$$

Hence N is isomorphic to a submodule of M/Q_1, and consequently has an associated prime which can be none other than the prime $\mathfrak{p}_1$ belonging to Q_1. This proves our theorem.

Theorem 3.6. *Let A be a Noetherian ring. Then the set of divisors of zero in A is the set-theoretic union of all primes belonging to primary ideals in a reduced primary decomposition of* 0.

Proof. An element of $a \in A$ is a divisor of 0 if and only if a_A is not injective. According to Proposition 2.9, this is equivalent to a lying in some associated prime of A (viewed as module over itself). Applying Theorem 3.5 concludes the proof.

§4. NAKAYAMA'S LEMMA

We let A denote a commutative ring, but not necessarily Noetherian.

When dealing with modules over a ring, many properties can be obtained first by localizing, thus reducing problems to modules over local rings. In practice, as in the present section, such modules will be finitely generated. This section shows that some aspects can be reduced to vector spaces over a field by reducing modulo the maximal ideal of the local ring. Over a field, a module always has a basis. We extend this property as far as we can to modules finite over a local ring. The first three statements which follow are known as **Nakayama's lemma**.

Lemma 4.1. *Let $\mathfrak{a}$ be an ideal of A which is contained in every maximal ideal of A. Let E be a finitely generated A-module. Suppose that $\mathfrak{a}E = E$. Then $E = \{0\}$.*

Proof. Induction on the number of generators of E. Let $x_1, \ldots, x_s$ be generators of E. By hypothesis, there exist elements $a_1, \ldots, a_s \in \mathfrak{a}$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s,$$

so there is an element a (namely a_s) in $\mathfrak{a}$ such that $(1 + a)x_s$ lies in the module generated by the first $s - 1$ generators. Furthermore $1 + a$ is a unit in A, otherwise $1 + a$ is contained in some maximal ideal, and since a lies in all maximal ideals, we conclude that 1 lies in a maximal ideal, which is not possible. Hence x_s itself lies in the module generated by $s - 1$ generators, and the proof is complete by induction.

Lemma 4.1 applies in particular to the case when A is a local ring, and $\mathfrak{a} = \mathfrak{m}$ is its maximal ideal.

Lemma 4.2. *Let A be a local ring, let E be a finitely generated A-module, and F a submodule. If $E = F + \mathfrak{m}E$, then $E = F$.*

Proof. Apply Lemma 4.1 to E/F.

Lemma 4.3. *Let A be a local ring. Let E be a finitely generated A-module. If $x_1, \ldots, x_n$ are generators for $E \bmod \mathfrak{m}E$, then they are generators for E.*

Proof. Take F to be the submodule generated by $x_1, \ldots, x_n$.

Theorem 4.4. *Let A be a local ring and E a finite projective A-module. Then E is free. In fact, if $x_1, \ldots, x_n$ are elements of E whose residue classes $\bar{x}_1, \ldots, \bar{x}_n$ are a basis of $E/\mathfrak{m}E$ over $A/\mathfrak{m}$, then $x_1, \ldots, x_n$ are a basis of E over A. If $x_1, \ldots, x_r$ are such that $\bar{x}_1, \ldots, \bar{x}_r$ are linearly independent over $A/\mathfrak{m}$, then they can be completed to a basis of E over A.*

Proof. I am indebted to George Bergman for the following proof of the first statement. Let F be a free module with basis $e_1, \ldots, e_n$, and let $f\colon F \to E$ be the homomorphism mapping e_i to x_i. We want to prove that f is an isomorphism. By Lemma 4.3, f is surjective. Since E is projective, it follows that f splits, i.e. we can write $F = P_0 \oplus P_1$, where $P_0 = \operatorname{Ker} f$ and P_1 is mapped isomorphically onto E by f. Now the linear independence of $x_1, \ldots, x_n \bmod \mathfrak{m}E$ shows that

$$P_0 \subset \mathfrak{m}F = \mathfrak{m}P_0 \oplus \mathfrak{m}P_1.$$

Hence $P_0 \subset \mathfrak{m}P_0$. Also, as a direct summand in a finitely generated module, P_0 is finitely generated. So by Lemma 4.3, $P_0 = (0)$ and f is an isomorphism, as was to be proved.

As to the second statement, it is immediate since we can complete a given

sequence $x_1, \ldots, x_r$ with $\bar{x}_1, \ldots, \bar{x}_r$ linearly independent over $A/\mathfrak{m}$, to a sequence $x_1, \ldots, x_n$ with $\bar{x}_1, \ldots, \bar{x}_n$ linearly independent over $A/\mathfrak{m}$, and then we can apply the first part of the proof. This concludes the proof of the theorem.

Let E be a module over a local ring A with maximal ideal $\mathfrak{m}$. We let $E(\mathfrak{m}) = E/\mathfrak{m}E$. If $f: E \to F$ is a homomorphism, then f induces a homomorphism

$$f_{(\mathfrak{m})}: E(\mathfrak{m}) \to F(\mathfrak{m}).$$

If f is surjective, then it follows trivially that $f_{(\mathfrak{m})}$ is surjective.

Proposition 4.5. *Let $f: E \to F$ be a homomorphism of modules, finite over a local ring A. Then:*

(i) *If $f_{(\mathfrak{m})}$ is surjective, so is f.*

(ii) *Assume f is injective. If $f_{(\mathfrak{m})}$ is surjective, then f is an isomorphism.*

(iii) *Assume that E, F are free. If $f_{(\mathfrak{m})}$ is injective (resp. an isomorphism) then f is injective (resp. an isomorphism).*

Proof. The proofs are immediate consequences of Nakayama's lemma and will be left to the reader. For instance, in the first statement, consider the exact sequence

$$E \to F \to F/\mathrm{Im} f \to 0$$

and apply Nakayama to the term on the right. In (iii), use the lifting of bases as in Theorem 4.4.

§5. FILTERED AND GRADED MODULES

Let A be a commutative ring and E a module. By a **filtration** of E one means a sequence of submodules

$$E = E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_n \supset \cdots$$

Strictly speaking, this should be called a descending filtration. We don't consider any other.

Example. Let $\mathfrak{a}$ be an ideal of a ring A, and E an A-module. Let

$$E_n = \mathfrak{a}^n E.$$

Then the sequence of submodules $\{E_n\}$ is a filtration.

More generally, let $\{E_n\}$ be any filtration of a module E. We say that it is an **$\mathfrak{a}$-filtration** if $\mathfrak{a}E_n \subset E_{n+1}$ for all n. The preceding example is an $\mathfrak{a}$-filtration.

We say that an $\mathfrak{a}$-filtration is **$\mathfrak{a}$-stable**, or **stable** if we have $\mathfrak{a}E_n = E_{n+1}$ for all n sufficiently large.

Proposition 5.1. *Let $\{E_n\}$ and $\{E'_n\}$ be stable $\mathfrak{a}$-filtrations of E. Then there exists a positive integer d such that*

$$E_{n+d} \subset E'_n \quad \text{and} \quad E'_{n+d} \subset E_n$$

for all $n \geqq 0$.

Proof. It suffices to prove the proposition when $E'_n = \mathfrak{a}^n E$. Since $\mathfrak{a}E_n \subset E_{n+1}$ for all n, we have $\mathfrak{a}^n E \subset E_n$. By the stability hypothesis, there exists d such that

$$E_{n+d} = \mathfrak{a}^n E_d \subset \mathfrak{a}^n E,$$

which proves the proposition.

A ring A is called **graded** (by the natural numbers) if one can write A as a direct sum (as abelian group),

$$A = \bigoplus_{n=0}^{\infty} A_n,$$

such that for all integers $m, n \geqq 0$ we have $A_n A_m \subset A_{n+m}$. It follows in particular that A_0 is a subring, and that each component A_n is an A_0-module.

Let A be a graded ring. A module E is called a **graded module** if E can be expressed as a direct sum (as abelian group)

$$E = \bigoplus_{n=0}^{\infty} E_n,$$

such that $A_n E_m \subset E_{n+m}$. In particular, E_n is an A_0-module. Elements of E_n are then called **homogeneous of degree** n. By definition, any element of E can be written uniquely as a finite sum of homogeneous elements.

Example. Let k be a field, and let $X_0, \ldots, X_r$ be independent variables. The polynomial ring $A = k[X_0, \ldots, X_r]$ is a graded algebra, with $k = A_0$. The homogeneous elements of degree n are the polynomials generated by the monomials in $X_0, \ldots, X_r$ of degree n, that is

$$X_0^{d_0} \cdots X_r^{d_r} \quad \text{with} \quad \sum_{i=0}^{r} d_i = n.$$

An ideal I of A is called homogeneous if it is graded, as an A-module. If this is the case, then the factor ring A/I is also a graded ring.

Proposition 5.2. *Let A be a graded ring. Then A is Noetherian if and only if A_0 is Noetherian, and A is finitely generated as A_0-algebra.*

Proof. A finitely generated algebra over a Noetherian ring is Noetherian, because it is a homomorphic image of the polynomial ring in finitely many variables, and we can apply Hilbert's theorem.

Conversely, suppose that A is Noetherian. The sum

$$A^+ = \bigoplus_{n=1}^{\infty} A_n$$

is an ideal of A, whose residue class ring is A_0, which is thus a homomorphic image of A, and is therefore Noetherian. Furthermore, A^+ has a finite number of generators $x_1, \ldots, x_s$ by hypothesis. Expressing each generator as a sum of homogeneous elements, we may assume without loss of generality that these generators are homogeneous, say of degrees $d_1, \ldots, d_s$ respectively, with all $d_i > 0$. Let B be the subring of A generated over A_0 by $x_1, \ldots, x_s$. We claim that $A_n \subset B$ for all n. This is certainly true for $n = 0$. Let $n > 0$. Let x be homogeneous of degree n. Then there exist elements $a_i \in A_{n-d_i}$ such that

$$x = \sum_{i=1}^{s} a_i x_i.$$

Since $d_i > 0$ by induction, each a_i is in $A_0[x_1, \ldots, x_s] = B$, so this shows $x \in B$ also, and concludes the proof.

We shall now see two ways of constructing graded rings from filtrations.

First, let A be a ring and $\mathfrak{a}$ an ideal. We view A as a filtered ring, by the powers $\mathfrak{a}^n$. We define the **first associated graded ring** to be

$$S_{\mathfrak{a}}(A) = S = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n.$$

Similarly, if E is an A-module, and E is filtered by an $\mathfrak{a}$-filtration, we define

$$E_S = \bigoplus_{n=0}^{\infty} E_n.$$

Then it is immediately verified that E_S is a graded S-module.

Observe that if A is Noetherian, and $\mathfrak{a}$ is generated by elements $x_1, \ldots, x_s$ then S is generated as an A-algebra also by $x_1, \ldots, x_s$, and is therefore also Noetherian.

Lemma 5.3. *Let A be a Noetherian ring, and E a finitely generated module, with an $\mathfrak{a}$-filtration. Then E_S is finite over S if and only if the filtration of E is $\mathfrak{a}$-stable.*

Proof. Let

$$F_n = \bigoplus_{i=0}^{n} E_i,$$

and let

$$G_n = E_0 \oplus \cdots \oplus E_n \oplus \mathfrak{a}E_n \oplus \mathfrak{a}^2E_n \oplus \mathfrak{a}^3E_n \oplus \cdots$$

Then G_n is an S-submodule of E_S, and is finite over S since F_n is finite over A. We have

$$G_n \subset G_{n+1} \quad \text{and} \quad \bigcup G_n = E_S.$$

Since S is Noetherian, we get:

$$\begin{aligned} E_S \text{ is finite over } S &\Leftrightarrow E_S = G_N \text{ for some } N \\ &\Leftrightarrow E_{N+m} = \mathfrak{a}^m E_N \text{ for all } m \geqq 0 \\ &\Leftrightarrow \text{the filtration of } E \text{ is } \mathfrak{a}\text{-stable.} \end{aligned}$$

This proves the lemma.

Theorem 5.4. (Artin-Rees). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal, E a finite A-module with a stable $\mathfrak{a}$-filtration. Let F be a submodule, and let $F_n = F \cap E_n$. Then $\{F_n\}$ is a stable $\mathfrak{a}$-filtration of F.*

Proof. We have

$$\mathfrak{a}(F \cap E_n) \subset \mathfrak{a}F \cap \mathfrak{a}E_n \subset F \cap E_{n+1},$$

so $\{F_n\}$ is an $\mathfrak{a}$-filtration of F. We can then form the associated graded S-module F_S, which is a submodule of E_S, and is finite over S since S is Noetherian. We apply Lemma 5.3 to conclude the proof.

We reformulate the Artin-Rees theorem in its original form as follows.

Corollary 5.5. *Let A be a Noetherian ring, E a finite A-module, and F a submodule. Let $\mathfrak{a}$ be an ideal. There exists an integer s such that for all integers $n \geqq s$ we have*

$$\mathfrak{a}^n E \cap F = \mathfrak{a}^{n-s}(\mathfrak{a}^s E \cap F).$$

Proof. Special case of Theorem 5.4 and the definitions.

Theorem 5.6. (Krull). *Let A be a Noetherian ring, and let $\mathfrak{a}$ be an ideal contained in every maximal ideal of A. Let E be a finite A-module. Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n E = 0.$$

Proof. Let $F = \bigcap \mathfrak{a}^n E$ and apply Nakayama's lemma to conclude the proof.

Corollary 5.7. *Let* $\mathfrak{o}$ *be a local Noetherian ring with maximal ideal* $\mathfrak{m}$. *Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0.$$

Proof. Special case of Theorem 5.6 when $E = A$.

The second way of forming a graded ring or module is done as follows. Let A be a ring and $\mathfrak{a}$ an ideal of A. We define the **second associated graded ring**

$$\mathrm{gr}_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}.$$

Multiplication is defined in the obvious way. Let $a \in \mathfrak{a}^n$ and let $\bar{a}$ denote its residue class mod $\mathfrak{a}^{n+1}$. Let $b \in \mathfrak{a}^m$ and let $\bar{b}$ denote its residue class mod $\mathfrak{a}^{m+1}$. We define the product $\bar{a}\bar{b}$ to be the residue class of ab mod $\mathfrak{a}^{m+n+1}$. It is easily verified that this definition is independent of the choices of representatives and defines a multiplication on $\mathrm{gr}_{\mathfrak{a}}(A)$ which makes $\mathrm{gr}_{\mathfrak{a}}(A)$ into a graded ring.

Let E be a filtered A-module. We define

$$\mathrm{gr}(E) = \bigoplus_{n=0}^{\infty} E_n/E_{n+1}.$$

If the filtration is an $\mathfrak{a}$-filtration, then $\mathrm{gr}(E)$ is a graded $\mathrm{gr}_{\mathfrak{a}}(A)$-module.

Proposition 5.8. *Assume that* A *is Noetherian, and let* $\mathfrak{a}$ *be an ideal of* A. *Then* $\mathrm{gr}_{\mathfrak{a}}(A)$ *is Noetherian. If* E *is a finite* A*-module with a stable* $\mathfrak{a}$*-filtration, then* $\mathrm{gr}(E)$ *is a finite* $\mathrm{gr}_{\mathfrak{a}}(A)$*-module.*

Proof. Let $x_1, \ldots, x_s$ be generators of $\mathfrak{a}$. Let $\bar{x}_i$ be the residue class of x_i in $\mathfrak{a}/\mathfrak{a}^2$. Then

$$\mathrm{gr}_{\mathfrak{a}}(A) = (A/\mathfrak{a})[\bar{x}_1, \ldots, \bar{x}_s]$$

is Noetherian, thus proving the first assertion. For the second assertion, we have for some d,

$$E_{d+m} = \mathfrak{a}^m E_d \qquad \text{for all } m \geqq 0.$$

Hence $\mathrm{gr}(E)$ is generated by the finite direct sum

$$\mathrm{gr}(E)_0 \oplus \cdots \oplus \mathrm{gr}(E)_d.$$

But each $\mathrm{gr}(E)_n = E_n/E_{n+1}$ is finitely generated over A, and annihilated by $\mathfrak{a}$, so is a finite $A/\mathfrak{a}$-module. Hence the above finite direct sum is a finite $A/\mathfrak{a}$-module, so $\mathrm{gr}(E)$ is a finite $\mathrm{gr}_{\mathfrak{a}}(A)$-module, thus concluding the proof of the proposition.

§6. THE HILBERT POLYNOMIAL

The main point of this section is to study the lengths of certain filtered modules over local rings, and to show that they are polynomials in appropriate cases. However, we first look at graded modules, and then relate filtered modules to graded ones by using the construction at the end of the preceding section.

We start with a graded Noetherian ring together with a finite graded A-module E, so

$$A = \bigoplus_{n=0}^{\infty} A_n \quad \text{and} \quad E = \bigoplus_{n=0}^{\infty} E_n.$$

We have seen in Proposition 5.2 that A_0 is Noetherian, and that A is a finitely generated A_0-algebra. The same type of argument shows that E has a finite number of homogeneous generators, and E_n is a finite A_0-module for all $n \geqq 0$.

Let φ be an Euler-Poincaré $\mathbf{Z}$-valued function on the class of all finite A_0-modules, as in Chapter III, §8. We define the **Poincaré series** with respect to φ to be the power series

$$P_\varphi(E, t) = \sum_{n=0}^{\infty} \varphi(E_n)t^n \in \mathbf{Z}[[t]].$$

We write $P(E, t)$ instead of $P_\varphi(E, t)$ for simplicity.

Theorem 6.1. (Hilbert-Serre). *Let s be the number of generators of A as A_0-algebra. Then $P(E, t)$ is a rational function of type*

$$P(E, t) = \frac{f(t)}{\prod_{i=1}^{s} (1 - t^{d_i})}$$

with suitable positive integers d_i, and $f(t) \in \mathbf{Z}[t]$.

Proof. Induction on s. For $s = 0$ the assertion is trivially true. Let $s \geqq 1$. Let $A = A_0[x_1, \ldots, x_s]$, deg. $x_i = d_i \geqq 1$. Multiplication by x_s on E gives rise to an exact sequence

$$0 \to K_n \to E_n \xrightarrow{x_s} E_{n+d_s} \to L_{n+d_s} \to 0.$$

Let

$$K = \bigoplus K_n \quad \text{and} \quad L = \bigoplus L_n.$$

Then K, L are finite A-modules (being submodules and factor modules of E), and are annihilated by x_s, so are in fact graded $A_0[x_1, \ldots, x_{s-1}]$-modules. By definition of an Euler-Poincaré function, we get

$$\varphi(K_n) - \varphi(E_n) + \varphi(E_{n+d_s}) - \varphi(L_{n+d_s}) = 0.$$

Multiplying by t^{n+d_s} and summing over n, we get

$$(1 - t^{d_s})P(E, t) = P(L, t) - t^{d_s}P(K, t) + g(t),$$

where $g(t)$ is a polynomial in $\mathbf{Z}[t]$. The theorem follows by induction.

Remark. In Theorem 6.1, if $A = A_0[x_1, \ldots, x_s]$ then $d_i = \deg x_i$ as shown in the proof. The next result shows what happens when all the degrees are equal to 1.

Theorem 6.2. *Assume that A is generated as an A_0-algebra by homogeneous elements of degree 1. Let d be the order of the pole of $P(E, t)$ at $t = 1$. Then for all sufficiently large n, $\varphi(E_n)$ is a polynomial in n of degree $d - 1$. (For this statement, the zero polynomial is assumed to have degree -1.)*

Proof. By Theorem 6.1, $\varphi(E_n)$ is the coefficient of t^n in the rational function

$$P(E, t) = f(t)/(1 - t)^s.$$

Cancelling powers of $1 - t$, we write $P(E, t) = h(t)/(1 - t)^d$, and $h(1) \neq 0$, with $h(t) \in \mathbf{Z}[t]$. Let

$$h(t) = \sum_{k=0}^{m} a_k t^k.$$

We have the binomial expansion

$$(1 - t)^{-d} = \sum_{k=0}^{\infty} \binom{d + k - 1}{d - 1} t^k.$$

For convenience we let $\binom{n}{-1} = 0$ for $n \geqq 0$ and $\binom{n}{-1} = 1$ for $n = -1$. We then get

$$\varphi(E_n) = \sum_{k=0}^{m} a_k \binom{d + n - k - 1}{d - 1} \qquad \text{for all } n \geqq m.$$

The sum on the right-hand side is a polynomial in n with leading term

$$(\sum a_k) \frac{n^{d-1}}{(d - 1)!} \neq 0.$$

This proves the theorem.

The polynomial of Theorem 6.2 is called the **Hilbert polynomial** of the graded module E, with respect to φ.

We now put together a number of results of this chapter, and give an application of Theorem 6.2 to certain filtered modules.

Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal. Then $A/\mathfrak{q}$ is also Noetherian and local. Since some power of $\mathfrak{m}$ is contained in $\mathfrak{q}$, it follows that $A/\mathfrak{q}$ has only one associated prime, viewed as module over itself, namely $\mathfrak{m}/\mathfrak{q}$ itself. Similarly, if M is a finite $A/\mathfrak{q}$-module, then M has only one associated prime, and the only simple $A/\mathfrak{q}$-module is in fact an $A/\mathfrak{m}$-module which is one-dimensional. Again since some power of $\mathfrak{m}$ is contained in $\mathfrak{q}$, it follows that $A/\mathfrak{q}$ has finite length, and M also has finite length. We now use the length function as an Euler-Poincaré function in applying Theorem 6.2.

Theorem 6.3. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal, and let E be a finitely generated A-module, with a stable $\mathfrak{q}$-filtration. Then:*

(i) *E/E_n has finite length for $n \geqq 0$.*

(ii) *For all sufficiently large n, this length is a polynomial $g(n)$ of degree $\leqq s$, where s is the least number of generators of $\mathfrak{q}$.*

(iii) *The degree and leading coefficient of $g(n)$ depend only on E and $\mathfrak{q}$, but not on the chosen filtration.*

Proof. Let

$$G = \mathrm{gr}_{\mathfrak{q}}(A) = \bigoplus \mathfrak{q}^n/\mathfrak{q}^{n+1}.$$

Then $\mathrm{gr}(E) = \bigoplus E_n/E_{n+1}$ is a graded G-module, and $G_0 = A/\mathfrak{q}$. By Proposition 5.8, G is Noetherian and $\mathrm{gr}(E)$ is a finite G-module. By the remarks preceding the theorem, E/E_n has finite length, and if φ denotes the length, then

$$\varphi(E/E_n) = \sum_{j=1}^{n} \varphi(E_{j-1}/E_j).$$

If $x_1, \ldots, x_s$ generate $\mathfrak{q}$, then the images $\bar{x}_1, \ldots, \bar{x}_s$ in $\mathfrak{q}/\mathfrak{q}^2$ generate G as $A/\mathfrak{q}$-algebra, and each $\bar{x}_i$ has degree 1. By Theorem 6.2 we see that

$$\varphi(E_n/E_{n+1}) = h(n)$$

is a polynomial in n of degree $\leqq s - 1$ for sufficiently large n. Since

$$\varphi(E/E_{n+1}) - \varphi(E/E_n) = h(n),$$

it follows by Lemma 6.4 below that $\varphi(E/E_n)$ is a polynomial $g(n)$ of degree $\leqq s$ for all large n. The last statement concerning the independence of the degree

of g and its leading coefficient from the chosen filtration follows immediately from Proposition 5.1, and will be left to the reader. This concludes the proof.

From the theorem, we see that there is a polynomial $\chi_{E,\mathfrak{q}}$ such that

$$\chi_{E,\mathfrak{q}}(n) = \text{length}(E/\mathfrak{q}^n E)$$

for all sufficiently large n. If $E = A$, then $\chi_{A,\mathfrak{q}}$ is usually called the **characteristic polynomial** of $\mathfrak{q}$. In particular, we see that

$$\chi_{A,\mathfrak{q}}(n) = \text{length}(A/\mathfrak{q}^n)$$

for all sufficiently large n.

For a continuation of these topics into dimension theory, see [AtM 69] and [Mat 80].

We shall now study a particularly important special case having to do with polynomial ideals. Let k be a field, and let

$$A = k[X_0, \ldots, X_N]$$

be the polynomial ring in $N + 1$ variable. Then A is graded, the elements of degree n being the homogeneous polynomials of degree n. We let $\mathfrak{a}$ be a homogeneous ideal of A, and for an integer $n \geqq 0$ we define:

$$\varphi(n) = \dim_k A_n$$

$$\varphi(n, \mathfrak{a}) = \dim_k \mathfrak{a}_n$$

$$\chi(n, \mathfrak{a}) = \dim_k A_n/\mathfrak{a}_n = \dim_k A_n - \dim_k \mathfrak{a}_n = \varphi(n) - \varphi(n, \mathfrak{a}).$$

As earlier in this section, A_n denotes the k-space of homogeneous elements of degree n in A, and similarly for $\mathfrak{a}_n$. Then we have

$$\varphi(n) = \binom{N + n}{N}.$$

We shall consider the **binomial polynomial**

$$\binom{T}{d} = \frac{T(T-1)\cdots(T-d+1)}{d!} = \frac{T^d}{d!} + \text{lower terms.} \tag{1}$$

If f is a function, we define the **difference function** Δf by

$$\Delta f(T) = f(T + 1) - f(T).$$

Then one verifies directly that

$$\Delta\binom{T}{d} = \binom{T}{d-1}. \tag{2}$$

Lemma 6.4. *Let $P \in \mathbf{Q}[T]$ be a polynomial of degree d with rational coefficients.*

(a) *If $P(n) \in \mathbf{Z}$ for all sufficiently large integers n, then there exist integers $c_0, \ldots, c_d$ such that*

$$P(T) = c_0\binom{T}{d} + c_1\binom{T}{d-1} + \ldots + c_d.$$

In particular, $P(n) \in \mathbf{Z}$ for all integers n.

(b) *If $f\colon \mathbf{Z} \to \mathbf{Z}$ is any function, and if there exists a polynomial $Q(T) \in \mathbf{Q}[T]$ such that $Q(\mathbf{Z}) \subset \mathbf{Z}$ and $\Delta f(n) = Q(n)$ for all n sufficiently large, then there exists a polynomial P as in (a) such that $f(n) = P(n)$ for all n sufficiently large.*

Proof. We prove (a) by induction. If the degree of P is 0, then the assertion is obvious. Suppose deg $P \geqq 1$. By (1) there exist rational numbers $c_0, \ldots, c_d$ such that $P(T)$ has the expression given in (a). But ΔP has degree strictly smaller than deg P. Using (2) and induction, we conclude that $c_0, \ldots, c_{d-1}$ must be integers. Finally c_d is an integer because $P(n) \in \mathbf{Z}$ for n sufficiently large. This proves (a).

As for (b), using (a), we can write

$$Q(T) = c_0\binom{T}{d-1} + \ldots + c_{d-1}$$

with integers $c_0, \ldots, c_{d-1}$. Let P_1 be the "integral" of Q, that is

$$P_1(T) = c_0\binom{T}{d} + \ldots + c_{d-1}\binom{T}{1}, \quad \text{so} \quad \Delta P_1 = Q.$$

Then $\Delta(f - P_1)(n) = 0$ for all n sufficiently large. Hence $(f - P_1)(n)$ is equal to a constant c_d for all n sufficiently large, so we let $P = P_1 + c_d$ to conclude the proof.

Proposition 6.5. *Let $\mathfrak{a}, \mathfrak{b}$ be homogeneous ideals in A. Then*

$$\varphi(n, \mathfrak{a}+\mathfrak{b}) = \varphi(n, \mathfrak{a}) + \varphi(n, \mathfrak{b}) - \varphi(n, \mathfrak{a} \cap \mathfrak{b})$$
$$\chi(n, \mathfrak{a}+\mathfrak{b}) = \chi(n, \mathfrak{a}) + \chi(n, \mathfrak{b}) - \chi(n, \mathfrak{a} \cap \mathfrak{b}).$$

Proof. The first is immediate, and the second follows from the definition of χ.

Theorem 6.6. *Let F be a homogeneous polynomial of degree d. Assume that F is not a divisor of zero mod $\mathfrak{a}$, that is: if $G \in A$, $FG \in \mathfrak{a}$, then $G \in \mathfrak{a}$. Then*

$$\chi\big(n, \mathfrak{a} + (F)\big) = \chi(n, \mathfrak{a}) - \chi(n - d, \mathfrak{a}).$$

Proof. First observe that trivially

$$\varphi(n, (F)) = \varphi(n - d),$$

because the degree of a product is the sum of the degrees. Next, using the hypothesis that F is not divisor of 0 mod $\mathfrak{a}$, we conclude immediately

$$\varphi(n, \mathfrak{a} \cap (F)) = \varphi(n - d, \mathfrak{a}).$$

Finally, by Proposition 6.5 (the formula for χ), we obtain:

$$\begin{aligned}
\chi(n, \mathfrak{a} + (F)) &= \chi(n, \mathfrak{a}) + \chi(n, (F)) - \chi(n, \mathfrak{a} \cap (F)) \\
&= \chi(n, \mathfrak{a}) + \varphi(n) - \varphi(n, (F)) - \varphi(n) + \varphi(n, \mathfrak{a} \cap (F)) \\
&= \chi(n, \mathfrak{a}) - \varphi(n - d) + \varphi(n - d, \mathfrak{a}) \\
&= \chi(n, \mathfrak{a}) - \chi(n - d, \mathfrak{a})
\end{aligned}$$

thus proving the theorem.

We denote by $\mathfrak{m}$ the maximal ideal $\mathfrak{m} = (X_0, \ldots, X_N)$ in A. We call $\mathfrak{m}$ the **irrelevant prime ideal**. An ideal is called **irrelevant** if some positive power of $\mathfrak{m}$ is contained in the ideal. In particular, a primary ideal $\mathfrak{q}$ is irrelevant if and only if $\mathfrak{m}$ belongs to $\mathfrak{q}$. Note that by the Hilbert nullstellensatz, the condition that some power of $\mathfrak{m}$ is contained in $\mathfrak{a}$ is equivalent with the condition that the only zero of $\mathfrak{a}$ (in some algebraically closed field containing k) is the trivial zero.

Proposition 6.7. *Let $\mathfrak{a}$ be a homogeneous ideal.*

(a) *If $\mathfrak{a}$ is irrelevant, then $\chi(n, \mathfrak{a}) = 0$ for n sufficiently large.*

(b) *In general, there is an expression $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ as a reduced primary decomposition such that all $\mathfrak{q}_i$ are homogeneous.*

(c) *If an irrelevant primary ideal occurs in the decomposition, let $\mathfrak{b}$ be the intersection of all other primary ideals. Then*

$$\chi(n, \mathfrak{a}) = \chi(n, \mathfrak{b})$$

for all n sufficiently large.

Proof. For (a), by assumption we have $A_n = \mathfrak{a}_n$ for n sufficiently large, so the assertion (a) is obvious. We leave (b) as an exercise. As to (c), say $\mathfrak{q}_s$ is irrelevant, and let $\mathfrak{b} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{s-1}$. By Proposition 6.5, we have

$$\chi(n, \mathfrak{b} + \mathfrak{q}_s) = \chi(n, \mathfrak{b}) + \chi(n, \mathfrak{q}_s) - \chi(n, \mathfrak{a}).$$

But $\mathfrak{b} + \mathfrak{q}_s$ is irrelevant, so (c) follows from (a), thus concluding the proof.

We now want to see that for any homogeneous ideal $\mathfrak{a}$ the function f such that

$$f(n) = \chi(n, \mathfrak{a})$$

satisfies the conditions of Lemma 6.4(b). First, we observe that if we change the ground field from k to an algebraically closed field K containing k, and we let $A_K = K[X_0, \ldots, X_N]$, $\mathfrak{a}_K = K\mathfrak{a}$, then

$$\dim_k A_n = \dim_K A_{K,n} \qquad \text{and} \qquad \dim_k \mathfrak{a}_n = \dim_K \mathfrak{a}_{K,n}.$$

Hence we can assume that k is algebraically closed.

Second, we shall need a geometric notion, that of dimension. Let V be a variety over k, say affine, with generic point $(x) = (x_1, \ldots, x_N)$. We define its **dimension** to be the transcendence degree of $k(x)$ over k. For a projective variety, defined by a homogeneous prime ideal $\mathfrak{p}$, we define its dimension to be the dimension of the homogeneous variety defined by $\mathfrak{p}$ minus 1.

We now need the following lemma.

Lemma 6.8. *Let V, W be varieties over a field k.*

If $V \supset W$ and $\dim V = \dim W$, *then $V = W$.*

Proof. Say V, W are in affine space $\mathbf{A}^N$. Let $\mathfrak{p}_V$ and $\mathfrak{p}_W$ be the respective prime ideals of V and W in $k[X]$. Then we have a canonical homomorphism

$$k[X]/\mathfrak{p}_V \approx k[x] \to k[y] \approx k[X]/\mathfrak{p}_W$$

from the affine coordinate ring of V onto the affine coordinate ring of W. If the transcendence degree of $k(x)$ is the same as that of $k(y)$, and say $y_1, \ldots, y_r$ form a transcendence basis of $k(y)$ over k, then $x_1, \ldots, x_r$ is a transcendence basis of $k(x)$ over k, the homomorphism $k[x] \to k[y]$ induces an isomorphism

$$k[x_1, \ldots, x_r] \xrightarrow{\sim} k[y_1, \ldots, y_r],$$

and hence an isomorphism on the finite extension $k[x]$ to $k[y]$, as desired.

Theorem 6.9. *Let $\mathfrak{a}$ be a homogeneous ideal in A. Let r be the maximum dimension of the irreducible components of the algebraic space in projective space defined by $\mathfrak{a}$. Then there exists a polynomial $P \in \mathbf{Q}[T]$ of degree $\leqq r$, such that $P(\mathbf{Z}) \subset \mathbf{Z}$, and such that*

$$P(n) = \chi(n, \mathfrak{a})$$

for all n sufficiently large.

Proof. By Proposition 6.7(c), we may assume that no primary component in the primary decomposition of $\mathfrak{a}$ is irrelevant. Let Z be the algebraic space of zeros of $\mathfrak{a}$ in projective space. We may assume k algebraically closed as noted previously. Then there exists a homogeneous polynomial $L \in k[X]$ of degree 1 (a linear form) which does not lie in any of the prime ideals belonging to the primary ideals in the given decomposition. In particular, L is not a divisor of zero mod $\mathfrak{a}$. Then the components of the algebraic space of zeros of $\mathfrak{a} + (L)$ must have dimension $\leqq r - 1$. By induction and Theorem 6.6, we conclude that the difference

$$\chi(n, \mathfrak{a}) - \chi(n - 1, \mathfrak{a})$$

satisfies the conditions of Lemma 6.4(b), which concludes the proof.

The polynomial in Theorem 6.9 is called the **Hilbert polynomial** of the ideal $\mathfrak{a}$.

Remark. The above results give an introduction for Hartshorne's [Ha 77], Chapter I, especially §7. If Z is not empty, and if we write

$$\chi(n, \mathfrak{a}) = c\frac{n^r}{r!} + \text{lower terms},$$

then $c > 0$ and c can be interpreted as the **degree** of Z, or in geometric terms, the number of points of intersection of Z with a sufficiently general linear variety of complementary dimension (counting the points with certain multiplicities). For explanations and details, see [Ha 77], Chapter I, Proposition 7.6 and Theorem 7.7; van der Waerden [vdW 29] which does the same thing for multihomogeneous polynomial ideals; [La 58], referred to at the end of Chapter VIII, §2; and the papers [MaW 85], [Ph 86], making the link with van der Waerden some six decades before.

Bibliography

[AtM 69] M. ATIYAH and I. MACDONALD, *Introduction to commutative algebra*, Addison-Wesley, 1969

[Ha 77] R. HARTSHORNE, *Algebraic Geometry*, Springer Verlag, 1977

[MaW 85] D. MASSER and G. WÜSTHOLZ, Zero estimates on group varieties II, *Invent. Math.* **80** (1985), pp. 233–267

[Mat 80] H. MATSUMURA, *Commutative algebra*, Second Edition, Benjamin-Cummings, 1980

[Ph 86] P. PHILIPPON, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* **114** (1986), pp. 355–383

[vdW 29] B. L. VAN DER WAERDEN, On Hilbert's function, series of composition of ideals and a generalization of the theorem of Bezout, *Proc. R. Soc. Amsterdam* **31** (1929), pp. 749–770

§7. INDECOMPOSABLE MODULES

Let A be a ring, not necessarily commutative, and E an A-module. We say that E is **Artinian** if E satisfies the descending chain condition on submodules, that is a sequence

$$E_1 \supset E_2 \supset E_3 \cdots$$

must stabilize: there exists an integer N such that if $n \geqq N$ then $E_n = E_{n+1}$.

Example 1. If k is a field, A is a k-algebra, and E is a finite-dimensional vector space over k which is also an A-module, then E is Artinian as well as Noetherian.

Example 2. Let A be a commutative Noetherian local ring with maximal ideal $\mathfrak{m}$, and let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal. Then for every positive integer n, $A/\mathfrak{q}^n$ is Artinian. Indeed, $A/\mathfrak{q}^n$ has a Jordan-Hölder filtration in which each factor is a finite dimensional vector space over the field $A/\mathfrak{m}$, and is a module of finite length. See Proposition 7.2.

Conversely, suppose that A is a local ring which is both Noetherian and Artinian. Let $\mathfrak{m}$ be the maximal ideal. Then there exists some positive integer n such that $\mathfrak{m}^n = 0$. Indeed, the descending sequence $\mathfrak{m}^n$ stabilizes, and Nakayama's lemma implies our assertion. It then also follows that every primary ideal is nilpotent.

As with Noetherian rings and modules, it is easy to verify the following statements:

Proposition 7.1. *Let A be a ring, and let*

$$0 \to E' \to E \to E'' \to 0$$

be an exact sequence of A-modules. Then E is Artinian if and only if E' and E'' are Artinian.

We leave the proof to the reader. The proof is the same as in the Noetherian case, reversing the inclusion relations between modules.

Proposition 7.2. *A module E has a finite simple filtration if and only if E is both Noetherian and Artinian.*

Proof. A simple module is generated by one element, and so is Noetherian. Since it contains no proper submodule $\neq 0$, it is also Artinian. Proposition 7.2 is then immediate from Proposition 7.1.

A module E is called **decomposable** if E can be written as a direct sum

$$E = E_1 \oplus E_2$$

with $E_1 \neq E$ and $E_2 \neq E$. Otherwise, E is called **indecomposable**. If E is decomposable as above, let e_1 be the projection on the first factor, and $e_2 = 1 - e_1$ the projection on the second factor. Then e_1, e_2 are idempotents such that

$$e_1 \neq 1, \qquad e_2 \neq 1, \qquad e_1 + e_2 = 1 \quad \text{and} \quad e_1 e_2 = e_2 e_1 = 0.$$

Conversely, if such idempotents exist in $\mathrm{End}(E)$ for some module E, then E is decomposable, and e_i is the projection on the submodule $e_i E$.

Let $u : E \to E$ be an endomorphism of some module E. We can form the descending sequence

$$\mathrm{Im}\, u \supset \mathrm{Im}\, u^2 \supset \mathrm{Im}\, u^3 \supset \cdots$$

If E is Artinian, this sequence stabilizes, and we have

$$\mathrm{Im}\, u^n = \mathrm{Im}\, u^{n+1} \qquad \text{for all sufficiently large } n.$$

We call this submodule $u^\infty(E)$, or $\mathrm{Im}\, u^\infty$.

Similarly, we have an ascending sequence

$$\mathrm{Ker}\, u \subset \mathrm{Ker}\, u^2 \subset \mathrm{Ker}\, u^3 \subset \cdots$$

which stabilizes if E is Noetherian, and in this case we write

$$\mathrm{Ker}\, u^\infty = \mathrm{Ker}\, u^n \qquad \text{for } n \text{ sufficiently large.}$$

Proposition 7.3. (Fitting's Lemma). *Assume that E is Noetherian and Artinian. Let $u \in \mathrm{End}(E)$. Then E has a direct sum decomposition*

$$E = \mathrm{Im}\, u^\infty \oplus \mathrm{Ker}\, u^\infty.$$

Furthermore, the restriction of u to $\mathrm{Im}\, u^\infty$ is an automorphism, and the restriction of u to $\mathrm{Ker}\, u^\infty$ is nilpotent.

Proof. Choose n such that $\mathrm{Im}\, u^\infty = \mathrm{Im}\, u^n$ and $\mathrm{Ker}\, u^\infty = \mathrm{Ker}\, u^n$. We have

$$\mathrm{Im}\, u^\infty \cap \mathrm{Ker}\, u^\infty = \{0\},$$

for if x lies in the intersection, then $x = u^n(y)$ for some $y \in E$, and then $0 = u^n(x) = u^{2n}(y)$. So $y \in \mathrm{Ker}\, u^{2n} = \mathrm{Ker}\, u^n$, whence $x = u^n(y) = 0$.

Secondly, let $x \in E$. Then for some $y \in u^n(E)$ we have

$$u^n(x) = u^n(y).$$

Then we can write

$$x = x - u^n(y) + u^n(y),$$

which shows that $E = \operatorname{Im} u^\infty + \operatorname{Ker} u^\infty$. Combined with the first step of the proof, this shows that E is a direct sum as stated.

The final assertion is immediate, since the restriction of u to $\operatorname{Im} u^\infty$ is surjective, and its kernel is 0 by the first part of the proof. The restriction of u to $\operatorname{Ker} u^\infty$ is nilpotent because $\operatorname{Ker} u^\infty = \operatorname{Ker} u^n$. This concludes the proof of the proposition.

We now generalize the notion of a local ring to a non-commutative ring. A ring A is called **local** if the set of non-units is a two-sided ideal.

Proposition 7.4. *Let E be an indecomposable module over the ring A. Assume E Noetherian and Artinian. Any endomorphism of E is either nilpotent or an automorphism. Furthermore* $\operatorname{End}(E)$ *is local.*

Proof. By Fitting's lemma, we know that for any endomorphism u, we have $E = \operatorname{Im} u^\infty$ or $E = \operatorname{Ker} u^\infty$. So we have to prove that $\operatorname{End}(E)$ is local. Let u be an endomorphism which is not a unit, so u is nilpotent. For any endomorphism v it follows that uv and vu are not surjective or injective respectively, so are not automorphisms. Let u_1, u_2 be endomorphisms which are not units. We have to show $u_1 + u_2$ is not a unit. If it is a unit in $\operatorname{End}(E)$, let $v_i = u_i(u_1 + u_2)^{-1}$. Then $v_1 + v_2 = 1$. Furthermore, $v_1 = 1 - v_2$ is invertible by the geometric series since v_2 is nilpotent. But v_1 is not a unit by the first part of the proof, contradiction. This concludes the proof.

Theorem 7.5. (Krull-Remak-Schmidt). *Let $E \neq 0$ be a module which is both Noetherian and Artinian. Then E is a finite direct sum of indecomposable modules. Up to a permutation, the indecomposable components in such a direct sum are uniquely determined up to isomorphism.*

Proof. The existence of a direct sum decomposition into indecomposable modules follows from the Artinian condition. If first $E = E_1 \oplus E_2$, then either E_1, E_2 are indecomposable, and we are done; or, say, E_1 is decomposable. Repeating the argument, we see that we cannot continue this decomposition indefinitely without contradicting the Artinian assumption.

There remains to prove uniqueness. Suppose

$$E = E_1 \oplus \cdots \oplus E_r = F_1 \oplus \cdots \oplus F_s$$

where E_i, F_j are indecomposable. We have to show that $r = s$ and after some permutation, $E_i \approx F_i$. Let e_i be the projection of E on E_i, and let u_j be the projection of E on F_j, relative to the above direct sum decompositions. Let:

$$v_j = e_1 u_j \quad \text{and} \quad w_j = u_j e_1.$$

Then $\sum u_j = \mathrm{id}_E$ implies that

$$\sum_{j=1}^{s} v_j w_j | E_1 = \mathrm{id}_{E_1}.$$

By Proposition 7.4, $\mathrm{End}(E_1)$ is local, and therefore some $v_j w_j$ is an automorphism of E_1. After renumbering, we may assume that $v_1 w_1$ is an automorphism of E_1. We claim that v_1 and w_1 induce isomorphisms between E_1 and F_1, This follows from a lemma.

Lemma 7.6. *Let M, N be modules, and assume N indecomposable. Let $u: M \to N$ and $v: N \to M$ be such that vu is an automorphism. Then u, v are isomorphisms.*

Proof. Let $e = u(vu)^{-1}v$. Then $e^2 = e$ is an idempotent, lying in $\mathrm{End}(N)$, and therefore equal to 0 or 1 since N is assumed indecomposable. But $e \neq 0$ because $\mathrm{id}_M \neq 0$ and

$$0 \neq \mathrm{id}_M = \mathrm{id}_M^2 = (vu)^{-1}vu(vu)^{-1}vu.$$

So $e = \mathrm{id}_N$. Then u is injective because vu is an automorphism; v is injective because $e = \mathrm{id}_N$ is injective; u is surjective because $e = \mathrm{id}_N$; and v is surjective because vu is an automorphism. This concludes the proof of the lemma.

Returning to the theorem, we now see that

$$E = F_1 \oplus (E_2 \oplus \cdots \oplus E_r).$$

Indeed, e_1 induces an isomorphism from F_1 to E_1, and since the kernel of e_1 is $E_2 \oplus \cdots \oplus E_r$ it follows that

$$F_1 \cap (E_2 \oplus \cdots \oplus E_r) = 0.$$

But also, $F_1 \equiv E_1 \pmod{E_2 \oplus \cdots \oplus E_r}$, so E is the sum of F_1 and $E_2 \oplus \cdots \oplus E_r$, whence E is the direct sum, as claimed. But then

$$E/F_1 \approx F_2 \oplus \cdots \oplus F_s \approx E_2 \oplus \cdots \oplus E_r.$$

The proof is then completed by induction.

We apply the preceding results to a commutative ring A. We note that an idempotent in A as a ring is the same thing as an idempotent as an element of $\mathrm{End}(A)$, viewing A as module over itself. Furthermore $\mathrm{End}(A) \approx A$. Therefore, we find the special cases:

Theorem 7.7. *Let A be a Noetherian and Artinian commutative ring.*

(i) *If A is indecomposable as a ring, then A is local.*

(ii) *In general, A is a direct product of local rings, which are Artinian and Noetherian.*

Another way of deriving this theorem will be given in the exercises.

EXERCISES

1. Let A be a commutative ring. Let M be a module, and N a submodule. Let $N = Q_1 \cap \cdots \cap Q_r$ be a primary decomposition of N. Let $\bar{Q}_i = Q_i/N$. Show that $0 = \bar{Q}_1 \cap \cdots \cap \bar{Q}_r$ is a primary decomposition of 0 in M/N. State and prove the converse.
2. Let $\mathfrak{p}$ be a prime ideal, and $\mathfrak{a}$, $\mathfrak{b}$ ideals of A. If $\mathfrak{ab} \subset \mathfrak{p}$, show that $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.
3. Let $\mathfrak{q}$ be a primary ideal. Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals, and assume $\mathfrak{ab} \subset \mathfrak{q}$. Assume that $\mathfrak{b}$ is finitely generated. Show that $\mathfrak{a} \subset \mathfrak{q}$ or there exists some positive integer n such that $\mathfrak{b}^n \subset \mathfrak{q}$.
4. Let A be Noetherian, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Show that there exists some $n \geqq 1$ such that $\mathfrak{p}^n \subset \mathfrak{q}$.
5. Let A be an arbitrary commutative ring and let S be a multiplicative subset. Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then $\mathfrak{p}$ intersects S if and only if $\mathfrak{q}$ intersects S. Furthermore, if $\mathfrak{q}$ does not intersect S, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary in $S^{-1}A$.
6. If $\mathfrak{a}$ is an ideal of A, let $\mathfrak{a}_S = S^{-1}\mathfrak{a}$. If $\varphi_S : A \to S^{-1}A$ is the canonical map, abbreviate $\varphi_S^{-1}(\mathfrak{a}_S)$ by $\mathfrak{a}_S \cap A$, even though φ_S is not injective. Show that there is a bijection between the prime ideals of A which do not intersect S and the prime ideals of $S^{-1}A$, given by

$$\mathfrak{p} \mapsto \mathfrak{p}_S \quad \text{and} \quad \mathfrak{p}_S \mapsto \mathfrak{p}_S \cap A = \mathfrak{p}.$$

   Prove a similar statement for primary ideals instead of prime ideals.
7. Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be a reduced primary decomposition of an ideal. Assume that $\mathfrak{q}_1, \ldots, \mathfrak{q}_i$ do not intersect S, but that $\mathfrak{q}_j$ intersects S for $j > i$. Show that

$$\mathfrak{a}_S = \mathfrak{q}_{1S} \cap \cdots \cap \mathfrak{q}_{iS}$$

   is a reduced primary decomposition of $\mathfrak{a}_S$.
8. Let A be a local ring. Show that any idempotent $\neq 0$ in A is necessarily the unit element. (An **idempotent** is an element $e \in A$ such that $e^2 = e$.)
9. Let A be an Artinian commutative ring. Prove:
   (a) All prime ideals are maximal. [*Hint*: Given a prime ideal $\mathfrak{p}$, let $x \in A$, $x(\mathfrak{p}) = 0$. Consider the descending chain $(x) \supset (x^2) \supset (x^3) \supset \cdots$.]

(b) There is only a finite number of prime, or maximal, ideals. [*Hint*: Among all finite intersections of maximal ideals, pick a minimal one.]

(c) The ideal N of nilpotent elements in A is nilpotent, that is there exists a positive integer k such that $N^k = (0)$. [*Hint*: Let k be such that $N^k = N^{k+1}$. Let $\mathfrak{a} = N^k$. Let $\mathfrak{b}$ be a minimal ideal $\neq 0$ such that $\mathfrak{ba} \neq 0$. Then $\mathfrak{b}$ is principal and $\mathfrak{ba} = \mathfrak{b}$.]

(d) A is Noetherian.

(e) There exists an integer r such that

$$A = \prod A/\mathfrak{m}^r$$

where the product is taken over all maximal ideals.

(f) We have

$$A = \prod A_{\mathfrak{p}},$$

where again the product is taken over all prime ideals $\mathfrak{p}$.

10. Let A, B be local rings with maximal ideals $\mathfrak{m}_A$, $\mathfrak{m}_B$, respectively. Let $f: A \to B$ be a homomorphism. We say that f is **local** if $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$. Suppose this is the case. Assume A, B Noetherian, and assume that:

1. $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is an isomorphism;

2. $\mathfrak{m}_A \to \mathfrak{m}_B/\mathfrak{m}_B^2$ is surjective;

3. B is a finite A-module, via f.

Prove that f is surjective. [*Hint*: Apply Nakayama twice.]

For an ideal $\mathfrak{a}$, recall from Chapter IX, §5 that $\mathfrak{Z}(\mathfrak{a})$ is the set of primes containing $\mathfrak{a}$.

11. Let A be a commutative ring and M an A-module. Define the **support** of M by

$$\operatorname{supp}(M) = \{\mathfrak{p} \in \operatorname{spec}(A) : M_{\mathfrak{p}} \neq 0\}.$$

If M is finite over A, show that $\operatorname{supp}(M) = \mathfrak{Z}(\operatorname{ann}(M))$, where $\operatorname{ann}(M)$ is the annihilator of M in A, that is the set of elements $a \in A$ such that $aM = 0$.

12. Let A be a Noetherian ring and M a finite A-module. Let I be an ideal of A such that $\operatorname{supp}(M) \subset \mathfrak{Z}(I)$. Then $I^n M = 0$ for some $n > 0$.

13. Let A be any commutative ring, and M, N modules over A. If M is finitely presented, and S is a multiplicative subset of A, show that

$$S^{-1}\operatorname{Hom}_A(M, N) \approx \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

This is usually applied when A is Noetherian and M finitely generated, in which case M is also finitely presented since the module of relations is a submodule of a finitely generated free module.

14. (a) Prove Proposition 6.7(b).

(b) Prove that the degree of the polynomial P in Theorem 6.9 is exactly r.

Locally constant dimensions

15. Let A be a Noetherian local ring. Let E be a finite A-module. Assume that A has no nilpotent elements. For each prime ideal $\mathfrak{p}$ of A, let $k(\mathfrak{p})$ be the residue class field. If $\dim_{k(\mathfrak{p})} E_{\mathfrak{p}}/\mathfrak{p}E_{\mathfrak{p}}$ is constant for all $\mathfrak{p}$, show that E is free. [*Hint*: Let $x_1, \ldots, x_r \in A$ be

such that the residue classes mod the maximal ideal form a basis for $E/\mathfrak{m}E$ over $k(\mathfrak{m})$. We get a surjective homomorphism

$$A^r \to E \to 0.$$

Let J be the kernel. Show that $J_\mathfrak{p} \subset \mathfrak{m}_\mathfrak{p} A_\mathfrak{p}^r$ for all $\mathfrak{p}$ so $J \subset \mathfrak{p}$ for all $\mathfrak{p}$ and $J = 0$.]

16. Let A be a Noetherian local ring without nilpotent elements. Let $f: E \to F$ be a homomorphism of A-modules, and suppose E, F are finite free. For each prime $\mathfrak{p}$ of A let

$$f_{(\mathfrak{p})}: E_\mathfrak{p}/\mathfrak{p}E_\mathfrak{p} \to F_\mathfrak{p}/\mathfrak{p}F_\mathfrak{p}$$

be the corresponding $k(\mathfrak{p})$-homomorphism, where $k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is the residue class field at $\mathfrak{p}$. Assume that

$$\dim_{k(\mathfrak{p})} \operatorname{Im} f_{(\mathfrak{p})}$$

is constant.

(a) Prove that $F/\operatorname{Im} f$ and $\operatorname{Im} f$ are free, and that there is an isomorphism

$$F \approx \operatorname{Im} f \oplus (F/\operatorname{Im} f).$$

[*Hint*: Use Exercise 15.]

(b) Prove that $\operatorname{Ker} f$ is free and $E \approx (\operatorname{Ker} f) \oplus (\operatorname{Im} f)$. [*Hint*: Use that finite projective is free.]

The next exercises depend on the notion of a complex, which we have not yet formally defined. A (**finite**) **complex** E is a sequence of homomorphisms of modules

$$0 \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} \cdots \xrightarrow{d^n} E^n \to 0$$

and homorphisms $d^i: E^i \to E^{i+1}$ such that $d^{i+1} \circ d^i = 0$ for all i. Thus $\operatorname{Im}(d^i) \subset \operatorname{Ker}(d^{i+1})$. The **homology** H^i of the complex is defined to be

$$H^i = \operatorname{Ker}(d^{i+1})/\operatorname{Im}(d^i).$$

By definition, $H^0 = E^0$ and $H^n = E^n/\operatorname{Im}(d^n)$. You may want to look at the first section of Chapter XX, because all we use here is the basic notion, and the following property, which you can easily prove. Let E, F be two complexes. By a **homomorphism** $f: E \to F$ we mean a sequence of homomorphisms

$$f_i: E^i \to F^i$$

making the diagram commutative for all i:

$$\begin{array}{ccc} E^i & \xrightarrow{d_E^i} & E^{i+1} \\ \uparrow{\scriptstyle f_i} & & \uparrow{\scriptstyle f_{i+1}} \\ F^i & \xrightarrow[d_F^i]{} & F^{i+1} \end{array}$$

Show that such a homomorphism f induces a homomorphism $H(f): H(E) \to H(F)$ on the homology; that is, for each i we have an induced homomorphism

$$H^i(f): H^i(E) \to H^i(F).$$

The following exercises are inspired from applications to algebraic geometry, as for instance in Hartshorne, *Algebraic Geometry*, Chapter III, Theorem 12.8. See also Chapter XXI, §1 to see how one can construct complexes such as those considered in the next exercises in order to compute the homology with respect to less tractable complexes.

Reduction of a complex mod $\mathfrak{p}$

17. Let $0 \to K^0 \to K^1 \to \cdots \to K^n \to 0$ be a complex of finite free modules over a local Noetherian ring A without nilpotent elements. For each prime $\mathfrak{p}$ of A and module E, let $E(\mathfrak{p}) = E_{\mathfrak{p}}/\mathfrak{p}E_{\mathfrak{p}}$, and similarly let $K(\mathfrak{p})$ be the complex localized and reduced mod $\mathfrak{p}$. For a given integer i, assume that

$$\dim_{k(\mathfrak{p})} H^i(K(\mathfrak{p}))$$

is constant, where H^i is the i-th homology of the reduced complex. Show that $H^i(K)$ is free and that we have a natural isomorphism

$$H^i(K)(\mathfrak{p}) \xrightarrow{\sim} H^i(K(\mathfrak{p})).$$

[*Hint*: First write $d^i_{(\mathfrak{p})}$ for the map induced by d^i on $K^i(\mathfrak{p})$. Write

$$\dim_{k(\mathfrak{p})} \operatorname{Ker} d^i_{(\mathfrak{p})} = \dim_{k(\mathfrak{p})} K^i(\mathfrak{p}) - \dim_{k(\mathfrak{p})} \operatorname{Im} d^i_{(\mathfrak{p})}.$$

Then show that the dimensions $\dim_{k(\mathfrak{p})} \operatorname{Im} d^i_{(\mathfrak{p})}$ and $\dim_{k(\mathfrak{p})} \operatorname{Im} d^{i-1}_{(\mathfrak{p})}$ must be constant. Then apply Exercise 12.]

Comparison of homology at the special point

18. Let A be a Noetherian local ring. Let K be a finite complex, as follows:

$$0 \to K^0 \to \cdots \to K^n \to 0,$$

such that K^i is *finite free* for all i. For some index i assume that

$$H^i(K)(\mathfrak{m}) \to H^i(K(\mathfrak{m}))$$

is surjective. Prove:

(a) This map is an isomorphism.

(b) The following exact sequences split:

$$0 \to \operatorname{Ker} d^i \to K^i \to \operatorname{Im} d^i \to 0$$

$$0 \to \operatorname{Im} d^i \to K^{i+1}$$

(c) Every term in these sequences is free.

19. Let A be a Noetherian local ring. Let K be a complex as in the previous exercise. For some i assume that

$$H^i(K)(\mathfrak{m}) \to H^i(K(\mathfrak{m}))$$

is surjective (or equivalently is an isomorphism by the previous exercise). Prove that

the following conditions are equivalent:

(a) $H^{i-1}(K)(\mathfrak{m}) \to H^{i-1}(K(\mathfrak{m}))$ is surjective.

(b) $H^{i-1}(K)(\mathfrak{m}) \to H^{i-1}(K(\mathfrak{m}))$ is an isomorphism.

(c) $H^i(K)$ is free.

[*Hint*: Lift bases until you are blue in the face.]

(d) If these conditions hold, then each one of the two inclusions

$$\operatorname{Im} d^{i-1} \subset \operatorname{Ker} d^i \subset K^i$$

splits, and each one of these modules is free. Reducing mod $\mathfrak{m}$ yields the corresponding inclusions

$$\operatorname{Im} d^{i-1}_{(\mathfrak{m})} \subset \operatorname{Ker} d^i_{(\mathfrak{m})} \subset K^i(\mathfrak{m}),$$

and induce the isomorphism on cohomology as stated in (b). [*Hint*: Apply the preceding exercise.]