1

Commutative rings and modules

This chapter discusses the very basic definitions and results.

§1 centres around the question of the existence of prime ideals. In §2 we treat Nakayama's lemma, modules over local rings and modules of finite presentation; we give a complete proof, following Kaplansky, of the fact that a projective module over a local ring is free (Theorem 2.5), although, since we will not make any subsequent use of this in the infinitely generated case, the reader may pass over it. In §3 we give a detailed treatment of finiteness conditions in the form of Emmy Noether's chain condition, discussing among other things Akizuki's theorem, I.S. Cohen's theorem and Formanek's proof of the Eakin–Nagata theorem.

1 Ideals

If A is a ring and I an ideal of A, it is often important to consider the residue class ring A/I. Set $\bar{A} = A/I$, and write $f: A \longrightarrow \bar{A}$ for the natural map; then ideals $\bar{J}$ of $\bar{A}$ and ideals $J = f^{-1}(\bar{J})$ of A containing I are in one-to-one correspondence, with $\bar{J} = J/I$ and $A/J \simeq \bar{A}/\bar{J}$. Hence, when we just want to think about ideals of A containing I, it is convenient to shift attention to A/I. (If I' is any ideal of A then $f(I')$ is an ideal of $\bar{A}$, with $f^{-1}(f(I')) = I + I'$, and $f(I') = (I + I')/I$.)

A is itself an ideal of A, often written (1) since it is generated by the identity element 1. An ideal distinct from (1) is called a *proper ideal*. An element $a \in A$ which has an inverse in A (that is, for which there exists $a' \in A$ with $aa' = 1$) is called a *unit* (or *invertible element*) of A; this holds if and only if the principal ideal (a) is equal to (1). If a is a unit and x is nilpotent then $a + x$ is again a unit: indeed, if $x^n = 0$ then setting $y = -a^{-1}x$, we have $y^n = 0$; now

$$(1 - y)(1 + y + \cdots + y^{n-1}) = 1 - y^n = 1,$$

so that $a + x = a(1 - y)$ has an inverse.

In a ring A we are allowed to have $1 = 0$, but if this happens then it follows that $a = 1 \cdot a = 0 \cdot a = 0$ for every $a \in A$, so that A has only one element 0; in this case we write $A = 0$. In definitions and theorems about

rings, it may sometimes happen that the condition $A \neq 0$ is omitted even when it is actually necessary. A ring A is an *integral domain* (or simply a *domain*) if $A \neq 0$, and if A has no zero-divisors other than 0. If A is an integral domain and every non-zero element of A is a unit then A is a *field*. A field is characterised by the fact that it is a ring having exactly two ideals (0) and (1).

An ideal which is maximal among all proper ideals is called a *maximal ideal*; an ideal $\mathfrak{m}$ of A is maximal if and only if $A/\mathfrak{m}$ is a field. Given a proper ideal I, let M be the set of ideals containing I and not containing 1, ordered by inclusion; then Zorn's lemma can be applied to M. Indeed, $I \in M$ so that M is non-empty, and if $L \subset M$ is a totally ordered subset then the union of all the ideals belonging to L is an ideal of A and obviously belongs to M, so is the least upper bound of L in M. Thus by Zorn's lemma M has got a maximal element. This proves the following theorem.

Theorem 1.1. If I is a proper ideal then there exists at least one maximal ideal containing I.

An ideal P of A for which A/P is an integral domain is called a *prime ideal*. In other words, P is prime if it satisfies

(i) $P \neq A$ and (ii) $x, y \notin P \Rightarrow xy \notin P$ for $x, y \in A$

A field is an integral domain, so that a maximal ideal is prime.

If I and J are ideals and P a prime ideal, then

$$I \not\subset P,\ J \not\subset P \Rightarrow IJ \not\subset P.$$

Indeed, taking $x \in I$ and $y \in J$ with $x, y \notin P$, we have $xy \in IJ$ but $xy \notin P$.

A subset S of A is *multiplicative* if it satisfies

(i) $x, y \in S \Rightarrow xy \in S$, and (ii) $1 \in S$;

(here condition (ii) is not crucial: given a subset S satisfying (i), there will usually not be any essential change on replacing S by $S \cup \{1\}$). If I is an ideal disjoint from S, then exactly as in the proof of Theorem 1 we see that the set of ideals containing I and disjoint from S has a maximal element. If P is an ideal which is maximal among ideals disjoint from S then P is prime. For if $x \notin P$, $y \notin P$, then since $P + xA$ and $P + yA$ both meet S, the product $(P + xA)(P + yA)$ also meets S. However,

$$(P + xA)(P + yA) \subset P + xyA,$$

so that we must have $xy \notin P$. We have thus obtained the following theorem.

Theorem 1.2. Let S be a multiplicative set and I an ideal disjoint from S; then there exists a prime ideal containing I and disjoint from S.

If I is an ideal of A then the set of elements of A, some power of which belongs to I, is an ideal of A (for $x^n \in I$ and $y^m \in I \Rightarrow (x+y)^{n+m-1} \in I$ and

$(ax)^n \in I$). This set is called the *radical* of I, and is sometimes written $\sqrt{I}$:

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ for some } n > 0\}.$$

If P is a prime ideal containing I then $x^n \in I \subset P$ implies that $x \in P$, and hence $\sqrt{I} \subset P$; conversely, if $x \notin \sqrt{I}$ then $S_x = \{1, x, x^2, \ldots\}$ is a multiplicative set disjoint from I, and by the previous theorem there exists a prime ideal containing I and not containing x. Thus, the radical of I is the intersection of all prime ideals containing I:

$$\sqrt{I} = \bigcap_{P \supset I} P.$$

In particular if we take $I = (0)$ then $\sqrt{(0)}$ is the set of all nilpotent elements of A, and is called the *nilradical* of A; we will write $\mathrm{nil}(A)$ for this. Then $\mathrm{nil}(A)$ is intersection of all the prime ideals of A. When $\mathrm{nil}(A) = 0$ we say that A is *reduced*. For any ring A we write A_{red} for $A/\mathrm{nil}(A)$; A_{red} is of course reduced.

The intersection of all maximal ideals of a ring $A (\neq 0)$ is called the *Jacobson radical*, or simply the *radical* of A, and written $\mathrm{rad}(A)$. If $x \in \mathrm{rad}(A)$ then for any $a \in A$, $1 + ax$ is an element of A not contained in any maximal ideal, and is therefore a unit of A by Theorem 1. Conversely if $x \in A$ has the property that $1 + Ax$ consists entirely of units of A then $x \in \mathrm{rad}(A)$ (prove this!).

A ring having just one maximal ideal is called a *local ring*, and a (non-zero) ring having only finitely many maximal ideals a *semilocal ring*. We often express the fact that A is a local ring with maximal ideal $\mathfrak{m}$ by saying that $(A, \mathfrak{m})$ is a local ring; if this happens then the field $k = A/\mathfrak{m}$ is called the *residue field* of A. We will say that $(A, \mathfrak{m}, k)$ is a local ring to mean that A is a local ring, $\mathfrak{m} = \mathrm{rad}(A)$ and $k = A/\mathfrak{m}$. If $(A, \mathfrak{m})$ is a local ring then the elements of A not contained in $\mathfrak{m}$ are units; conversely a (non-zero) ring A whose non-units form an ideal is a local ring.

In general the product II' of two ideals I, I' is contained in $I \cap I'$, but does not necessarily coincide with it. However, if $I + I' = (1)$ (in which case we say that I and I' are *coprime*), then $II' = I \cap I'$; indeed, then $I \cap I' = (I \cap I')(I + I') \subset II' \subset I \cap I'$. Moreover, if I and I', as well as I and I'' are coprime, then I and $I'I''$ are coprime:

$$(1) = (I + I')(I + I'') \subset I + I'I'' \subset (1).$$

By induction we obtain the following theorem.

Theorem 1.3. If $I_1, I_2, \ldots, I_n$ are ideals which are coprime in pairs then

$$I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \cdots \cap I_n.$$

In particular if A is a semilocal ring and $\mathfrak{m}_1, \ldots \mathfrak{m}_n$ are all of its maximal ideals then

$$\mathrm{rad}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \ldots \mathfrak{m}_n.$$

Furthermore, if $I + I' = (1)$ then $A/II' \simeq A/I \times A/I'$. To see this it is enough to prove that the natural injective map from $A/II' = A/I \cap I'$ to $A/I \times A/I'$ is surjective; taking $e \in I$, $e' \in I'$ such that $e + e' = 1$, we have $ae' + a'e \equiv a \pmod{I}$ $ae' + a'e \equiv a' \pmod{I'}$ for any a, $a' \in A$, giving the surjectivity. By induction we get the following theorem.

Theorem 1.4. If $I_1, \ldots, I_n$ are ideals which are coprime in pairs then

$$A/I_1 \ldots I_n \simeq A/I_1 \times \cdots \times A/I_n.$$

Example 1. Let A be a ring, and consider the ring $A[\![X]\!]$ of formal power series over A. A power series $f = a_0 + a_1 X + a_2 X^2 + \cdots$ with $a_i \in A$ is a unit of $A[\![X]\!]$ if and only if a_0 is a unit of A. Indeed, if there exists an inverse $f^{-1} = b_0 + b_1 X + \cdots$ then $a_0 b_0 = 1$; and conversely if $a_0^{-1} \in A$, then

$$\begin{aligned} 1 &= (a_0 + a_1 X + \cdots)(b_0 + b_1 X + \cdots) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + \cdots \end{aligned}$$

can be solved for b_0, $b_1, \ldots$: we just find b_0, $b_1, \ldots$ successively from $a_0 b_0 = 1$, $a_0 b_1 + a_1 b_0 = 0, \ldots$.

Since the formal power series ring in several variables $A[\![X_1, \ldots, X_n]\!]$ can be thought of as $(A[\![X_1, \ldots, X_{n-1}]\!])[\![X_n]\!]$, here also $f = a_0 + \sum a_i X_i + \sum a_{ij} X_i X_j + \cdots$ is a unit if and only if the constant term a_0 is a unit of A; from this we see that if $g \in (X_1, \ldots, X_n)$ then $1 + gh$ is a unit for any power series h, so that $g \in \operatorname{rad}(A[\![X_1, \ldots, X_n]\!])$, and hence

$$(X_1, \ldots, X_n) \subset \operatorname{rad}(A[\![X_1, \ldots, X_n]\!]).$$

If k is a field then $k[\![X_1, \ldots, X_n]\!]$ is a local ring with maximal ideal $(X_1, \ldots, X_n)$. If A is any ring and we set $B = A[\![X_1, \ldots, X_n]\!]$, then since any maximal ideal of B contains $(X_1, \ldots, X_n)$, it corresponds to a maximal ideal of $B/(X_1, \ldots, X_n) \simeq A$, and so is of the form $\mathfrak{m}B + (X_1, \ldots, X_n)$, where $\mathfrak{m}$ is a maximal ideal of A. If we write $\mathfrak{m}$ for this then $\mathfrak{m} \cap A = \mathfrak{m}$.

By contrast the case of polynomial rings is quite complicated; here it is just not true that a maximal ideal of $A[X]$ must contain X. For example, $X - 1$ is a non-unit of $A[X]$, and so there exists a maximal ideal $\mathfrak{m}$ containing it, and $X \notin \mathfrak{m}$. Also, if $\mathfrak{m}$ is a maximal ideal of $A[X]$, it does not necessarily follow that $\mathfrak{m} \cap A$ is a maximal ideal of A.

If A is an integral domain then so are both $A[X]$ and $A[\![X]\!]$: if $f = a_r X^r + a_{r+1} X^{r+1} + \cdots$ and $g = b_s X^s + b_{s+1} X^{s+1} + \cdots$ with $a_r \neq 0$, $b_s \neq 0$ then $fg = a_r b_s X^{r+s} + \cdots \neq 0$. If I is an ideal of A we write $I[X]$ or $I[\![X]\!]$ for the set of polynomials or power series with coefficients in I; these are ideals of $A[X]$ or $A[\![X]\!]$, the kernels of the homomorphisms

$$A[X] \longrightarrow (A/I)[X] \text{ or } A[\![X]\!] \longrightarrow (A/I)[\![X]\!]$$

obtained by reducing coefficients modulo I. Hence

$$A[X]/I[X] \simeq (A/I)[X], \quad \text{and} \quad A[\![X]\!]/I[\![X]\!] \simeq (A/I)[\![x]\!];$$

in particular if P is a prime ideal then $P[X]$ and $P[\![X]\!]$ are prime ideals of $A[X]$ and $A[\![X]\!]$, respectively.

If I is finitely generated, that is $I = a_1A + \cdots + a_rA$, then $I[\![X]\!] = a_1A[\![X]\!] + \cdots + a_rA[\![X]\!] = I \cdot A[\![X]\!]$; however, if I is not finitely generated then $I[\![X]\!]$ is bigger than $I \cdot A[\![X]\!]$. In the polynomial ring this distinction does not arise, and we always have $I[X] = I \cdot A[X]$.

Example 2. For a ring A and $a, b \in A$, we have $aA \subset bA$ if and only if a is divisible by b, that is $a = bc$ for some $c \in A$. We assume that A is an integral domain in what follows. An element $a \in A$ is said to be *irreducible* if a is not a unit of A and satisfies the condition

$$a = bc \Rightarrow b \text{ or } c \text{ is a unit of } A.$$

This is equivalent to saying that aA is maximal among proper principal ideals. If aA is a prime ideal then a is said to be *prime*. As one sees easily, a prime element is irreducible, but the converse does not always hold.

Suppose that an element a has two expressions as products of prime elements:

$$a = p_1p_2 \dots p_n = p'_1 \dots p'_m, \text{ with } p_i \text{ and } p'_j \text{ prime.}$$

Then $n = m$, and after a suitable reordering of the p'_j we have $p_iA = p'_iA$; for $p'_1 \cdots p'_m$ is divisible by p_1, and so one of the factors, say p'_1, is divisible by p_1. Now since both p_1 and p'_1 are irreducible, $p_1A = p'_1A$ hence $p'_1 = up_1$, with u a unit, and $p_2 \cdots p_n = up'_2 \cdots p'_m$. We can replace p'_2 by up'_2, and induction on n completes the proof. In this sense, factorisation into prime elements (whenever possible) is unique.

An integral domain in which any element which is neither 0 nor a unit can be expressed as a product of prime elements is called a *unique factorisation domain* (abbreviated to UFD), or a factorial ring. It is well known that a principal ideal domain, that is an integral domain in which every ideal is principal, is a UFD (see Ex. 1.4). If A is a principal ideal domain then the prime ideals are of the form (0) or pA with p a prime element, and the latter are maximal ideals.

If k is a field then $k[X_1, \dots, X_n]$ is a UFD, as is well-known (see Ex. 20.2). If $f(X_1, \dots, X_n)$ is an irreducible polynomial then (f) is a prime ideal, but is not maximal if $n > 1$ (see §5).

$\mathbb{Z}[\sqrt{-5}]$ is not a UFD; indeed if $\alpha = n + m\sqrt{-5}$ with $n, m \in \mathbb{Z}$ then $\alpha\bar{\alpha} = n^2 + 5m^2$, and since $2 = n^2 + 5m^2$ has no integer solutions it follows that 2 is an irreducible element of $\mathbb{Z}[\sqrt{-5}]$, but we see from $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ that 2 is not a prime element. We write

$A = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5)$; then setting $k = \mathbb{Z}/2\mathbb{Z}$ we have

$$A/2A = \mathbb{Z}[X]/(2, X^2+5) = k[X]/(X^2-1) = k[X]/(X-1)^2.$$

Then $P = (2, 1-\sqrt{-5})$ is a maximal ideal of A containing 2.

Exercises to §1. Prove the following propositions.

1.1. Let A be a ring, and $I \subset \mathrm{nil}(A)$ an ideal made up of nilpotent elements; if $a \in A$ maps to a unit of A/I then a is a unit of A.

1.2. Let $A_1, \ldots, A_n$ be rings; then the prime ideals of $A_1 \times \cdots \times A_n$ are of the form
$A_1 \times \cdots \times A_{i-1} \times P_i \times A_{i+1} \times \cdots \times A_n$,
where P_i is a prime ideal of A_i.

1.3. Let A and B be rings, and $f: A \longrightarrow B$ a surjective homomorphism.
(*a*) Prove that $f(\mathrm{rad}\, A) \subset \mathrm{rad}\, B$, and construct an example where the inclusion is strict.
(*b*) Prove that if A is a semilocal ring then $f(\mathrm{rad}\, A) = \mathrm{rad}\, B$.

1.4. Let A be an integral domain. Then A is a UFD if and only if every irreducible element is prime and the principal ideals of A satisfy the ascending chain condition. (Equivalently, every non-empty family of principal ideals has a maximal element.)

1.5. Let $\{P_\lambda\}_{\lambda \in \Lambda}$ be a non-empty family of prime ideals, and suppose that the P_λ are totally ordered by inclusion; then $\bigcap P_\lambda$ is a prime ideal. Also, if I is any proper ideal, the set of prime ideals containing I has a minimal element.

1.6. Let A be a ring, $I, P_1, \ldots, P_r$ ideals of A, and suppose that $P_3, \ldots, P_r$ are prime, and that I is not contained in any of the P_i; then there exists an element $x \in I$ not contained in any P_i.

2 Modules

Let A be a ring and M an A-module. Given submodules N, N' of M, the set $\{a \in A \mid aN' \subset N\}$ is an ideal of A, which we write $N:N'$ or $(N:N')_A$. Similarly, if $I \subset A$ is an ideal then $\{x \in M \mid Ix \subset N\}$ is a submodule of M, which we write $N:I$ or $(N:I)_M$. For $a \in A$ we define $N:a$ similarly. The ideal $0:M$ is called the *annihilator* of M, and written $\mathrm{ann}(M)$. We can consider M as a module over $A/\mathrm{ann}(M)$. If $\mathrm{ann}(M) = 0$ we say that M is a *faithful* A-module. For $x \in M$ we write $\mathrm{ann}(x) = \{a \in A \mid ax = 0\}$.

If M and M' are A-modules, the set of A-linear maps from M to M' is written $\mathrm{Hom}_A(M, M')$. This becomes an A-module if we define the sum $f+g$ and the scalar product af by

$$(f+g)(x) = f(x) + g(x), \quad (af)(x) = a \cdot f(x);$$

(the fact that af is A-linear depends on A being commutative).

To say that M is an A-module is to say that M is an Abelian group under addition, and that a scalar product ax is defined for $a \in A$ and $x \in M$ such that the following hold:

(*) $\quad a(x+y) = ax + ay, \quad (ab)x = a(bx), \quad (a+b)x = ax + bx, \quad 1x = x;$

for fixed $a \in A$ the map $x \mapsto ax$ is an endomorphism of M as an additive group. Let E be the set of endomorphisms of the additive group M; defining the sum and product of $\lambda, \mu \in E$ by

$$(\lambda + \mu)(x) = \lambda(x) + \mu(x), \quad (\lambda\mu)(x) = \lambda(\mu(x))$$

makes E into a ring (in general non-commutative), and giving M an A-module structure is the same thing as giving a homomorphism $A \longrightarrow E$. Indeed, if we write a_L for the element of E defined by $x \mapsto ax$ then (*) become

$$(ab)_L = a_L b_L, \quad (a+b)_L = a_L + b_L, \quad (1_A)_L = 1_E.$$

We can express the fact that $\varphi : M \longrightarrow M$ is A-linear by saying that $\varphi \in E$ and that φ commutes with a_L for $a \in A$, that is $a_L \varphi = \varphi a_L$. Since A is commutative, a_L is itself an A-linear map of M for $a \in A$. We normally write simply $a : M \longrightarrow M$ for the map a_L.

If M is a B-module and $f : A \longrightarrow B$ a ring homomorphism, then we can make M into an A-module by defining $a \cdot x = f(a) \cdot x$ for $a \in A$ and $x \in M$. This is the A-module structure defined by the composite of $f : A \longrightarrow B$ with $B \longrightarrow E$, where E is the endomorphism ring of the additive group of M, and $B \longrightarrow E$ is the map defining the B-module structure of M.

If M is finitely generated as an A-module we say simply that M is a *finite* A-module, or is *finite over* A. A standard technique applicable to finite A-modules is the 'determinant trick', one form of which is as follows (taken from Atiyah and Macdonald [AM]).

Theorem 2.1. Suppose that M is an A-module generated by n elements, and that $\varphi \in \mathrm{Hom}_A(M, M)$; let I be an ideal of A such that $\varphi(M) \subset IM$. Then there is a relation of the form

(**) $\quad \varphi^n + a_1 \varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0,$

with $a_i \in I^i$ for $1 \leqslant i \leqslant n$ (where both sides are considered as endomorphisms of M).

Proof. Let $M = A\omega_1 + \cdots + A\omega_n$; by the assumption $\varphi(M) \subset IM$ there exist $a_{ij} \in I$ such that $\varphi(\omega_i) = \sum_{j=1}^n a_{ij}\omega_j$. This can be rewritten

$$\sum_{j=1}^{n} (\varphi\delta_{ij} - a_{ij})\,\omega_j = 0 \quad (\text{for } 1 \leqslant i \leqslant n),$$

where δ_{ij} is the Kronecker symbol. The coefficients of this system of linear equations can be viewed as a square matrix $(\varphi\delta_{ij} - a_{ij})$ of elements of $A'[\varphi]$, the commutative subring of the endomorphism ring E of M generated by the image A' of A together with φ; let b_{ij} denote its (i,j)th cofactor, and

d its determinant. By multiplying the above equation through by b_{ik} and summing over i, we get $d\omega_k = 0$ for $1 \leqslant k \leqslant n$. Hence $d \cdot M = 0$, so that $d = 0$ as an element of E. Expanding the determinant d gives a relation of the form (**). ■

Remark. As one sees from the proof, the left-hand side of (**) is the characteristic polynomial of (a_{ij}),

$$f(X) = \det(X\delta_{ij} - a_{ij})$$

with φ substituted for X. If M is the free A-module with basis $\omega_1, \ldots, \omega_n$ and $I = A$, the above result is nothing other than the classical Cayley–Hamilton theorem: let $f(X)$ be the characteristic polynomial of the square matrix $\varphi = (a_{ij})$; then $f(\varphi) = 0$.

Theorem 2.2 (NAK). Let M be a finite A-module and I an ideal of A. If $M = IM$ then there exists $a \in A$ such that $aM = 0$ and $a \equiv 1 \bmod I$. If in addition $I \subset \operatorname{rad}(A)$ then $M = 0$.

Proof. Setting $\varphi = 1_M$ in the previous theorem gives the relation $a = 1 + a_1 + \cdots + a_n = 0$ as endomorphisms of M, that is $aM = 0$, and $a \equiv 1 \bmod I$. If $I \subset \operatorname{rad}(A)$ then a is a unit of A, so that on multiplying both sides of $aM = 0$ by a^{-1} we get $M = 0$. ■

Remark. This theorem is usually referred to as Nakayama's lemma, but the late Professor Nakayama maintained that it should be referred to as a theorem of Krull and Azumaya; it is in fact difficult to determine which of these three first had the result in the case of commutative rings, so we refer to it as NAK in this book. Of course, this result can easily be proved without using determinants, by induction on the number of generators of M.

Corollary. Let A be a ring and I an ideal contained in $\operatorname{rad}(A)$. Suppose that M is an A-module and $N \subset M$ a submodule such that M/N is finite over A. Then $M = N + IM$ implies $M = N$.

Proof. Setting $\bar{M} = M/N$ we have $\bar{M} = I\bar{M}$ so that, by the theorem, $\bar{M} = 0$. ■

If W is a set of generators of an A-module M which is minimal, in the sense that any proper subset of W does not generate M, then W is said to be a *minimal basis* of M. Two minimal bases do not necessarily have the same number of elements; for example, when $M = A$, if x and y are non-units of A such that $x + y = 1$ then both $\{1\}$ and $\{x, y\}$ are minimal bases of A. However, if A is a local ring then the situation is clear:

Theorem 2.3. Let $(A, \mathfrak{m}, k)$ be a local ring and M a finite A-module; set $\bar{M} = M/\mathfrak{m}M$. Now $\bar{M}$ is a finite-dimensional vector space over k, and we

write n for its dimension. Then:

(i) If we take a basis $\{\bar{u}_1,\dots,\bar{u}_n\}$ for $\bar{M}$ over k, and choose an inverse image $u_i \in M$ of each $\bar{u}_i$, then $\{u_1,\dots,u_n\}$ is a minimal basis of M;

(ii) conversely every minimal basis of M is obtained in this way, and so has n elements.

(iii) If $\{u_1,\dots,u_n\}$ and $\{v_1,\dots,v_n\}$ are both minimal bases of M, and $v_i = \sum a_{ij}u_j$ with $a_{ij} \in A$ then $\det(a_{ij})$ is a unit of A, so that (a_{ij}) is an invertible matrix.

Proof. (i) $M = \sum Au_i + \mathfrak{m}M$, and M is finitely generated (hence also $M/\sum Au_i$), so that by the above corollary $M = \sum Au_i$. If $\{u_1,\dots,u_n\}$ is not minimal, so that, for example, $\{u_2,\dots,u_n\}$ already generates M then $\{\bar{u}_2,\dots,\bar{u}_n\}$ generates $\bar{M}$, which is a contradiction. Hence $\{u_1,\dots,u_n\}$ is a minimal basis.

(ii) If $\{u_1,\dots,u_m\}$ is a minimal basis of M and we set $\bar{u}_i$ for the image of u_i in $\bar{M}$, then $\bar{u}_1,\dots,\bar{u}_m$ generate $\bar{M}$, and are linearly independent over k; indeed, otherwise some proper subset of $\{\bar{u}_1,\dots,\bar{u}_m\}$ would be a basis of $\bar{M}$, and then by (i) a proper subset of $\{u_1,..,u_m\}$ would generate M, which is a contradiction.

(iii) Write $\bar{a}_{ij}$ for the image in k of a_{ij}, so that $\bar{v}_i = \sum \bar{a}_{ij}\bar{u}_j$ holds in $\bar{M}$. Since $(\bar{a}_{ij})$ is the matrix transforming one basis of the vector space $\bar{M}$ into another, its determinant is non-zero. Since $\det(a_{ij}) \bmod \mathfrak{m} = \det(\bar{a}_{ij}) \neq 0$ it follows that $\det(a_{ij})$ is a unit of A. By Cramér's formula the inverse matrix of (a_{ij}) exists as a matrix with entries in A. ■

We give another interesting application of NAK, the proof of which is due to Vasconcelos [2].

Theorem 2.4. Let A be a ring and M a finite A-module. If $f: M \longrightarrow M$ is an A-linear map and f is surjective then f is also injective, and is thus an automorphism of M.

Proof. Since f commutes with scalar multiplication by elements of A, we can view M as an $A[X]$-module by setting $X \cdot m = f(m)$ for $m \in M$. Then by assumption $XM = M$, so that by NAK there exists $Y \in A[X]$ such that $(1 + XY)M = 0$. Now for $u \in \mathrm{Ker}(f)$ we have $0 = (1 + XY)(u) = u + Yf(u) = u$, so that f is injective. ■

Theorem 2.5. Let $(A, \mathfrak{m})$ be a local ring; then a projective module over A is free (for the definition of projective module, see Appendix B, p. 277).

Proof. This is easy when M is finite: choose a minimal basis $\omega_1,\dots,\omega_n$ of M and define a surjective map $\varphi: F \longrightarrow M$ from the free module $F = Ae_1 \oplus \cdots \oplus Ae_n$ to M by $\varphi(\sum a_i e_i) = \sum a_i \omega_i$; if we set $K = \mathrm{Ker}(\varphi)$ then, from

the minimal basis property,

$$\sum a_i\omega_i = 0 \Rightarrow a_i \in \mathfrak{m} \quad \text{for all } i.$$

Thus $K \subset \mathfrak{m}F$. Because M is projective, there exists $\psi: M \longrightarrow F$ such that $F = \psi(M) \oplus K$, and it follows that $K = \mathfrak{m}K$. On the other hand, K is a quotient of F, therefore finite over A, so that $K = 0$ by NAK and $F \simeq M$.

The result was proved by Kaplansky [2] without the assumption that M is finite. He proves first of all the following lemma, which holds for any ring (possibly non-commutative).

Lemma 1. Let R be any ring, and F an R-module which is a direct sum of countably generated submodules; if M is an arbitrary direct summand of F then M is also a direct sum of countably generated submodules.

Proof of Lemma 1. Suppose that $F = M \oplus N$, and that $F = \bigoplus_{\lambda\in\Lambda} E_\lambda$, where each E_λ is countably generated. By transfinite induction, we construct a well-ordered family $\{F_\alpha\}$ of submodules of F with the following properties:

(i) if $\alpha < \beta$ then $F_\alpha \subset F_\beta$,
(ii) $F = \bigcup_\alpha F_\alpha$,
(iii) if α is a limiting ordinal then $F_\alpha = \bigcup_{\beta<\alpha} F_\beta$,
(iv) $F_{\alpha+1}/F_\alpha$ is countably generated,
(v) $F_\alpha = M_\alpha \oplus N_\alpha$, where $M_\alpha = M \cap F_\alpha$, $N_\alpha = N \cap F_\alpha$,
(vi) each F_α is a direct sum of E_λ taken over a suitable subset of Λ.

We now construct such a family $\{F_\alpha\}$. Firstly, set $F_0 = (0)$. For an ordinal α, assume that F_β has been defined for all ordinals $\beta < \alpha$. If α is a limiting ordinal, set $F_\alpha = \bigcup_{\beta<\alpha} F_\beta$. If α is of the form $\alpha = \beta + 1$, let Q_1 be any one of the E_λ not contained in F_β (if $F_\beta = F$ then the construction stops at F_β). Take a set $x_{11}, x_{12}, \ldots$ of generators of Q_1, and decompose x_{11} into its M- and N-components; now let Q_2 be the direct sum of the finitely many E_λ which are necessary to write each of these two components in the decomposition $F = \oplus E_\lambda$, and let $x_{21}, x_{22}, \ldots$ be generators of Q_2. Next decompose x_{12} into its M- and N-components, let Q_3 be the direct sum of the finitely many E_λ needed to write these components, and let $x_{31}, x_{32}, \ldots$ be generators of Q_3. Then carry out the same procedure with x_{21}, getting $x_{41}, x_{42}, \ldots$, then do the same for x_{13}. Carrying out the same procedure for each of the x_{ij} in the order $x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \ldots$ we get countably many elements x_{ij}. We let F_α be the submodule of F generated by F_β and the x_{ij}, and this satisfies all our requirements. This gives the family $\{F_\alpha\}$.

Now $M = \bigcup M_\alpha$, with each M_α a direct summand of F, and $M_{\alpha+1} \supset M_\alpha$, so that M_α is also a direct summand of $M_{\alpha+1}$. Moreover,

$$F_{\alpha+1}/F_\alpha = (M_{\alpha+1}/M_\alpha) \oplus (N_{\alpha+1}/N_\alpha),$$