CHAPTER III

Modules

Although this chapter is logically self-contained and prepares for future topics, in practice readers will have had some acquaintance with vector spaces over a field. We generalize this notion here to modules over rings. It is a standard fact (to be reproved) that a vector space has a basis, but for modules this is not always the case. Sometimes they do; most often they do not. We shall look into cases where they do.

For examples of modules and their relations to those which have a basis, the reader should look at the comments made at the end of §4.

§1. BASIC DEFINITIONS

Let A be a ring. A **left module** over A, or a left A-module M is an abelian group, usually written additively, together with an operation of A on M (viewing A as a multiplicative monoid by **RI 2**), such that, for all $a, b \in A$ and $x, y \in M$ we have

$$(a + b)x = ax + bx \quad \text{and} \quad a(x + y) = ax + ay.$$

We leave it as an exercise to prove that $a(-x) = -(ax)$ and that $0x = 0$. By definition of an operation, we have $1x = x$.

In a similar way, one defines a **right A-module**. We shall deal only with left A-modules, unless otherwise specified, and hence call these simply **A-modules**, or even **modules** if the reference is clear.

Let M be an A-module. By a **submodule** N of M we mean an additive subgroup such that $AN \subset N$. Then N is a module (with the operation induced by that of A on M).

Examples

We note that A is a module over itself.

Any commutative group is a $\mathbf{Z}$-module.

An additive group consisting of 0 alone is a module over any ring.

Any left ideal of A is a module over A.

Let J be a two-sided ideal of A. Then the factor ring A/J is actually a module over A. If $a \in A$ and $x + J$ is a coset of J in A, then one defines the operation to be $a(x + J) = ax + J$. The reader can verify at once that this defines a module structure on A/J. More general, if M is a module and N a submodule, we shall define the factor module below. Thus if L is a left ideal of A, then A/L is also a module. For more examples in this vein, see §4.

A module over a field is called a **vector space**. Even starting with vector spaces, one is led to consider modules over rings. Indeed, let V be a vector space over the field K. The reader no doubt already knows about linear maps (which will be recalled below systematically). Let R be the ring of all linear maps of V into itself. Then V is a module over R. Similarly, if $V = K^n$ denotes the vector space of (vertical) n-tuples of elements of K, and R is the ring of $n \times n$ matrices with components in K, then V is a module over R. For more comments along these lines, see the examples at the end of §2.

Let S be a non-empty set and M an A-module. Then the set of maps $\mathrm{Map}(S, M)$ is an A-module. We have already noted previously that it is a commutative group, and for $f \in \mathrm{Map}(S, M)$, $a \in A$ we define af to be the map such that $(af)(s) = af(s)$. The axioms for a module are then trivially verified.

For further examples, see the end of this section.

For the rest of this section, we deal with a fixed ring A, and hence may omit the prefix A-.

Let A be an *entire* ring and let M be an A-module. We define the **torsion submodule** M_{tor} to be the subset of elements $x \in M$ such that there exists $a \in A$, $a \neq 0$ such that $ax = 0$. It is immediately verified that M_{tor} is a submodule. Its structure in an important case will be determined in §7.

Let $\mathfrak{a}$ be a left ideal, and M a module. We define $\mathfrak{a}M$ to be the set of all elements

$$a_1x_1 + \cdots + a_nx_n$$

with $a_i \in \mathfrak{a}$ and $x_i \in M$. It is obviously a submodule of M. If $\mathfrak{a}$, $\mathfrak{b}$ are left ideals, then we have associativity, namely

$$\mathfrak{a}(\mathfrak{b}M) = (\mathfrak{a}\mathfrak{b})M.$$

We also have some obvious distributivities, like $(\mathfrak{a} + \mathfrak{b})M = \mathfrak{a}M + \mathfrak{b}M$. If N, N' are submodules of M, then $\mathfrak{a}(N + N') = \mathfrak{a}N + \mathfrak{a}N'$.

Let M be an A-module, and N a submodule. We shall define a module structure on the factor group M/N (for the additive group structure). Let $x + N$ be a coset of N in M, and let $a \in A$. We define $a(x + N)$ to be the coset $ax + N$. It is trivial to verify that this is well defined (i.e. if y is in the same coset as x, then ay is in the same coset as ax), and that this is an operation of A on M/N satisfying the required condition, making M/N into a module, called the **factor module** of M by N.

By a **module-homomorphism** one means a map

$$f: M \to M'$$

of one module into another (over the same ring A), which is an additive group-homomorphism, and such that

$$f(ax) = af(x)$$

for all $a \in A$ and $x \in M$. It is then clear that the collection of A-modules is a category, whose morphisms are the module-homomorphisms usually also called homomorphisms for simplicity, if no confusion is possible. If we wish to refer to the ring A, we also say that f is an **A-homomorphism**, or also that it is an **A-linear map**.

If M is a module, then the identity map is a homomorphism. For any module M', the map $\zeta: M \to M'$ such that $\zeta(x) = 0$ for all $x \in M$ is a homomorphism, called **zero**.

In the next section, we shall discuss the homomorphisms of a module into itself, and as a result we shall give further examples of modules which arise in practice. Here we continue to tabulate the translation of basic properties of groups to modules.

Let M be a module and N a submodule. We have the canonical additive group-homomorphism

$$f: M \to M/N$$

and one verifies trivially that it is a module-homomorphism.

Equally trivially, one verifies that f is universal in the category of homomorphisms of M whose kernel contains N.

If $f: M \to M'$ is a module-homomorphism, then its kernel and image are submodules of M and M' respectively (trivial verification).

Let $f: M \to M'$ be a homomorphism. By the **cokernel** of f we mean the factor module $M'/\operatorname{Im} f = M'/f(M)$. One may also mean the canonical homomorphism

$M' \to M'/f(M)$ rather than the module itself. The context should make clear which is meant. Thus the cokernel is a factor module of M'.

Canonical homomorphisms discussed in Chapter I, §3 apply to modules *mutatis mutandis*. For the convenience of the reader, we summarise these homomorphisms:

Let N, N' be two submodules of a module M. Then $N + N'$ is also a submodule, and we have an isomorphism

$$N/(N \cap N') \approx (N + N')/N'.$$

If $M \supset M' \supset M''$ are modules, then

$$(M/M'')/(M'/M'') \approx M/M'.$$

If $f: M \to M'$ is a module-homomorphism, and N' is a submodule of M', then $f^{-1}(N')$ is a submodule of M and we have a canonical injective homomorphism

$$\bar{f}: M/f^{-1}(N') \to M'/N'.$$

If f is surjective, then $\bar{f}$ is a module-isomorphism.

The proofs are obtained by verifying that all homomorphisms which appeared when dealing with abelian groups are now A-homomorphisms of modules. We leave the verification to the reader.

As with groups, we observe that a module-homomorphism which is bijective is a module-isomorphism. Here again, the proof is the same as for groups, adding only the observation that the inverse map, which we know is a group-isomorphism, actually is a module-isomorphism. Again, we leave the verification to the reader.

As with abelian groups, we define a sequence of module-homomorphisms

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

to be **exact** if $\operatorname{Im} f = \operatorname{Ker} g$. We have an exact sequence associated with a submodule N of a module M, namely

$$0 \to N \to M \to M/N \to 0,$$

the map of N into M being the inclusion, and the subsequent map being the canonical map. The notion of exactness is due to Eilenberg-Steenrod.

If a homomorphism $u: N \to M$ is such that

$$0 \to N \xrightarrow{u} M$$

is exact, then we also say that u is a **monomorphism** or an **embedding**. Dually, if

$$N \xrightarrow{u} M \to 0$$

is exact, we say that u is an **epimorphism**.

Algebras

There are some things in mathematics which satisfy all the axioms of a ring except for the existence of a unit element. We gave the example of $L^1(\mathbf{R})$ in Chapter II, §1. There are also some things which do not satisfy associativity, but satisfy distributivity. For instance let R be a ring, and for $x, y \in R$ define the **bracket product**

$$[x, y] = xy - yx.$$

Then this bracket product is not associative in most cases when R is not commutative, but it satisfies the distributive law.

Examples. A typical example is the ring of differential operators with C^∞ coefficients, operating on the ring of C^∞ functions on an open set in $\mathbf{R}^n$. The bracket product

$$[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$$

of two differential operators is again a differential operator. In the theory of Lie groups, the tangent space at the origin also has such a bracket product.

Such considerations lead us to define a more general notion than a ring. Let A be a commutative ring. Let E, F be modules. By a **bilinear map**

$$g: E \times E \to F$$

we mean a map such that given $x \in E$, the map $y \mapsto g(x, y)$ is A-linear, and given $y \in E$, the map $x \mapsto g(x, y)$ is A-linear. By an A-**algebra** we mean a module together with a bilinear map $g: E \times E \to E$. We view such a map as a law of composition on E. But in this book, unless otherwise specified, we shall assume that our algebras are associative and have a unit element.

Aside from the examples already mentioned, we note that the group ring $A[G]$ (or monoid ring when G is a monoid) is an A-algebra, also called the **group** (or **monoid**) **algebra**. Actually the group algebra can be viewed as a special case of the following situation.

Let $f: A \to B$ be a ring-homomorphism such that $f(A)$ is contained in the center of B, i.e., $f(a)$ commutes with every element of B for every $a \in A$. Then we may view B as an A-module, defining the operation of A on B by the map

$$(a, b) \mapsto f(a)b$$

for all $a \in A$ and $b \in B$. The axioms for a module are trivially satisfied, and the multiplicative law of composition $B \times B \to B$ is clearly bilinear (i.e., A-bilinear). In this book, unless otherwise specified, by an **algebra** over A, we shall always mean a ring-homomorphism as above. We say that the algebra is **finitely generated** if B is finitely generated as a ring over $f(A)$.

Several examples of modules over a polynomial algebra or a group algebra will be given in the next section, where we also establish the language of representations.

§2. THE GROUP OF HOMOMORPHISMS

Let A be a ring, and let X, X' be A-modules. We denote by $\mathrm{Hom}_A(X', X)$ the set of A-homomorphisms of X' into X. Then $\mathrm{Hom}_A(X', X)$ is an abelian group, the law of addition being that of addition for mappings into an abelian group.

If A *is commutative* then we can make $\mathrm{Hom}_A(X', X)$ into an A-module, by defining af for $a \in A$ and $f \in \mathrm{Hom}_A(X', X)$ to be the map such that

$$(af)(x) = af(x).$$

The verification that the axioms for an A-module are satisfied is trivial. However, if A is not commutative, then we view $\mathrm{Hom}_A(X', X)$ simply as an abelian group.

We also view Hom_A as a functor. It is actually a functor of two variables, contravariant in the first and covariant in the second. Indeed, let Y be an A-module, and let

$$X' \xrightarrow{f} X$$

be an A-homomorphism. Then we get an induced homomorphism

$$\mathrm{Hom}_A(f, Y) : \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X', Y)$$

(reversing the arrow!) given by

$$g \mapsto g \circ f.$$

This is illustrated by the following sequence of maps:

$$X' \xrightarrow{f} X \xrightarrow{g} Y.$$

The fact that $\mathrm{Hom}_A(f, Y)$ is a homomorphism is simply a rephrasing of the property $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$, which is trivially verified. If $f = \mathrm{id}$, then composition with f acts as an identity mapping on g, i.e. $g \circ \mathrm{id} = g$.

If we have a sequence of A-homomorphisms

$$X' \to X \to X'',$$

then we get an induced sequence

$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y).$$

Proposition 2.1. *A sequence*

$$X' \xrightarrow{\lambda} X \to X'' \to 0$$

is exact if and only if the sequence

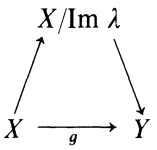
$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y) \leftarrow 0$$

is exact for all Y.

Proof. This is an important fact, whose proof is easy. For instance, suppose the first sequence is exact. If $g : X'' \to Y$ is an A-homomorphism, its image in $\mathrm{Hom}_A(X, Y)$ is obtained by composing g with the surjective map of X on X''. If this composition is 0, it follows that $g = 0$ because $X \to X''$ is surjective. As another example, consider a homomorphism $g : X \to Y$ such that the composition

$$X' \xrightarrow{\lambda} X \xrightarrow{g} Y$$

is 0. Then g vanishes on the image of λ. Hence we can factor g through the factor module,



Since $X \to X''$ is surjective, we have an isomorphism

$$X/\mathrm{Im}\ \lambda \leftrightarrow X''.$$

Hence we can factor g through X'', thereby showing that the kernel of

$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y)$$

is contained in the image of

$$\mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y).$$

The other conditions needed to verify exactness are left to the reader. So is the converse.

We have a similar situation with respect to the second variable, but then the functor is covariant. Thus if X is fixed, and we have a sequence of A-homomorphisms

$$Y' \to Y \to Y'',$$

then we get an induced sequence

$$\mathrm{Hom}_A(X, Y') \to \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X, Y'').$$

Proposition 2.2. *A sequence*

$$0 \to Y' \to Y \to Y'',$$

is exact if and only if

$$0 \to \mathrm{Hom}_A(X, Y') \to \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X, Y'')$$

is exact for all X.

The verification will be left to the reader. It follows at once from the definitions.

We note that to say that

$$0 \to Y' \to Y$$

is exact means that Y' is embedded in Y, i.e. is isomorphic to a submodule of Y. A homomorphism into Y' can be viewed as a homomorphism into Y if we have $Y' \subset Y$. This corresponds to the injection

$$0 \to \mathrm{Hom}_A(X, Y') \to \mathrm{Hom}_A(X, Y).$$

Let $\mathrm{Mod}(A)$ and $\mathrm{Mod}(B)$ be the categories of modules over rings A and B, and let $F: \mathrm{Mod}(A) \to \mathrm{Mod}(B)$ be a functor. One says that F is **exact** if F transforms exact sequences into exact sequences. We see that the Hom functor in either variable need not be exact if the other variable is kept fixed. In a later section, we define conditions under which exactness is preserved.

Endomorphisms. Let M be an A-module. From the relations

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$$

and its analogue on the right, namely

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2,$$

and the fact that there is an identity for composition, namely id_M, we conclude that $\mathrm{Hom}_A(M, M)$ is a ring, the multiplication being defined as composition of mappings. If n is an integer $\geqq 1$, we can write f^n to mean the iteration of f with itself n times, and define f^0 to be id. According to the general definition of endomorphisms in a category, we also write $\mathrm{End}_A(M)$ instead of $\mathrm{Hom}_A(M, M)$, and we call $\mathrm{End}_A(M)$ the ring of **endomorphisms**.

Since an A-module M is an abelian group, we see that $\mathrm{Hom}_{\mathbf{Z}}(M, M)$ (= set of group-homomorphisms of M into itself) is a ring, and that we could have defined an operation of A on M to be a ring-homomorphism $A \to \mathrm{Hom}_{\mathbf{Z}}(M, M)$.

Let A be *commutative*. Then M is a module over $\mathrm{End}_A(M)$. If R is a subring of $\mathrm{End}_A(M)$ then M is *a fortiori* a module over R. More generally, let R be a ring and let $\rho: R \to \mathrm{End}_A(M)$ be a ring homomorphism. Then ρ is called a **representation** of R on M. This occurs especially if $A = K$ is a field. The linear algebra of representations of a ring will be discussed in Part III, in several contexts, mostly finite-dimensional. Infinite-dimensional examples occur in analysis, but then the representation theory mixes algebra with analysis, and thus goes beyond the level of this course.

Example. Let K be a field and let V be a vector space over K. Let $D: V \to V$ be an endomorphism (K-linear map). For every polynomial $P(X) \in K[X]$, $P(X) = \sum a_i X^i$ with $a_i \in K$, we can define

$$P(D) = \sum a_i D^i \colon V \to V$$

as an endomorphism of V. The association $P(X) \mapsto P(D)$ gives a representation

$$\rho \colon K[X] \to \mathrm{End}_K(V),$$

which makes V into a $K[X]$-module. It will be shown in Chapter IV that $K[X]$ is a principal ring. In §7 we shall give a general structure theorem for modules over principal rings, which will be applied to the above example in the context of linear algebra for finite-dimensional vector spaces in Chapter XIV, §3. Readers acquainted with basic linear algebra from an undergraduate course may wish to read Chapter XIV already at this point.

Examples for infinite-dimensional vector spaces occur in analysis. For instance, let V be the vector space of complex-valued C^∞ functions on $\mathbf{R}$. Let $D = d/dt$ be the derivative (if t is the variable). Then $D \colon V \to V$ is a linear map, and $\mathbf{C}[X]$ has the representation $\rho \colon \mathbf{C}[X] \to \mathrm{End}_{\mathbf{C}}(V)$ given by $P \mapsto P(D)$. A similar situation exists in several variables, when we let V be the vector space of C^∞ functions in n variables on an open set of $\mathbf{R}^n$. Then we let $D_i = \partial/\partial t_i$ be the partial derivative with respect to the i-th variable ($i = 1, \ldots, n$). We obtain a representation

$$\rho \colon \mathbf{C}[X_1, \ldots, X_n] \to \mathrm{End}_{\mathbf{C}}(V)$$

such that $\rho(X_i) = D_i$.

Example. Let H be a Hilbert space and let A be a bounded hermitian operator on A. Then one considers the homomorphism $\mathbf{R}[X] \to \mathbf{R}[A] \subset \mathrm{End}(H)$, from the polynomial ring into the algebra of endomorphisms of H, and one extends this homomorphism to the algebra of continuous functions on the spectrum of A. *Cf.* my *Real and Functional Analysis*, Springer Verlag, 1993.

Representations form a category as follows. We define a **morphism** of a representation $\rho \colon R \to \mathrm{End}_A(M)$ into a representation $\rho' \colon R \to \mathrm{End}_A(M')$, or in other words a **homomorphism of one representation of R to another**, to be an A-module homomorphism $h \colon M \to M'$ such that the following diagram is commutative for every $\alpha \in R$:

$$\begin{array}{ccc} M & \xrightarrow{h} & M' \\ {\scriptstyle \rho(\alpha)}\downarrow & & \downarrow{\scriptstyle \rho'(\alpha)} \\ M & \xrightarrow[h]{} & M' \end{array}$$

In the case when h is an isomorphism, then we may replace the above diagram by the commutative diagram

$$\begin{array}{ccc} & & \mathrm{End}_A(M) \\ & {\scriptstyle \rho}\nearrow & \downarrow{\scriptstyle [h]} \\ R & & \\ & {\scriptstyle \rho'}\searrow & \mathrm{End}_A(M') \end{array}$$

where the symbol $[h]$ denotes conjugation by h, i.e. for $f \in \mathrm{End}_A(M)$ we have $[h]f = h \circ f \circ h^{-1}$.

Representations: from a monoid to the monoid algebra. Let G be a monoid. By a **representation of** G on an A-module M, we mean a homomorphism $\rho: G \to \mathrm{End}_A(M)$ of G into the multiplicative monoid of $\mathrm{End}_A(M)$. Then we may extend ρ to a homomorphism of the monoid algebra

$$A[G] \to \mathrm{End}_A(M),$$

by letting

$$\rho\left(\sum_{x \in G} a_x x\right) = \sum_{x \in G} a_x \rho(x).$$

It is immediately verified that this extension of ρ to $A[G]$ is a ring homomorphism, coinciding with the given ρ on elements of G.

Examples: modules over a group ring. The next examples will follow a certain pattern associated with groups of automorphisms. Quite generally, suppose we have some category of objects, and to each object K there is associated an abelian group $F(K)$, functorially with respect to isomorphisms. This means that if $\sigma: K \to K'$ is an isomorphism, then there is an associated isomorphism $F(\sigma): F(K) \to F(K')$ such that $F(\mathrm{id}_K) = \mathrm{id}_{K'}$ and $F(\sigma\tau) = F(\sigma) \circ F(\tau)$. Then the group of automorphisms $\mathrm{Aut}(K)$ of an object operates on $F(K)$; that is, we have a natural homomorphism

$$\mathrm{Aut}(K) \to \mathrm{Aut}(F(K)) \quad \text{given by} \quad \sigma \mapsto F(\sigma).$$

Let $G = \mathrm{Aut}(K)$. Then $F(K)$ (written additively) can be made into a module over the group ring $\mathbf{Z}[G]$ as above. Given an element $\alpha = \sum a_\sigma \sigma \in \mathbf{Z}[G]$, with $a_\sigma \in \mathbf{Z}$, and an element $x \in F(K)$, we define

$$\alpha x = \sum a_\sigma F(\sigma) x.$$

The conditions defining a module are trivially satisfied. We list several concrete cases from mathematics at large, so there are no holds barred on the terminology.

Let K be a number field (i.e. a finite extension of the rational numbers). Let G be its group of automorphisms. Associated with K we have the following objects:

the ring of algebraic integers $\mathfrak{o}_K$;

the group of units $\mathfrak{o}_K^*$;

the group of ideal classes $C(K)$;

the group of roots of unity $\boldsymbol{\mu}(K)$.

Then G operates on each of those objects, and one problem is to determine the structure of these objects as $\mathbf{Z}[G]$-modules. Already for cyclotomic fields this

determination gives rise to substantial theories and to a number of unsolved problems.

Suppose that K is a Galois extension of k with Galois group G (see Chapter VI). Then we may view K itself as a module over the group ring $k[G]$. In Chapter VI, §13 we shall prove that K is isomorphic to $k[G]$ as module over $k[G]$ itself.

In topology, one considers a space X_0 and a finite covering X. Then $\mathrm{Aut}(X/X_0)$ operates on the homology of X, so this homology is a module over the group ring.

With more structure, suppose that X is a projective non-singular variety, say over the complex numbers. Then to X we can associate:

the group of divisor classes (Picard group) $\mathrm{Pic}(X)$;

in a given dimension, the group of cycle classes or Chow group $\mathrm{CH}^p(X)$;

the ordinary homology of X;

the sheaf cohomology in general.

If X is defined over a field K finitely generated over the rationals, we can associate a fancier cohomology defined algebraically by Grothendieck, and functorial with respect to the operation of Galois groups.

Then again all these objects can be viewed as modules over the group ring of automorphism groups, and major problems of mathematics consist in determining their structure. I direct the reader here to two surveys, which contain extensive bibliographies.

[CCFT 91] P. CASSOU-NOGUES, T. CHINBURG, A. FRÖHLICH, M. J. TAYLOR, *L*-functions and Galois modules, in *L-functions and Arithmetic* J. Coates and M. J. Taylor (eds.), *Proceedings of the Durham Symposium* July 1989, *London Math, Soc. Lecture Note Series* **153**, Cambridge University Press (1991), pp. 75-139

[La 82] S. LANG, Units and class groups in number theory and algebraic geometry, *Bull. AMS* **Vol. 6 No. 3** (1982), pp. 253-316

§3. DIRECT PRODUCTS AND SUMS OF MODULES

Let A be a ring. Let $\{M_i\}_{i\in I}$ be a family of modules. We defined their direct product as abelian groups in Chapter I, §9. Given an element $(x_i)_{i\in I}$ of the direct product, and $a \in A$, we define $a(x_i) = (ax_i)$. In other words, we multiply by an element a componentwise. Then the direct product $\prod M_i$ is an A-module. The reader will verify at once that it is also a **direct product** in the category of A-modules.

Similarly, let

$$M = \bigoplus_{i \in I} M_i$$

be their direct sum as abelian groups. We define on M a structure of A-module: If $(x_i)_{i \in I}$ is an element of M, i.e. a family of elements $x_i \in M_i$ such that $x_i = 0$ for almost all i, and if $a \in A$, then we define

$$a(x_i)_{i \in I} = (ax_i)_{i \in I},$$

that is we define multiplication by a componentwise. It is trivially verified that this is an operation of A on M which makes M into an A-module. If one refers back to the proof given for the existence of direct sums in the category of abelian groups, one sees immediately that this proof now extends in the same way to show that M is a direct sum of the family $\{M_i\}_{i \in I}$ as A-modules. (For instance, the map

$$\lambda_j : M_j \to M$$

such that $\lambda_j(x)$ has j-th component equal to x and i-th component equal to 0 for $i \neq j$ is now seen to be an A-homomorphism.)

This direct sum is a **coproduct in the category of A-modules**. Indeed, the reader can verify at once that given a family of A-homomorphisms $\{f_i : M_i \to N\}$, the map f defined as in the proof for abelian groups is also an A-isomorphism and has the required properties. See Proposition 7.1 of Chapter I.

When I is a finite set, there is a useful criterion for a module to be a direct product.

Proposition 3.1. *Let M be an A-module and n an integer $\geqq 1$. For each $i = 1, \ldots, n$ let $\varphi_i : M \to M$ be an A-homomorphism such that*

$$\sum_{i=1}^{n} \varphi_i = \mathrm{id} \quad \text{and} \quad \varphi_i \circ \varphi_j = 0 \qquad \text{if } i \neq j.$$

Then $\varphi_i^2 = \varphi_i$ for all i. Let $M_i = \varphi_i(M)$, and let $\varphi : M \to \prod M_i$ be such that

$$\varphi(x) = (\varphi_1(x), \ldots, \varphi_n(x)).$$

Then φ is an A-isomorphism of M onto the direct product $\prod M_i$.

Proof. For each j, we have

$$\varphi_j = \varphi_j \circ \mathrm{id} = \varphi_j \circ \sum_{i=1}^{n} \varphi_i = \varphi_j \circ \varphi_j = \varphi_j^2,$$

thereby proving the first assertion. It is clear that φ is an A-homomorphism. Let x be in its kernel. Since

$$x = \mathrm{id}(x) = \sum_{i=1}^{n} \varphi_i(x)$$

we conclude that $x = 0$, so φ is injective. Given elements $y_i \in M_i$ for each $i = 1, \ldots, n$, let $x = y_1 + \cdots + y_n$. We obviously have $\varphi_j(y_i) = 0$ if $i \neq j$. Hence

$$\varphi_j(x) = y_j$$

for each $j = 1, \ldots, n$. This proves that φ is surjective, and concludes the proof of our proposition.

We observe that when I is a finite set, the direct sum and the direct product are equal.

Just as with abelian groups, we use the symbol $\oplus$ to denote direct sum.

Let M be a module over a ring A and let S be a subset of M. By a **linear combination** of elements of S (with coefficients in A) one means a sum

$$\sum_{x \in S} a_x x$$

where $\{a_x\}$ is a set of elements of A, almost all of which are equal to 0. These elements a_x are called the **coefficients** of the linear combination. Let N be the set of all linear combinations of elements of S. Then N is a submodule of M, for if

$$\sum_{x \in S} a_x x \quad \text{and} \quad \sum_{x \in S} b_x x$$

are two linear combinations, then their sum is equal to

$$\sum_{x \in S} (a_x + b_x)x,$$

and if $c \in A$, then

$$c\left(\sum_{x \in S} a_x x\right) = \sum_{x \in S} c a_x x,$$

and these elements are again linear combinations of elements of S. We shall call N the submodule **generated** by S, and we call S a set of **generators** for N. We sometimes write $N = A\langle S \rangle$. If S consists of one element x, the module generated by x is also written Ax, or simply (x), and sometimes we say that (x) is a **principal module**.

A module M is said to be **finitely generated**, or of **finite type**, or **finite** over A, if it has a finite number of generators.

A *subset* S of a module M is said to be **linearly independent** (over A) if whenever we have a linear combination

$$\sum_{x \in S} a_x x$$

which is equal to 0, then $a_x = 0$ for all $x \in S$. If S is linearly independent and if two linear combinations

$$\sum a_x x \quad \text{and} \quad \sum b_x x$$

are equal, then $a_x = b_x$ for all $x \in S$. Indeed, subtracting one from the other yields $\sum (a_x - b_x)x = 0$, whence $a_x - b_x = 0$ for all x. If S is linearly independent we shall also say that its elements are linearly independent. Similarly, a *family* $\{x_i\}_{i \in I}$ of elements of M is said to be linearly independent if whenever we have a linear combination

$$\sum_{i \in I} a_i x_i = 0,$$

then $a_i = 0$ for all i. A subset S (resp. a family $\{x_i\}$) is called **linearly dependent** if it is not linearly independent, i.e. if there exists a relation

$$\sum_{x \in S} a_x x = 0 \quad \text{resp.} \quad \sum_{i \in I} a_i x_i = 0$$

with not all a_x (resp. a_i) $= 0$. **Warning.** Let x be a single element of M which is linearly independent. Then the family $\{x_i\}_{i=1,\ldots,n}$ such that $x_i = x$ for all i is linearly dependent if $n > 1$, but the set consisting of x itself is linearly independent.

Let M be an A-module, and let $\{M_i\}_{i \in I}$ be a family of submodules. Since we have inclusion-homomorphisms

$$\lambda_i : M_i \to M$$

we have an induced homomorphism

$$\lambda_* : \bigoplus M_i \to M$$

which is such that for any family of elements $(x_i)_{i \in I}$, all but a finite number of which are 0, we have

$$\lambda_*((x_i)) = \sum_{i \in I} x_i.$$

If λ_* is an isomorphism, then we say that the family $\{M_i\}_{i \in I}$ is a **direct sum decomposition** of M. This is obviously equivalent to saying that every element of M has a unique expression as a sum

$$\sum x_i$$

with $x_i \in M_i$, and almost all $x_i = 0$. By abuse of notation, we also write

$$M = \bigoplus M_i$$

in this case.

If the family $\{M_i\}$ is such that every element of M has *some* expression as a sum $\sum x_i$ (not necessarily unique), then we write $M = \sum M_i$. In any case, if $\{M_i\}$ is an arbitrary family of submodules, the image of the homomorphism λ_* above is a submodule of M, which will be denoted by $\sum M_i$.

If M is a module and N, N' are two submodules such that $N + N' = M$ and $N \cap N' = 0$, then we have a module-isomorphism

$$M \approx N \oplus N',$$

just as with abelian groups, and similarly with a finite number of submodules.

We note, of course, that our discussion of abelian groups is a special case of our discussion of modules, simply by viewing abelian groups as modules over $\mathbf{Z}$. However, it seems usually desirable (albeit inefficient) to develop first some statements for abelian groups, and then point out that they are valid (obviously) for modules in general.

Let M, M', N be modules. Then we have an isomorphism of abelian groups

$$\boxed{\mathrm{Hom}_A(M \oplus M', N) \xleftrightarrow{\approx} \mathrm{Hom}_A(M, N) \times \mathrm{Hom}_A(M', N),}$$

and similarly

$$\boxed{\mathrm{Hom}_A(N, M \times M') \xleftrightarrow{\approx} \mathrm{Hom}_A(N, M) \times \mathrm{Hom}_A(N, M').}$$

The first one is obtained as follows. If $f : M \oplus M' \to N$ is a homomorphism, then f induces a homomorphism $f_1 : M \to N$ and a homomorphism $f_2 : M' \to N$ by composing f with the injections of M and M' into their direct sum respectively:

$$M \to M \oplus \{0\} \subset M \oplus M' \xrightarrow{f} N,$$

$$M' \to \{0\} \oplus M' \subset M \oplus M' \xrightarrow{f} N.$$

We leave it to the reader to verify that the association

$$f \mapsto (f_1, f_2)$$

gives an isomorphism as in the first box. The isomorphism in the second box is obtained in a similar way. Given homomorphisms

$$f_1 : N \to M$$

and

$$f_2 : N \to M'$$

we have a homomorphism $f: N \to M \times M'$ defined by

$$f(x) = (f_1(x), f_2(x)).$$

It is trivial to verify that the association

$$(f_1, f_2) \mapsto f$$

gives an isomorphism as in the second box.

Of course, the direct sum and direct product of two modules are isomorphic, but we distinguished them in the notation for the sake of functoriality, and to fit the infinite case, see Exercise 22.

Proposition 3.2. *Let* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *be an exact sequence of modules. The following conditions are equivalent:*

1. *There exists a homomorphism* $\varphi: M'' \to M$ *such that* $g \circ \varphi = \mathrm{id}$.
2. *There exists a homomorphism* $\psi: M \to M'$ *such that* $\psi \circ f = \mathrm{id}$.

If these conditions are satisfied, then we have isomorphisms:

$$M = \operatorname{Im} f \oplus \operatorname{Ker} \psi, \qquad M = \operatorname{Ker} g \oplus \operatorname{Im} \varphi,$$

$$M \approx M' \oplus M''.$$

Proof. Let us write the homomorphisms on the right:

$$M \underset{\varphi}{\overset{g}{\rightleftarrows}} M'' \to 0.$$

Let $x \in M$. Then

$$x - \varphi(g(x))$$

is in the kernel of g, and hence $M = \operatorname{Ker} g + \operatorname{Im} \varphi$.

This sum is direct, for if

$$x = y + z$$

with $y \in \operatorname{Ker} g$ and $z \in \operatorname{Im} \varphi$, $z = \varphi(w)$ with $w \in M''$, and applying g yields $g(x) = w$. Thus w is uniquely determined by x, and therefore z is uniquely determined by x. Hence so is y, thereby proving the sum is direct.

The arguments concerning the other side of the sequence are similar and will be left as exercises, as well as the equivalence between our conditions. When these conditions are satisfied, the exact sequence of Proposition 3.2 is said to **split**. One also says that ψ **splits** f and φ **splits** g.

Abelian categories

Much in the theory of modules over a ring is arrow-theoretic. In fact, one needs only the notion of kernel and cokernel (factor modules). One can axiomatize the special notion of a category in which many of the arguments are valid, especially the arguments used in this chapter. Thus we give this axiomatization now, although for concreteness, at the beginning of the chapter, we continue to use the language of modules. Readers should strike their own balance when they want to slide into the more general framework.

Consider first a category $\mathfrak{A}$ such that $\mathrm{Mor}(E, F)$ is an abelian group for each pair of objects E, F of $\mathfrak{A}$, satisfying the following two conditions:

AB 1. The law of composition of morphisms is bilinear, and there exists a zero object 0, i.e. such that $\mathrm{Mor}(0, E)$ and $\mathrm{Mor}(E, 0)$ have precisely one element for each object E.

AB 2. Finite products and finite coproducts exist in the category.

Then we say that $\mathfrak{A}$ is an **additive category**.

Given a morphism $E \xrightarrow{f} F$ in $\mathfrak{A}$, we define a **kernel** of f to be a morphism $E' \to E$ such that for all objects X in the category, the following sequence is exact:

$$0 \to \mathrm{Mor}(X, E') \to \mathrm{Mor}(X, E) \to \mathrm{Mor}(X, F).$$

We define a **cokernel** for f to be a morphism $F \to F''$ such that for all objects X in the category, the following sequence is exact:

$$0 \to \mathrm{Mor}(F'', X) \to \mathrm{Mor}(F, X) \to \mathrm{Mor}(E, X).$$

It is immediately verified that kernels and cokernels are universal in a suitable category, and hence uniquely determined up to a unique isomorphism if they exist.

AB 3. Kernels and cokernels exist.

AB 4. If $f: E \to F$ is a morphism whose kernel is 0, then f is the kernel of its cokernel. If $f: E \to F$ is a morphism whose cokernel is 0, then f is the cokernel of its kernel. A morphism whose kernel and cokernel are 0 is an isomorphism.

A category $\mathfrak{A}$ satisfying the above four axioms is called an **abelian category**.

In an abelian caegory, the group of morphisms is usually denoted by Hom, so for two objects E, F we write

$$\mathrm{Mor}(E, F) = \mathrm{Hom}(E, F).$$

The morphisms are usually called **homomorphisms**. Given an exact sequence

$$0 \to M' \to M,$$

we say that M' is a **subobject** of M, or that the homomorphism of M' into M is a **monomorphism**. Dually, in an exact sequence

$$M \to M'' \to 0,$$

we say that M'' is a **quotient object** of M, or that the homomorphism of M to M'' is an **epimorphism**, instead of saying that it is surjective as in the category of modules. Although it is convenient to think of modules and abelian groups to construct proofs, usually such proofs will involve only arrow-theoretic arguments, and will therefore apply to any abelian category. However, all the abelian categories we shall meet in this book will have elements, and the kernels and cokernels will be defined in a natural fashion, close to those for modules, so readers may restrict their attention to these concrete cases.

Examples of abelian categories. Of course, modules over a ring form an abelian category, the most common one. Finitely generated modules over a Noetherian ring form an abelian category, to be studied in Chapter X.

Let k be a field. We consider pairs (V, A) consisting of a finite-dimensional vector space V over k, and an endomorphism $A: V \to V$. By a **homomorphism** (**morphism**) of such pairs $f: (V, A) \to (W, B)$ we mean a k-homomorphism $f: V \to W$ such that the following diagram is commutative:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle A}\downarrow & & \downarrow{\scriptstyle B} \\ V & \xrightarrow[f]{} & W \end{array}$$

It is routinely verified that such pairs and the above defined morphisms form an abelian category. Its elements will be studied in Chapter XIV.

Let k be a field and let G be a group. Let $\mathrm{Mod}_k(G)$ be the category of finite-dimensional vector spaces V over k, with an operation of G on V, i.e. a homomorphism $G \to \mathrm{Aut}_k(V)$. A homomorphism (morphism) in that category is a k-homomorphism $f: V \to W$ such that $f(ax) = af(x)$ for all $x \in V$ and $a \in G$. It is immediate that $\mathrm{Mod}_k(G)$ is an abelian category. This category will be studied especially in Chapter XVIII.

In Chapter XX, §1 we shall consider the category of complexes of modules over a ring. This category of complexes is an abelian category.

In topology and differential geometry, the category of vector bundles over a topological space is an abelian category.

Sheaves of abelian groups over a topological space form an abelian category, which will be defined in Chapter XX, §6.

§4. FREE MODULES

Let M be a module over a ring A and let S be a subset of M. We shall say that S is a **basis** of M if S is not empty, if S generates M, and if S is linearly independent. If S is a basis of M, then in particular $M \neq \{0\}$ if $A \neq \{0\}$ and every element of M has a unique expression as a linear combination of elements of S. Similarly, let $\{x_i\}_{i \in I}$ be a non-empty family of elements of M. We say that it is a **basis** of M if it is linearly independent and generates M.

If A is a ring, then as a module over itself, A admits a basis, consisting of the unit element 1.

Let I be a non-empty set, and for each $i \in I$, let $A_i = A$, viewed as an A-module. Let

$$F = \bigoplus_{i \in I} A_i.$$

Then F admits a basis, which consists of the elements e_i of F whose i-th component is the unit element of A_i, and having all other components equal to 0.

By a **free** module we shall mean a module which admits a basis, or the zero module.

Theorem 4.1. *Let A be a ring and M a module over A. Let I be a non-empty set, and let $\{x_i\}_{i \in I}$ be a basis of M. Let N be an A-module, and let $\{y_i\}_{i \in I}$ be a family of elements of N. Then there exists a unique homomorphism $f: M \to N$ such that $f(x_i) = y_i$ for all i.*

Proof. Let x be an element of M. There exists a unique family $\{a_i\}_{i \in I}$ of elements of A such that

$$x = \sum_{i \in I} a_i x_i.$$

We define

$$f(x) = \sum a_i y_i.$$

It is then clear that f is a homomorphism satisfying our requirements, and that it is the unique such, because we must have

$$f(x) = \sum a_i f(x_i).$$

Corollary 4.2. *Let the notation be as in the theorem, and assume that $\{y_i\}_{i \in I}$ is a basis of N. Then the homomorphism f is an isomorphism, i.e. a module-isomorphism.*

Proof. By symmetry, there exists a unique homomorphism

$$g: N \to M$$

such that $g(y_i) = x_i$ for all i, and $f \circ g$ and $g \circ f$ are the respective identity mappings.

Corollary 4.3. *Two modules having bases whose cardinalities are equal are isomorphic.*

Proof. Clear.

We shall leave the proofs of the following statements as exercises.

Let M be a free module over A, with basis $\{x_i\}_{i \in I}$, so that

$$M = \bigoplus_{i \in I} Ax_i.$$

Let $\mathfrak{a}$ be a two sided ideal of A. Then $\mathfrak{a}M$ is a submodule of M. Each $\mathfrak{a}x_i$ is a submodule of Ax_i. *We have an isomorphism* (of A-modules)

$$\boxed{M/\mathfrak{a}M \approx \bigoplus_{i \in I} Ax_i/\mathfrak{a}x_i.}$$

Furthermore, each $Ax_i/\mathfrak{a}x_i$ is isomorphic to $A/\mathfrak{a}$, as A-module.

Suppose in addition that A is commutative. Then $A/\mathfrak{a}$ is a ring. Furthermore $M/\mathfrak{a}M$ is a free module over $A/\mathfrak{a}$, and each $Ax_i/\mathfrak{a}x_i$ is free over $A/\mathfrak{a}$. If $\bar{x}_i$ is the image of x_i under the canonical homomorphism

$$Ax_i \to Ax_i/\mathfrak{a}x_i,$$

then the single element $\bar{x}_i$ is a basis of $Ax_i/\mathfrak{a}x_i$ over $A/\mathfrak{a}$.

All of these statements should be easily verified by the reader. Now let A be an arbitrary commutative ring. A module M is called **principal** if there exists an element $x \in M$ such that $M = Ax$. The map

$$a \mapsto ax \text{ (for } a \in A)$$

is an A-module homomorphism of A onto M, whose kernel is a left ideal $\mathfrak{a}$, and inducing an isomorphism of A-modules

$$A/\mathfrak{a} \approx M.$$

Let M be a finitely generated module, with generators $\{v_1, \ldots, v_n\}$. Let F be a free module with basis $\{e_1, \ldots, e_n\}$. Then there is a unique surjective homomorphism $f\colon F \to M$ such that $f(e_i) = v_i$. The kernel of f is a submodule M_1. Under certain conditions, M_1 is finitely generated (*cf.* Chapter X, §1 on Noetherian rings), and the process can be continued. The systematic study of this process will be carried out in the chapters on resolutions of modules and homology.

Of course, even if M is not finitely generated, one can carry out a similar construction, by using an arbitrary indexing set. Indeed, let $\{v_i\}$ $(i \in I)$ be a family of generators. For each i, let F_i be free with basis consisting of a single element e_i, so $F_i \approx A$. Let F be the direct sum of the modules F_i $(i \in I)$, as in Proposition 3.1. Then we obtain a surjective homomorphism $f\colon F \to M$ such that $f(e_i) = v_i$. Thus every module is a factor module of a free module.

Just as we did for abelian groups in Chapter I, §7, we can also define the **free module** over a ring A **generated by a non-empty set** S. We let $A\langle S\rangle$ be the set of functions $\varphi : S \to A$ such that $\varphi(x) = 0$ for almost all $x \in S$. If $a \in A$ and $x \in S$, we denote by ax the map φ such that $\varphi(x) = a$ and $\varphi(y) = 0$ for $y \neq x$. Then as for abelian groups, given $\varphi \in A\langle S\rangle$ there exist elements $a_i \in A$ and $x_i \in S$ such that

$$\varphi = a_1x_1 + \cdots + a_nx_n.$$

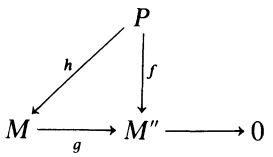
It is immediately verified that the family of functions $\{\delta_x\}$ $(x \in S)$ such that $\delta_x(x) = 1$ and $\delta_x(y) = 0$ for $y \neq x$ form a basis for $A\langle S\rangle$. In other words, the expression of φ as $\sum a_ix_i$ above is unique. This construction can be applied when S is a group or a monoid G, and gives rise to the group algebra as in Chapter II, §5.

Projective modules

There exists another important type of module closely related to free modules, which we now discuss.

Let A be a ring and P a module. The following properties are equivalent, and define what it means for P to be a **projective module**.

P 1. Given a homomorphism $f\colon P \to M''$ and surjective homomorphism $g\colon M \to M''$, there exists a homomorphism $h\colon P \to M$ making the following diagram commutative.



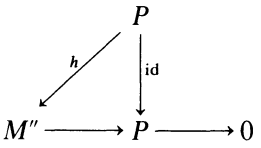
P 2. Every exact sequence $0 \to M' \to M'' \to P \to 0$ splits.

P 3. There exists a module M such that $P \oplus M$ is free, or in words, P is a direct summand of a free module.

P 4. The functor $M \mapsto \mathrm{Hom}_A(P, M)$ is exact.

We prove the equivalence of the four conditions.

Assume **P 1**. Given the exact sequence of **P 2**, we consider the map $f = \mathrm{id}$ in the diagram



Then h gives the desired splitting of the sequence.

Assume **P 2.** Then represent P as a quotient of a free module (cf. Exercise 1) $F \to P \to 0$, and apply **P 2** to this sequence to get the desired splitting, which represents F as a direct sum of P and some module.

Assume **P 3**. Since $\mathrm{Hom}_A(X \oplus Y, M) = \mathrm{Hom}_A(X, M) \oplus \mathrm{Hom}_A(Y, M)$, and since $M \mapsto \mathrm{Hom}_A(F, M)$ is an exact functor if F is free, it follows that $\mathrm{Hom}_A(P, M)$ is exact when P is a direct summand of a free module, which proves **P 4**.

Assume **P 4**. The proof of **P 1** will be left as an exercise.

Examples. It will be proved in the next section that a vector space over a field is always free, i.e. has a basis. Under certain circumstances, it is a theorem that projective modules are free. In §7 we shall prove that a finitely generated projective module over a principal ring is free. In Chapter X, Theorem 4.4 we shall prove that such a module over a local ring is free; in Chapter XVI, Theorem 3.8 we shall prove that a finite flat module over a local ring is free; and in Chapter XXI, Theorem 3.7, we shall prove the Quillen-Suslin theorem that if $A = k[X_1, \ldots, X_n]$ is the polynomial ring over a field k, then every finite projective module over A is free.

Projective modules give rise to the Grothendieck group. Let A be a ring. Isomorphism classes of finite projective modules form a monoid. Indeed, if P is finite projective, let $[P]$ denote its isomorphism class. We define

$$[P] + [Q] = [P \oplus Q].$$

This sum is independent of the choice of representatives P, Q in their class. The conditions defining a monoid are immediately verified. The corresponding Grothendieck group is denoted by $K(A)$.

We can impose a further equivalence relation that P is equivalent to P' if there exist finite free modules F and F' such that $P \oplus F$ is isomorphic to $P' \oplus F'$. Under this equivalence relation we obtain another group denoted by $K_0(A)$. If A is a Dedekind ring (Chapter II, §1 and Exercises 13–19) it can be shown that this group is isomorphic in a natural way with the group of ideal classes $\mathrm{Pic}(A)$ (defined in Chapter II, §1). See Exercises 11, 12, 13. It is also a

problem to determine $K_0(A)$ for as many rings as possible, as explicitly as possible. Algebraic number theory is concerned with $K_0(A)$ when A is the ring of algebraic integers of a number field. The Quillen-Suslin theorem shows if A is the polynomial ring as above, then $K_0(A)$ is trivial.

Of course one can carry out a similar construction with all finite modules. Let $[M]$ denote the isomorphism class of a finite module M. We define the sum to be the direct sum. Then the isomorphism classes of modules over the ring form a monoid, and we can associate to this monoid its Grothendieck group. This construction is applied especially when the ring is commutative. There are many variations on this theme. See for instance the book by Bass, *Algebraic K-theory*, Benjamin, 1968.

There is a variation of the definition of Grothendieck group as follows. Let F be the free abelian group generated by isomorphism classes of finite modules over a ring R, or of modules of bounded cardinality so that we deal with sets. In this free abelian group we let Γ be the subgroup generated by all elements

$$[M] - [M'] - [M'']$$

for which there exists an exact sequence $0 \to M' \to M \to M'' \to 0$. The factor group F/Γ is called the **Grothendieck group** $K(R)$. We shall meet this group again in §8, and in Chapter XX, §3. Note that we may form a similar Grothendieck group with any family of modules such that M is in the family if and only if M' and M'' are in the family. Taking for the family finite projective modules, one sees easily that the two possible definitions of the Grothendieck group coincide in that case.

§5. VECTOR SPACES

A module over a field is called a **vector space**.

Theorem 5.1. *Let V be a vector space over a field K, and assume that $V \neq \{0\}$. Let Γ be a set of generators of V over K and let S be a subset of Γ which is linearly independent. Then there exists a basis $\mathfrak{B}$ of V such that $S \subset \mathfrak{B} \subset \Gamma$.*

Proof. Let $\mathfrak{T}$ be the set whose elements are subsets T of Γ which contain S and are linearly independent. Then $\mathfrak{T}$ is not empty (it contains S), and we contend that $\mathfrak{T}$ is inductively ordered. Indeed, if $\{T_i\}$ is a totally ordered subset

of $\mathfrak{T}$ (by ascending inclusion), then $\bigcup T_i$ is again linearly independent and contains S. By Zorn's lemma, let $\mathfrak{B}$ be a maximal element of $\mathfrak{T}$. Then $\mathfrak{B}$ is linearly independent. Let W be the subspace of V generated by $\mathfrak{B}$. If $W \neq V$, there exists some element $x \in \Gamma$ such that $x \notin W$. Then $\mathfrak{B} \cup \{x\}$ is linearly independent, for given a linear combination

$$\sum_{y \in \mathfrak{B}} a_y y + bx = 0, \qquad a_y, b \in K,$$

we must have $b = 0$, otherwise we get

$$x = -\sum_{y \in \mathfrak{B}} b^{-1} a_y y \in W.$$

By construction, we now see that $a_y = 0$ for all $y \in \mathfrak{B}$, thereby proving that $\mathfrak{B} \cup \{x\}$ is linearly independent, and contradicting the maximality of $\mathfrak{B}$. It follows that $W = V$, and furthermore that $\mathfrak{B}$ is not empty since $V \neq \{0\}$. This proves our theorem.

If V is a vector space $\neq \{0\}$, then in particular, we see that every set of linearly independent elements of V can be extended to a basis, and that a basis may be selected from a given set of generators.

Theorem 5.2. *Let V be a vector space over a field K. Then two bases of V over K have the same cardinality.*

Proof. Let us first assume that there exists a basis of V with a finite number of elements, say $\{v_1, \ldots, v_m\}$, $m \geqq 1$. We shall prove that any other basis must also have m elements. For this it will suffice to prove: If $w_1, \ldots, w_n$ are elements of V which are linearly independent over K, then $n \leqq m$ (for we can then use symmetry). We proceed by induction. There exist elements $c_1, \ldots, c_m$ of K such that

$$w_1 = c_1 v_1 + \cdots + c_m v_m, \tag{1}$$

and some c_i, say c_1, is not equal to 0. Then v_1 lies in the space generated by $w_1, v_2, \ldots, v_m$ over K, and this space must therefore be equal to V itself. Furthermore, $w_1, v_2, \ldots, v_m$ are linearly independent, for suppose $b_1, \ldots, b_m$ are elements of K such that

$$b_1 w_1 + b_2 v_2 + \cdots + b_m v_m = 0.$$

If $b_1 \neq 0$, divide by b_1 and express w_1 as a linear combination of $v_2, \ldots, v_m$. Subtracting from (1) would yield a relation of linear dependence among the v_i, which is impossible. Hence $b_1 = 0$, and again we must have all $b_i = 0$ because the v_i are linearly independent.

Suppose inductively that after a suitable renumbering of the v_i, we have found $w_1, \ldots, w_r$ $(r < n)$ such that

$$\{w_1, \ldots, w_r, v_{r+1}, \ldots, v_m\}$$

is a basis of V. We express w_{r+1} as a linear combination

$$w_{r+1} = c_1 w_1 + \cdots + c_r w_r + c_{r+1} v_{r+1} + \cdots + c_m v_m \tag{2}$$

with $c_i \in K$. The coefficients of the v_i in this relation cannot all be 0; otherwise there would be a linear dependence among the w_j. Say $c_{r+1} \neq 0$. Using an argument similar to that used above, we can replace v_{r+1} by w_{r+1} and still have a basis of V. This means that we can repeat the procedure until $r = n$, and therefore that $n \leqq m$, thereby proving our theorem.

We shall leave the general case of an infinite basis as an exercise to the reader. [*Hint*: Use the fact that a finite number of elements in one basis is contained in the space generated by a finite number of elements in another basis.]

If a vector space V admits one basis with a finite number of elements, say m, then we shall say that V is **finite dimensional** and that m is its **dimension**. In view of Theorem 5.2, we see that m is the number of elements in *any* basis of V. If $V = \{0\}$, then we define its dimension to be 0, and say that V is 0-dimensional. We abbreviate "dimension" by "dim" or "$\dim_K$" if the reference to K is needed for clarity.

When dealing with vector spaces over a field, we use the words **subspace** and **factor space** instead of **submodule** and **factor module**.

Theorem 5.3. *Let V be a vector space over a field K, and let W be a subspace. Then*

$$\dim_K V = \dim_K W + \dim_K V/W.$$

If $f: V \to U$ is a homomorphism of vector spaces over K, then

$$\dim V = \dim \operatorname{Ker} f + \dim \operatorname{Im} f.$$

Proof. The first statement is a special case of the second, taking for f the canonical map. Let $\{u_i\}_{i \in I}$ be a basis of $\operatorname{Im} f$, and let $\{w_j\}_{j \in J}$ be a basis of $\operatorname{Ker} f$. Let $\{v_i\}_{i \in I}$ be a family of elements of V such that $f(v_i) = u_i$ for each $i \in I$. We contend that

$$\{v_i, w_j\}_{i \in I, j \in J}$$

is a basis for V. This will obviously prove our assertion.

Let x be an element of V. Then there exist elements $\{a_i\}_{i \in I}$ of K almost all of which are 0 such that

$$f(x) = \sum_{i \in I} a_i u_i.$$

Hence $f(x - \sum a_i v_i) = f(x) - \sum a_i f(v_i) = 0$. Thus

$$x - \sum a_i v_i$$

is in the kernel of f, and there exist elements $\{b_j\}_{j \in J}$ of K almost all of which are 0 such that

$$x - \sum a_i v_i = \sum b_j w_j.$$

From this we see that $x = \sum a_i v_i + \sum b_j w_j$, and that $\{v_i, w_j\}$ generates V. It remains to be shown that the family $\{v_i, w_j\}$ is linearly independent. Suppose that there exist elements c_i, d_j such that

$$0 = \sum c_i v_i + \sum d_j w_j.$$

Applying f yields

$$0 = \sum c_i f(v_i) = \sum c_i u_i,$$

whence all $c_i = 0$. From this we conclude at once that all $d_j = 0$, and hence that our family $\{v_i, w_j\}$ is a basis for V over K, as was to be shown.

Corollary 5.4. *Let V be a vector space and W a subspace. Then*

$$\dim W \leqq \dim V.$$

If V is finite dimensional and $\dim W = \dim V$ *then $W = V$.*

Proof. Clear.

§6. THE DUAL SPACE AND DUAL MODULE

Let E be a free module over a commutative ring A. We view A as a free module of rank 1 over itself. By the **dual module** $E^\vee$ of E we shall mean the module $\mathrm{Hom}(E, A)$. Its elements will be called **functionals**. Thus a functional on E is an A-linear map $f: E \to A$. If $x \in E$ and $f \in E^\vee$, we sometimes denote $f(x)$ by $\langle x, f \rangle$. Keeping x fixed, we see that the symbol $\langle x, f \rangle$ as a function of $f \in E^\vee$ is A-linear in its second argument, and hence that x induces a linear map on $E^\vee$, which is 0 if and only if $x = 0$. Hence we get an injection $E \to E^{\vee\vee}$ which is not always a surjection.

Let $\{x_i\}_{i \in I}$ be a basis of E. For each $i \in I$ let f_i be the unique functional such that $f_i(x_j) = \delta_{ij}$ (in other words, 1 if $i = j$ and 0 if $i \neq j$). Such a linear map exists by general properties of bases (Theorem 4.1).

Theorem 6.1. *Let E be a finite free module over the commutative ring A, of finite dimension n. Then $E^\vee$ is also free, and* $\dim E^\vee = n$. *If $\{x_1, \ldots, x_n\}$ is a basis for E, and f_i is the functional such that $f_i(x_j) = \delta_{ij}$, then $\{f_1, \ldots, f_n\}$ is a basis for $E^\vee$.*

Proof. Let $f \in E^\vee$ and let $a_i = f(x_i)$ $(i = 1, \ldots, n)$. We have

$$f(c_1x_1 + \cdots + c_nx_n) = c_1f(x_1) + \cdots + c_nf(x_n).$$

Hence $f = a_1f_1 + \cdots + a_nf_n$, and we see that the f_i generate $E^\vee$. Furthermore, they are linearly independent, for if

$$b_1f_1 + \cdots + b_nf_n = 0$$

with $b_i \in K$, then evaluating the left-hand side on x_i yields

$$b_if_i(x_i) = 0,$$

whence $b_i = 0$ for all i. This proves our theorem.

Given a basis $\{x_i\}$ $(i = 1, \ldots, n)$ as in the theorem, we call the basis $\{f_i\}$ the **dual basis**. In terms of these bases, we can express an element A of E with coordinates $(a_1, \ldots, a_n)$, and an element B of $E^\vee$ with coordinates $(b_1, \ldots, b_n)$, such that

$$A = a_1x_1 + \cdots + a_nx_n, \qquad B = b_1f_1 + \cdots + b_nf_n.$$

Then in terms of these coordinates, we see that

$$\langle A, B \rangle = a_1b_1 + \cdots + a_nb_n = A \cdot B$$

is the usual dot product of n-tuples.

Corollary 6.2. *When E is free finite dimensional, then the map $E \to E^{\vee\vee}$ which to each $x \in V$ associates the functional $f \mapsto \langle x, f \rangle$ on $E^\vee$ is an isomorphism of E onto $E^{\vee\vee}$.*

Proof. Note that since $\{f_1, \ldots, f_n\}$ is a basis for $E^\vee$, it follows from the definitions that $\{x_1, \ldots, x_n\}$ is the dual basis in E, so $E = E^{\vee\vee}$.

Theorem 6.3. *Let U, V, W be finite free modules over the commutative ring A, and let*

$$0 \to W \xrightarrow{\lambda} V \xrightarrow{\varphi} U \to 0$$

be an exact sequence of A-homomorphisms. Then the induced sequence

$$0 \to \mathrm{Hom}_A(U, A) \to \mathrm{Hom}_A(V, A) \to \mathrm{Hom}_A(W, A) \to 0$$

i.e.

$$0 \to U^\vee \to V^\vee \to W^\vee \to 0$$

is also exact.

Proof. This is a consequence of **P2**, because a free module is projective.

We now consider properties which have specifically to do with vector spaces, because we are going to take factor spaces. So we assume that we deal with vector spaces over a field K.

Let V, V' be two vector spaces, and suppose given a mapping

$$V \times V' \to K$$

denoted by

$$(x, x') \mapsto \langle x, x' \rangle$$

for $x \in V$ and $x' \in V'$. We call the mapping **bilinear** if for each $x \in V$ the function $x' \mapsto \langle x, x' \rangle$ is linear, and similarly for each $x' \in V'$ the function $x \mapsto \langle x, x' \rangle$ is linear. An element $x \in V$ is said to be **orthogonal** (or **perpendicular**) to a subset S' of V' if $\langle x, x' \rangle = 0$ for all $x' \in S'$. We make a similar definition in the opposite direction. It is clear that the set of $x \in V$ orthogonal to S' is a subspace of V.

We define the **kernel** of the bilinear map on the left to be the subspace of V which is orthogonal to V', and similarly for the kernel on the right.

Given a bilinear map as above,

$$V \times V' \to K,$$

let W' be its kernel on the right and let W be its kernel on the left. Let x' be an element of V'. Then x' gives rise to a functional on V, by the rule $x \mapsto \langle x, x' \rangle$, and this functional obviously depends only on the coset of x' modulo W'; in other words, if $x'_1 \equiv x'_2 \pmod{W'}$, then the functionals $x \mapsto \langle x, x'_1 \rangle$ and $x \mapsto \langle x, x'_2 \rangle$ are equal. Hence we get a homomorphism

$$V' \to V^\vee$$

whose kernel is precisely W' by definition, whence an injective homomorphism

$$0 \to V'/W' \to V^\vee.$$

Since all the functionals arising from elements of V' vanish on W, we can view them as functionals on V/W, i.e. as elements of $(V/W)^\vee$. So we actually get an injective homomorphism

$$0 \to V'/W' \to (V/W)^\vee.$$

One could give a name to the homomorphism

$$g : V' \to V^\vee$$

such that

$$\langle x, x' \rangle = \langle x, g(x') \rangle$$

for all $x \in V$ and $x' \in V'$. However, it will usually be possible to describe it by an arrow and call it the induced map, or the natural map. Giving a name to it would tend to make the terminology heavier than necessary.

Theorem 6.4. *Let $V \times V' \to K$ be a bilinear map, let W, W' be its kernels on the left and right respectively, and assume that V'/W' is finite dimensional. Then the induced homomorphism $V'/W' \to (V/W)^\vee$ is an isomorphism.*

Proof. By symmetry, we have an induced homomorphism

$$V/W \to (V'/W')^\vee$$

which is injective. Since

$$\dim(V'/W')^\vee = \dim V'/W'$$

it follows that V/W is finite dimensional. From the above injective homomorphism and the other, namely

$$0 \to V'/W' \to (V/W)^\vee,$$

we get the inequalities

$$\dim V/W \leqq \dim V'/W'$$

and

$$\dim V'/W' \leqq \dim V/W,$$

whence an equality of dimensions. Hence our homomorphisms are surjective and inverse to each other, thereby proving the theorem.

Remark 1. Theorem 6.4 is the analogue for vector spaces of the duality Theorem 9.2 of Chapter I.

Remark 2. Let A be a commutative ring and let E be an A-module. Then we may form two types of dual:

$E^\wedge = \operatorname{Hom}(E, \mathbf{Q}/\mathbf{Z})$, viewing E as an abelian group;

$E^\vee = \operatorname{Hom}_A(E, A)$, viewing E as an A-module.

Both are called **dual**, and they usually are applied in different contexts. For instance, $E^\vee$ will be considered in Chapter XIII, while $E^\wedge$ will be considered in the theory of injective modules, Chapter XX, §4. For an example of dual module $E^\vee$ see Exercise 11. If by any chance the two duals arise together and there is need to distinguish between them, then we may call $E^\wedge$ the **Pontrjagin dual**.

Indeed, in the theory of topological groups G, the group of continuous homomorphisms of G into $\mathbf{R}/\mathbf{Z}$ is the classical Pontrjagin dual, and is classically denoted by $G^\wedge$, so I find the preservation of that terminology appropriate.

Instead of $\mathbf{R}/\mathbf{Z}$ one may take other natural groups isomorphic to $\mathbf{R}/\mathbf{Z}$. The most common such group is the group of complex numbers of absolute value 1, which we denote by $\mathbf{S}^1$. The isomorphism with $\mathbf{R}/\mathbf{Z}$ is given by the map

$$x \mapsto e^{2\pi i x}.$$

Remark 3. A bilinear map $V \times V \to K$ for which $V' = V$ is called a **bilinear form**. We say that the form is **non-singular** if the corresponding maps

$$V' \to V^\vee \quad \text{and} \quad V \to (V')^\vee$$

are isomorphisms. Bilinear maps and bilinear forms will be studied at greater length in Chapter XV. See also Exercise 33 of Chapter XIII for a nice example.

§7. MODULES OVER PRINCIPAL RINGS

Throughout this section, we assume that R is a principal entire ring. All modules are over R, and homomorphisms are R-homomorphisms, unless otherwise specified.

The theorems will generalize those proved in Chapter I for abelian groups. We shall also point out how the proofs of Chapter I can be adjusted with substitutions of terminology so as to yield proofs in the present case.

Let F be a free module over R, with a basis $\{x_i\}_{i \in I}$. Then the cardinality of I is uniquely determined, and is called the **dimension** of F. We recall that this is proved, say by taking a prime element p in R, and observing that F/pF is a vector space over the field R/pR, whose dimension is precisely the cardinality of I. We may therefore speak of the dimension of a free module over R.

Theorem 7.1. *Let F be a free module, and M a submodule. Then M is free, and its dimension is less than or equal to the dimension of F.*

Proof. For simplicity, we give the proof when F has a finite basis $\{x_i\}$, $i = 1, \ldots, n$. Let M_r be the intersection of M with $(x_1, \ldots, x_r)$, the module generated by $x_1, \ldots, x_r$. Then $M_1 = M \cap (x_1)$ is a submodule of (x_1), and is therefore of type $(a_1 x_1)$ with some $a_1 \in R$. Hence M_1 is either 0 or free, of dimension 1. Assume inductively that M_r is free of dimension $\leqq r$. Let $\mathfrak{a}$ be the set consisting of all elements $a \in R$ such that there exists an element $x \in M$ which can be written

$$x = b_1 x_1 + \cdots + b_r x_r + a x_{r+1}$$

with $b_i \in R$. Then $\mathfrak{a}$ is obviously an ideal, and is principal, generated say by an element a_{r+1}. If $a_{r+1} = 0$, then $M_{r+1} = M_r$ and we are done with the inductive step. If $a_{r+1} \neq 0$, let $w \in M_{r+1}$ be such that the coefficient of w with respect to x_{r+1} is a_{r+1}. If $x \in M_{r+1}$ then the coefficient of x with respect to x_{r+1} is divisible by a_{r+1}, and hence there exists $c \in R$ such that $x - cw$ lies in M_r. Hence

$$M_{r+1} = M_r + (w).$$

On the other hand, it is clear that $M_r \cap (w)$ is 0, and hence that this sum is direct, thereby proving our theorem. (For the infinite case, see Appendix 2, §2.)

Corollary 7.2. *Let E be a finitely generated module and E' a submodule. Then E' is finitely generated.*

Proof. We can represent E as a factor module of a free module F with a finite number of generators: If $v_1, \ldots, v_n$ are generators of E, we take a free module F with basis $\{x_1, \ldots, x_n\}$ and map x_i on v_i. The inverse image of E' in F is a submodule, which is free, and finitely generated, by the theorem. Hence E' is finitely generated. The assertion also follows using simple properties of Noetherian rings and modules.

If one wants to translate the proofs of Chapter I, then one makes the following definitions. A free 1-dimensional module over R is called **infinite cyclic**. An infinite cyclic module is isomorphic to R, viewed as module over itself. Thus every non-zero submodule of an infinite cyclic module is infinite cyclic. The proof given in Chapter I for the analogue of Theorem 7.1 applies without further change.

Let E be a module. We say that E is a **torsion** module if given $x \in E$, there exists $a \in R$, $a \neq 0$, such that $ax = 0$. The generalization of **finite abelian group** is **finitely generated torsion module**. An element x of E is called a **torsion element** if there exists $a \in R$, $a \neq 0$, such that $ax = 0$.

Let E be a module. We denote by E_{tor} the submodule consisting of all torsion elements of E, and call it the **torsion submodule** of E. If $E_{\mathrm{tor}} = 0$, we say that E is **torsion free**.

Theorem 7.3. *Let E be finitely generated. Then E/E_{tor} is free. There exists a free submodule F of E such that E is a direct sum*

$$E = E_{\mathrm{tor}} \oplus F.$$

The dimension of such a submodule F is uniquely determined.

Proof. We first prove that E/E_{tor} is torsion free. If $x \in E$, let $\bar{x}$ denote its residue class mod E_{tor}. Let $b \in R$, $b \neq 0$ be such that $b\bar{x} = 0$. Then $bx \in E_{\mathrm{tor}}$, and hence there exists $c \in R$, $c \neq 0$, such that $cbx = 0$. Hence $x \in E_{\mathrm{tor}}$ and $\bar{x} = 0$, thereby proving that E/E_{tor} is torsion free. It is also finitely generated.

Assume now that M is a torsion free module which is finitely generated. Let $\{v_1, \ldots, v_n\}$ be a maximal set of elements of M among a given finite set of generators $\{y_1, \ldots, y_m\}$ such that $\{v_1, \ldots, v_n\}$ is linearly independent. If y is one of the generators, there exist elements $a, b_1, \ldots, b_n \in R$ not all 0, such that

$$ay + b_1v_1 + \cdots + b_nv_n = 0.$$

Then $a \neq 0$ (otherwise we contradict the linear independence of $v_1, \ldots, v_n$). Hence ay lies in $(v_1, \ldots, v_n)$. Thus for each $j = 1, \ldots, m$ we can find $a_j \in R$, $a_j \neq 0$, such that a_jy_j lies in $(v_1, \ldots, v_n)$. Let $a = a_1 \cdots a_m$ be the product. Then aM is contained in $(v_1, \ldots, v_n)$, and $a \neq 0$. The map

$$x \mapsto ax$$

is an injective homomorphism, whose image is contained in a free module. This image is isomorphic to M, and we conclude from Theorem 7.1 that M is free, as desired.

To get the submodule F we need a lemma.

Lemma 7.4. *Let E, E' be modules, and assume that E' is free. Let $f : E \to E'$ be a surjective homomorphism. Then there exists a free submodule F of E such that the restriction of f to F induces an isomorphism of F with E', and such that $E = F \oplus \operatorname{Ker} f$.*

Proof. Let $\{x_i'\}_{i \in I}$ be a basis of E'. For each i, let x_i be an element of E such that $f(x_i) = x_i'$. Let F be the submodule of E generated by all the elements x_i, $i \in I$. Then one sees at once that the family of elements $\{x_i\}_{i \in I}$ is linearly independent, and therefore that F is free. Given $x \in E$, there exist elements $a_i \in R$ such that

$$f(x) = \sum a_i x_i'.$$

Then $x - \sum a_i x_i$ lies in the kernel of f, and therefore $E = \operatorname{Ker} f + F$. It is clear that $\operatorname{Ker} f \cap F = 0$, and hence that the sum is direct, thereby proving the lemma.

We apply the lemma to the homomorphism $E \to E/E_{\text{tor}}$ in Theorem 7.3 to get our decomposition $E = E_{\text{tor}} \oplus F$. The dimension of F is uniquely determined, because F is isomorphic to E/E_{tor} for any decomposition of E into a direct sum as stated in the theorem.

The dimension of the free module F in Theorem 7.3 is called the **rank** of E.

In order to get the structure theorem for finitely generated modules over R, one can proceed exactly as for abelian groups. We shall describe the dictionary which allows us to transport the proofs essentially without change.

Let E be a module over R. Let $x \in E$. The map $a \mapsto ax$ is a homomorphism of R onto the submodule generated by x, and the kernel is an ideal, which is principal, generated by an element $m \in R$. We say that m is a **period** of x. We

note that m is determined up to multiplication by a unit (if $m \neq 0$). An element $c \in R, c \neq 0$, is said to be an **exponent** for E (resp. for x) if $cE = 0$ (resp. $cx = 0$).

Let p be a prime element. We denote by $E(p)$ the submodule of E consisting of all elements x having an exponent which is a power p^r ($r \geqq 1$). A p-submodule of E is a submodule contained in $E(p)$.

We select once and for all a system of representatives for the prime elements of R (modulo units). For instance, if R is a polynomial ring in one variable over a field, we take as representatives the irreducible polynomials with leading coefficient 1.

Let $m \in R, m \neq 0$. We denote by E_m the kernel of the map $x \mapsto mx$. It consists of all elements of E having exponent m.

A module E is said to be **cyclic** if it is isomorphic to $R/(a)$ for some element $a \in R$. Without loss of generality if $a \neq 0$, one may assume that a is a product of primes in our system of representatives, and then we could say that a is the order of the module.

Let $r_1, \ldots, r_s$ be integers $\geqq 1$. A p-module E is said to be of **type**

$$(p^{r_1}, \ldots, p^{r_s})$$

if it is isomorphic to the product of cyclic modules $R/(p^{r_i})$ ($i = 1, \ldots, s$). If p is fixed, then one could say that the module is of type $(r_1, \ldots, r_s)$ (relative to p).

All the proofs of Chapter I, §8 now go over without change. Whenever we argue on the size of a positive integer m, we have a similar argument on the number of prime factors appearing in its prime factorization. If we deal with a prime power p^r, we can view the order as being determined by r. The reader can now check that the proofs of Chapter I, §8 are applicable.

However, we shall develop the theory once again without assuming any knowledge of Chapter I, §8. Thus our treatment is self-contained.

Theorem 7.5. *Let E be a finitely generated torsion module $\neq 0$. Then E is the direct sum*

$$E = \bigoplus_p E(p),$$

taken over all primes p such that $E(p) \neq 0$. Each $E(p)$ can be written as a direct sum

$$E(p) = R/(p^{v_1}) \oplus \cdots \oplus R/(p^{v_s})$$

with $1 \leqq v_1 \leqq \cdots \leqq v_s$. The sequence $v_1, \ldots, v_s$ is uniquely determined.

Proof. Let a be an exponent for E, and suppose that $a = bc$ with $(b, c) = (1)$. Let $x, y \in R$ be such that

$$1 = xb + yc.$$

We contend that $E = E_b \oplus E_c$. Our first assertion then follows by induction, expressing a as a product of prime powers. Let $v \in E$. Then

$$v = xbv + ycv.$$

Then $xbv \in E_c$ because $cxbv = xav = 0$. Similarly, $ycv \in E_b$. Finally $E_b \cap E_c = 0$, as one sees immediately. Hence E is the direct sum of E_b and E_c.

We must now prove that $E(p)$ is a direct sum as stated. If $y_1, \ldots, y_m$ are elements of a module, we shall say that they are **independent** if whenever we have a relation

$$a_1 y_1 + \cdots + a_m y_m = 0$$

with $a_i \in R$, then we must have $a_i y_i = 0$ for all i. (Observe that **independent** does not mean **linearly independent**.) We see at once that $y_1, \ldots, y_m$ are independent if and only if the module $(y_1, \ldots, y_m)$ has the direct sum decomposition

$$(y_1, \ldots, y_m) = (y_1) \oplus \cdots \oplus (y_m)$$

in terms of the cyclic modules (y_i), $i = 1, \ldots, m$.

We now have an analogue of Lemma 7.4 for modules having a prime power exponent.

Lemma 7.6. *Let E be a torsion module of exponent p^r ($r \geqq 1$) for some prime element p. Let $x_1 \in E$ be an element of period p^r. Let $\bar{E} = E/(x_1)$. Let $\bar{y}_1, \ldots, \bar{y}_m$ be independent elements of $\bar{E}$. Then for each i there exists a representative $y_i \in E$ of $\bar{y}_i$, such that the period of y_i is the same as the period of $\bar{y}_i$. The elements $x_1, y_1, \ldots, y_m$ are independent.*

Proof. Let $\bar{y} \in \bar{E}$ have period p^n for some $n \geqq 1$. Let y be a representative of $\bar{y}$ in E. Then $p^n y \in (x_1)$, and hence

$$p^n y = p^s c x_1, \qquad c \in R, p \nmid c,$$

for some $s \leqq r$. If $s = r$, we see that y has the same period as $\bar{y}$. If $s < r$, then $p^s c x_1$ has period p^{r-s}, and hence y has period p^{n+r-s}. We must have

$$n + r - s \leqq r,$$

because p^r is an exponent for E. Thus we obtain $n \leqq s$, and we see that

$$y - p^{s-n} c x_1$$

is a representative for $\bar{y}$, whose period is p^n.

Let y_i be a representative for $\bar{y}_i$ having the same period. We prove that $x_1, y_1, \ldots, y_m$ are independent. Suppose that $a, a_1, \ldots, a_m \in R$ are elements such that

$$a x_1 + a_1 y_1 + \cdots + a_m y_m = 0.$$

Then

$$a_1\bar{y}_1 + \cdots + a_m\bar{y}_m = 0.$$

By hypothesis, we must have $a_i\bar{y}_i = 0$ for each i. If p^{r_i} is the period of $\bar{y}_i$, then p^{r_i} divides a_i. We then conclude that $a_i y_i = 0$ for each i, and hence finally that $ax_1 = 0$, thereby proving the desired independence.

To get the direct sum decomposition of $E(p)$, we first note that $E(p)$ is finitely generated. We may assume without loss of generality that $E = E(p)$. Let x_1 be an element of E whose period p^{r_1} is such that r_1 is maximal. Let $\bar{E} = E/(x_1)$. We contend that $\dim \bar{E}_p$ as vector space over R/pR is strictly less than $\dim E_p$. Indeed, if $\bar{y}_1, \ldots, \bar{y}_m$ are linearly independent elements of $\bar{E}_p$ over R/pR, then Lemma 7.6 implies that $\dim E_p \geqq m + 1$ because we can always find an element of (x_1) having period p, independent of $y_1, \ldots, y_m$. Hence $\dim \bar{E}_p < \dim E_p$. We can prove the direct sum decomposition by induction. If $E \neq 0$, there exist elements $\bar{x}_2, \ldots, \bar{x}_s$ having periods $p^{r_2}, \ldots, p^{r_s}$ respectively, such that $r_2 \geqq \cdots \geqq r_s$. By Lemma 7.6, there exist representatives $x_2, \ldots, x_r$ in E such that x_i has period p^{r_i} and $x_1, \ldots, x_r$ are independent. Since p^{r_1} is such that r_1 is maximal, we have $r_1 \geqq r_2$, and our decomposition is achieved.

The uniqueness will be a consequence of a more general uniqueness theorem, which we state next.

Theorem 7.7. *Let E be a finitely generated torsion module, $E \neq 0$. Then E is isomorphic to a direct sum of non-zero factors*

$$R/(q_1) \oplus \cdots \oplus R/(q_r),$$

where $q_1, \ldots, q_r$ are non-zero non-units of R, and $q_1 \mid q_2 \mid \cdots \mid q_r$. The sequence of ideals $(q_1), \ldots, (q_r)$ is uniquely determined by the above conditions.

Proof. Using Theorem 7.5, decompose E into a direct sum of p-submodules, say $E(p_1) \oplus \cdots \oplus E(p_l)$, and then decompose each $E(p_i)$ into a direct sum of cyclic submodules of periods $p_i^{r_{ij}}$. We visualize these symbolically as described by the following diagram:

$$\begin{array}{lcccc} E(p_1): & r_{11} & \leqq & r_{12} & \leqq \cdots \\ E(p_2): & r_{21} & \leqq & r_{22} & \leqq \cdots \\ \vdots & \vdots & & \vdots & \vdots \\ E(p_l): & r_{l1} & \leqq & r_{l2} & \leqq \cdots \end{array}$$

A horizontal row describes the type of the module with respect to the prime at the left. The exponents r_{ij} are arranged in increasing order for each fixed $i = 1, \ldots, l$. We let $q_1, \ldots, q_r$ correspond to the columns of the matrix of exponents, in other words

$$q_1 = p_1^{r_{11}} p_2^{r_{21}} \cdots p_l^{r_{l1}},$$

$$q_2 = p_1^{r_{12}} p_2^{r_{22}} \cdots p_l^{r_{l2}},$$

$$\cdots$$

The direct sum of the cyclic modules represented by the first column is then isomorphic to $R/(q_1)$, because, as with abelian groups, the direct sum of cyclic modules whose periods are relatively prime is also cyclic. We have a similar remark for each column, and we observe that our proof actually orders the q_j by increasing divisibility, as was to be shown.

Now for uniqueness. Let p be any prime, and suppose that $E = R/(pb)$ for some $b \in R$, $b \neq 0$. Then E_p is the submodule $bR/(pb)$, as follows at once from unique factorization in R. But the kernel of the composite map

$$R \to bR \to bR/(pb)$$

is precisely (p). Thus we have an isomorphism

$$R/(p) \approx bR/(pb).$$

Let now E be expressed as in the theorem, as a direct sum of r terms. An element

$$v = v_1 \oplus \cdots \oplus v_r, \qquad v_i \in R/(q_i)$$

is in E_p if and only if $pv_i = 0$ for all i. Hence E_p is the direct sum of the kernel of multiplication by p in each term. But E_p is a vector space over $R/(p)$, and its dimension is therefore equal to the number of terms $R/(q_i)$ such that p divides q_i.

Suppose that p is a prime dividing q_1, and hence q_i for each $i = 1, \ldots, r$. Let E have a direct sum decomposition into d terms satisfying the conditions of the theorem, say

$$E = R/(q'_1) \oplus \cdots \oplus R/(q'_s).$$

Then p must divide at least r of the elements q'_j, whence $r \leqq s$. By symmetry, $r = s$, and p divides q'_j for all j.

Consider the module pE. By a preceding remark, if we write $q_i = pb_i$, then

$$pE \approx R/(b_1) \oplus \cdots \oplus R/(b_r),$$

and $b_1 | \cdots | b_r$. Some of the b_i may be units, but those which are not units determine their principal ideal uniquely, by induction. Hence if

$$(b_1) = \cdots = (b_j) = 1$$

but $(b_{j+1}) \neq (1)$, then the sequence of ideals

$$(b_{j+1}), \ldots, (b_r)$$

is uniquely determined. This proves our uniqueness statement, and concludes the proof of Theorem 7.7.

The ideals $(q_1), \ldots, (q_r)$ are called the **invariants** of E.

For one of the main applications of Theorem 7.7 to linear algebra, see Chapter XV, §2.

The next theorem is included for completeness. It is called the **elementary divisors** theorem.

Theorem 7.8. *Let F be a free module over R, and let M be a finitely generated submodule $\neq 0$. Then there exists a basis $\mathfrak{B}$ of F, elements $e_1, \ldots, e_m$ in this basis, and non-zero elements $a_1, \ldots, a_m \in R$ such that:*

(i) *The elements $a_1e_1, \ldots, a_me_m$ form a basis of M over R.*

(ii) *We have $a_i | a_{i+1}$ for $i = 1, \ldots, m-1$.*

The sequence of ideals $(a_1), \ldots, (a_m)$ is uniquely determined by the preceding conditions.

Proof. Write a finite set of generators for M as linear combination of a finite number of elements in a basis for F. These elements generate a free submodule of finite rank, and thus it suffices to prove the theorem when F has finite rank, which we now assume. We let $n = \operatorname{rank}(F)$.

The uniqueness is a corollary of Theorem 7.7. Suppose we have a basis as in the theorem. Say $a_1, \ldots, a_s$ are units, and so can be taken to be $= 1$, and $a_{s+j} = q_j$ with $q_1 | q_2 | \ldots | q_r$ non-units. Observe that $F/M = \bar{F}$ is a finitely generated module over R, having the direct sum expression

$$F/M = \bar{F} \approx \bigoplus_{j=1}^{r} (R/q_jR)\bar{e}_j \oplus \text{free module of rank } n - (r+s)$$

where a bar denotes the class of an element of F mod M. Thus the direct sum over $j = 1, \ldots, r$ is the torsion submodule of $\bar{F}$, whence the elements $q_1, \ldots, q_r$ are uniquely determined by Theorem 7.7. We have $r + s = m$, so the rank of F/M is $n - m$, which determines m uniquely. Then $s = m - r$ is uniquely determined as the number of units among $a_1, \ldots, a_m$. This proves the uniqueness part of the theorem. Next we prove existence.

Let λ be a functional on F, in other words, an element of $\operatorname{Hom}_R(F, R)$. We let $J_\lambda = \lambda(M)$. Then J_λ is an ideal of R. Select λ_1 such that $\lambda_1(M)$ is maximal in the set of ideals $\{J_\lambda\}$, that is to say, there is no properly larger ideal in the set $\{J_\lambda\}$.

Let $\lambda_1(M) = (a_1)$. Then $a_1 \neq 0$, because there exists a non-zero element of M, and expressing this element in terms of some basis for F over R, with some non-zero coordinate, we take the projection on this coordinate to get a functional whose value on M is not 0. Let $x_1 \in M$ be such that $\lambda_1(x_1) = a_1$. For any functional g we must have $g(x_1) \in (a_1)$ [immediate from the maximality of

$\lambda_1(M)$]. Writing x_1 in terms of any basis of F, we see that its coefficients must all be divisible by a_1. (If some coefficient is not divisible by a_1, project on this coefficient to get an impossible functional.) Therefore we can write $x_1 = a_1 e_1$ with some element $e_1 \in F$.

Next we prove that F is a direct sum

$$F = Re_1 \oplus \operatorname{Ker} \lambda_1.$$

Since $\lambda_1(e_1) = 1$, it is clear that $Re_1 \cap \operatorname{Ker} \lambda_1 = 0$. Furthermore, given $x \in F$ we note that $x - \lambda_1(x)e_1$ is in the kernel of λ_1. Hence F is the sum of the indicated submodules, and therefore the direct sum.

We note that $\operatorname{Ker} \lambda_1$ is free, being a submodule of a free module (Theorem 7.1). We let

$$F_1 = \operatorname{Ker} \lambda_1 \quad \text{and} \quad M_1 = M \cap \operatorname{Ker} \lambda_1.$$

We see at once that $M = Rx_1 \oplus M_1$.

Thus M_1 is a submodule of F_1 and its dimension is one less than the dimension of M. From the maximality condition on $\lambda_1(M)$, it follows at once that for any functional λ on F_1, the image $\lambda(M)$ will be contained in $\lambda_1(M)$ (because otherwise, a suitable linear combination of functionals would yield an ideal larger than (a_1)). We can therefore complete the existence proof by induction.

In Theorem 7.8, we call the ideals $(a_1), \ldots, (a_m)$ the **invariants** of M in F. For another characterization of these invariants, see Chapter XIII, Proposition 4.20.

Example. First, see examples of situations similar to those of Theorem 7.8 in Exercises 5, 7, and 8, and for Dedekind rings in Exercise 13.

Example. Another way to obtain a module M as in Theorem 7.8 is as a module of relations. Let W be a finitely generated module over R, with generators $w_1, \ldots, w_n$. By a **relation** among $\{w_1, \ldots, w_n\}$ we mean an element $(a_1, \ldots, a_n) \in R^n$ such that $\sum a_i w_i = 0$. The set of such relations is a submodule of R^n, to which Theorem 7.8 may be applied.

It is also possible to formulate a proof of Theorem 7.8 by considering M as a submodule of R^n, and applying the method of row and column operations to get a desired basis. In this context, we make some further comments which may serve to illustrate Theorem 7.8. We assume that the reader is acquainted with matrices over a ring. By **row operations** we mean: interchanging two rows; adding a multiple of one row to another; multiplying a row by a unit in the ring. We define **column operations** similarly. These row and column operations correspond to multiplication with the so-called elementary matrices in the ring.

Theorem 7.9. *Assume that the elementary matrices in R generate $GL_n(R)$. Let (x_{ij}) be a non-zero matrix with components in R. Then with a finite number of row and column operations, it is possible to bring the matrix to the form*

$$\begin{pmatrix} a_1 & 0 & \cdots & \cdot & \cdot & \cdots & 0 \\ 0 & a_2 & \cdots & \cdot & \cdot & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdot & \cdots & a_m & \cdot & \cdots & 0 \\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{pmatrix}.$$

with $a_1 \cdots a_m \neq 0$ *and* $a_1 \mid a_2 \mid \cdots \mid a_m$.

We leave the proof for the reader. Either Theorem 7.9 can be viewed as equivalent to Theorem 7.8, or a direct proof may be given. In any case, Theorem 7.9 can be used in the following context. Consider a system of linear equations

$$c_{11}x_1 + \cdots + c_{1n}x_n = 0$$
$$\cdots$$
$$c_{r1}x_1 + \cdots + c_{rn}x_n = 0.$$

with coefficients in R. Let F be the submodule of R^n generated by the vectors $X = (x_1, \ldots, x_n)$ which are solutions of this system. By Theorem 7.1, we know that F is free of dimension $\leqq n$. Theorem 7.9 can be viewed as providing a normalized basis for F in line with Theorem 7.8.

Further example. As pointed out by Paul Cohen, the row and column method can be applied to modules over a power series ring $\mathfrak{o}[[X]]$, where $\mathfrak{o}$ is a complete discrete valuation ring. Cf. Theorem 3.1 of Chapter 5 in my *Cyclotomic Fields* I *and* II (Springer Verlag, 1990). For instance, one could pick $\mathfrak{o}$ itself to be a power series ring $k[[T]]$ in one variable over a field k, but in the theory of cyclotomic fields in the above reference, $\mathfrak{o}$ is taken to be the ring of p-adic integers. On the other hand, George Bergman has drawn my attention to P. M. Cohn's "On the structure of GL_2 of a ring," *IHES Publ. Math.* No. 30 (1966), giving examples of principal rings where one cannot use row and column operations in Theorem 7.9.

§8. EULER-POINCARÉ MAPS

The present section may be viewed as providing an example and application of the Jordan-Hölder theorem for modules. But as pointed out in the examples and references below, it also provides an introduction for further theories.

Again let A be a ring. We continue to consider A-modules. Let Γ be an abelian group, written additively. Let φ be a rule which to certain modules associates an element of Γ, subject to the following condition:

If $0 \to M' \to M \to M'' \to 0$ *is exact, then* $\varphi(M)$ *is defined if and only if* $\varphi(M')$ *and* $\varphi(M'')$ *are defined, and in that case, we have*

$$\varphi(M) = \varphi(M') + \varphi(M'').$$

Furthermore $\varphi(0)$ *is defined and equal to* 0.

Such a rule φ will be called an **Euler-Poincaré mapping** on the category of A-modules. If M' is isomorphic to M, then from the exact sequence

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

we conclude that $\varphi(M')$ is defined if $\varphi(M)$ is defined, and that $\varphi(M') = \varphi(M)$. Thus if $\varphi(M)$ is defined for a module M, φ is defined on every submodule and factor module of M. In particular, if we have an exact sequence of modules

$$M' \to M \to M''$$

and if $\varphi(M')$ and $\varphi(M'')$ are defined, then so is $\varphi(M)$, as one sees at once by considering the kernel and image of our two maps, and using the definition.

Examples. We could let $A = \mathbf{Z}$, and let φ be defined for all finite abelian groups, and be equal to the order of the group. The value of φ is in the multiplicative group of positive rational numbers.

As another example, we consider the category of vector spaces over a field k. We let φ be defined for finite dimensional spaces, and be equal to the dimension. The values of φ are then in the additive group of integers.

In Chapter XV we shall see that the characteristic polynomial may be considered as an Euler-Poincaré map.

Observe that the natural map of a finite module into its image in the Grothendieck group defined at the end of §4 is a universal Euler-Poincaré mapping. We shall develop a more extensive theory of this mapping in Chapter XX, §3.

If M is a module (over a ring A), then a sequence of submodules

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

is also called a **finite filtration**, and we call r the **length** of the filtration. A module M is said to be **simple** if it does not contain any submodule other than 0 and M itself, and if $M \neq 0$. A filtration is said to be **simple** if each M_i/M_{i+1} is simple. *The Jordan-Hölder theorem asserts that two simple filtrations of a module are equivalent.*

A module M is said to be of **finite length** if it is 0 or if it admits a simple (finite) filtration. By the Jordan-Hölder theorem for modules (proved the same way as for groups), the length of such a simple filtration is uniquely determined, and is called the **length of the module**. In the language of Euler characteristics, the Jordan-Hölder theorem can be reformulated as follows:

Theorem 8.1. *Let φ be a rule which to each simple module associates an element of a commutative group Γ, and such that if $M \approx M'$ then*

$$\varphi(M) = \varphi(M').$$

Then φ has a unique extension to an Euler-Poincaré mapping defined on all modules of finite length.

Proof. Given a simple filtration

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

we define

$$\varphi(M) = \sum_{i=1}^{r-1} \varphi(M_i/M_{i+1}).$$

The Jordan-Hölder theorem shows immediately that this is well-defined, and that this extension of φ is an Euler-Poincaré map.

In particular, we see that the length function is the Euler-Poincaré map taking its values in the additive group of integers, and having the value 1 for any simple module.

§9. THE SNAKE LEMMA

This section gives a very general lemma, which will be used many times, so we extract it here. The reader may skip it until it is encountered, but already we give some exercises which show how it is applied: the five lemma in Exercise 15 and also Exercise 26. Other substantial applications in this book will occur in Chapter XVI, §3 in connection with the tensor product, and in Chapter XX in connection with complexes, resolutions, and derived functors.

We begin with routine comments. Consider a commutative diagram of homomorphisms of modules.

$$\begin{array}{ccc} M' & \xrightarrow{f} & M \\ {\scriptstyle d'}\downarrow & & \downarrow{\scriptstyle d} \\ N' & \xrightarrow[h]{} & N \end{array}$$

Then f induces a homomorphism

$$\operatorname{Ker} d' \to \operatorname{Ker} d.$$

Indeed, suppose $d'x' = 0$. Then $df(x') = 0$ because $df(x') = hd'(x') = 0$.

Similarly, h induces a homomorphism

$$\text{Coker } d' \to \text{Coker } d$$

in a natural way as follows. Let $y' \in N'$ represent an element of $N'/d'M'$. Then $hy' \bmod dM$ does not depend on the choice of y' representing the given element, because if $y'' = y' + d'x'$, then

$$hy'' = hy' + hd'x' = hy' + dfx' \equiv hy' \bmod dM.$$

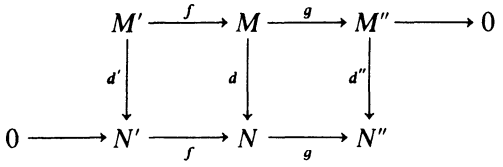
Thus we get a map

$$h_*: N'/d'M' = \text{Coker } d' \to N/dM = \text{Coker } d,$$

which is immediately verified to be a homomorphism.

In practice, given a commutative diagram as above, one sometimes writes f instead of h, so one writes f for the horizontal maps both above and below the diagram. This simplifies the notation, and is not so incorrect: we may view M', N' as the two components of a direct sum, and similarly for M, N. Then f is merely a homomorphism defined on the direct sum $M' \oplus N'$ into $M \oplus N$.

The snake lemma concerns a commutative and exact diagram called a **snake diagram**:



Let $z'' \in \text{Ker } d''$. We can construct elements of N' as follows. Since g is surjective, there exists an element $z \in M$ such that $gz = z''$. We now move vertically down by d, and take dz. The commutativity $d''g = gd$ shows that $gdz = 0$ whence dz is in the kernel of g in N. By exactness, there exists an element $z' \in N'$ such that $fz' = dz$. In brief, we write

$$z' = f^{-1} \circ d \circ g^{-1} z''.$$

Of course, z' is not well defined because of the choices made when taking inverse images. However, the snake lemma will state exactly what goes on.

Lemma 9.1. (Snake Lemma). *Given a snake diagram as above, the map*

$$\delta : \text{Ker } d'' \to \text{Coker } d'$$

induced by $\delta z'' = f^{-1} \circ d \circ g^{-1} z''$ *is well defined, and we have an exact sequence*

$$\text{Ker } d' \to \text{Ker } d \to \text{Ker } d'' \xrightarrow{\delta} \text{Coker } d' \to \text{Coker } d \to \text{Coker } d''$$

where the maps besides δ *are the natural ones.*

Proof. It is a routine verification that the class of $z' \bmod \operatorname{Im} d'$ is independent of the choices made when taking inverse images, whence defining the map δ. The proof of the exactness of the sequence is then routine, and consists in chasing around diagrams. It should be carried out in full detail by the reader who wishes to acquire a feeling for this type of triviality. As an example, we shall prove that

$$\operatorname{Ker} \delta \subset \operatorname{Im} g_*$$

where g_* is the induced map on kernels. Suppose the image of z'' is 0 in Coker d'. By definition, there exists $u' \in M'$ such that $z' = d'u'$. Then

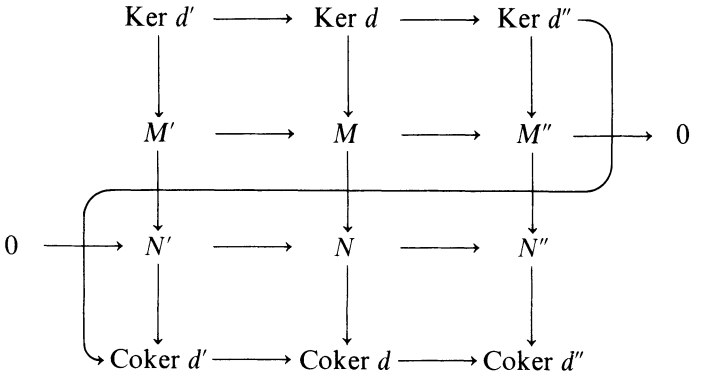
$$dz = fz' = fd'u' = dfu'$$

by commutativity. Hence

$$d(z - fu') = 0,$$

and $z - fu'$ is in the kernel of d. But $g(z - fu') = gz = z''$. This means that z'' is in the image of g_*, as desired. All the remaining cases of exactness will be left to the reader.

The original snake diagram may be completed by writing in the kernels and cokernels as follows (whence the name of the lemma):



§10. DIRECT AND INVERSE LIMITS

We return to limits, which we considered for groups in Chapter I. We now consider limits in other categories (rings, modules), and we point out that limits satisfy a universal property, in line with Chapter I, §11.

Let $I = \{i\}$ be a directed system of indices, defined in Chapter I, §10. Let $\mathfrak{A}$ be a category, and $\{A_i\}$ a family of objects in $\mathfrak{A}$. For each pair i, j such that

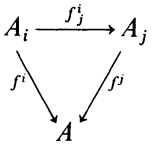
$i \leqq j$ assume given a morphism

$$f_j^i : A_i \to A_j$$

such that, whenever $i \leqq j \leqq k$, we have

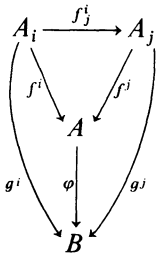
$$f_k^j \circ f_j^i = f_k^i \quad \text{and} \quad f_i^i = \mathrm{id}.$$

Such a family will be called a **directed family of morphisms**. A **direct limit** for the family $\{f_j^i\}$ is a universal object in the following category $\mathfrak{C}$. $\mathrm{Ob}(\mathfrak{C})$ consists of pairs $(A, (f^i))$ where $A \in \mathrm{Ob}(\mathfrak{A})$ and (f^i) is a family of morphisms $f^i : A_i \to A$, $i \in I$, such that for all $i \leqq j$ the following diagram is commutative:



(Universal of course means universally repelling.)

Thus if $(A, (f^i))$ is the direct limit, and if $(B, (g^i))$ is any object in the above category, then there exists a unique morphism $\varphi : A \to B$ which makes the following diagram commutative:



For simplicity, one usually writes

$$A = \varinjlim_i A_i,$$

omitting the f_j^i from the notation.

Theorem 10.1. *Direct limits exist in the category of abelian groups, or more generally in the category of modules over a ring.*

Proof. Let $\{M_i\}$ be a directed system of modules over a ring. Let M be their direct sum. Let N be the submodule generated by all elements

$$x_{ij} = (\ldots, 0, x, 0, \ldots, -f_j^i(x), 0, \ldots)$$

where, for a given pair of indices (i, j) with $j \geqq i$, x_{ij} has component x in M_i, $f_j^i(x)$ in M_j, and component 0 elsewhere. Then we leave to the reader the verification that the factor module M/N is a direct limit, where the maps of M_i into M/N are the natural ones arising from the composite homomorphism

$$M_i \to M \to M/N.$$

Example. Let X be a topological space, and let $x \in X$. The open neighborhoods of x form a directed system, by inclusion. Indeed, given two open neighborhoods U and V, then $U \cap V$ is also an open neighborhood contained in both U and V. In sheaf theory, one assigns to each U an abelian group $A(U)$ and to each pair $U \supset V$ a homomorphism $h_V^U\colon A(U) \to A(V)$ such that if $U \supset V \supset W$ then $h_W^V \circ h_V^U = h_W^U$. Then the family of such homomorphisms is a directed family. The direct limit

$$\varinjlim_U A(U)$$

is called the **stalk** at the point x. We shall give the formal definition of a sheaf of abelian groups in Chapter XX, §6. For further reading, I recommend at least two references. First, the self-contained short version of Chapter II in Hartshorne's *Algebraic Geometry*, Springer Verlag, 1977. (Do all the exercises of that section, concerning sheaves.) The section is only five pages long. Second, I recommend the treatment in Gunning's *Introduction to Holomorphic Functions of Several Variables*, Wadsworth and Brooks/Cole, 1990.

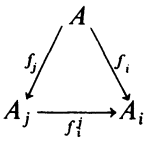
We now reverse the arrows to define inverse limits. We are again given a directed set I and a family of objects A_i. If $j \geqq i$ we are now given a morphism

$$f_i^j\colon A_j \to A_i$$

satisfying the relations

$$f_k^i \circ f_i^j = f_k^j \quad \text{and} \quad f_i^i = \mathrm{id},$$

if $j \geqq i$ and $i \geqq k$. As in the direct case, we can define a category of objects (A, f_i) with $f_i\colon A \to A_i$ such that for all i, j the following diagram is commutative:



A universal object in this category is called an **inverse limit** of the system (A_i, f_j^i).

As before, we often say that

$$A = \varprojlim_i A_i$$

is the inverse limit, omitting the f_j^i from the notation.

Theorem 10.2. *Inverse limits exist in the category of groups, in the category of modules over a ring, and also in the category of rings.*

Proof. Let $\{G_i\}$ be a directed family of groups, for instance, and let Γ be their inverse limit as defined in Chapter I, §10. Let $p_i: \Gamma \to G_i$ be the projection (defined as the restriction from the projection of the direct product, since Γ is a subgroup of $\prod G_i$). It is routine to verify that these data give an inverse limit in the category of groups. The same construction also applies to the category of rings and modules.

Example. Let p be a prime number. For $n \geqq m$ we have a canonical surjective ring homomorphism

$$f_m^n: \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^m\mathbf{Z}.$$

The projective limit is called the ring of ***p*-adic integers**, and is denoted by $\mathbf{Z}_p$. For a consideration of this ring as a complete discrete valuation ring, see Exercise 17 and Chapter XII.

Let k be a field. The power series ring $k[[T]]$ in one variable may be viewed as the inverse limit of the factor polynomial rings $k[T]/(T^n)$, where for $n \geqq m$ we have the canonical ring homomorphism

$$f_m^n: k[T]/(T^n) \to k[T]/(T^m).$$

A similar remark applies to power series in several variables.

More generally, let R be a commutative ring and let J be a proper ideal. If $n \geqq m$ we have the canonical ring homomorphism

$$f_m^n: R/J^n \to R/J^m.$$

Let $\bar{R}_J = \lim R/J^n$ be the inverse limit. Then R has a natural homomorphism into $\bar{R}_J$. If R is a Noetherian local ring, then by Krull's theorem (Theorem 5.6 of Chapter X), one knows that $\cap J^n = \{0\}$, and so the natural homorphism of R in its completion is an embedding. This construction is applied especially when J is the maximal ideal. It gives an algebraic version of the notion of holomorphic functions for the following reason.

Let R be a commutative ring and J a proper ideal. Define a J-**Cauchy sequence** $\{x_n\}$ to be a sequence of elements of R satisfying the following condition. Given a positive integer k there exists N such that for all $n, m \geqq N$ we have $x_n - x_m \in J^k$. Define a **null sequence** to be a sequence for which given k there exists N such that for all $n \geqq N$ we have $x_n \in J^k$. Define addition and multipli-

cation of sequences termwise. Then the Cauchy sequences form a ring $\mathfrak{C}$, the null sequences form an ideal $\mathcal{N}$, and the factor ring $\mathfrak{C}/\mathcal{N}$ is called the J-**adic completion** of R. Prove these statements as an exercise, and also prove that there is a natural isomorphism

$$\mathfrak{C}/\mathcal{N} \approx \varprojlim R/J^n.$$

Thus the inverse limit $\varprojlim R/J^n$ is also called the J-adic completion. See Chapter XII for the completion in the context of absolute values on fields.

Examples. In certain situations one wants to determine whether there exist solutions of a system of a polynomial equation $f(X_1, \ldots, X_n) = 0$ with coefficients in a power series ring $k[[T]]$, say in one variable. One method is to consider the ring mod (T^N), in which case this equation amounts to a finite number of equations in the coefficients. A solution of $f(X) = 0$ is then viewed as an inverse limit of truncated solutions. For an early example of this method see [La 52], and for an extension to several variables [Ar 68].

[La 52] S. LANG, On quasi algebraic closure, *Ann of Math.* **55** (1952), pp. 373-390

[Ar 68] M. ARTIN, On the solutions of analytic equations, *Invent. Math.* **5** (1968), pp. 277-291

See also Chapter XII, §7.

In Iwasawa theory, one considers a sequence of Galois cyclic extensions K_n over a number field k of degree p^n with p prime, and with $K_n \subset K_{n+1}$. Let G_n be the Galois group of K_n over k. Then one takes the inverse limit of the group rings $(\mathbf{Z}/p^n\mathbf{Z})[G_n]$, following Iwasawa and Serre. Cf. my *Cyclotomic Fields*, Chapter 5. In such towers of fields, one can also consider the projective limits of the modules mentioned as examples at the end of §1. Specifically, consider the group of p^n-th roots of unity $\boldsymbol{\mu}_{p^n}$, and let $K_n = \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})$, with $K_0 = \mathbf{Q}(\boldsymbol{\mu}_p)$. We let

$$T_p(\boldsymbol{\mu}) = \varprojlim \boldsymbol{\mu}_{p^n}$$

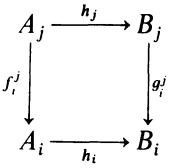
under the homomorphisms $\boldsymbol{\mu}_{p^{n+1}} \to \boldsymbol{\mu}_{p^n}$ given by $\zeta \mapsto \zeta^p$. Then $T_p(\boldsymbol{\mu})$ becomes a module for the projective limits of the group rings. Similarly, one can consider inverse limits for each one of the modules given in the examples at the end of §1. (See Exercise 18.) The determination of the structure of these inverse limits leads to fundamental problems in number theory and algebraic geometry.

After such examples from real life after basic algebra, we return to some general considerations about inverse limits.

Let $(A_i, f_i^j) = (A_i)$ and $(B_i, g_i^j) = (B_i)$ be two inverse systems of abelian groups indexed by the same indexing set. A **homomorphism** $(A_i) \to (B_i)$ is the obvious thing, namely a family of homomorphisms

$$h_i : A_i \to B_i$$

for each i which commute with the maps of the inverse systems:



A sequence

$$0 \to (A_i) \to (B_i) \to (C_i) \to 0$$

is said to be **exact** if the corresponding sequence of groups is exact for each i.

Let (A_n) be an inverse system of sets, indexed for simplicity by the positive integers, with connecting maps

$$u_{m,n} : A_m \to A_n \quad \text{for} \quad m \geqq n.$$

We say that this system satisfies the **Mittag-Leffler condition ML** if for each n, the decreasing sequence $u_{m,n}(A_m)$ $(m \geqq n)$ stabilizes, i.e. is constant for m sufficiently large. This condition is satisfied when $u_{m,n}$ is surjective for all m, n.

We note that trivially, the inverse limit functor is left exact, in the sense that given an exact sequence

$$0 \to (A_n) \to (B_n) \to (C_n) \to 0$$

then

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$$

is exact.

Proposition 10.3. *Assume that* (A_n) *satisfies* **ML**. *Given an exact sequence*

$$0 \to (A_n) \to (B_n) \xrightarrow{g} (C_n) \to 0$$

of inverse systems, then

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

is exact.

Proof. The only point is to prove the surjectivity on the right. Let (c_n) be an element of the inverse limit. Then each inverse image $g^{-1}(c_n)$ is a coset of A_n, so in bijection with A_n. These inverse images form an inverse system, and the **ML** condition on (A_n) implies **ML** on $(g^{-1}(c_n))$. Let S_n be the stable subset

$$S_n = \bigcap_{m \geqq n} u^B_{m,n}(g^{-1}(c_m)).$$

Then the connecting maps in the inverse system (S_n) are surjective, and so there is an element (b_n) in the inverse limit. It is immediate that g maps this element on the given (c_n), thereby concluding the proof of the Proposition.

Proposition 10.4. *Let (C_n) be an inverse system of abelian groups satisfying* **ML**, *and let $(u_{m,n})$ be the system of connecting maps. Then we have an exact sequence*

$$0 \to \varprojlim C_n \to \prod C_n \xrightarrow{1-u} \prod C_n \to 0.$$

Proof. For each positive integer N we have an exact sequence with a finite product

$$0 \to \lim_{1 \leqq n \leqq N} C_n \to \prod_{n=1}^{N} C_n \xrightarrow{1-u} \prod_{n=1}^{N} C_n \to 0.$$

The map u is the natural one, whose effect on a vector is

$$(0, \ldots, 0, c_m, 0, \ldots, 0) \mapsto (0, \ldots, 0, u_{m,m-1}c_m, 0, \ldots, 0).$$

One sees immediately that the sequence is exact. The infinite products are inverse limits taken over N. The hypothesis implies at once that **ML** is satisfied for the inverse limit on the left, and we can therefore apply Proposition 10.3 to conclude the proof.

EXERCISES

1. Let V be a vector space over a field K, and let U, W be subspaces. Show that
$$\dim U + \dim W = \dim(U + W) + \dim(U \cap W).$$
2. Generalize the dimension statement of Theorem 5.2 to free modules over a non zero commutative ring. [*Hint*: Recall how an analogous statement was proved for free abelian groups, and use a maximal ideal instead of a prime number.]
3. Let R be an entire ring containing a field k as a subring. Suppose that R is a finite dimensional vector space over k under the ring multiplication. Show that R is a field.
4. **Direct sums.**
   (a) Prove in detail that the conditions given in Proposition 3.2 for a sequence to split are equivalent. Show that a sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ splits if and only if there exists a submodule N of M such that M is equal to the direct sum $\operatorname{Im} f \oplus N$, and that if this is the case, then N is isomorphic to M''. Complete all the details of the proof of Proposition 3.2.

(b) Let E and $E_i (i = 1, \ldots, m)$ be modules over a ring. Let $\varphi_i: E_i \to E$ and $\psi_i: E \to E_i$ be homomorphisms having the following properties:

$$\psi_i \circ \varphi_i = \mathrm{id}, \qquad \psi_i \circ \varphi_j = 0 \qquad \text{if } i \neq j,$$

$$\sum_{i=1}^{m} \varphi_i \circ \psi_i = \mathrm{id}.$$

Show that the map $x \mapsto (\psi_1 x, \ldots, \psi_m x)$ is an isomorphism of E onto the direct product of the E_i $(i = 1, \ldots, m)$, and that the map

$$(x_1, \ldots, x_m) \mapsto \varphi_1 x_1 + \cdots + \varphi_m x_m$$

is an isomorphism of this direct product onto E.

Conversely, if E is equal to a direct product (or direct sum) of submodules E_i $(i = 1, \ldots, m)$, if we let φ_i be the inclusion of E_i in E, and ψ_i the projection of E on E_i, then these maps satisfy the above-mentioned properties.

5. Let A be an additive subgroup of Euclidean space $\mathbf{R}^n$, and assume that in every bounded region of space, there is only a finite number of elements of A. Show that A is a free abelian group on $\leqq n$ generators. [*Hint*: Induction on the maximal number of linearly independent elements of A over $\mathbf{R}$. Let $v_1, \ldots, v_m$ be a maximal set of such elements, and let A_0 be the subgroup of A contained in the $\mathbf{R}$-space generated by $v_1, \ldots, v_{m-1}$. By induction, one may assume that any element of A_0 is a linear integral combination of $v_1, \ldots, v_{m-1}$. Let S be the subset of elements $v \in A$ of the form $v = a_1 v_1 + \cdots + a_m v_m$ with real coefficients a_i satisfying

$$0 \leqq a_i < 1 \qquad \text{if } i = 1, \ldots, m-1$$

$$0 \leqq a_m \leqq 1.$$

If v'_m is an element of S with the smallest $a_m \neq 0$, show that $\{v_1, \ldots, v_{m-1}, v'_m\}$ is a basis of A over $\mathbf{Z}$.]

Note. The above exercise is applied in algebraic number theory to show that the group of units in the ring of integers of a number field modulo torsion is isomorphic to a lattice in a Euclidean space. See Exercise 4 of Chapter VII.

6. (Artin-Tate). Let G be a finite group operating on a finite set S. For $w \in S$, denote $1 \cdot w$ by $[w]$, so that we have the direct sum

$$\mathbf{Z}\langle S \rangle = \sum_{w \in S} \mathbf{Z}[w].$$

Define an action of G on $\mathbf{Z}\langle S \rangle$ by defining $\sigma[w] = [\sigma w]$ (for $w \in S$), and extending σ to $\mathbf{Z}\langle S \rangle$ by linearity. Let M be a subgroup of $\mathbf{Z}\langle S \rangle$ of rank $\#[S]$. Show that M has a $\mathbf{Z}$-basis $\{y_w\}_{w \in S}$ such that $\sigma y_w = y_{\sigma w}$ for all $w \in S$. (Cf. my *Algebraic Number Theory*, Chapter IX, §4, Theorem 1.)

7. Let M be a finitely generated abelian group. By a **seminorm** on M we mean a real-valued function $v \mapsto |v|$ satisfying the following properties:

$$|v| \geqq 0 \text{ for all } v \in M;$$
$$|nv| = |n|\,|v| \text{ for } n \in \mathbf{Z};$$
$$|v + w| \leqq |v| + |w| \text{ for all } v, w \in M.$$

By the **kernel** of the seminorm we mean the subset of elements v such that $|v| = 0$.

(a) Let M_0 be the kernel. Show that M_0 is a subgroup. If $M_0 = \{0\}$, then the seminorm is called a **norm**.

(b) Assume that M has rank r. Let $v_1, \ldots, v_r \in M$ be linearly independent over $\mathbf{Z}$ mod M_0. Prove that there exists a basis $\{w_1, \ldots, w_r\}$ of M/M_0 such that

$$|w_i| \leqq \sum_{j=1}^{i} |v_j|.$$

[*Hint*: An explicit version of the proof of Theorem 7.8 gives the result. Without loss of generality, we can asume $M_0 = \{0\}$. Let $M_1 = \langle v_1, \ldots, v_r \rangle$. Let d be the exponent of M/M_1. Then dM has a finite index in M_1. Let $n_{j,j}$ be the smallest positive integer such that there exist integers $n_{j,1}, \ldots, n_{j,j-1}$ satisfying

$$n_{j,1}v_1 + \cdots + n_{j,j}v_j = dw_j \text{ for some } w_j \in M.$$

Without loss of generality we may assume $0 \leqq n_{j,k} \leqq d - 1$. Then the elements $w_1, \ldots, w_r$ form the desired basis.]

8. Consider the multiplicative group $\mathbf{Q}^*$ of non-zero rational numbers. For a non-zero rational number $x = a/b$ with $a, b \in \mathbf{Z}$ and $(a, b) = 1$, define the **height**

$$h(x) = \log \max(|a|, |b|).$$

(a) Show that h defines a seminorm on $\mathbf{Q}^*$, whose kernel consists of ± 1 (the torsion group).

(b) Let M_1 be a finitely generated subgroup of $\mathbf{Q}^*$, generated by rational numbers $x_1, \ldots, x_m$. Let M be the subgroup of $\mathbf{Q}^*$ consisting of those elements x such that $x^s \in M_1$ for some positive integer s. Show that M is finitely generated, and using Exercise 7, find a bound for the seminorm of a set of generators of M in terms of the seminorms of $x_1, \ldots, x_m$.

Note. The above two exercises are applied in questions of diophantine approximation. See my Diophantine approximation on toruses, *Am. J. Math.* **86** (1964), pp. 521-533, and the discussion and references I give in *Encyclopedia of Mathematical Sciences, Number Theory III*, Springer Verlag, 1991, pp. 240-243.

Localization

9. (a) Let A be a commutative ring and let M be an A-module. Let S be a multiplicative subset of A. Define $S^{-1}M$ in a manner analogous to the one we used to define $S^{-1}A$, and show that $S^{-1}M$ is an $S^{-1}A$-module.

(b) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, show that the sequence $0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$ is exact.

10. (a) If $\mathfrak{p}$ is a prime ideal, and $S = A - \mathfrak{p}$ is the complement of $\mathfrak{p}$ in the ring A, then $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$. Show that the natural map

$$M \to \prod M_{\mathfrak{p}}$$

of a module M into the direct product of all localizations $M_{\mathfrak{p}}$ where $\mathfrak{p}$ ranges over all *maximal* ideals, is injective.

(b) Show that a sequence $0 \to M' \to M \to M'' \to 0$ is exact if and only if the sequence $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$ is exact for all primes $\mathfrak{p}$.

(c) Let A be an entire ring and let M be a torsion-free module. For each prime $\mathfrak{p}$ of A show that the natural map $M \to M_{\mathfrak{p}}$ is injective. In particular $A \to A_{\mathfrak{p}}$ is injective, but you can see that directly from the imbedding of A in its quotient field K.

Projective modules over Dedekind rings

For the next exercise we assume you have done the exercises on Dedekind rings in the preceding chapter. We shall see that for such rings, some parts of their module theory can be reduced to the case of principal rings by localization. We let $\mathfrak{o}$ be a Dedekind ring and K its quotient field.

11. Let M be a finitely generated torsion-free module over $\mathfrak{o}$. Prove that M is projective. [*Hint*: Given a prime ideal $\mathfrak{p}$, the localized module $M_{\mathfrak{p}}$ is finitely generated torsion-free over $\mathfrak{o}_{\mathfrak{p}}$, which is principal. Then $M_{\mathfrak{p}}$ is projective, so if F is finite free over $\mathfrak{o}$, and $f\colon F \to M$ is a surjective homomorphism, then $f_{\mathfrak{p}}\colon F_{\mathfrak{p}} \to M_{\mathfrak{p}}$ has a splitting $g_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to F_{\mathfrak{p}}$, such that $f_{\mathfrak{p}} \circ g_{\mathfrak{p}} = \mathrm{id}_{M_{\mathfrak{p}}}$. There exists $c_{\mathfrak{p}} \in \mathfrak{o}$ such that $c_{\mathfrak{p}} \notin \mathfrak{p}$ and $c_{\mathfrak{p}} g_{\mathfrak{p}}(M) \subset F$. The family $\{c_{\mathfrak{p}}\}$ generates the unit ideal $\mathfrak{o}$ (why?), so there is a finite number of elements $c_{\mathfrak{p}_i}$ and elements $x_i \in \mathfrak{o}$ such that $\sum x_i c_{\mathfrak{p}_i} = 1$. Let

$$g = \sum x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}.$$

Then show that $g\colon M \to F$ gives a homomorphism such that $f \circ g = \mathrm{id}_M$.]

12. (a) Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Show that there is an isomorphism of $\mathfrak{o}$-modules

$$\mathfrak{a} \oplus \mathfrak{b} \xrightarrow{\approx} \mathfrak{o} \oplus \mathfrak{a}\mathfrak{b}$$

[*Hint*: First do this when $\mathfrak{a}, \mathfrak{b}$ are relatively prime. Consider the homomorphism $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{a} + \mathfrak{b}$, and use Exercise 10. Reduce the general case to the relatively prime case by using Exercise 19 of Chapter II.]

(b) Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals, and let $f\colon \mathfrak{a} \to \mathfrak{b}$ be an isomorphism (of $\mathfrak{o}$-modules, of course). Then f has an extension to a K-linear map $f_K\colon K \to K$. Let $c = f_K(1)$. Show that $\mathfrak{b} = c\mathfrak{a}$ and that f is given by the mapping $m_c\colon x \to cx$ (multiplication by c).

(c) Let $\mathfrak{a}$ be a fractional ideal. For each $b \in \mathfrak{a}^{-1}$ the map $m_b\colon \mathfrak{a} \to \mathfrak{o}$ is an element of the dual $\mathfrak{a}^\vee$. Show that $\mathfrak{a}^{-1} = \mathfrak{a}^\vee = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{a}, \mathfrak{o})$ under this map, and so $\mathfrak{a}^{\vee\vee} = \mathfrak{a}$.

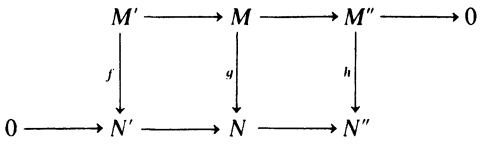
13. (a) Let M be a projective finite module over the Dedekind ring $\mathfrak{o}$. Show that there exist free modules F and F' such that $F \supset M \supset F'$, and F, F' have the same rank, which is called the **rank** of M.

(b) Prove that there exists a basis $\{e_1, \ldots, e_n\}$ of F and ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ such that $M = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_n e_n$, or in other words, $M \approx \oplus\, \mathfrak{a}_i$.

(c) Prove that $M \approx \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ for some ideal $\mathfrak{a}$, and that the association $M \mapsto \mathfrak{a}$ induces an isomorphism of $K_0(\mathfrak{o})$ with the group of ideal classes $\mathrm{Pic}(\mathfrak{o})$. (The group $K_0(\mathfrak{o})$ is the group of equivalence classes of projective modules defined at the end of §4.)

A few snakes

14. Consider a commutative diagram of R-modules and homomorphisms such that each row is exact:



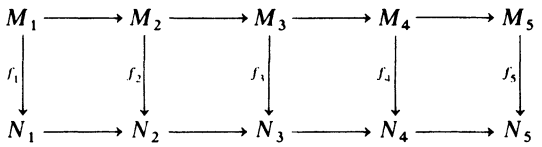
Prove:

(a) If f, h are monomorphisms then g is a monomorphism.

(b) If f, h are surjective, then g is surjective.

(c) Assume in addition that $0 \to M' \to M$ is exact and that $N \to N'' \to 0$ is exact. Prove that if any two of f, g, h are isomorphisms, then so is the third. [*Hint*: Use the snake lemma.]

15. **The five lemma.** Consider a commutative diagram of R-modules and homomorphisms such that each row is exact:



Prove:

(a) If f_1 is surjective and f_2, f_4 are monomorphisms, then f_3 is a monomorphism.

(b) If f_5 is a monomorphism and f_2, f_4 are surjective, then f_3 is surjective. [*Hint*: Use the snake lemma.]

Inverse limits

16. Prove that the inverse limit of a system of simple groups in which the homomorphisms are surjective is either the trivial group, or a simple group.

17. (a) Let n range over the positive integers and let p be a prime number. Show that the abelian groups $A_n = \mathbf{Z}/p^n\mathbf{Z}$ form an inverse system under the canonical homomorphism if $n \geqq m$. Let $\mathbf{Z}_p$ be its inverse limit. Show that $\mathbf{Z}_p$ maps surjectively on each $\mathbf{Z}/p^n\mathbf{Z}$; that $\mathbf{Z}_p$ has no divisors of 0, and has a unique maximal ideal generated by p. Show that $\mathbf{Z}_p$ is factorial, with only one prime, namely p itself.

(b) Next consider all non zero ideals of $\mathbf{Z}$ as forming a directed system, by divisibility. Prove that

$$\varprojlim_{(a)} \mathbf{Z}/(a) = \prod_p \mathbf{Z}_p,$$

where the limit is taken over all non zero ideals (a), and the product is taken over all primes p.

18. (a) Let $\{A_n\}$ be an inversely directed sequence of commutative rings, and let $\{M_n\}$ be an inversely directed sequence of modules, M_n being a module over A_n such that the following diagram is commutative:

$$\begin{array}{ccccc} A_{n+1} & \times & M_{n+1} & \to & M_{n+1} \\ \downarrow & & \downarrow & & \downarrow \\ A_n & \times & M_n & \to & M_n \end{array}$$

The vertical maps are the homomorphisms of the directed sequence, and the horizontal maps give the operation of the ring on the module. Show that $\varprojlim M_n$ is a module over $\varprojlim A_n$.

(b) Let M be a p-divisible group. Show that $T_p(A)$ is a module over $\mathbf{Z}_p$.

(c) Let M, N be p-divisible groups. Show that $T_p(M \oplus N) = T_p(M) \oplus T_p(N)$, as modules over $\mathbf{Z}_p$.

Direct limits

19. Let (A_i, f_j^i) be a directed family of modules. Let $a_k \in A_k$ for some k, and suppose that the image of a_k in the direct limit A is 0. Show that there exists some index $j \geqq k$ such that $f_j^k(a_k) = 0$. In other words, whether some element in some group A_i vanishes in the direct limit can already be seen within the original data. One way to see this is to use the construction of Theorem 10.1.

20. Let I, J be two directed sets, and give the product $I \times J$ the obvious ordering that $(i, j) \leqq (i', j')$ if $i \leqq i'$ and $j \leqq j'$. Let A_{ij} be a family of abelian groups, with homomorphisms indexed by $I \times J$, and forming a directed family. Show that the direct limits

$$\varinjlim_i \varinjlim_j A_{ij} \quad \text{and} \quad \varinjlim_j \varinjlim_i A_{ij}$$

exist and are isomorphic in a natural way. State and prove the same result for inverse limits.

21. Let (M_i', f_j^i), (M_i, g_j^i) be directed systems of modules over a ring. By a **homomorphism**

$$(M_i') \xrightarrow{u} (M_i)$$

one means a family of homomorphisms $u_i : M_i' \to M_i$ for each i which commute with the f_j^i, g_j^i. Suppose we are given an exact sequence

$$0 \to (M_i') \xrightarrow{u} (M_i) \xrightarrow{v} (M_i'') \to 0$$

of directed systems, meaning that for each i, the sequence

$$0 \to M_i' \to M_i \to M_i'' \to 0$$

is exact. Show that the direct limit preserves exactness, that is

$$0 \to \varinjlim M_i' \to \varinjlim M_i \to \varinjlim M_i'' \to 0$$

is exact.

22. (a) Let $\{M_i\}$ be a family of modules over a ring. For any module N show that

$$\mathrm{Hom}(\bigoplus M_i, N) = \prod \mathrm{Hom}(M_i, N)$$

(b) Show that

$$\mathrm{Hom}(N, \prod M_i) = \prod \mathrm{Hom}(N, M_i).$$

23. Let $\{M_i\}$ be a directed family of modules over a ring. For any module N show that

$$\varinjlim \mathrm{Hom}(N, M_i) = \mathrm{Hom}(N, \varinjlim M_i)$$

24. Show that any module is a direct limit of finitely generated submodules.

A module M is called **finitely presented** if there is an exact sequence

$$F_1 \to F_0 \to M \to 0$$

where F_0, F_1 are free with finite bases. The image of F_1 in F_0 is said to be the submodule of **relations**, among the free basis elements of F_0.

25. Show that any module is a direct limit of finitely presented modules (not necessarily submodules). In other words, given M, there exists a directed system $\{M_i, f_j^i\}$ with M_i finitely presented for all i such that

$$M \approx \varinjlim M_i.$$

[*Hint*: Any finitely generated submodule is such a direct limit, since an infinitely generated module of relations can be viewed as a limit of finitely generated modules of relations. Make this precise to get a proof.]

26. Let E be a module over a ring. Let $\{M_i\}$ be a directed family of modules. If E is finitely generated, show that the natural homomorphism

$$\varinjlim \mathrm{Hom}(E, M_i) \to \mathrm{Hom}(E, \varinjlim M_i)$$

is injective. If E is finitely presented, show that this homomorphism is an isomorphism. *Hint*: First prove the statements when E is free with finite basis. Then, say E is finitely presented by an exact sequence $F_1 \to F_0 \to E \to 0$. Consider the diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \varinjlim \mathrm{Hom}(E, M_i) & \longrightarrow & \varinjlim \mathrm{Hom}(F_0, M_i) & \longrightarrow & \varinjlim \mathrm{Hom}(F_1, M_i) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(E, \varinjlim M_i) & \longrightarrow & \mathrm{Hom}(F_0, \varinjlim M_i) & \longrightarrow & \mathrm{Hom}(F_1, \varinjlim M_i)
\end{array}$$

Graded Algebras

Let A be an algebra over a field k. By a **filtration** of A we mean a sequence of k-vector spaces A_i $(i = 0, 1, \ldots)$ such that

$$A_0 \subset A_1 \subset A_2 \subset \cdots \qquad \text{and} \qquad \bigcup A_i = A,$$

and $A_iA_j \subset A_{i+j}$ for all $i, j \geqq 0$. We then call A a filtered algebra. Let R be an algebra. We say that R is **graded** if R is a direct sum $R = \bigoplus R_i$ of subspaces such that $R_iR_j \subset R_{i+j}$ for all $i, j \geqq 0$.

27. Let A be a filtered algebra. Define R_i for $i \geqq 0$ by $R_i = A_i/A_{i-1}$. By definition, $A_{-1} = \{0\}$. Let $R = \bigoplus R_i$, and $R_i = \mathrm{gr}_i(A)$. Define a natural product on R making R into a graded algebra, denoted by $\mathrm{gr}(A)$, and called the **associated graded algebra**.

28. Let A, B be filtered algebras, $A = \bigcup A_i$ and $B = \bigcup B_i$. Let $L: A \to B$ be a k-linear map preserving the filtration, that is $L(A_i) \subset B_i$ for all i, and $L(ca) = L(c)L(a)$ for $c \in k$ and $a \in A_i$ for all i.
    (a) Show that L induces a k-linear map
    $$\mathrm{gr}_i(L): \mathrm{gr}_i(A) \to \mathrm{gr}_i(B) \qquad \text{for all } i.$$
    (b) Suppose that $\mathrm{gr}_i(L)$ is an isomorphism for all i. Show that L is a k-linear isomorphism.

29. Suppose k has characteristic 0. Let $\mathfrak{n}$ be the set of all strictly upper triangular matrices of a given size $n \times n$ over k.
    (a) For a given matrix $X \in \mathfrak{n}$, let $D_1(X), \ldots, D_n(X)$ be its diagonals, so $D_1 = D_1(X)$ is the main diagonal, and is 0 by the definition of $\mathfrak{n}$. Let $\mathfrak{n}_i$ be the subset of $\mathfrak{n}$ consisting of those matrices whose diagonals $D_1, \ldots, D_{n-i}$ are 0. Thus $\mathfrak{n}_0 = \{0\}$, $\mathfrak{n}_1$ consists of all matrices whose components are 0 except possibly for x_{nn}; $\mathfrak{n}_2$ consists of all matrices whose components are 0 except possibly those in the last two diagonals; and so forth. Show that each $\mathfrak{n}_i$ is an algebra, and its elements are nilpotent (in fact the $(i+1)$-th power of its elements is 0).
    (b) Let U be the set of elements $I + X$ with $X \in \mathfrak{n}$. Show that U is a multiplicative group.
    (c) Let exp be the exponential series defined as usual. Show that exp defines a polynomial function on $\mathfrak{n}$ (all but a finite number of terms are 0 when evaluated on a nilpotent matrix), and establishes a bijection
    $$\exp: \mathfrak{n} \to U.$$
    Show that the inverse is given by the standard log series.