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 $(a + b)M = aM + bM$. If N, N' are submodules of M, then $a(N + N') = aN + aN'$.

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**.

III, §1

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

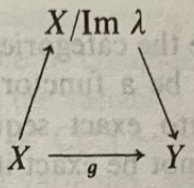
$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y) \leftarrow 0$$

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

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

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

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

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 $D : V \to V$ is a linear map, and $\mathbf{C}[X]$ has the representation $\rho : \mathbf{C}[X] \to \mathrm{End}_{\mathbf{C}}(V)$ 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

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

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 $\rho : R \to \mathrm{End}_A(M)$ into a representation $\rho' : R \to \mathrm{End}_A(M')$, or in other words a **homomorphism of one representation of R to another**, to be an A-module homomorphism $h : M \to M'$ 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

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

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 $\mu(K)$.

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 ri
problems.

Suppose that K is
VI). Then we may viev
VI, §13 we shall prov

In topology, one c
operates on the homo
ring.

With more structu
over the complex nu

the group of divis
in a given dimens
the ordinary hom
the sheaf cohomo

If X is defined o
associate a fancier c
torial with respect t

Then again all t
of automorphism gr
mining their structu
extensive bibliogra

[CCFT 91] P. Cass
L-func
and M
Londo
(1991

[La 82] S. Lang
Bull.

§3. DIRECT SUMS C

Let A be a ring
product as abelian
product, and $a \in$
element a compo
reader will verify
A-modules.

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*

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

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, 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 with $x \neq 0$. 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. Suppose 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 $\{M_i\}$ ... sum $\sum x_i$ (not necessa... $\{M_i\}$ is an arbitrary fa... above is a submodule...

If M is a module ... and $N \cap N' = 0$, then ...

just as with abelian ...

We note, of cour... of our discussion of ... over $\mathbf{Z}$. However, it ... some statements fo... (obviously) for mod...

Let M, M', N be ...

Hom_A(...

and similarly

Hom(...

The first one i... then f induces a h... by composing f ... spectively:

We leave it to th...

gives an isomor... is obtained in a...

and

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

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

and similarly

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

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.

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

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 it 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.

algebraic integers in 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 $W \neq V$, then 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

(1)
$$w_1 = c_1 v_1 + \cdots + c_m v_m,$$

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

$$f(c_1 x_1 + \cdots + c_n x_n) = c_1 f(x_1) + \cdots + c_n f(x_n).$$

Hence $f = a_1 f_1 + \cdots + a_n f_n$, and we see that the f_i generate $E^\vee$. Furthermore, they are linearly independent, for if

$$b_1 f_1 + \cdots + b_n f_n = 0$$

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

$$b_i f_i(x_i) = 0,$$

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

$$A = a_1 x_1 + \cdots + a_n x_n, \qquad B = b_1 f_1 + \cdots + b_n f_n.$$

Then in terms of these coordinates, we see that

$$\langle A, B \rangle = a_1 b_1 + \cdots + a_n b_n = A \cdot B$$

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 a be the set consisting of all elements $a \in R$ such that there exists an element $x \in M$ which can be written

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