NOTES ON MODULES AND ALGEBRAS

WILLIAM SCHMITT

1. Some Remarks about Categories

Throughout these notes, we will be using some of the basic terminology and notation from category theory. Roughly speaking, a *category* $\mathbf{C}$ consists of some class of mathematical structures, called the *objects* of $\mathbf{C}$, together with the appropriate type of mappings between objects, called the *morphisms*, or *arrows*, of $\mathbf{C}$. Here are a few examples:

Category	Objects	Morphisms
Set	sets	functions
Grp	groups	group homomorphisms
Ab	abelian groups	group homomorphisms
$\mathbf{Mod}_R$	left R-modules (where R is some fixed ring)	R-linear maps

For objects A and B belonging to a category $\mathbf{C}$ we denote by $\mathrm{C}(A, B)$ the set of all morphisms from A to B in $\mathbf{C}$ and, for any $f \in \mathrm{C}(A, B)$, the objects A and B are called, respectively, the *domain* and *codomain* of f. For example, if A and B are abelian groups, and we denote by $U(A)$ and $U(B)$ the underlying sets of A and B, then $\mathrm{Ab}(A, B)$ is the set of all group homomorphisms having domain A and codomain B, while $\mathrm{Set}(U(A), U(B))$ is the set of all functions from A to B, where the group structure is ignored.

Whenever it is understood that A and B are objects in some category $\mathbf{C}$ then by a morphism from A to B we shall always mean a morphism from A to B *in the category* $\mathbf{C}$. For example if A and B are rings, a morphism $f\colon A \to B$ is a ring homomorphism, not just a homomorphism of underlying additive abelian groups or multiplicative monoids, or a function between underlying sets.

2. Modules

2.1. **Idea and basic definitions.** Throughout these notes, we shall assume that all rings have unit elements, and that homomorphisms between rings preserve units. Unless explicited indicated otherwise, all modules considered are over commutative rings.

Date: September 9, 2006.

The archetypal example of a group is the collection $\mathrm{Perm}(S)$ of all permutations of a set S, with functional composition as binary operation. Indeed, the beautiful, but almost completely useless, Cayley's theorem states that any group G is isomorphic to a subgroup of $\mathrm{Perm}(S)$ for some set S and, in particular, taking S to be the underlying set $U(G)$ of G always works. (The reason this result is not so useful is that the imbedding of G in $\mathrm{Perm}(U(G))$ given by the theorem is typically so sparse that it yields virtually no information about G.)

There is an analogous result for rings which, for some reason, most algebra textbooks fail to mention. For any abelian group M, the set $\mathrm{End}(M)$ of all endomorphisms of M (i.e., homomorphisms from M into itself) is a ring, with functional composition as multiplication, and pointwise addition, that is, for all $\alpha, \beta \in \mathrm{End}(M)$, the endomorphisms $\alpha\beta$ and $\alpha+\beta$ are respectively determined by $(\alpha\beta)(x) = \alpha(\beta(x))$ and $(\alpha + b)(x) = \alpha(x) + \beta(x)$, for all $x \in M$.

We now show that any ring R is isomorphic to a subring of $\mathrm{End}(U_{\mathbf{Ab}}(R))$, where $U_{\mathbf{Ab}}(R)$ is the underlying additive abelian group of R. Given an element $r \in R$, let $\mu_r \colon R \to R$ be the function determined by $\mu_r(x) = rx$, for all $x \in R$. The left distributive law implies that μ_r in fact belongs to $\mathrm{End}(U_{\mathbf{Ab}}(R))$. Associativity of multiplication is equivalent to the statement that that $\mu_{rs} = \mu_r\mu_s$, while the right distributive law means that $\mu_{r+s} = \mu_r + \mu_s$, for all $r, s \in R$; therefore the mapping $R \to \mathrm{End}(U_{\mathbf{Ab}}(R))$ given by $r \mapsto \mu_r$ is a ring homomorphism. The fact that R has a unit element ensures that this homomorphism is injective, and hence R is isomorphic to a subring of $\mathrm{End}(U_{\mathbf{Ab}}(R))$.

While the interpretation of a group G as a subgroup of $\mathrm{Perm}(U(G))$ is not usually of much interest, the idea of a *representation* of G by permutations, that is, a homomorphism of the form $G \to \mathrm{Perm}(S)$ for some set S (also known as an *action* of G on S) is of fundamental importance; in particular, group actions are among the basic tools in the structure theory of groups, as well as in the theory of enumeration.

The version of Cayley's theorem for rings suggests that, just as groups naturally act on sets, rings act on abelian groups. Indeed, the appropriate notion of representation for a ring R is given by a ring homomorphism $\alpha \colon R \to \mathrm{End}(M)$, for some abelian group M. Such a representation is known as an *R-module*. Writing rx instead of $\alpha(r)(x)$, for $r \in R$ and $x \in M$, allows us to give the following more traditional, equivalent definition.

Definition 2.1. Let R be a ring with unit element 1. An *R-module* consists of an abelian group M together with a map $R \times M \to M$, denoted by $(r, x) \mapsto rx$, such that

(1) $r(x + y) = rx + ry$
(2) $(r + s)x = rx + sx$
(3) $(rs)x = r(sx)$
(4) $1x = x$,

for all $r, s \in R$ and $x, y \in M$.

We remark that the definition we have given here is that of *left* R-module; this is because we have adopted the convention that composition of functions is read from right to left, that is, $\alpha\beta$ means first do β, then do α. Let us write $\mathrm{End}(M)^{\mathrm{op}}$ for the ring of endomorphisms of M with the opposite notational convention for functional composition: $\alpha\beta$ means first do α, then do β. A homomorphism of rings $\alpha\colon R \to \mathrm{End}(M)^{\mathrm{op}}$ is called *right* R-module. Equivalently, we have the following definition.

Definition 2.2. Let R be a ring with unit element 1. An *right R-module* consists of an abelian group M together with a map $R \times M \to M$, denoted by $(r, x) \mapsto xr$, such that

(1) $(x + y)r = xr + yr$
(2) $x(r + s) = xr + xs$
(3) $x(rs) = (xr)s$
(4) $x1 = x$,

for all $r, s \in R$ and $x, y \in M$.

When the ring R is commutative, as it shall be throughout these notes, there is no essential difference between left and right modules.

A *homomorphism* of R-modules, also called an *R-linear map*, is a function $f\colon M \to N$ that is a morphism of underlying abelian groups and commutes with the action of the ring R, that is,

$$f(x + y) = f(x) + f(y) \quad \text{and} \quad f(rx) = rf(x),$$

for all $x, y \in M$ and $r \in R$. We denote by $\mathbf{Mod}_R$ the category of all R-modules, with R-linear maps as morphisms. Hence, if M and N are R-modules, the set of all R-linear maps from M to N is denoted by $\mathrm{Mod}_R(M, N)$.

A subset N of an R-module M is a *submodule* of M if its underlying abelian group is a subgroup of that of M and it is closed under the action of the ring. If $N \subseteq M$ is a submodule, then the quotient abelian group M/N is an R-module, with action defined by $r(x+N) = rx+N$, for all $r \in R$ and $x \in M$. The familiar isomorphism and correspondence theorems for abelian groups hold for modules as well, with essentially no modifications necessary. Some of the more familiar examples of modules are mentioned in the following examples.

Example 2.3. If K is a field, then a K-module is simply a vector space over K and submodules are subspaces.

Example 2.4. Every abelian group is a $\mathbb{Z}$-module and conversely. The action is given by letting nx be the n-fold sum $x + \cdots + x$, for $n \geq 0$ and the $|n|$-fold sum $(-x) + \cdots + (-x)$, for n negative. A submodule of an abelian group, considered as a $\mathbb{Z}$-module, is the same thing as a subgroup.

Example 2.5. Every ring R is a module over itself, with action given by multiplication in R. The R-submodules of R are its ideals. (For noncommutative R, there is both a left and right action of R on itself, given by

multiplication on the left and on the right. The submodules for the left action are the left ideals of R, and the submodules for the right action are the right ideals.)

2.2. **Free modules.** For any subset S of an R-module M, the submodule *generated* by S, denoted by RS, is the smallest submodule of M containing S; it may be described either as the intersection of all submodules of M that contain S, or as the set of all finite sums of the form $\sum_i r_i x_i$, with $r_i \in R$ and $x_i \in S$. A subset $S \subseteq M$ is *linearly independent* if, whenever $x_1, \ldots, x_n$ belong to S and $r_1 x_1 + \cdots + r_n x_n = 0$ for some $r_1, \ldots, r_n \in R$, then $r_1 = \cdots = r_n = 0$. An R-module M is *free* if it is contains a *basis*, that is, a linearly independent subset B such that $RB = M$.

Example 2.6. Every ring R, considered as a module over itself, is free with basis $\{1_R\}$.

Example 2.7. If K is a field, then every K-vector space is a free K-module.

The fact that vector spaces always have bases, and are thus free modules, follows immediately from the following proposition:

Proposition 2.8. *Suppose that V is a K-vector space, S is an independent subset of V, and $x \in V$ is such that $S \cup \{x\}$ is dependent. Then x is contained in the subspace KS generated by S.*

Proof. Since $S \cup \{x\}$ is dependent there exist elements $s_1, \ldots, s_n$ of S, and $r_0, \ldots, r_n$ in R, with some $r_i \neq 0$, such that $r_0 x + r_1 s_1 + \cdots + r_n s_n = 0$. Because S is independent, it follows that $r_0 \neq 0$, and thus we may use the fact that K is a field to write $x = r_1' s_1 + \cdots + r_n' s_n$, where $r_i' = -r_i/r_0$. Hence $x \in KS$. □

In order to prove that any vector space V has a basis, simply use Zorn's Lemma to obtain a maximal independent subset B; it then follows from Proposition 2.8 that B generates, and is thus a basis for, V.

We remark that the converse of Proposition 2.8 holds over any ring R: If S is any subset of an R-module M, and x an element of the submodule RS, then $S \cup \{x\}$ is dependent.

For any set S, the *free module on* S, denoted by $R\{S\}$, consists of all finite formal R-linear combinations of elements of S, under the obvious operations. The module $R\{S\}$ has basis S, and is characterized by the fact that, for any R-module M, restriction of R-linear maps $R\{S\} \to M$ to the set S defines a bijection

$$\mathrm{Mod}_R(R\{S\}, M) \to \mathrm{Set}(S, U(M)).$$

The inverse bijection may be described as "extending by linearity," that is, for any function $f\colon S \to U(M)$, let $\bar{f}\colon R\{S\} \to M$ be the homomorphism defined by $\bar{f}(\sum_i r_i s_i) = \sum_i r_i f(s_i)$; then $f \mapsto \bar{f}$ is the inverse bijection. We refer to $R\{S\}$ as "the" free R-module on S, but the definite article here is being used, as it often is in mathematics, in a weak sense; the module $R\{S\}$

is unique only up to canonical isomorphism; there are (infinitely) many ways of constructing the "formal R-linear combinations" comprising $R\{S\}$.

If M is free with basis $\{b_i : i \in I\}$, then each $x \in M$ may be expressed as a unique R-linear combination of some finite number of b_i's. It follows that M is isomorphic to the direct sum $\bigoplus_{i\in I} R_i$, where each R_i is a copy of the R-module R.

Example 2.9. Any free abelian group, that is, free $\mathbb{Z}$-module, is isomorphic to a direct sum of copies of $\mathbb{Z}$ and thus, in particular, is infinite. Hence any finite abelian group is not free.

One fact that deserves mention here is that a submodule of a free module need not be free. For example, if p and q are prime numbers, then the ring $\mathbb{Z}_{pq}$ of integers modulo pq is free as a module over itself, but it contains as submodules copies of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, which are too small to be free as $\mathbb{Z}_{pq}$-modules. Over certain rings, however, submodules of free modules are always free; for instance, all principal ideal domains have this property.

A word of caution is in order at this point: it is possible for a free module to have bases of different cardinalities. The next example gives a typical instance of this phenomenon:

Example 2.10. Suppose that $M = R\{b_1, b_2, \dots\}$ is the free R-module with basis $\{b_1, b_2, \dots\}$ and that $A = \mathrm{End}_R(M)$ is the endomorphism ring of M. Like any ring, $A = A\{1_A\}$ is free as a module over itself, with basis consisting of the unit element of A, which is the identity map on M in this case. Now let $\varphi_1, \varphi_2 \in A$ be the endomorphisms of M determined by

$$\varphi_1(b_i) \;=\; \begin{cases} b_{(i+1)/2} & \text{if } i \text{ is odd,} \\ 0 & \text{if } i \text{ is even,} \end{cases}$$

and

$$\varphi_2(b_i) \;=\; \begin{cases} 0 & \text{if } i \text{ is odd,} \\ b_{i/2} & \text{if } i \text{ is even.} \end{cases}$$

The A-module A is also free with basis $\{\varphi_1, \varphi_2\}$. To see this, first note that for any $g_1, g_2 \in A$ the endomorphism $h = g_1\varphi_1 + g_2\varphi_2$ satisfies

$$h(b_{2i}) \;=\; g_2\varphi_2(b_{2i}) \;=\; g_2(b_i) \quad \text{and} \quad h(b_{2i-1}) \;=\; g_1\varphi_1(b_{2i-1}) \;=\; g_1(b_i),$$

for all $i \geq 1$. Hence if $g_1\varphi_1 + g_2\varphi_2$ is the zero endomorphism, then g_1 and g_2 must equal zero; thus the set $\{\varphi_1, \varphi_2\}$ is linearly independent.

On the other hand, given any $f \in A$, let f_1, f_2 be the endomorphisms of M determined by

$$f_1(b_i) \;=\; f(b_{2i-1}) \quad \text{and} \quad f_2(b_i) \;=\; f(b_{2i}),$$

for all $i \geq 1$. It follows immediately that $f = f_1\varphi_1 + f_2\varphi_2$; hence $\{\varphi_1, \varphi_2\}$ generates, and is thus a basis for, A.

Fortunately, for modules over a very large class of rings, those said to have *invariant basis number* (which includes all commutative rings, in particular) this cannot occur; all free modules over such rings have well-defined *rank*, given by the cardinality of any basis.

2.3. **Pairings and Duality.** For any R-modules M and N, the set $\mathrm{Mod}_R(M,N)$ of all morphisms from M to N is an abelian group, with addition determined pointwise. Furthermore, since we are assuming the ring R is commutative $\mathrm{Mod}_R(M,N)$ is in fact an R-module, with pointwise R-action: $(rf)(x) = r(f(x))$.

Definition 2.11. The *dual* of an R-module M is the R-module $M^* = \mathrm{Mod}_R(M,R)$, with addition and R-action determined pointwise.

Suppose that M,N and P are R-modules. A mapping $f\colon M \times N \to P$ is called R-*bilinear* if, for each $x_0 \in M$ and $y_0 \in N$, the mappings $f(x_0, -)\colon N \to P$ and $f(-, y_0)\colon M \to P$, given respectively by

$$y \mapsto f(x_0, y) \qquad \text{and} \qquad x \mapsto f(x, y_0),$$

are R-linear. A *pairing from M to N* is a bilinear map $M \times N \to R$. We usually denote the value of a pairing on (x,y) by $\langle x\,, y\rangle$. A pairing $p\colon M \times N \to R$ gives rise to linear maps $\lambda = \lambda_p\colon M \to N^*$ and $\rho = \rho_p\colon N \to M^*$, defined by

$$x \mapsto \langle x\,, \_\rangle \qquad \text{and} \qquad y \mapsto \langle \_\,, y\rangle,$$

respectively. The pairing p is *nondegenerate* if, for each $x \in M$ and $y \in N$, there exist $x' \in N$ and $y' \in M$ such that $\langle x\,, x'\rangle$ and $\langle y'\,, y\rangle$ are nonzero. Equivalently, the pairing p is nondegenerate if each of the maps λ_p and ρ_p is injective.

The *canonical pairing* of the dual module M^* to M is given by the evaluation map:

$$\langle \alpha\,, x\rangle \;=\; \alpha(x),$$

for all $\alpha \in M^*$ and $x \in M$. The maps λ and ρ associated to the canonical pairing are, respectively, the identity map on M^*, and the natural map from M into the double dual M^{**}.

Suppose that M is a free module with basis $B = \{b_1, \ldots, b_n\}$. For $1 \leq i \leq n$, let b_i' be the element of the dual module M^* defined by

$$\langle b_i'\,, b_j\rangle \;=\; \delta_{ij} = \begin{cases} 1_R & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

It is readily verified that the set $B' = \{b_1', \ldots, b_n'\}$ is a basis for the dual module M^* (the proof is identical to the corresponding result for vector spaces), and hence M and M^* are isomorphic R-modules. The basis B' is said to be *dual* to the basis B. The expression for $\alpha \in M^*$ in terms of the

dual basis B' is

$$\alpha = \sum_{i=1}^{n} \langle \alpha \, , b_i \rangle \, b_i',$$

while the expression for $x \in M$ in terms of the basis B is

$$x = \sum_{i=1}^{n} \langle b_i' \, , x \rangle \, b_i.$$

If M is free of finite rank, say $M = R\{b_1, \ldots, b_n\}$, we may define a pairing of M to itself by $\langle b_i \, , b_j \rangle = \delta_{ij}$. This pairing is clearly nondegenerate, and the associated maps λ and ρ are isomorphisms (in fact the same isomorphism) from M onto M^*. We may thus identify M with M^* once we have chosen a basis for M.

We now consider duality for free modules of infinite rank. Now suppose that M is a free R-module with infinite basis $\{b_i\}_{i \in I}$ and again, define $b_i' \in M^*$ by $\langle b_i' \, , b_j \rangle = \delta_{ij}$. We denote by M' the direct product of free modules $\Pi_{i \in I} R\{b_i'\}$, and write the elements $(r_i b_j')_{i \in I}$ of M' as (infinite) formal sums $\sum_{i \in I} r_i b_i'$. (Note that $R\{b_i'\}$ and R are isomorphic R-modules, via the morphism determined by $1_R \mapsto b_i'$.) Even though the elements of M' are infinite linear combinations of the b_i''s, the rule $\langle b_i' \, , b_j \rangle = \delta_{ij}$ determines a well-defined pairing from M' to M, because elements of M are finite linear combinations of b_i's. This pairing induces an isomorphism $\lambda \colon M' \to M^*$, under the inverse of which the element $\alpha \in M^*$ corresponds to $\sum_{i \in I} \langle \alpha \, , b_i \rangle b_i'$. The set $B = \{b_i'\}_{i \in I}$ is independent in M^* but is not a basis because elements of M^* cannot, in general, be written as finite linear combinations of elements of B. In this situation we refer to B, rather, as a *pseudobasis* of M^*. In particular, we note that M is not isomorphic to M^* in this case, but instead is isomorphic to a proper submodule of M^*.

2.4. **Gradings.**

Definition 2.12. An R-module M is *graded* if it is equipped with a direct sum decomposition $\bigoplus_{n \geq 0} M_n$. If M and N are graded R-modules, and $k \in \mathbb{Z}$, an R-module morphism $f \colon M \to N$ is said to be *homogeneous of degree* k if $f(M_n) \subseteq N_{n+k}$, for all $n \geq 0$. (For $k < 0$, we define $N_i = \{0\}$, for all $i < 0$.)

The R-modules M_n are called the *homogeneous components* of the graded module $M = \bigoplus_{n \geq 0} M_n$; an element $x \in M$ is *homogeneous* if it belongs to M_n for some n, in which case the *degree* of x, denote by $|x|$, is equal to n.

Definition 2.13. The *graded dual* of a graded R-module $M = \bigoplus_{n \geq 0} M_n$ is the module $M^{*g} = \bigoplus_{n \geq 0} M_n^*$.

In general, the graded dual of a graded module M is a submodule, and is not equal to, the full dual $\mathrm{Mod}_R(M, R)$ of M.

Definition 2.14. A graded module $M = \bigoplus_{n \geq 0} M_n$ is *free, of finite type* if each homogenous component M_n is a free module of finite rank.

It follows immediately from the discussion above that if a graded module M is free of finite type then it is isomorphic to its graded dual.

2.5. **Tensor Products.**

Definition 2.15. The *tensor product* (*over* R) of R-modules M and N is the R-module $M \otimes N$ generated by the symbols $x \otimes y$, for $x \in M$ and $y \in N$, subject to the relations:

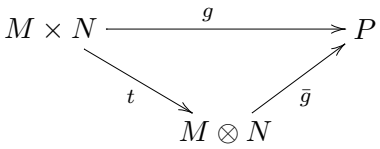
$$(x + x') \otimes y = x \otimes y + x' \otimes y \qquad x \otimes (y + y') = x \otimes y + x \otimes y',$$
$$(rx) \otimes y = r(x \otimes y) = x \otimes (ry),$$

for all $x, x' \in M$, $y, y' \in N$ and $r \in R$.

Exercise 1. Show that $x \otimes 0 = 0 \otimes y = 0$ in $M \otimes N$, for all $x \in M$ and $y \in N$.

In some cases M and N may be modules over more than one ring. Because of the last of the above relations, the choice of ring over which the tensor product is formed plays an important role in determining $M \otimes N$; roughly speaking, the bigger the ring is, the smaller the module $M \otimes N$ will be. Whenever there is possibility of ambiguity, we use the symbol $\otimes_R$, rather than $\otimes$, to denote the tensor product operation.

The relations satisfied by the generators $x \otimes y$ are precisely those needed to ensure that the map $t\colon M \times N \to M \otimes N$ given by $t(x, y) = x \otimes y$ is R-bilinear. The bilinear map t is thus *universal* in the following sense: For any module P and bilinear map $g\colon M \times N \to P$, there exists a unique R-linear map $\bar{g}\colon M \otimes N \to P$ such that $g = \bar{g}t$. This property is most clearly indicated by the statement that the diagram



commutes. (Whenever such a diagram has the property that the composition of morphisms along any two directed paths from one object to another yields the same morphism, the diagram is said to commute.) Another way to state the universal property of the bilinear map t is that the correspondence

$$\mathrm{Mod}_R(M \otimes N, P) \to \mathrm{Bil}_R(M \times N, P), \tag{2.16}$$

given by $f \mapsto ft$ (where $\mathrm{Bil}_R(M \times N, P)$ denotes the set of all R-bilinear maps $M \times N \to P$) is a bijection, with inverse $g \mapsto \bar{g}$.

As is always the case for things satifying universal properties, the tensor product is determined uniquely, up to canonical isomorphism, by its universal property. More precisely, we have the following proposition.

Proposition 2.17. *Suppose that M and N are R-modules, and that $M \otimes' N$ is an R-module and $t'\colon M \times N \to M \otimes' N$ a bilinear map such that, for any R-module P and bilinear map $g\colon M \times N \to P$, there exists a unique R-linear*

map $\hat{g}\colon M \otimes' N \to P$ such that $g = \hat{g}t'$. Then there is a unique R-module isomorphism $f\colon M \otimes N \to M \otimes' N$ such that $ft = t'$.

Proof. The universal property of $t\colon M \times N \to M \otimes N$ implies the existence of a unique R-linear map $f\colon M \otimes N \to M \otimes' N$ such that $ft = t'$, while the universal property of $t'\colon M \times N \to M \otimes' N$ gives a unique R-linear $h\colon M \otimes' N \to M \otimes N$ such that $ht' = t$. We thus have $hft = t$ and $fht' = t'$, and by uniqueness it follows that hf and fh are the identity maps on $M \otimes N$ and $M \otimes' N$, respectively. □

A careful reader will notice that in Definition 2.15 we described the tensor product $M \otimes N$ of R-modules M and N, but did not in fact give a construction of it. For those readers (who might, justifiably, be concerned that tensor products might not even exist in some cases) we briefly describe the construction here. Given R-modules M and N, let F be the free module on the set $M \times N$. (Note that the module structures of M and N play no role in the definition of F.) Let J be the submodule of F generated by all elements of the form

$$(x + x', y) - (x, y) - (x', y) \qquad (x, y + y') - (x, y) - (x, y')$$

$$(rx, y) - r(x, y) \qquad (x, ry) - r(x, y),$$

for $x, x' \in M$, $y, y' \in N$ and $r \in R$. (Note that the module structures of M and N play essential roles in defining J.) The quotient module F/J is the tensor product $M \otimes N$, and the map $t\colon M \times N \to M \otimes N$ is the composition $M \times N \hookrightarrow F \to F/J$ of the canonical projection with the inclusion. For all $x \in M$ and $y \in N$, the element $x \otimes y$ of $M \otimes N$ is the image under t of the pair (x, y).

Sometimes surprising things can happen when forming tensor products, due to the fact that the relations satisfied by the generators $x \otimes y$ can cause more to vanish than one might initially suspect. A standard example of this behavior (Example 2.19) is due to the following proposition.

Proposition 2.18. *Suppose that M and N are abelian groups, and that $x \in M$ and $y \in N$ have orders $|x| = m$ and $|y| = n$. Then the order of $x \otimes y$ in $M \otimes N = M \otimes_{\mathbb{Z}} N$ divides $d = \gcd(m, n)$.*

Proof. Choose integers r and s such that $d = rm + sn$. Then

$$\begin{aligned} d(x \otimes y) &= rm(x \otimes y) + sn(x \otimes y) \\ &= (rmx) \otimes y + x \otimes (sny) \\ &= 0. \end{aligned}$$

□

Example 2.19. If the integers m and n are relatively prime then $\gcd(|x|, |y|) = 1$, for all nonzero $x \in \mathbb{Z}_m$ and $y \in \mathbb{Z}_n$. Thus it follows from Proposition 2.18 that $\mathbb{Z}_m \otimes \mathbb{Z}_n = \{0\}$.

Example 2.20. Viewing the rational numbers $\mathbb{Q}$ as just an abelian group, we have $\mathbb{Q} \otimes M = \{0\}$, for any finite abelian group M. To see this, consider an element $r \otimes x$ in $\mathbb{Q} \otimes M$, with x of order n; then

$$\begin{aligned} r \otimes x &= n(1/n)(r \otimes x) \\ &= (1/n)r \otimes (nx) \\ &= 0. \end{aligned}$$

It is necessary to exercise caution when attempting to define a module morphism $f\colon M \otimes N \to P$ whose domain is a tensor product. When specifying f one needs to make sure that the values $f(x \otimes y)$ satisfy relations in P corresponding to the defining relations on the elements $x \otimes y$; in other words, that

$$f((x+x')\otimes y) = f(x\otimes y) + f(x'\otimes y) \qquad f(x\otimes(y+y')) = f(x\otimes y) + f(x\otimes y'),$$
$$f((rx)\otimes y) = rf(x\otimes y) = f(x\otimes(ry)),$$

for all $x, x' \in M$, $y, y' \in N$ and $r \in R$. The usual technique for doing this is to first define a bilinear map $g\colon M \times N \to P$, then use the universal property of the tensor product, characterized by the bijection (2.16), to obtain a morphism $\bar{g}\colon M \otimes N \to P$; and then let $f = \bar{g}$.

The next proposition shows that, in the case of free modules (of which we shall encounter many), the operation of tensor product is very simple. The proof of the proposition provides a good illustration of the above technique for defining morphisms on tensor products.

Proposition 2.21. *If $M = R\{B\}$ and $N = R\{C\}$ are free R-modules with bases B and C, respectively, then the tensor product $M \otimes N$ is free with basis $\{b \otimes c : b \in B \text{ and } c \in C\}$; in other words, the correspondence $(b, c) \to b \otimes c$ determines an isomorphism from $R\{B \times C\}$ onto $R\{B\} \otimes R\{C\}$.*

Proof. Define a map $\alpha\colon R\{B\} \times R\{C\} \to R\{B \times C\}$ by

$$\left(\sum_i r_i b_i\,,\ \sum_j s_j c_j\right) \mapsto \sum_{i,j} r_i s_j (b_i, c_j).$$

It is readily verified that α is bilinear, and hence induces a morphism $\bar{\alpha}\colon R\{B\} \otimes R\{C\} \to R\{B \times C\}$, under which

$$\left(\sum_i r_i b_i\right) \otimes \left(\sum_j s_j c_j\right) \mapsto \sum_{i,j} r_i s_j (b_i, c_j).$$

On the other hand, since $R\{B \times C\}$ is free, the correspondence $(b, c) \mapsto b \otimes c$ defines a unique morphism $R\{B \times C\} \to R\{B\} \otimes R\{C\}$, and this morphism is inverse to $\bar{\alpha}$. □

Exercise 2. For all all $n, m \geq 2$, the abelian groups $\mathbb{Z}_m \otimes \mathbb{Z}_n$ and $\mathbb{Z}_{\gcd(m,\,n)}$ are isomorphic.

Exercise 3. Suppose that M and N are R-modules, and that $A \subseteq M$ and $B \subseteq N$ are submodules. Show that $M/A \otimes N/B$ is isomorphic to $(M \otimes N)/J$ where $J = A \otimes N + M \otimes B$.

Exercise 4. Given R-modules M, N and P, show that there exist unique isomorphisms

(i) $\lambda = \lambda_M \colon R \otimes M \to M$ and $\rho = \rho_M \colon M \otimes R \to M$,
(ii) $\tau = \tau_{M,N} \colon M \otimes N \to N \otimes M$,
(iii) $\alpha = \alpha_{M,N,P} \colon (M \otimes N) \otimes P \to M \otimes (N \otimes P)$,

satisfying

(i) $\lambda(r \otimes x) = \rho(x \otimes r) = rx$,
(ii) $\tau(x \otimes y) = y \otimes x$,
(iii) $\alpha((x \otimes y) \otimes z) = x \otimes (y \otimes z)$,

for all $r \in R$, $x \in M$, $y \in N$ and $z \in P$.

The families of maps λ, ρ, τ and α are called, respectively, the *left* and *right unit constraints*, the *twist*, and the *associator*.

2.6. **The tensor product of module homomorphisms.**

Proposition 2.22. *If $f_1 \colon M_1 \to N_1$ and $f_2 \colon M_2 \to N_2$ are morphisms of R-modules, then there exists a unique morphism $(f_1 \otimes f_2) \colon M_1 \otimes M_2 \to N_1 \otimes N_2$ satisfying*

$$(f_1 \otimes f_2)(x_1 \otimes x_2) \;=\; f_1(x_1) \otimes f_2(x_2),$$

for all $x_1 \in M_1$ and $x_2 \in M_2$.

Proof. The map $g \colon M_1 \times M_2 \to N_1 \otimes N_2$ given by $g(x_1, x_2) = f_1(x_1) \otimes f_2(x_2)$ is easily checked to be bilinear. Let $f_1 \otimes f_2$ equal $\bar{g}$. □

The map $f_1 \otimes f_2$ is called the *tensor product* of f_1 and f_2.

Proposition 2.23. *If the morphisms $f_1 \colon M_1 \to N_1$ and $f_2 \colon M_2 \to N_2$ are surjective, then the tensor product $(f_1 \otimes f_2) \colon M_1 \otimes M_2 \to N_1 \otimes N_2$ is also surjective.*

Proof. The proof is immediate from the definition of $f_1 \otimes f_2$ and the fact that $N_1 \otimes N_2$ is generated by the set $\{y_1 \otimes y_2 : \; y_1 \in N_1 \text{ and } y_2 \in N_2\}$. □

Important Fact: If R-module morphisms $f_1 \colon M_1 \to N_1$ and $f_2 \colon M_2 \to N_2$ are injective, then it is *not* necessarily the case that $(f_1 \otimes f_2) \colon M_1 \otimes M_2 \to N_1 \otimes N_2$ is injective.

Example 2.24. Suppose that $f \colon \mathbb{Z} \to \mathbb{Q}$ is the inclusion and $g \colon \mathbb{Z}_n \to \mathbb{Z}_n$ is the identity map. Then f and g are injective, while $f \otimes g \colon \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_n \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n$ is not, since $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \mathbb{Z}_n$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$.

Example 2.24 illustrates an important point, which is that a tensor product of submodules need not be a submodule of the tensor product; given submodules $M' \subseteq M$ and $N' \subseteq N$, the tensor product of the inclusion maps $M' \hookrightarrow M$ and $N' \hookrightarrow N$ is a morphism $M' \otimes N' \to M \otimes N$, but is not necessarily injective.

3. Algebras

Definition 3.1. An *R-algebra* is a set A, equipped with both R-module and ring structures having the same underlying additive structure, and such that

$$r(xy) = (rx)y = x(ry), \tag{3.2}$$

for all $r \in R$ and $x, y \in A$. A *homomorphism* of R-algebras is an R-linear ring homomorphism.

Example 3.3. The polynomial ring $R[x]$ is an R-algebra, with the usual multiplication of polynomials by ring elements. More generally, for any set S we denote by $R[S]$ the polynomial algebra having S as set of "independent indeterminants".

Example 3.4. The *divided powers algebra* is the free module $D = R\{d_0, d_1, \dots\}$, with product defined by

$$d_i d_j = \binom{i+j}{i} d_{i+j},$$

for all $i, j \geq 0$. The R-linear map $R[x] \to D$ determined by $x^n \mapsto n! d_n$, for all n, is an algebra homomorphism; if the ring R contains the rational numbers, then this map is an isomorphism.

Example 3.5. If M is any R-module, then the set $\mathrm{End}(M) = \mathrm{Mod}_R(M, M)$ of all endomorphisms of M is an R-algebra, with pointwise addition, multiplication given by functional composition, and R-action given by $(rf)(x) = r(f(x))$, for all $r \in R$, $f \in \mathrm{End}(M)$, and $x \in M$.

Example 3.6. The set $M_n(R)$ of all $n \times n$ matrices with entries in R is an R-algebra under the usual matrix operations. If M is a free R-module of rank n, then choosing a basis for M determines an isomorphism between $M_n(R)$ and the algebra $\mathrm{End}(M)$ of the previous example.

Example 3.7. If S is any set, then the set $\mathrm{Set}(S, U(R))$, of all functions from S into the underlying set of R, is an R-algebra, with all operations defined pointwise.

Example 3.8 ("Ring-first" Definition of Algebra). Suppose that A is a, not necessarily commutative, ring and that $\eta\colon R \to A$ is a ring homomorphism whose image is contained in the center of A (i.e., $\eta(R) \subseteq \{a \in A : ax = xa, \text{ for all } x \in A\}$). The ring A becomes an R-algebra, with R-action defined setting rx equal to the product $\eta(r)x$ in A. On the other hand, any R-algebra A is of the above form, where $\eta\colon R \to A$ is the unique ring homomorphism determined by $\eta(1_R) = 1_A$.

In order to fully understand the dual relationship between the notions of algebra and coalgebra (to be defined in the next section), it is necessary to express the definition of algebra solely in terms of morphisms in the category of R-modules. We begin with the multiplication:

The distributivity of multiplication in an algebra A, together with Equation 3.2, which expresses the compatibility of the multiplication and R-action, means that, viewing A as an R-module, the map $m\colon A \times A \to A$ defined by $(x, y) \mapsto xy$ is R-bilinear. Hence there is a unique R-linear map $\mu\colon A \otimes A \to A$ satisfying $\mu(x \otimes y) = xy$; we refer to the map μ, as well as the binary operation m, as the multiplication on A. Associativity of multiplication now can be expressed by the equality of two different compositions of R-module homomorphisms, most clearly indicated by the commutativity of the diagram

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu\otimes 1} & A \otimes A \\ {\scriptstyle 1\otimes\mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow{\mu} & A. \end{array} \tag{3.9}$$

(Here, and in all other diagrams, 1 denotes the appropriate identity map, rather than the unit element of some ring or algebra.)

The map $\eta\colon R \to A$ in Example 3.8 is called the *unit map* of the algebra A; note that η may be regarded as either as a ring homomorphism or an R-linear map. We now translate the defining property of the unit element 1_A into a corresponding statement about the map η. Consider the diagram of R-modules and R-linear maps

$$\begin{array}{ccccc} R \otimes A & \xrightarrow{\eta\otimes 1} & A \otimes A & \xleftarrow{1\otimes\eta} & A \otimes R \\ & {\scriptstyle\cong}\searrow & \downarrow{\scriptstyle\mu} & \swarrow{\scriptstyle\cong} & \\ & & A, & & \end{array} \tag{3.10}$$

where the diagonal arrows are the canonical isomorphisms $\lambda\colon R\otimes A \to A$ and $\rho\colon A\otimes R \to A$, given by $r\otimes x \mapsto rx$ and $x\otimes r \mapsto rx$, respectively (see Exercise 4). The fact that the unit element $1_A = \eta(1_R)$ satisfies $1_A \cdot x = x = x \cdot 1_A$ means precisely that $\mu(\eta \otimes 1) = \lambda$ and $\mu(1 \otimes \eta) = \rho$. Hence the unit property of 1_A is equivalent to the fact that the diagram commutes. We therefore make the following definition:

Definition 3.11. An *R-algebra* is a triple (A, μ, η), where A is an R-module and $\mu\colon A\otimes A \to A$ and $\eta\colon R \to A$ are R-linear maps such that the diagrams (3.9) and (3.10) commute.

We usually denote the algebra (A, μ, η) simply by A, and write μ_A and η_A for the product and unit maps of A whenever necessary to avoid confusion.

Example 3.12. If G is any monoid, then the free module $R\{G\}$ becomes an R-algebra with product given by the unique map $\mu\colon R\{G\}\otimes R\{G\} \to R\{G\}$ satisfying $\mu(x \otimes y) = xy$, for all $x, y \in G$; in other words, μ is the unique multiplication on $R\{G\}$ extending that of the monoid G. The unit map η of $R\{G\}$ satisfies $\eta(r) = r1_G$, for all $r \in R$; in other words, the unit element of $R\{G\}$ is the identity element of G. The algebra $R\{G\}$ is called the *monoid*

algebra of G. If G happens to be a group, then $R\{G\}$ is called the *group algebra* of G.

Example 3.13. The *free monoid* on a set S is the set $\langle S\rangle$ of all finite sequences of elements of S (that is *words* on S), with concatenation as binary operation. The empty word is the unit element of $\langle S\rangle$. The monoid $\langle S\rangle$ is characterized by the following universal property: for any monoid G, and any function f from S into the underlying set of G, there exists a unique monoid homomorphism $\bar{f}\colon \langle S\rangle \to G$ such that $\bar{f}i = f$, where i denotes the inclusion of S into $\langle S\rangle$. (The homomorphism $\bar{f}$ is defined by $\bar{f}(a_1 \cdots a_n) = f(a_1)\cdots f(a_n)$, for all $a_1 \cdots a_n \in \langle S\rangle$.)

The *free R-algebra* on the set S is the monoid algebra of the free monoid $\langle S\rangle$, and is denoted by $R\langle S\rangle$ (rather than $R\{\langle S\rangle\}$). Hence $R\langle S\rangle$ has as basis the set of all words on S, and is characterized by a combination of the universal properties of free monoids and free R-modules; that is, for any R-algebra A, and any function f from S into the underlying set of A, there exists a unique algebra homomorphism $\bar{f}\colon R\langle S\rangle \to A$ such that $\bar{f}i = f$, where i is the inclusion of S into $R\langle S\rangle$.

Suppose that A and B are R-algebras. The tensor product $A \otimes B$ of underlying R-modules is then an R-algebra, with product determined by $(x_1 \otimes y_1)(x_2 \otimes y_2) = x_1x_2 \otimes y_1y_2$, and unit element $1_{A\otimes B} = 1_A \otimes 1_B$. In terms of module homomorphisms, we have

$$\mu_{A\otimes B} \;=\; (\mu_A \otimes \mu_B)(1 \otimes \tau \otimes 1)$$

and

$$\eta_{A\otimes B} \;=\; (\eta_A \otimes \eta_B)\kappa,$$

where $\tau = \tau_{B,A}\colon B \otimes A \to A \otimes B$ is the twist map and $\kappa\colon R \to R \otimes R$ is the natural isomorphism (which is equal to both the left and right unit constraints; $\lambda_R = \rho_R$, in this case).

Exercise 5. (i) Show that $R[x] \otimes R[x] \cong R[x, y]$, as algebras.

(ii) More generally, show that the algebras $R[S] \otimes R[T]$ and $R[S + T]$ are isomorphic for any sets S and T, where $S + T$ denotes the disjoint union of S and T.

Definition 3.14. An algebra A is *graded* if it has a direct sum decomposition $A = \bigoplus_{n\geq 0} A_n$ (that is, it is graded as an R-module), such that $1_A \in A_0$ and the product $A_iA_j = \{xy\colon x \in A_i \text{ and } y \in A_j\}$ is contained in A_{i+j}, for all $i, j \geq 0$.

Example 3.15. The polynomial algebra $R[x]$ is graded, with homogeneous components $R[x]_n = R\{x^n\}$, for all $n \geq 0$. The divided powers algebra $D = R\{d_0, d_1, \dots\}$ is graded, with $D_n = R\{d_n\}$. Any algebra A may be considered as graded, with all elements homogeneous of degree zero.

If M and N are graded R-modules, then the tensor product $M \otimes N$ is graded, with homogeneous components given by

$$(M \otimes N)_n = \bigoplus_{i+j=n} M_i \otimes N_j,$$

for all $n \geq 0$. We also consider the ring R as graded, with all elements homogeneous of degree zero. An R-algebra A is thus graded if and only if A is graded as an R-module and the product $\mu\colon A \otimes A \to A$ and unit $\eta\colon R \to A$ are homogeneous degree zero maps.