X. Modules over Noncommutative Rings, 553-591

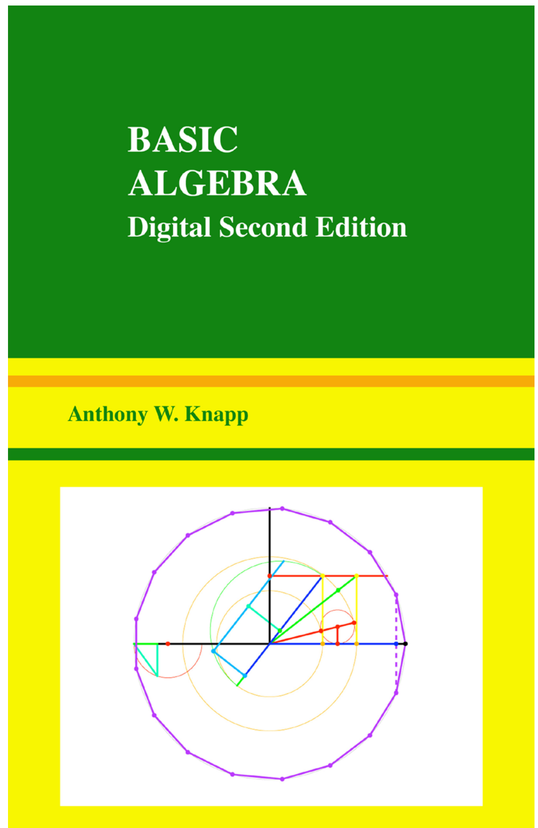
DOI: 10.3792/euclid/9781429799980-10

from

Basic Algebra
Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799980
ISBN: 978-1-4297-9998-0



Distributed by Project Euclid.
For copyright information, see the following page.

Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/∼aknapp

Title: Basic Algebra
Cover: Construction of a regular heptadecagon, the steps shown in color sequence; see page 505.

Mathematics Subject Classification (2010): 15–01, 20–01, 13–01, 12–01, 16–01, 08–01, 18A05, 68P30.

First Edition, ISBN-13 978-0-8176-3248-9
c 2006 Anthony W. Knapp
Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN
c 2016 Anthony W. Knapp
Published by the Author

All rights reserved. This file is a digital second edition of the above named book. The text, images, and other data contained in this file, which is in portable document format (PDF), are proprietary to the author, and the author retains all rights, including copyright, in them. The use in this file of trade names, trademarks, service marks, and similar items, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

All rights to print media for the first edition of this book have been licensed to Birkhäuser Boston, c/o Springer Science+Business Media Inc., 233 Spring Street, New York, NY 10013, USA, and this organization and its successor licensees may have certain rights concerning print media for the digital second edition. The author has retained all rights worldwide concerning digital media for both the first edition and the digital second edition.

The file is made available for limited noncommercial use for purposes of education, scholarship, and research, and for these purposes only, or for fair use as understood in the United States copyright law. Users may freely download this file for their own use and may store it, post it online, and transmit it digitally for purposes of education, scholarship, and research. They may not convert it from PDF to any other format (e.g., EPUB), they may not edit it, and they may not do reverse engineering with it. In transmitting the file to others or posting it online, users must charge no fee, nor may they include the file in any collection of files for which a fee is charged. Any exception to these rules requires written permission from the author.

Except as provided by fair use provisions of the United States copyright law, no extracts or quotations from this file may be used that do not consist of whole pages unless permission has been granted by the author (and by Birkhäuser Boston if appropriate).

The permission granted for use of the whole file and the prohibition against charging fees extend to any partial file that contains only whole pages from this file, except that the copyright notice on this page must be included in any partial file that does not consist exclusively of the front cover page. Such a partial file shall not be included in any derivative work unless permission has been granted by the author (and by Birkhäuser Boston if appropriate).

Inquiries concerning print copies of either edition should be directed to Springer Science+Business Media Inc.

CHAPTER X

Modules over Noncommutative Rings

Abstract. This chapter contains two sets of tools for working with modules over a ring R with identity. The first set concerns finiteness conditions on modules, and the second set concerns the Hom and tensor product functors.

Sections 1–3 concern finiteness conditions on modules. Section 1 deals with simple and semisimple modules. A simple module over a ring is a nonzero unital module with no proper nonzero submodules, and a semisimple module is a module generated by simple modules. It is proved that semisimple modules are direct sums of simple modules and that any quotient or submodule of a semisimple module is semisimple. Section 2 establishes an analog for modules of the Jordan–Hölder Theorem for groups that was proved in Chapter IV; the theorem says that any two composition series have matching consecutive quotients, apart from the order in which they appear. Section 3 shows that a module has a composition series if and only if it satisfies both the ascending chain condition and the descending chain condition for its submodules.

Sections 4–6 concern the Hom and tensor product functors. Section 4 regards $\mathrm{Hom}_R(M, N)$, where M and N are unital left R modules, as a contravariant functor of the M variable and as a covariant functor of the N variable. The section examines the interaction of these functors with the direct sum and direct product functors, the relationship between Hom and matrices, the role of bimodules, and the use of Hom to change the underlying ring. Section 5 introduces the tensor product $M \otimes_R N$ of a unital right R module M and a unital left R module N, regarding tensor product as a covariant functor of either variable. The section examines the effect of interchanging M and N, the interaction of tensor product with direct sum, an associativity formula for triple tensor products, an associativity formula involving a mixture of Hom and tensor product, and the use of tensor product to change the underlying ring. Section 6 introduces the notions of a complex and an exact sequence in the category of all unital left R modules and in the category of all unital right R modules. It shows the extent to which the Hom and tensor product functors respect exactness for part of a short exact sequence, and it gives examples of how Hom and tensor product may fail to respect exactness completely.

1. Simple and Semisimple Modules

This chapter develops further theory for unital modules over a ring with identity beyond what is in Section VIII.1. Results about modules that take advantage of commutativity of the ring were included in Chapter VIII. In the present chapter the ring may or may not be commutative. We shall be interested in those modules whose structure is especially easy to analyze and in constructions that create new modules from old ones. The chapter consists of tools for working with such modules and their related rings and algebras. There are no major theorems in the chapter, but the material here is essential for the developments in several of the chapters of *Advanced Algebra*.

Throughout this chapter, R will denote a ring with identity. We shall work with the category $\mathcal{C}$ of all unital left R modules. Specifically the objects of $\mathcal{C}$ are left unital R modules, and the space of morphisms between two such modules M and N consists of all R homomorphisms from M into N. It is customary to write $\mathrm{Hom}_R(M, N)$ for this set of morphisms.[1] In the special case that R is a field, the notation $\mathrm{Hom}_R(M, N)$ reduces to notation we introduced in Section II.3 for the set of linear maps from one vector space over R to another. For general R, the set $\mathrm{Hom}_R(M, N)$ is an abelian group under addition of the values: $(\varphi_1 + \varphi_2)(m) = \varphi_1(m) + \varphi_2(m)$. Without some further hypothesis on R, $\mathrm{Hom}_R(M, N)$ does not have a natural R module structure.

However, there is some residual action by scalars. Any element z in the **center** Z of R, i.e., any element with $cr = rc$ for all r in R, acts on $\mathrm{Hom}_R(M, N)$. The definition is that $(c\varphi)(m) = \varphi(cm)$. The function $c\varphi$ certainly respects addition, and it respects action by a scalar r in R because $(c\varphi)(rm) = \varphi(crm) = \varphi(rcm) = r\varphi(cm) = r(c\varphi)(m)$; thus $c\varphi$ is in $\mathrm{Hom}_R(M, N)$, and $\mathrm{Hom}_R(M, N)$ becomes a Z module. The center Z automatically contains the multiplicative identity 1 and its integer multiples $\mathbb{Z}\,1$.

We shall tend to ignore this action by the center except in two special cases. One is that R is commutative, and then $\mathrm{Hom}_R(M, N)$ is an R module. The other is that R is an associative algebra (with identity) over a field F. In this case the action of members of F on the identity of R embeds F into R, and F may thus be identified with a subfield of the center of R. The result is that when R is an associative algebra over a field F, then $\mathrm{Hom}_R(M, N)$ is a vector space over F.

We write $\mathrm{End}_R(M)$ for $\mathrm{Hom}_R(M, M)$. This abelian group has the structure of a ring with identity, multiplication being composition: $(\varphi\psi)(m) = \varphi(\psi(m))$. The distributive laws need to be checked: the formula $(\varphi_1 + \varphi_2)\psi = \varphi_1\psi + \varphi_2\psi$ is immediate from the calculation

$$\begin{aligned}((\varphi_1 + \varphi_2)\psi)(m) &= (\varphi_1 + \varphi_2)(\psi(m)) \\ &= \varphi_1(\psi(m)) + \varphi_2(\psi(m)) = (\varphi_1\psi + \varphi_2\psi)(m),\end{aligned}$$

while the formula $\varphi(\psi_1 + \psi_2) = \varphi\psi_1 + \varphi\psi_2$ makes use of the fact that φ respects addition and is proved by the calculation

$$\begin{aligned}(\varphi(\psi_1 + \psi_2))(m) &= \varphi(\psi_1(m) + \psi_2(m)) \\ &= \varphi(\psi_1(m)) + \varphi(\psi_2(m)) = (\varphi\psi_1 + \varphi\psi_2)(m).\end{aligned}$$

[1] The notation $\mathrm{Hom}(M, N)$ with no subscript is sometimes used for $\mathrm{Hom}_{\mathbb{Z}}(M, N)$, i.e., to denote the group of homomorphisms from one abelian group to another.

If Z is the center of R, then $\mathrm{End}_R(M)$ is a Z module, as well as a ring, and the two structures are compatible; the result is that $\mathrm{End}_R(M)$ is an associative Z algebra in the sense of Example 15 in Section VIII.1. In particular, when R is an associative algebra over a field F, then $\mathrm{End}_R(M)$ is an associative F algebra.

There is usually no need to re-prove for right R modules an analog of each result about left R modules. The reason is that we can make use of the **opposite ring** R^o of R, defined to be the same underlying abelian group but with reversed multiplication: $a \circ b = ba$. Any left R module M then becomes a right R^o module M^o under the definition $mr^o = rm$ for r in R, m in M, and r^o equal to the same set-theoretic member of R^o as r. The theory of unital left R modules for all R thereby yields a theory of unital right R modules for all R.

A unital left R module M is said to be **simple**, or **irreducible**, if $M \neq 0$ and if M has no proper nonzero R submodules. If M is simple, then $M = Rx$ for each $x \neq 0$ in M; conversely if $M \neq 0$ has $M = Rx$ for each $x \neq 0$ in M, then M is simple. Whenever $M = Rx$ for an element x, then M is isomorphic as a unital left R module to R/I, where I is the left ideal $I = \{r \in R \mid rx = 0\}$.

A unital left R module M is said to be **semisimple** if M is generated by simple left R submodules, i.e., if it is the sum of simple left R submodules. In this definition, the sum may be empty (and then $M = 0$), it may be finite, or it may be infinite. Evidently simple implies semisimple for unital left R modules.

We come to examples in a moment. First we prove that the sum of simple left R modules in a semisimple module may always be taken to be a direct sum, i.e., that semisimple modules are **completely reducible**.

Proposition 10.1. If the unital left R module M is semisimple, then M is the direct sum of some family of simple R submodules. In more detail if $\{M_s \mid s \in S\}$ is a family of simple R submodules of the unital left R module M whose sum is M, then there is a subset T of S with the property that

$$M = \bigoplus_{t \in T} M_t.$$

PROOF. Call a subset U of S "independent" if the sum $\sum_{u \in U} M_u$ is direct. This condition means that for every finite subset $\{u_1, \dots, u_n\}$ of U and every set of elements $m_i \in M_{u_i}$, the equation $m_1 + \cdots + m_n = 0$ implies that each m_i is 0. From this formulation it follows that the union of any increasing chain of independent subsets of S is itself independent. By Zorn's Lemma there is a maximal independent subset T of S. By definition the sum $M_0 = \sum_{t \in T} M_t$ is direct. Consequently it suffices to show that M_0 is all of M. By the hypothesis on S, it is enough to show that each M_s is contained in M_0. For s in T, this conclusion is clear. Thus suppose s is not in T. By the maximality of T, $T \cup \{s\}$ is not independent. Consequently the sum $M_s + M_0$ is not direct, and it follows that $M_s \cap M_0 \neq 0$. But this intersection is an R submodule of M_s. Since M_s is simple, a nonzero R submodule of M_s must be all of M_s. Thus $M_s \cap M_0 = M_s$, and M_s is contained in M_0. □

EXAMPLES OF SEMISIMPLE MODULES.

(1) Let F be a field. Left and right amount to the same thing for modules when the underlying ring is commutative. We know that the unital F modules are just the vector spaces over F. Such a vector space V is a simple F module if and only if it is 1-dimensional, since 1-dimensionality is the necessary and sufficient condition to have $V \neq 0$ be of the form $V = Fx$ for all $x \neq 0$ in V. Any vector space V is the sum of all of its 1-dimensional subspaces, and consequently every unital F module is semisimple. Theorem 2.42 shows that each vector space V has a basis; this theorem is therefore a special case of Proposition 10.1, which says that any semisimple module is the *direct* sum of simple modules.

(2) Let D be a division ring. Division rings were defined in Section IV.4 as rings with identity $1 \neq 0$ such that the nonzero elements form a group under multiplication. Every field is a division ring, and the quaternions form a division ring that is not a field. Let M be a unital left D module, and let $x \neq 0$ be in M. Then the left D module Dx is simple because if $N \subseteq Dx$ is a nonzero D submodule and if y is in N, then we can write $y = dx$ with d in D and see from the formula $d^{-1}y = x$ that x is in N and $N = Dx$. Any unital left D module is the sum of its D submodules Dx for x in M, and therefore every unital left D module is semisimple. From Proposition 10.1 we can conclude that every unital left D module M is the direct sum of simple modules. In other words, M has a basis, just as if D were a field. Consequently it is customary to refer to unital left D modules as **left vector spaces** over D. A notion of (left) dimension, equal to a well-defined nonnegative integer or ∞, will emerge from the discussion in the next section.

(3) Let D be a division ring. Section V.2 introduced the ring of n-by-n matrices over any commutative ring with identity, and Example 4 of rings in Section VIII.1 extended the definition to the case that the ring is noncommutative. Thus let R be the ring $M_n(D)$. Let $M = D^n$ be the abelian group of n-component column vectors with entries in D. Under multiplication of matrices times column vectors, M becomes a unital left R module. Let us prove that M is simple. It is enough to show that $Rm = M$ for every nonzero m in M. Let m' be in M with entries m'_i, and suppose that the i_0^{th} component m_{i_0} of m is $\neq 0$. Then we can multiply on the left of m by the matrix r whose $(i, j)^{\text{th}}$ entry r_{ij} is $m'_i m_{i_0}^{-1}$ if $(i, j) = (i, j_0)$ and is 0 otherwise, and the product is the column vector m'. Thus m' is in Rm, and $Rm = M$ as required. Hence $M = D^n$ is an example of a simple R module.

(4) Again let D be a division ring, and let $R = M_n(D)$. Let us see that the left R module R is semisimple. In fact, if R_j is the additive subgroup of R whose

nonzero entries are all in the j^{th} column, then R_j is a left R submodule of R that is R isomorphic to D^n. Thus we see that $R = R_1 \oplus \cdots \oplus R_n$ as left R modules, and the left R module R is semisimple as a consequence of Example 3.

(5) Let G be a group, and let $\mathbb{C}G$ be the complex group algebra defined in Example 16 in Section VIII.1. Let V be a vector space over $\mathbb{C}$, and let $\Phi : G \to GL(V)$ be a representation of G on V. The universal mapping property of complex group algebras described in that example and pictured in Figure 8.4 shows that the representation Φ of G extends to $\mathbb{C}G$ and makes V into a unital left $\mathbb{C}G$ module. Conversely if the complex vector space V is a unital left $\mathbb{C}G$ module, then we obtain a representation of G by restriction from $\mathbb{C}G$ to G. What needs to be checked here is that each member of G acts by an invertible linear mapping. This is a consequence of the unital property; since 1 acts as 1, the action by g^{-1} inverts the action of g. Thus we have a one-one correspondence of representations of G on complex vector spaces with unital left $\mathbb{C}G$ module structures. Under this correspondence, irreducible representations of G (i.e., nonzero representations having no proper nonzero invariant subspace) correspond to simple $\mathbb{C}G$ modules. Now suppose that G is finite. Readers who have looked at Section VII.4 know from Corollary 7.21 that every finite-dimensional representation of a finite group G on a complex vector space is the direct sum of irreducible representations; the corresponding $\mathbb{C}G$ modules are therefore semisimple. But more is true. If V is *any* $\mathbb{C}G$ module for the finite group G and if x is in V, then $\mathbb{C}Gx$ is a vector subspace spanned by $\{gx \mid g \in G\}$ and consequently is finite-dimensional. Applying what is known from Section VII.4, we can write $\mathbb{C}Gx$ as the direct sum of simple $\mathbb{C}G$ modules. Therefore the sum of all simple $\mathbb{C}G$ modules in V is all of V, and V is semisimple. From Proposition 10.1 we conclude that every unital left $\mathbb{C}G$ module is semisimple if G is a finite group.

The next proposition shows that decompositions of semisimple modules as direct sums of simple modules behave in a fashion analogous to decompositions of vector spaces as direct sums of 1-dimensional vector subspaces. However, the simple modules need not all be isomorphic to one another, as is shown by Example 5. A theory that takes the isomorphism types of simple modules into account appears in Problems 12–20 at the end of the chapter.

Proposition 10.2. Let M be a semisimple left R module, and suppose that $M = \bigoplus_{s \in S} M_s$ is the direct sum of simple R modules M_s. Let N be any R submodule of M. Then

(a) the quotient module M/N is semisimple. In more detail there is a subset T of S with the property that the submodule $M_T = \bigoplus_{t \in T} M_t$ of M maps R isomorphically onto M/N.

(b) N is a direct summand of M. In more detail, $M = N \oplus M_T$, where M_T is as in (a).

(c) N is semisimple. In more detail choose T as in (a), and write T' for the complement of T in S. Then the quotient mapping $M \to M/M_T$ restricts to an R isomorphism of N onto M/M_T, and M/M_T is R isomorphic to $M_{T'}$.

PROOF. Each simple R submodule M_s of M maps to an R submodule $\overline{M}_s$ of M/N. This image either is simple (and then is R isomorphic to M_s) or is zero. We let U be the subset of S for which it is simple. Then M/N is evidently the sum of the simple R submodules $\{\overline{M}_s \mid s \in U\}$. By Proposition 10.1 there is a subset T of U such that

$$M/N = \bigoplus_{t \in T} \overline{M}_t.$$

This proves (a).

For (b), we use the following elementary observation: if N and N' are R submodules of M, then $M = N \oplus N'$ if and only if the quotient map $M \to M/N$ carries N' isomorphically onto the quotient M/N. Taking $N' = M_T$ and applying (a), we obtain (b).

For (c), the same observation when applied first to $M = N \oplus M_T$ and then to $M = M_{T'} \oplus M_T$ shows that the quotient map $M \to M/M_T$ carries N isomorphically onto M/M_T and carries $M_{T'}$ isomorphically onto M/M_T. Therefore $N \cong M/M_T \cong M_{T'}$, and (c) is proved. □

In the context of simple modules, $\mathrm{Hom}_R(M, N)$ has special properties. Readers who have looked at Section VII.4 have seen these special properties in the context of representations of finite groups on complex vector spaces. There they were captured by Schur's Lemma (Proposition 7.18). If we pass from representations on complex vector spaces to $\mathbb{C}G$ modules, following the prescription in Example 5, we obtain a result about $\mathrm{Hom}_{\mathbb{C}G}(M, N)$ when G is a finite group. Lemma 10.3 and Proposition 10.4 generalize this to a result about $\mathrm{Hom}_R(M, N)$ for arbitrary R.

Lemma 10.3. Suppose that E is a simple left R module and that $M = \bigoplus_{a \in A} M_a$ is a direct-sum decomposition of the unital left R module M into arbitrary R submodules, not necessarily simple. Then

$$\mathrm{Hom}_R(E, M) \cong \bigoplus_{a \in A} \mathrm{Hom}_R(E, M_a)$$

as an isomorphism of abelian groups.

REMARKS. The hypothesis that E is simple is critical here. Without it a map into a direct sum might have nonzero projections into infinitely many of the summands, and then it could not be represented as a finite sum of maps into summands. Proposition 10.12 below will point out that the correct identity without a special hypothesis on E is $\mathrm{Hom}_R(E, \prod_{a\in A} M_a) \cong \prod_{a\in A} \mathrm{Hom}_R(E, M_a)$.

PROOF. Suppose φ is in $\mathrm{Hom}_R(E, M)$. Write φ_a for the composition of φ with the projection $M \to M_a$. The map from left to right in the displayed isomorphism is to be $\varphi \mapsto \{\varphi_a\}_{a\in A}$. Suppose for the moment that the image is contained in the direct sum on the right. The mapping is one-one since M is the sum of the M_a's, and it is onto since the mapping is the identity on each subgroup $\mathrm{Hom}_R(E, M_a)$ of $\mathrm{Hom}_R(E, M)$.

Thus we must show for each φ that only finitely many of the maps φ_a are nonzero. Choose e in E with $\varphi(e) \neq 0$, and write

$$\varphi(e) = m_1 + \cdots + m_n \qquad \text{with } m_i \in M_{a_i}.$$

Since E is simple, $E = Re$. Therefore

$$\begin{aligned}\varphi(E) = R\varphi(e) = R(m_1 + \cdots + m_n) &\subseteq Rm_1 + \cdots + Rm_n \\ &\subseteq M_{a_1} \oplus \cdots \oplus M_{a_n}.\end{aligned}$$

Consequently only $\varphi_{a_1}, \dots, \varphi_{a_n}$ can be nonzero. $\square$

Lemma 10.3 enables us to study maps between semisimple modules in terms of maps between simple modules. The latter are described by the next result.

Proposition 10.4 (Schur's Lemma). Suppose that M and N are simple left R modules.

(a) If M and N are not R isomorphic, then $\mathrm{Hom}_R(M, N) = 0$.

(b) $\mathrm{End}_R(M)$ is a division ring.

(c) (Dixmier) If R is an associative algebra over an algebraically closed field F and if the vector-space dimension of M over F is less than the cardinality of F, then $\mathrm{End}_R(M)$ consists of the F multiples of the identity.

REMARK. In the setting of representations of a finite group G as in Section VII.4, or in the case that G is a finite group and $R = \mathbb{C}G$ in the current setting, any singly generated R module such as M or N is finite-dimensional over $\mathbb{C}$. Part (a) in that case reduces to the statement that the vector space of intertwining operators between two inequivalent irreducible representations is 0. Part (c) in that case says that the space of self-intertwining operators for an irreducible representation consists of the scalar multiples of the identity. For a general R, we get only the weaker conclusion of (b) that $\mathrm{End}_R(M)$ is a division ring. If R is an associative algebra over a field F, we have seen that $\mathrm{End}_R(M)$ is an associative algebra over F, and (c) gives a condition under which we can improve upon (b).

PROOF. Suppose that φ is nonzero in $\mathrm{Hom}_R(M, N)$. Then $\ker\varphi$ is a proper R submodule of M, and we must have $\ker\varphi = 0$ since M is simple. Similarly $\mathrm{image}\,\varphi$ is a nonzero R submodule of N, and we must have $\mathrm{image}\,\varphi = F$ since N is simple. Therefore φ is an R isomorphism of M onto N. This proves (a) and (b).

For (c) let m be a nonzero element of M. The map $\varphi \mapsto \varphi(m)$ is F linear and one-one from $\mathrm{End}_R(M)$ into M by (b). Thus $\mathrm{End}_R(M)$ as an associative division algebra over F has vector-space dimension at most the vector-space dimension of M, and the latter by hypothesis is strictly less than the cardinality of F. Arguing by contradiction, let us assume that $\mathrm{End}_R(M)$ is not equal to F; say $\mathrm{End}_R(M)$ contains an element φ not in F.

The smallest division subalgebra of $\mathrm{End}_R(M)$ containing F and φ is the field $\overline{F}$ generated by F and φ. Since F is algebraically closed, φ is not a root of any nonzero polynomial with coefficients in F. Thus the substitution homomorphism equal to the identity on F and carrying X to φ is one-one from $F[X]$ into $\overline{F}$. By the universal mapping property of fields of fractions (Proposition 8.6), the substitution homomorphism factors through the field of fractions $F(X)$. Thus we may regard $F(X)$ as a subfield of $\overline{F}$. In the field $F(X)$, the set of elements $\{(X-c)^{-1} \mid c \in F\}$ is linearly independent over F, as we see by assuming a nontrivial linear dependence and clearing fractions, and hence $\dim_F F(X)$ is $\geq$ the cardinality of F. Since $\mathrm{End}_R(M) \supseteq \overline{F} \supseteq F(X)$ under our identification, the dimension of $\mathrm{End}_R(M)$ over F is $\geq$ the cardinality of F. This conclusion contradicts the observation of the previous paragraph that the dimension of $\mathrm{End}_R(M)$ is strictly less than the cardinality of F. So the assumption that $\mathrm{End}_R(M)$ contains an element not in F must be false, and (c) follows. $\square$

2. Composition Series

We continue with R as a ring with identity, and we work with the category of all unital left R modules. In this section we shall say what is meant by a unital left R module of "finite length," and we shall investigate semisimplicity for such modules.

A **finite filtration** of a unital left R module M is a finite descending chain

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$$

of R submodules. We do not insist on this particular indexing, and with the obvious adjustments, we allow also a finite increasing chain to be called a finite filtration. Relative to the displayed inclusions, the modules M_i/M_{i+1} for $0 \leq i \leq n-1$ are called the **consecutive quotients** of the filtration. The finite filtration is called a **composition series** if the consecutive quotients are all simple

R modules; in particular, they are to be nonzero. The consecutive quotients in this case are called **composition factors**.

We encountered an analogous notion with groups in Section IV.8, but there was a complication in that case. The complication was that each subgroup had to be normal in the next-larger subgroup in order for the consecutive quotients to be groups. The overlap between the current treatment and the earlier treatment occurs for abelian groups, which on the one hand are unital $\mathbb{Z}$ modules and on the other hand are groups whose subgroups are automatically normal.

We are going to obtain analogs for the category of unital left R modules of the group-theoretic results of Zassenhaus, Schreier, and Jordan–Hölder in Section IV.8. The ones here will be a little easier to prove than those in Section IV.8 since we do not have the complication of checking whether subgroups are normal. Let

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_m = 0$$

and

$$M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = 0$$

be two finite filtrations of M. We say that the second is a **refinement** of the first if there is a one-one function $f : \{0, \dots, m\} \to \{0, \dots, n\}$ with $M_i = N_{f(i)}$ for $0 \leq i \leq m$. The two finite filtrations of M are said to be **equivalent** if $m = n$ and if the order of the consecutive quotients $M_0/M_1, M_1/M_2, \dots, M_{m-1}/M_m$ may be rearranged so that they are respectively isomorphic to $N_0/N_1, N_1/N_2, \dots, N_{m-1}/N_m$.

Lemma 10.5 (Zassenhaus). Let M_1, M_2, M_1', and M_2' be R submodules of a unital left R module M with $M_1' \subseteq M_1$ and $M_2' \subseteq M_2$. Then

$$\begin{aligned}((M_1 \cap M_2) + M_1')/((M_1 \cap M_2') + M_1')& \\ \cong ((M_1 \cap M_2) + M_2')/((M_1' \cap M_2) + M_2').&\end{aligned}$$

PROOF. By the Second Isomorphism Theorem (Theorem 8.4),

$$\begin{aligned}(M_1 \cap M_2)/(((M_1 \cap M_2') + M_1') \cap (M_1 \cap M_2))& \\ \cong ((M_1 \cap M_2) + (M_1 \cap M_2') + M_1')/((M_1 \cap M_2') + M_1')& \\ = ((M_1 \cap M_2) + M_1')/((M_1 \cap M_2') + M_1').&\end{aligned}$$

Since we have

$$\begin{aligned}((M_1 \cap M_2') + M_1') \cap (M_1 \cap M_2) &= ((M_1 \cap M_2') + M_1') \cap M_2 \\ &= (M_1 \cap M_2') + (M_1' \cap M_2),\end{aligned}$$

we can rewrite the above isomorphism as

$$\begin{aligned}(M_1 \cap M_2)/((M_1 \cap M_2') + (M_1' \cap M_2))& \\ \cong ((M_1 \cap M_2) + M_1')/((M_1 \cap M_2') + M_1').&\end{aligned}$$

The left side of this isomorphism is symmetric under interchange of the indices 1 and 2. Hence so is the right side, and the lemma follows. $\square$

Theorem 10.6 (Schreier). Any two finite filtrations of a module M in $\mathcal{C}$ have equivalent refinements.

PROOF. Let the two finite filtrations be

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_m = 0$$

and
$$M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = 0,$$

and define

$$M_{ij} = (M_i \cap N_j) + M_{i+1} \qquad \text{for } 0 \le i \le m-1 \text{ and } 0 \le j \le n,$$

$$N_{ji} = (M_i \cap N_j) + N_{j+1} \qquad \text{for } 0 \le i \le m \text{ and } 0 \le j \le n-1.$$

Then

$$\begin{aligned} M &= M_{00} \supseteq M_{01} \supseteq \cdots \supseteq M_{0n} \\ &\supseteq M_{10} \supseteq M_{11} \supseteq \cdots \supseteq M_{1n} \supseteq \cdots \supseteq M_{m-1,n} = 0 \end{aligned}$$

and
$$\begin{aligned} M &= N_{00} \supseteq N_{01} \supseteq \cdots \supseteq N_{0m} \\ &\supseteq N_{10} \supseteq N_{11} \supseteq \cdots \supseteq N_{1m} \supseteq \cdots \supseteq N_{n-1,m} = 0 \end{aligned}$$

are refinements of the respective given filtrations. The containments $M_{in} \supseteq M_{i+1,0}$ and $N_{jm} \supseteq N_{j+1,0}$ are equalities here, and the only nonzero consecutive quotients are therefore of the form $M_{ij}/M_{i,j+1}$ and $N_{ji}/N_{j,i+1}$. For these we have

$$\begin{aligned} &M_{ij}/M_{i,j+1} \\ &\quad = ((M_i \cap N_j) + M_{i+1})/((M_i \cap N_{j+1} + M_{i+1}) && \text{by definition} \\ &\quad \cong ((M_i \cap N_j) + N_{j+1})/((M_{i+1} \cap N_j) + N_{j+1}) && \text{by Lemma 10.5} \\ &\quad = N_{ji}/N_{j,i+1} && \text{by definition,} \end{aligned}$$

and thus the above refinements are equivalent. □

Corollary 10.7 (Jordan–Hölder Theorem). If M is a unital left R module with a composition series, then

(a) any finite filtration of M in which all consecutive quotients are nonzero can be refined to a composition series, and
(b) any two composition series of M are equivalent.

PROOF. We apply Theorem 10.6 to a given filtration and a known composition series. After discarding redundant terms from each refinement (those that lead to 0 as a consecutive quotient), we arrive at a refinement of our given finite filtration that is equivalent to the known composition series. Hence the refinement is a composition series. This proves (a). If we specialize this argument to the case that the given filtration is a composition series, then we obtain (b). □

Corollary 10.7 implies that the composition factors for a given composition series depend only on M, not on the particular composition series. Moreover, if $M' \supseteq M''$ are R submodules of an M with a composition series such that M'/M'' is simple, then M'/M'' is a composition factor of M. This fact follows by eliminating redundant terms from the finite filtration $M \supseteq M' \supseteq M'' \supseteq 0$ and applying Corollary 10.7a to the result.

If a unital left R module M has a composition series, then we say that M has **finite length**. This notion is closed under passage to submodules and quotients. In fact, if

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$$

is a composition series of M and if M' is an R submodule of M, then

$$M' = M_0 \cap M' \supseteq M_1 \cap M' \supseteq \cdots \supseteq M_n \cap M' = 0$$

is a finite filtration of M' in which each consecutive quotient is simple or 0. Discarding redundant terms (which lead to 0 as a consecutive quotient), we obtain a composition series for M'. A similar argument works for M/M'.

Let us see that if the unital left R modules M' and M/M' have finite length, then so does M. In fact, we take a composition series for M/M', pull it back to M, and concatenate it to a composition series for M'. The result is a composition series for M, and the assertion follows. In particular, the direct sum of two unital left R modules of finite length has finite length.

If M has a composition series of the form $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$, then we say that M has **length** n. If it has no composition series, we say it has infinite length. According to Corollary 10.7, this notion of length is independent of the particular composition series that we use. The argument in the previous paragraph shows that if M' is an R submodule of M, then

$$\text{length}(M) = \text{length}(M') + \text{length}(M/M'),$$

with the finiteness of either side implying the finiteness of the other side. One consequence is that if M' is a length-n submodule of a length-n module M with n finite, then $M' = M$. Another consequence is that if M is a semisimple left R module, then M has a composition series if and only if M is the *finite* direct sum of simple left R modules.

From the last of these observations, we see that if F is a field, then the vector spaces over F that have a composition series are the finite-dimensional vector spaces, and in this case the length of the vector space is its dimension. The structure of finite-dimensional vector spaces is so elementary that the Jordan–Hölder Theorem is of no interest in this case, and it was for that reason that no version of the Jordan–Hölder Theorem for vector spaces appeared earlier in the book.

In the case that $R = D$ is a division ring, matters are slightly subtler. We know from Example 2 in Section 1 that every unital left D module is semisimple, and we noted that such D modules are therefore called left vector spaces. Corollary 10.7 shows that the number of summands in any decomposition of a left vector space V as the direct sum of simple D modules is either an integer $n \geq 0$ independent of the decomposition or is infinite, independently of the decomposition. This number, the integer n or ∞, is called the **dimension** of the left vector space V.

We saw one other example of a semisimple left R module. Specifically if D is a division ring, then we saw in Example 4 of Section 1 that $R = M_n(D)$ is semisimple as a left R module. The number of simple summands is n, and hence R has length n. So R has a composition series when considered as a left R module.

There are two other cases in which composition series give something familiar. One is the case that R is the ring $\mathbb{Z}$ of integers. A unital $\mathbb{Z}$ module is an abelian group, and we know that the simple abelian groups are the cyclic groups of prime order. For an abelian group with a composition series, the order of the group is the product of the orders of the consecutive quotients and hence is finite. Consequently an abelian group has a composition series if and only if it is a finite abelian group. Such a group need not be semisimple; the group C_4, for example, is not the direct sum of cyclic groups of prime order.

The other case concerns triangular form, Jordan canonical form, and related decompositions, as explained in Sections V.3 and V.6 and as reinterpreted after Corollary 8.29. Let V be a finite-dimensional vector space over a field $\mathbb{K}$, and let $L : V \to V$ be a linear mapping from V to itself. Put $R = \mathbb{K}[X]$, and make V into a unital R module by the definition $A(X)(v) = A(L)v$ for any $A(X)$ in $\mathbb{K}[X]$ and v in V. The R submodules are the vector subspaces of V that are invariant under L. The finite dimensionality of V forces V to have a composition series as an R module. Let us suppose for a moment that $\mathbb{K}$ is algebraically closed. Proposition 5.6 says that the matrix of L in some ordered basis is upper triangular, and linear combinations of the first k vectors in this basis form an invariant subspace under L of dimension k. These subspaces are nested, and thus we obtain a composition series. Thus obtaining a composition series when $\mathbb{K}$ is algebraically closed is equivalent to obtaining triangular form. The existence of Jordan form is a finer result. The discussion after Corollary 8.29 shows that V is a finite direct sum of R modules $R/(X - c_j)^{k_j}$ with c_j in $\mathbb{K}$ and $k_j > 0$. For each of these, the discussion at the end of Section VIII.6 shows how to refine $R/(X - c_j)^{k_j}$ to a composition series for which there is an R submodule of each possible dimension from 0 to k_j; the finer structure is hidden in the way that each invariant subspace is obtained from the next smaller invariant subspace. If $\mathbb{K}$ is not necessarily algebraically closed, then $(X - c_j)^{k_j}$ is to be replaced by $P_j(X)^{k_j}$ for some prime polynomial $P_j(X)$, and the consecutive quotients for $R/(P_j(X))^{k_j}$ have dimension equal to the degree of $P_j(X)$.

3. Chain Conditions

We continue with R as a ring with identity, and we work with the category of all unital left R modules. Except in special cases we did not address conditions in Section 2 under which a unital left R module M has a composition series. In this section we shall see that a necessary and sufficient condition for M to have a composition series is that it satisfy two "chain conditions," an ascending one and a descending one, that we shall define. We already encountered the ascending chain condition in Proposition 8.30 for the special case that R is a commutative ring with identity, and the proof for general R requires only cosmetic changes.

Proposition 10.8. If R is a ring with identity and M is a unital left R module, then the following conditions on R submodules of M are equivalent:

(a) (**ascending chain condition**) every strictly ascending chain of R submodules $M_1 \subsetneqq M_2 \subsetneqq \cdots$ terminates in finitely many steps,

(b) (**maximum condition**) every nonempty collection of R submodules has a maximal element under inclusion,

(c) (**finite basis condition**) every R submodule is finitely generated.

PROOF. To see that (a) implies (b), let $\mathcal{S}$ be a nonempty collection of R submodules of M. Take M_1 in $\mathcal{S}$. If M_1 is not maximal, choose M_2 in $\mathcal{S}$ properly containing M_1. If M_2 is not maximal, choose M_3 in $\mathcal{S}$ properly containing M_2. Continue in this way. By (a), this process must terminate, and then we have found a maximal R submodule in $\mathcal{S}$.

To see that (b) implies (c), let N be an R submodule of M, and let $\mathcal{S}$ be the collection of all finitely generated R submodules of N. This collection is nonempty since 0 is in it. By (b), $\mathcal{S}$ has a maximal element, say N'. If x is in N but x is not in N', then $N' + Rx$ is a finitely generated R submodule of N that properly contains N' and therefore gives a contradiction. We conclude that $N' = N$, and therefore N is finitely generated.

To see that (c) implies (a), let $M_1 \subsetneqq M_2 \subsetneqq \cdots$ be given, and put $N = \bigcup_{n=1}^{\infty} M_n$. By (c), N is finitely generated. Since the M_n are increasing with n, we can find some M_{n_0} containing all the generators. Then the sequence stops no later than at M_{n_0}. $\square$

The corresponding result for descending chains is as follows.

Proposition 10.9. If R is a ring with identity and M is a unital left R module, then the following conditions on R submodules of M are equivalent:

(a) (**descending chain condition**) every strictly descending chain of R submodules $M_1 \supsetneqq M_2 \supsetneqq \cdots$ terminates in finitely many steps,

(b) (**minimum condition**) every nonempty collection of R submodules has a minimal element under inclusion.

PROOF. To see that (a) implies (b), let $\mathcal{S}$ be a nonempty collection of R submodules of M. Take M_1 in $\mathcal{S}$. If M_1 is not minimal, choose M_2 in $\mathcal{S}$ properly contained in M_1. If M_2 is not minimal, choose M_3 in $\mathcal{S}$ properly contained in M_2. Continue in this way. By (a), this process must terminate, and then we have found a minimal R submodule in $\mathcal{S}$.

To see that (b) implies (a), we observe that the members of any strictly descending chain would be a family without a minimal element. Since (b) says that any nonempty family has a minimal element, there can be no such chain. $\square$

Proposition 10.10. Let R be a ring with identity, let M be a unital left R module, and let N be an R submodule of M. Then

(a) M satisfies the ascending chain condition if and only if N and M/N satisfy the ascending chain condition,

(b) M satisfies the descending chain condition if and only if N and M/N satisfy the descending chain condition.

PROOF. We prove (a), and the proof of (b) is completely similar. Suppose M satisfies the ascending chain condition and hence also the maximum condition by Proposition 10.8. The R submodules of N are in particular R submodules of M and hence satisfy the maximum condition. The R submodules of M/N lift back to R submodules of M containing N, and they too must satisfy the maximum condition. By Proposition 10.8, N and M/N satisfy the ascending chain condition.

Conversely suppose that N and M/N satisfy the ascending chain condition. Let $\{M_l\}$ be an ascending chain of R submodules of M; we are to show that $\{M_l\}$ is constant from some point on. Since N and M/N satisfy the ascending chain condition, we can find an n such that

$$M_{n+k} \cap N = M_n \cap N \qquad \text{and} \qquad (M_{n+k} + N)/N = (M_n + N)/N$$

for all $k \geq 0$. Combining the Second Isomorphism Theorem (Theorem 8.4) and the first of these identities gives

$$(M_{n+k} + N)/N \cong M_{n+k}/(M_{n+k} \cap N) = M_{n+k}/(M_n \cap N)$$

for all $k \geq 0$. Combining this result and two applications of the second of the identities gives

$$M_{n+k}/(M_n \cap N) = M_n/(M_n \cap N).$$

The First Isomorphism Theorem (Theorem 8.3) shows that

$$\big(M_{n+k}/(M_n \cap N)\big)\big/\big(M_n/(M_n \cap N)\big) \cong M_{n+k}/M_n.$$

Since the left side is the 0 module, the right side is the 0 module. Therefore $M_{n+k} = M_n$ for all $k \geq 0$. $\square$

Proposition 10.11. If R is a ring with identity and M is a unital left R module, then M has a composition series if and only if M satisfies both the ascending chain condition and the descending chain condition.

PROOF. If M has a composition series of length n, then the Jordan–Hölder Theorem (Corollary 10.7a) shows that every finite filtration of M with nonzero consecutive quotients has length $\leq n$, and hence M satisfies both chain conditions.

Conversely suppose that M satisfies both chain conditions. By the maximum condition, choose if possible a maximal proper R submodule N_1 of M, then choose if possible a maximal proper R submodule N_2 of N_1, and so on. If all these choices are possible, we obtain a strictly descending chain $M \supsetneqq N_1 \supsetneqq N_2 \supsetneqq \cdots$, and the consecutive quotients will be simple at each stage. The minimum condition says that we cannot have such a chain, and thus the choice is impossible for the first time at some stage k. That means that some N_k has no proper R submodule, and N_k must be 0. Then $M = N_1 \supsetneqq N_2 \supsetneqq \cdots \supsetneqq N_k = 0$ is a composition series. $\square$

4. Hom and End for Modules

We continue to work with the category $\mathcal{C}$ of unital left R modules, where R is a ring with identity, not necessarily commutative. Our interest in this section is with $\mathrm{Hom}_R(M, N)$ and $\mathrm{End}_R(M)$, where M and N are modules in $\mathcal{C}$. Recall from Section 1 that $\mathrm{Hom}_R(M, N)$ is a unital Z module, where Z is the center of R, and that $\mathrm{End}_R(M)$ is a Z algebra, the multiplication being composition. We shall tend to ignore Z except when R is commutative or R is an associative algebra over a field. However, Z will implicitly play a role in the context of bimodules, which we introduce near the end of this section.

In this section we shall be interested in interactions of $\mathrm{Hom}_R(M, N)$ and $\mathrm{End}_R(M)$ within the category $\mathcal{C}$, in identities that they satisfy, in the naturality of such identities, and in the use of $\mathrm{Hom}_R(M, N)$ in "change of rings," also known as "extension of scalars." The next section will carry out a similar investigation for a notion of tensor product that generalizes the tensor products in Chapter VI, and we shall obtain in addition one important formula involving Hom and tensor products at the same time. Finally in Section VI we shall examine the effect of Hom and tensor product on "exact sequences."

The first observation is that Hom_R is a functor, either a functor of one variable with the other variable held fixed or, less satisfactorily, a functor of two variables. To be precise, let $\mathcal{D}$ be the category of all abelian groups. For fixed M in $\mathrm{Obj}(\mathcal{C})$, we define

$$F(N) = \mathrm{Hom}_R(M, N).$$

If φ is in $\mathrm{Hom}_R(N, N')$, we define $F(\varphi)$ in $\mathrm{Hom}_{\mathbb{Z}}\big(\mathrm{Hom}_R(M,N), \mathrm{Hom}_R(M,N')\big)$ by the formula

$$F(\varphi)(\tau) = \varphi\tau \qquad \text{for } \tau \in \mathrm{Hom}_R(M, N),$$

where $\varphi\tau$ denotes the composition of τ followed by φ. In other words, $F(\varphi)$ is given by *post*multiplication by φ. By inspection we see that $F(1_N)$ is the identity from $\mathrm{Hom}_R(M, N)$ to itself if 1_N is the identity on N and that $F(\varphi'\varphi) = F(\varphi')F(\varphi)$ if φ' is in $\mathrm{Hom}_R(N', N'')$; the latter formula comes down to the associativity formula $(\varphi'\varphi)\tau = \varphi'(\varphi\tau)$ for functions under composition. Therefore F is a covariant functor from the category $\mathcal{C}$ to the category $\mathcal{D}$. We write $\mathrm{Hom}(1, \varphi)$ for $F(\varphi)$, so that $\mathrm{Hom}(1, \varphi)(\tau) = \varphi\tau$.

Similarly for fixed N in $\mathrm{Obj}(\mathcal{C})$, we define

$$G(M) = \mathrm{Hom}_R(M, N).$$

On morphisms, G is given by *pre*multiplication. Specifically for a morphism ψ in $\mathrm{Hom}_R(M, M')$, we define $G(\psi)$ in $\mathrm{Hom}_{\mathbb{Z}}\big(\mathrm{Hom}_R(M', N), \mathrm{Hom}_R(M, N)\big)$ by the formula

$$G(\psi)(\tau) = \tau\psi \qquad \text{for } \tau \in \mathrm{Hom}_R(M', N).$$

We readily check that G is a contravariant functor from $\mathcal{C}$ to $\mathcal{D}$. We write $\mathrm{Hom}(\psi, 1)$ for $G(\psi)$, so that $\mathrm{Hom}(\psi, 1)(\tau) = \tau\psi$.

To create a single functor H from F and G, we can try to define a functor H from $\mathcal{C}^2$ to $\mathcal{D}$ by $H(M, N) = \mathrm{Hom}_R(M, N)$. If $\varphi \in \mathrm{Hom}_R(N, N')$ and $\psi \in \mathrm{Hom}_R(M, M')$ are given, we can try the formula $H(\psi, \varphi)(\tau) = \varphi\tau\psi$ as a definition for τ in $\mathrm{Hom}_R(M', N)$. The trouble is that H is mixed as contravariant in the first variable and covariant in the second variable. To get H to be covariant, we can use the same formulas but regard H as defined on $\mathcal{C}^{\text{opp}} \times \mathcal{C}$, where $\mathcal{C}^{\text{opp}}$ is the opposite category of $\mathcal{C}$, as defined in Problems 78–80 at the end of Chapter IV. But this is getting to be a complicated structure for describing something simple, and we shall simply avoid this construction altogether,[2] working with F or G as circumstances dictate.

Even though we shall not work with H as a functor, it is convenient to combine $\mathrm{Hom}(1, \varphi)$ and $\mathrm{Hom}(\psi, 1)$ into a single definition of $\mathrm{Hom}(\psi, \varphi)$ as $\mathrm{Hom}(\psi, \varphi)(\tau) = \varphi\tau\psi$. In particular, $\mathrm{Hom}(1, \varphi)$ and $\mathrm{Hom}(\psi, 1)$ commute with each other; the commutativity follows from the associative law

$$\mathrm{Hom}(\psi, 1) \circ \mathrm{Hom}(1, \varphi)(\tau) = (\varphi\tau)\psi = \varphi(\tau\psi) = \mathrm{Hom}(1, \varphi) \circ \mathrm{Hom}(\psi, 1)(\tau).$$

[2] In category theory one sometimes proceeds in another way, defining a "bifunctor" to be a functor-like thing depending on two variables, covariant or contravariant in each but maybe not the same in each, and satisfying an appropriate commutativity property for the two variables.

Now let us turn to three identities involving Hom_R and to their ramifications. Each identity will assert some isomorphism involving Hom, and we consider each side of the identity as the value of a functor. We shall be interested in knowing that the isomorphism is natural in each case, the notion of naturality having been defined in Section VI.6. The naturality need be proved in just one direction in each case, since the inverse of an isomorphism that is natural is an isomorphism that is natural.

The first two identities concern the interaction of Hom_R with direct products and direct sums. Direct products and direct sums of unital left R modules were defined in Examples 7 and 8 of modules in Section VIII.1, and they were seen to be the product and coproduct functors for the category $\mathcal{C}$. If S is a nonempty set, then the direct product $\prod_{s\in S} M_s$ of a family of unital left R modules $\{M_s \mid s \in S\}$ is the module whose underlying set is the Cartesian product of the sets M_s and whose operations are defined coordinate by coordinate. The direct sum $\bigoplus_{s\in S} M_s$ is the R submodule of elements of $\prod_{s\in S} M_s$ that are nonzero in only finitely many coordinates.

Proposition 10.12. Let S be a nonempty set, let M_s and N_s be unital left R modules for each $s \in S$, and let M and N be unital left R modules. Then there are isomorphisms of abelian groups

(a) $\mathrm{Hom}_R\left(\bigoplus_{s\in S} M_s, N\right) \cong \prod_{s\in S} \mathrm{Hom}_R(M_s, N)$,

(b) $\mathrm{Hom}_R\left(M, \prod_{s\in S} N_s\right) \cong \prod_{s\in S} \mathrm{Hom}_R(M, N_s)$.

Moreover, the isomorphism in (a) is natural in the variable $\{M_s\}_{s\in S}$ and in the variable N, and the isomorphism in (b) is natural in the variable M and in the variable $\{N_s\}_{s\in S}$.

REMARKS. In each instance the assertion of naturality is that some square diagram is commutative, as illustrated in Figure 6.3. For example, if the mapping from left to right in the isomorphism (a) is denoted for fixed N by $\Phi_{\{M_s\}_{s\in S}}$ and if a system of R homomorphisms $\varphi_s : M_s \to M_s'$ is given, then one assertion of naturality for (a) is that $\Phi_{\{M_s'\}_{s\in S}} \circ \{\mathrm{Hom}(\oplus\varphi_s, 1)\} = \{\mathrm{Hom}(\oplus\varphi_s, 1)\} \circ \Phi_{\{M_s\}_{s\in S}}$. The other says for fixed $\{M_s\}_{s\in S}$ and for an R homomorphism $\psi : N \to N'$ that $\Phi_{N'} \circ \mathrm{Hom}(1, \psi) = \mathrm{Hom}(1, \psi) \circ \Phi_N$ if the isomorphism (a) is denoted for fixed $\bigoplus M_s$ by Φ_N and if $\psi : N \to N'$ is an R homomorphism. Two corresponding assertions are made about (b). To simplify the notation, we shall usually drop the subscripts from Φ.

PROOF. For (a), let $e_s : M_s \to \bigoplus_t M_t$ be the s^{th} inclusion, and let $p_s : \bigoplus_t M_t \to M_s$ be the s^{th} projection; the latter is defined as the restriction of the projection associated with the direct product. The map from left to right in (a) is given by $\Phi(\sigma) = \{\sigma \circ e_s\}_{s\in S}$ for σ in $\mathrm{Hom}_R\left(\bigoplus_s M_s, N\right)$, and the expected formula for the inverse is $\Phi'(\{\tau_s\}_{s\in S}) = \sum_s (\tau_s \circ p_s)$. Then we have

$$\Phi'(\Phi(\sigma)) = \Phi'(\{\sigma \circ e_s\}_s) = \sum_s (\sigma \circ e_s \circ p_s) = \sigma$$

and
$$\Phi(\Phi'(\{\tau_s\}_s)) = \Phi\big(\sum_s (\tau_s \circ p_s)\big) = \big\{\big(\sum_s (\tau_s \circ p_s)\big) \circ e_t\big\}_t$$
$$= \{\tau_s \circ p_s \circ e_s\}_s = \{\tau_s\}_s.$$

Hence Φ is an isomorphism with inverse Φ'.

Next let the system of R homomorphisms $\varphi_s : M'_s \to M_s$ be given, let $e'_s : M'_s \to \bigoplus_t M'_t$ be the s^{th} inclusion, and fix N. For σ in $\operatorname{Hom}_R\big(\bigoplus_s M_s, N\big)$, we have

$$\begin{aligned}\{\operatorname{Hom}(\oplus\varphi_s, 1)\}_s(\Phi(\sigma)) &= \{\operatorname{Hom}(\oplus\varphi_s, 1)\}_s(\{\sigma \circ e_s\}_s) = \{\sigma \circ e_s\}_s \circ \{\varphi_s\}_s\\ &= \{\sigma \circ e_s \circ \varphi_s\}_s = \{\sigma \circ \varphi_s \circ e'_s\}_s = \{\sigma \circ \{\varphi_s\}_s \circ e'_t\}_t\\ &= \Phi(\sigma \circ \{\varphi_s\}_s) = \Phi(\{\operatorname{Hom}(\oplus\varphi_s, 1)\}_s(\sigma)).\end{aligned}$$

This proves naturality in the variable $\{M_s\}_s$. If an R homomorphism $\varphi : N \to N'$ is given and if σ is in $\operatorname{Hom}_R\big(\bigoplus_s M_s, N\big)$, then

$$\begin{aligned}\Phi(\operatorname{Hom}(1, \varphi)(\sigma)) &= \Phi(\varphi \circ \sigma) = \{\varphi \circ \sigma \circ e_s\}_s\\ &= \operatorname{Hom}(1, \varphi)(\{\sigma \circ e_s\}_s) = \operatorname{Hom}(1, \varphi)(\Phi(\sigma)).\end{aligned}$$

This proves naturality in the variable N.

For (b), let $p_s : \prod N_t \to N_s$ be the s^{th} projection. The map from left to right in (b) is given by $\Phi(\sigma) = \{p_s \circ \sigma\}_s$ for σ in $\operatorname{Hom}_R\big(M, \prod_s N_s\big)$, and the inverse is given by $\Phi'(\{\tau_s\}_s) = \tau$, where $\tau(m) = \{\tau_s(m)\}_s$. The proof of naturality is similar to the corresponding proof in (a) and is omitted. $\square$

One ramification of Proposition 10.12 is the correspondence of "linear" maps to matrices when the ring R of scalars is noncommutative. If R is a field and V is an n-dimensional vector space over R, then we know that $\operatorname{End}_R(V)$ is isomorphic as an R algebra to the space $M_n(R)$ of n-by-n matrices over R, the isomorphism being fixed once we choose an ordered basis of V. Things are more subtle when R is noncommutative.

Corollary 10.13. Let V be a unital left R module, and let S be the ring $S = \operatorname{End}_R(V)$. For integers $m \geq 1$ and $n \geq 1$, there is a canonical isomorphism of abelian groups
$$\operatorname{Hom}_R(V^n, V^m) \cong M_{mn}(S)$$
such that composition of R homomorphisms, given as a mapping

$$\operatorname{Hom}_R(V^n, V^m) \times \operatorname{Hom}_R(V^p, V^n) \longrightarrow \operatorname{Hom}_R(V^p, V^m),$$

corresponds to matrix multiplication

$$M_{mn}(S) \times M_{np}(S) \longrightarrow M_{mp}(S).$$

In particular, in the special case that $m = n$, this canonical isomorphism becomes an isomorphism of rings

$$\operatorname{End}_R(V^n) \cong M_n(S).$$

REMARKS. For $V = R$, this isomorphism takes the form

$$\operatorname{End}_R(R^n) \cong M_n(\operatorname{End}_R(R))$$

and looks like something familiar from the case that R is a field. If $\operatorname{End}_R(R)$ were to be isomorphic as a ring to R, then the correspondence would be exactly what we might expect between R linear mappings from a free R module of rank n into itself, with n-by-n matrices with entries in R. However, $\operatorname{End}_R(R)$ is not ordinarily isomorphic to R, and the correspondence is something different and unexpected. We shall sort out these matters in Proposition 10.14 and Corollary 10.15.

PROOF. Let $e_j : V \to V^n = \bigoplus_{k=1}^n V = \prod_{k=1}^n V$ be the j^{th} inclusion for whatever n is under discussion, and let $p_i : V^m \to V$ be the i^{th} projection for whatever m is under discussion. For f in $\operatorname{Hom}_R(V^n, V^m)$, define $f_{ij} = p_i f e_j$. Then f_{ij} is R linear from V into V, hence is in $S = \operatorname{End}_R(V)$. If also g is in $\operatorname{Hom}_R(V^p, V^n)$, so that $f \circ g$ is in $\operatorname{Hom}_R(V^p, V^m)$, then the formula $\sum_{k=1}^n e_k p_k = 1$ on V^n gives

$$(f \circ g)_{ij} = p_i f g e_j = \sum_{k=1}^n p_i f e_k p_k g e_j = \sum_{k=1}^n f_{ik} g_{kj}.$$

Thus $f \circ g$ corresponds to the matrix product $[f_{ij}][g_{ij}]$, and the mapping is a ring homomorphism. Since

$$\sum_{i,j} e_i f_{ij} p_j = \sum_{i,j} e_i p_i f e_j p_j = \big(\sum_i e_i p_i\big) f \big(\sum_j e_j p_j\big) = 1 f 1 = f,$$

the mapping is one-one. If an arbitrary member $[u_{ij}]$ of $M_{mn}(S)$ is given, then we can define $f = \sum_{k,l} e_k u_{kl} p_l$, obtain $f_{ij} = p_i f e_j = \sum_{k,l} p_i e_k u_{kl} p_l e_j = p_i e_i u_{ij} p_j e_j = u_{ij}$, and conclude that the mapping is onto. $\square$

Proposition 10.14. The mapping $\varphi \mapsto \varphi(1)$ is a ring isomorphism $\operatorname{End}_R(R) \cong R^o$ of $\operatorname{End}_R(R)$ onto the opposite ring R^o of R.

PROOF. The mapping $\varphi \mapsto \varphi(1)$ certainly respects addition. If φ maps to $\varphi(1)$ and τ maps to $\tau(1)$, then $\varphi\tau$ maps to $(\varphi\tau)(1) = \varphi(\tau(1)) = \varphi(\tau(1)1) = \tau(1)\varphi(1)$ since φ respects left multiplication by the element $\tau(1)$ of R. The order of multiplication is therefore reversed, and $\varphi \mapsto \varphi(1)$ is a ring homomorphism of $\mathrm{End}_R(R)$ into R^o.

If r is given in R^o, define $\varphi_r(s) = sr$ for s in R. Then φ_r respects addition, and it respects left multiplication by R because $\varphi_r(r's) = r'sr = r'\varphi_r(s)$. Therefore φ_r is a member of $\mathrm{End}_R(R)$ such that $\varphi_r(1) = r$, and $\varphi \mapsto \varphi(1)$ is onto R^o.

If φ in $\mathrm{End}_R(R)$ has $\varphi(1) = 0$, then the R linearity of φ implies that $\varphi(r) = \varphi(r1) = r\varphi(1) = r0 = 0$, so that $\varphi = 0$. Consequently the map $\varphi \mapsto \varphi(1)$ is one-one. $\square$

Corollary 10.15. For any integer $n \geq 1$, $\mathrm{End}_R(R^n)$ is ring isomorphic to $M_n(R^o)$.

REMARKS. Now we can complete the remarks with Corollary 10.13: the case in which R is commutative might lead us to believe that $\mathrm{End}_R(R^n)$ is isomorphic to $M_n(R)$, but the correct isomorphism is with $M_n(R^o)$ instead.

PROOF. Corollary 10.13 shows that $\mathrm{End}_R(R^n)$ is isomorphic to $M_n(\mathrm{End}_R(R))$, and Proposition 10.14 shows that the latter ring is isomorphic to $M_n(R^o)$. $\square$

The third identity involving Hom_R concerns $\mathrm{Hom}_R(R, M)$, where M is a unital left R module. Ordinarily $\mathrm{Hom}_R(N, M)$, when N and M are two unital left R modules, is not an R module, but in the case that $N = R$, it is. The definition of the scalar multiplication by $r \in R$ is $(r\varphi)(r') = \varphi(r'r)$ for $r' \in R$ and $\varphi \in \mathrm{Hom}_R(R, M)$. To see that $r\varphi$ is in $\mathrm{Hom}_R(R, M)$, we let s be in R and compute that $(r\varphi)(sr') = \varphi((sr')r) = \varphi(s(r'r)) = s(\varphi(r'r)) = s((r\varphi)(r'))$, as required. To see that $(sr)\varphi = s(r\varphi)$, we compute that $((sr)\varphi)(r') = \varphi(r'(sr)) = \varphi((r's)r) = (r\varphi)(r's) = (s(r\varphi))(r')$. Proposition 10.16 identifies $\mathrm{Hom}_R(R, M)$ as an R module.

Proposition 10.16. For any unital left R module M, there is a canonical R isomorphism

$$\mathrm{Hom}_R(R, M) \cong M,$$

and this isomorphism is natural in the variable M.

PROOF. The map Φ from left to right is given by $\Phi(\sigma) = \sigma(1)$, and the inverse will be seen to be given by $\Phi'(m) = \tau_m$ with $\tau_m(r) = rm$. The computation $\Phi(r\sigma) = (r\sigma)(1) = \sigma(1r) = \sigma(r1) = r(\sigma(1)) = r(\Phi(\sigma))$ shows that Φ is an R homomorphism, and the computation $\tau_m(sr) = (sr)m = s(rm) = s(\tau_m(r))$ shows that τ_m is in $\mathrm{Hom}_R(R, M)$.

To see that Φ is an isomorphism with inverse Φ', we observe that $\Phi'\Phi$ carries $\mathrm{Hom}_R(R, M)$ into itself and has $(\Phi'\Phi)(\sigma) = \Phi'(\sigma(1)) = \tau_{\sigma(1)}$, where $\tau_{\sigma(1)}(r) = r\sigma(1) = \sigma(r)$; thus $(\Phi'\Phi)(\sigma) = \sigma$, and $\Phi'\Phi$ is the identity. Also, $(\Phi\Phi')(m) =$

$\Phi(\tau_m) = \tau_m(1) = 1m = m$, and $\Phi\Phi'$ is the identity.

For the naturality let $\varphi : M \to M'$ be an R homomorphism. Then we have $\Phi(\mathrm{Hom}(1, \varphi)(\sigma)) = \Phi(\varphi\sigma) = \varphi\sigma(1) = \varphi(\Phi(\sigma))$, and naturality is proved. $\square$

A relevant observation about the construction whose result is identified in Proposition 10.16 is that we could get by with something more general than R in the first variable of Hom_R. In fact, the construction would have worked for $\mathrm{Hom}_R(P, M)$ for any unital (R, R) "bimodule" P, i.e., any abelian group P that is a unital left R module and unital right R module in such a way that the two actions commute: $(rp)r' = r(pr')$. More generally let S be a second ring with identity. We say that P is a unital (R, S) **bimodule** if P is simultaneously a unital left R module and a unital right S module in such a way that $(rp)s = r(ps)$ for $r \in R$, $s \in S$, and $p \in P$. The following proposition shows that P allows us to construct a unital left S module out of any unital left R module M.

Proposition 10.17. If R and S are two rings with identity, if P is a unital (R, S) bimodule, and if M is any unital left R module, then the abelian group $\mathrm{Hom}_R(P, M)$ becomes a unital left S module under the definition $(s\varphi)(p) = \varphi(ps)$ for $s \in S$, $\varphi \in \mathrm{Hom}_R(P, M)$, and $p \in P$.

PROOF. To see that $s\varphi$ is an R homomorphism, we compute that $(s\varphi)(rp) = \varphi((rp)s) = \varphi(r(ps)) = r(\varphi(ps)) = r((s\varphi)(p))$. It is clear that 1 acts as 1, and the distributive laws are routine. What needs checking is the formula $(ss')\varphi = s(s'\varphi)$ for s and s' in S and φ in $\mathrm{Hom}_R(P, M)$. We compute that $((ss')\varphi)(p) = \varphi(p(ss')) = \varphi((ps)s') = (s'\varphi)(ps) = s((s'\varphi))(p)$, and the result follows. $\square$

An example of a unital (R, S) bimodule P is a ring S with identity such that R is a subring of S with the same identity. Then we can take $P = S$, with the result that R acts on the left, S acts on the right, and the two actions commute by the associative law for multiplication in S. In this situation the passage from R to $\mathrm{Hom}_R(S, M)$ is called a **change of rings**, or **extension of scalars**, for M.

In the special case that the rings are fields and the modules are vector spaces, we saw a different kind of change of rings in Section VI.6. What we saw there is that if $\mathbb{K} \subseteq \mathbb{L}$ is an inclusion of fields and if E is a vector space over $\mathbb{K}$, then $E^{\mathbb{L}} = E \otimes_{\mathbb{K}} \mathbb{L}$ has a canonical scalar multiplication by members of $\mathbb{L}$ under the definition that multiplication by $c \in \mathbb{L}$ is the linear mapping $1 \otimes (l \mapsto cl)$. In the next section we shall see that this change of rings by means of tensor products for vector spaces generalizes to give a second construction of a change of rings for modules over a ring with identity.

5. Tensor Product for Modules

In this section, R is still a ring with identity, and others rings will play a role as well. We are going to generalize the discussion of tensor products of Section VI.6, extending the notion from the tensor product of two vector spaces over a field to the tensor product of a unital right R module and a unital left R module. The tensor product will ordinarily not have the structure of an R module; it will be just an abelian group. Additional structure on the tensor product will come from a bimodule structure on one or both of the given R modules. For example it will be seen that the tensor product, in the current sense, of two vector spaces over a field F is a vector space over F because both vector spaces can be regarded as unital bimodules over F. We return to this detail after giving the definition and the theorem. Later in this section we shall obtain two fundamental associativity formulas, one for triple tensor products and one involving tensor product and Hom together.

Let M be a unital *right* R module, and let N be a unital *left* R module. An R **bilinear function** from $M \times N$ into an abelian group is a function b such that

$$\begin{aligned} b(m_1 + m_2, n) &= b(m_1, n) + b(m_2, n) \quad \text{for all } m_1 \in M, m_2 \in M, n \in N, \\ b(m, n_1 + n_2) &= b(m, n_1) + b(m, n_2) \quad \text{for all } m \in M, n_1 \in N, n_2 \in N, \\ b(mr, n) &= b(m, rn) \quad \text{for all } m \in M, n \in N, r \in R. \end{aligned}$$

The first two conditions are summarized by saying that b is **additive** in each variable. A **tensor product** of M and N over R is a pair (V, ι) consisting of an abelian group V and an R bilinear map $\iota : M \times N \to V$ having the following universal mapping property: whenever b is an R bilinear function from $M \times N$ into an abelian group A, then there exists a unique abelian-group homomorphism $L : V \to A$ such that the diagram in Figure 10.1 commutes, i.e., such that $L\iota = b$ holds in the diagram. When ι is understood, one frequently refers to V itself as the tensor product. The abelian-group homomorphism $L : V \to A$ is called the **additive extension** of b to the tensor product.[3] Theorem 10.18 below will address existence and essential uniqueness of the tensor product. Because of the essential uniqueness, it is customary to denote a tensor product by $M \otimes_R N$, and Figure 10.1 incorporates this notation.[4] The image $\iota(m, n)$ of the member (m, n) of $M \times N$ under ι is denoted by $m \otimes n$.

---

[3] *Warning.* The name "additive extension" is in analogy with the situation for the tensor product of vector spaces over a field, in which the extension is linear and really is an extension. Example 2 below will show that the tensor product of nonzero modules can be 0, and hence we do not always get something for general R that we can regard intuitively as an extension.

[4] Sometimes the notation $M \otimes_R N$ refers to the constructed abelian group in the proof of Theorem 10.18, and sometimes it refers to any abelian group as in the definition of tensor product.

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "\iota"'] & A \\ M \otimes_R N \arrow[ur, dashed, "L"'] & \end{tikzcd}$$

FIGURE 10.1. Universal mapping property of a tensor product of a right R module M and a left R module N.

Theorem 10.18. Let R be a ring with identity. If M is a unital right R module and N is a unital left R module, then there exists a tensor product $(M \otimes_R N, \iota)$ of M and N over R, and it is unique in the following sense: if (V_1, ι_1) and (V_2, ι_2) are two tensor products, then there exists a unique abelian-group homomorphism $\Phi : V_1 \to V_2$ such that $\Phi \circ \iota_1 = \iota_2$, and it is an isomorphism. Any tensor product is generated as an abelian group by the image of $M \times N$ in it. Moreover, tensor product is a covariant functor from the category of pairs consisting of a unital right R module and a unital left R module to the category of abelian groups under the following definition: if $\varphi : M \to M'$ is a homomorphism of unital right R modules and $\psi : N \to N'$ is a homomorphism of unital left R modules, then there exists a unique homomorphism of abelian groups $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ such that $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$ for all $m \in M$ and $n \in N$.

PROOF. Form the free abelian group G with a $\mathbb{Z}$ basis parametrized by the elements of $M \times N$. We write $e(m, n)$ for the basis element in G corresponding to the element (m, n) of $M \times N$, and we regard e as a one-one function from $M \times N$ onto the $\mathbb{Z}$ basis of G. Let H be the subgroup of G generated by all elements of any of the forms

$$\begin{gathered} e(m_1 + m_2, n) - e(m_1, n) - e(m_2, n), \\ e(m, n_1 + n_2) - e(m, n_1) - e(m, n_2), \\ e(mr, n) - e(m, rn), \end{gathered} \tag{$*$}$$

where the elements m, m_1, m_2 are in M, the elements n, n_1, n_2 are in N, and the scalar r is in R. We define $M \otimes_R N$ to be the quotient group G/H, $q : G \to G/H$ to be the quotient homomorphism, and ι to be the function $(m, n) \mapsto e(m, n) + H$ from $M \times N$ into G/H. The function ι is therefore given by $\iota = q \circ e$.

Let us prove that $(M \otimes_R N, \iota)$ is a tensor product of M and N over R. Each of the elements in $(*)$ lies in H and hence is mapped by q into the 0 coset of G/H. Since q is a homomorphism and since $\iota = q \circ e$, we obtain

$$\iota(m_1 + m_2, n) = \iota(m_1, n) + \iota(m_2, n)$$

from the first relation in $(*)$ and similar equalities from the other two relations. Therefore $\iota : M \times N \to M \otimes_R N$ is an R bilinear function.

Now let $b : M \times N \to A$ be an R bilinear function from $M \times N$ into an abelian group A. The universal mapping property in Figure 8.2 for free abelian groups shows that there exists a unique group homomorphism $\widetilde{L} : G \to A$ such that $\widetilde{L}(e(m, n)) = b(m, n)$ for all (m, n) in $M \times N$. For the first expression in $(*)$, we have

$$\begin{aligned}\widetilde{L}\big(e(m_1 + m_2, n) - e(m_1, n) - e(m_2, n)\big)& \\ &= \widetilde{L}(e(m_1 + m_2, n)) - \widetilde{L}(e(m_1, n)) - \widetilde{L}(e(m_2, n)) \\ &= b(m_1 + m_2, n) - b(m_1, n) - b(m_2, n).\end{aligned}$$

The right side is 0 since b is R bilinear, and a similar conclusion applies to the other two expressions in $(*)$. Therefore each member of $(*)$ lies in the kernel of $\widetilde{L}$, and the generated subgroup H lies in the kernel of $\widetilde{L}$. Consequently $\widetilde{L}$ descends to a group homomorphism $L : G/H \to A$, i.e., there exists L with $\widetilde{L} = L \circ q$. On any element (m, n) in $M \times N$, we then have $L \circ \iota = L \circ q \circ e = \widetilde{L} \circ e = b$. This proves the existence asserted by the universal mapping property for a tensor product over R. For the asserted uniqueness, the formula $L \circ \iota = b$ shows that L is determined uniquely by b on $\iota(M \times N)$. It is immediate from the definition of $M \otimes_R N$ that $\iota(M \times N)$ generates $M \otimes_R N$, and thus L is determined uniquely on all of $M \otimes_R N$.

Therefore $(M \otimes_R N, \iota)$ is a tensor product. Problems 18–22 at the end of Chapter VI show that the uniqueness up to the asserted isomorphism follows from general category theory.

We are left with defining $\varphi \otimes \psi$ when $\varphi : M \to M'$ and $\psi : N \to N'$ are given, and to showing that this definition makes tensor product into a covariant functor. Define $b : M \times N \to M' \otimes_R N'$ by $b(m, n) = \varphi(m) \otimes \psi(n)$. Then b is R bilinear into an abelian group, the property $b(mr, n) = b(m, rn)$ being verified by the calculation

$$\begin{aligned}b(mr, n) &= \varphi(mr) \otimes \psi(n) = \varphi(m)r \otimes \psi(n) \\ &= \varphi(m) \otimes r\psi(n) = \varphi(m) \otimes \psi(rn) = b(m, rn).\end{aligned}$$

The additive extension of b to $M \otimes_R N$ is taken to be $\varphi \otimes \psi$. The formula is therefore $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$. If we are given also $\varphi' : M' \to M''$ and $\psi' : N' \to N''$, then

$$\begin{aligned}(\varphi' \otimes \psi')(\varphi \otimes \psi)(m \otimes n) &= (\varphi' \otimes \psi')(\varphi(m) \otimes \psi(n)) = \varphi'\varphi(m) \otimes \psi'\psi(n) \\ &= (\varphi'\varphi \otimes \psi'\psi)(m \otimes n).\end{aligned}$$

Since the elements $m \otimes n$ generate $M \otimes_R N$, we obtain $(\varphi' \otimes \psi')(\varphi \otimes \psi) = \varphi'\varphi \otimes \psi'\psi$. Similarly we check that $1_M \otimes 1_N = 1_{M \otimes N}$. Therefore tensor product is a covariant functor. □

As in the last part of the above proof, the general procedure for constructing an abelian-group homomorphism $L : M \otimes_R N \to A$ is somehow to define an R bilinear function $b : M \times N \to A$ and to take the additive extension from Theorem 10.18 as the desired homomorphism. Once one has observed that the expression $b(m, n)$ is of a form that makes it R bilinear, then the homomorphism L is defined and is uniquely determined by its values on elements $m \otimes n$, according to the theorem.

In practice, M or N often has some additional structure, and that structure may be reflected in some additional property of the tensor product. The corollary below addresses some situations of this kind.

Corollary 10.19. Let R, S, and T be rings with identity, and suppose that M is a unital right R module and N is a unital left R module. Under the additional hypothesis that

(a) M is a unital (S, R) bimodule, then $M \otimes_R N$ is a unital left S module in a unique way such that $s(m \otimes n) = sm \otimes n$ for all $m \in M$, $n \in N$, and $s \in S$,

(b) N is a unital (R, T) bimodule, then $M \otimes_R N$ is a unital right T module in a unique way such that $(m \otimes n)t = m \otimes nt$ for all $m \in M$, $n \in N$, and $t \in T$,

(c) M is a unital (S, R) bimodule and N is a unital (R, T) bimodule, then $M \otimes_R N$ is a unital (R, T) bimodule under the left R module structure in (a) and the right T module structure in (b).

PROOF. In (a), let left multiplication by $s \in S$ within M be given by $\varphi_s : M \to M$ with $\varphi_s(m) = sm$. Then multiplication by s in S within $M \otimes_R N$ is given by $\varphi_s \otimes 1$. The covariant-functor property makes $\varphi_s \varphi_{s'} = \varphi_{ss'}$ and $\varphi_1 = 1$, and the distributive properties follow from the definitions and the fact that each φ_s is a homomorphism of the additive group M. This proves (a), and (b) is proved similarly. For (c), if left multiplication by $s \in S$ within M is given by φ_s and if right multiplication by $t \in T$ within N is given by ψ_t, then the commutativity of the operations on $M \otimes_R N$ follows from the fact that the additive homomorphisms $\varphi_s \otimes 1$ and $1 \otimes \psi_t$ commute with each other. $\square$

EXAMPLES.

(1) $R \otimes_R M \cong M$ as an isomorphism of left R modules whenever M is a left R module. Here we regard R as a unital (R, R) bimodule, so that $R \otimes_R M \cong M$ has the structure of a unital left R module by Corollary 10.19a. The mapping of left to right is the additive extension Φ of the R bilinear function $b(r, m) = rm$, satisfying $\Phi(r \otimes m) = rm$. It respects the left action by R. The two-sided inverse Φ' to Φ is given by $\Phi'(m) = 1 \otimes m$. Then $\Phi' \circ \Phi$ is the identity since

$\Phi'(\Phi(r \otimes m)) = \Phi'(rm) = 1 \otimes rm = r \otimes m$, and $\Phi \circ \Phi'$ is the identity since $\Phi(\Phi'(m)) = \Phi(1 \otimes m) = 1m = m$. The R isomorphism $R \otimes_R M \cong M$ is natural in M. In fact, if $\varphi : M \to M'$ is given, then

$$\begin{aligned}\varphi(\Phi(r \otimes m)) &= \varphi(rm) = r\varphi(m)\\ &= \Phi(r \otimes \varphi(m)) = \Phi\big((1 \otimes \varphi)(r \otimes m)\big).\end{aligned}$$

(2) $R = \mathbb{Z}$. In this case, $M \otimes_{\mathbb{Z}} N$ is the **tensor product of abelian groups**. Let us consider what abelian group we obtain when M and N are both finitely generated. Proposition 10.21 below shows that direct sums pull out of any tensor product, and hence it is enough to treat the tensor product of two cyclic groups. For $\mathbb{Z} \otimes_{\mathbb{Z}} A$, we get A by Example 1, and Proposition 10.20 below shows that $A \otimes_{\mathbb{Z}} \mathbb{Z}$ gives the same thing. Problem 3 at the end of the chapter identifies the tensor product of two arbitrary finite cyclic groups $(\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/l\mathbb{Z})$. For now, let us verify in the special case that $\mathrm{GCD}(k, l) = 1$ that $(\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/l\mathbb{Z}) = 0$. This tensor product is a unital $\mathbb{Z}$ module, being an abelian group, and Corollary 10.19a shows that the action by $\mathbb{Z}$ is given by $c(a \otimes b) = ca \otimes b$ for any integer c. Then we have $0 = (k1) \otimes 1 = k(1 \otimes 1)$ and $0 = 1 \otimes (l1) = (1l) \otimes 1 = (l1) \otimes 1 = l(1 \otimes 1)$. Choosing integers x and y such that $xk + yl = 1$, we see that $1 \otimes 1 = x(k(1 \otimes 1)) + y(l(1 \otimes 1)) = 0 + 0 = 0$. The tensor product is generated by $1 \otimes 1$, and thus the tensor product is 0.

(3) R equal to a commutative ring with identity. Then M is an (R, R) bimodule, since any unital left module for a commutative ring is a right module under the definition $mr = rm$ and vice versa. Corollary 10.19 shows therefore that $M \otimes_R N$ is a unital R module. The special case that R is a field was treated in Section VI.6.

(4) M equal to a ring S with R as a subring with the same identity. Then we can regard S as a unital (S, R) bimodule, and Corollary 10.19a shows that $S \otimes_R M$ is a unital left S module. The passage from M to $S \otimes_R M$ is a second kind of **change of rings**, or **extension of scalars**, the first kind being the passage from M to $\mathrm{Hom}_R(S, M)$ as in the previous section. Complexification of a real vector space V as $V \otimes_{\mathbb{R}} \mathbb{C}$ is an instance of this change of rings by means of tensor products. (Here we are taking into account the isomorphism $V \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} V$ given in Proposition 10.20 below.)

(5) M and N equal to associative R algebras with identity over a commutative ring R with identity. Proposition 10.24 below shows that $M \otimes_R N$ is another associative algebra with identity over R, with a multiplication such that

$$(m_1 \otimes n_1)(m_2 \otimes n_2) = m_1m_2 \otimes n_1n_2.$$

In this case the additional structure on the tensor product is not a consequence of Corollary 10.19, and additional argument is necessary.

The rest of this section will be devoted to establishing some identities for tensor product, together with their naturality, and to proving that the tensor product over R of two R algebras, for a commutative ring R with identity, is again an R algebra. Each identity involves setting up a homomorphism involving one or more tensor products, and it is necessary to prove in each case that the homomorphism is an isomorphism. For this purpose it is often inconvenient to prove directly that the homomorphism has 0 kernel and is onto. In such cases one constructs what ought to be the inverse homomorphism and proves that it is indeed a two-sided inverse.

Proposition 10.20. Let R be a ring with identity, let M be a unital right R module, and let N be a unital left R module. Let R^o be the opposite ring of R, let M^o be M regarded as a left R^o module, and let N^o be N regarded as a right R^o module. Then

$$M \otimes_R N \cong N^o \otimes_{R^o} M^o$$

under the unique homomorphism of abelian groups carrying $m \otimes n$ in $M \otimes_R N$ into $n \otimes m$ in $N^o \otimes_{R^o} M^o$. The isomorphism is natural in the variables M and N.

REMARK. To make the proof below a little clearer, we shall distinguish between elements of M and M^o, writing m in the first case and m^o in the second case, even though $m^o = m$ under our definitions. A similar notational convention will be in force for N.

PROOF. The map $(m, n) \mapsto n^o \otimes m^o$ is additive in each variable and carries (m, rn) to $(rn)^o \otimes m^o = n^o r^o \otimes m^o = n^o \otimes r^o m^o = n^o \otimes (mr)^o$. This expression is the image also of (mr, n), and hence $(m, n) \mapsto n^o \otimes m^o$ is R bilinear and has an additive extension Φ to $M \otimes_R N$. Arguing similarly, we readily construct a homomorphism $\Phi' : N^o \otimes_{R^o} M^o \to M \otimes_R N$. It is immediate that Φ' is a two-sided inverse to Φ, and the isomorphism follows. For the naturality in M, suppose that $\varphi : M \to M'$ is an R homomorphism. Write φ^o for the homomorphism with $\varphi^o(m^o) = (\varphi(m))^o$. Then $(1 \otimes \varphi^o)(\Phi(m \otimes n)) = (1 \otimes \varphi^o)(n^o \otimes m^o) = n^o \otimes \varphi^o(m^o) = n^o \otimes (\varphi(m))^o = \Phi(\varphi(m) \otimes n) = \Phi((\varphi \otimes 1)(m \otimes n))$. This proves the naturality in the M variable, and naturality in the N variable is proved similarly. $\square$

Proposition 10.21. Let R be a ring with identity, let S be a nonempty set, let M_s be a unital right R module for each $s \in S$, and let N be a unital left R module. Then

$$\Big(\bigoplus_{s \in S} M_s\Big) \otimes_R N \cong \bigoplus_{s \in S} (M_s \otimes_R N)$$

as abelian groups, and the isomorphism is natural in the tuple $(\{M_s\}_{s \in S}, N)$.

REMARKS. A similar conclusion holds if the direct sum occurs in the second member of the tensor product, as a consequence of Proposition 10.20. The naturality carries with it some additional conclusions. For example, if each M_s is a unital (T, R) bimodule for a ring T with identity, then the displayed isomorphism is an isomorphism of left T modules.

PROOF. The map $(\{m_s\}_s, n) \mapsto \{m_s \otimes n\}_s$ is R bilinear from $\left(\bigoplus_{s\in S} M_s\right) \times N$ into $\bigoplus_{s\in S} (M_s \otimes_R N)$, and its additive extension Φ is the homomorphism from left to right in the displayed isomorphism. It has $\Phi(\{m_s\}_s \otimes n) = \{m_s \otimes n\}_s$. To construct the inverse, let $i_s : M_s \to \bigoplus_{t\in S} M_t$ be the s^{th} inclusion. Then $(m_s, n) \mapsto i_s(m_s) \otimes n$ is R bilinear into $\left(\bigoplus_{s\in S} M_s\right) \otimes_R N$ and has an additive extension carrying $m_s \otimes n$ to $i_s(m_s) \otimes n$ in $\left(\bigoplus_{s\in S} M_s\right) \otimes_R N$. The universal mapping property of direct sums of abelian groups then gives us a corresponding abelian-group homomorphism $\Phi' : \bigoplus_{s\in S} (M_s \otimes_R N) \to \left(\bigoplus_{s\in S} M_s\right) \otimes_R N$. It has $\Phi'(\{m_s \otimes n\}_s) = \{m_s\}_s \otimes n$. It is immediate that $\Phi' \circ \Phi$ fixes each $\{m_s\}_s \otimes n$ and hence is the identity, and that $\Phi \circ \Phi'$ fixes each $\{m_s \otimes n\}_s$ and hence is the identity.

For the naturality let $\varphi_s : M_s \to M'_s$ be an R homomorphism of right R modules, and let $\psi : N \to N'$ be an R homomorphism of left R modules. Then

$$\begin{aligned}\Phi\big((\{\varphi_s\}_s \otimes \psi)(\{m_s\}_s \otimes n)\big) &= \Phi\big(\{\varphi_s(m_s)\}_s \otimes \psi(n)\big) = \{\varphi_s(m_s) \otimes \psi(n)\}_s \\ &= \{\varphi_s \otimes \psi\}_s(\{m_s \otimes n\}) = \{\varphi_s \otimes \psi\}_s(\Phi(\{m_s\} \otimes n),\end{aligned}$$

and naturality is proved. □

Proposition 10.22. Let R and S be rings with identity, let M be a unital right R module, let N be a unital (R, S) bimodule, and let P be a unital left S module. Then

$$(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$$

under the unique homomorphism Φ of abelian groups such that $\Phi((m \otimes n) \otimes p) = m \otimes (n \otimes p)$. The isomorphism is natural in the triple (M, N, P).

REMARKS. As with Proposition 10.21, the naturality carries with it some additional conclusions. For example, if T is a ring with identity and M is actually a unital (T, R) bimodule, then the isomorphism is one of left T modules.

PROOF. For fixed p, the map $(m, n, p) \mapsto m \otimes (n \otimes p)$ is R bilinear. In fact, the map is certainly additive in m and in n. For the transformation law with an element r of R, the calculation is $(mr, n, p) \mapsto mr \otimes (n \otimes p) = m \otimes r(n \otimes p) = m \otimes (rn \otimes p)$, and this is the image of (m, rn, p).

Thus for each fixed p, we have a unique well-defined extension, additive in m and n, carrying $(m \otimes n, p)$ to $m \otimes (n \otimes p)$. Using the uniqueness, we see that this extended map is additive in the variables $m \otimes n$ and p. Also, if s is in S, then $((m \otimes n)s, p) = (m \otimes ns, p)$ maps to $m \otimes (ns \otimes p) = m \otimes (n \otimes sp)$, which is the image of $(m \otimes n, sp)$, and therefore $(m \otimes n, p) \mapsto m \otimes (n \otimes p)$ is S bilinear. Consequently there exists a homomorphism Φ of abelian groups as in the statement of the proposition.

A similar argument produces a homomorphism Φ' of abelian groups carrying the right member of the display to the left member such that $\Phi'(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$. On the generating elements, we see that $\Phi' \circ \Phi$ and $\Phi \circ \Phi'$ are the identity. This proves the isomorphism.

For the naturality, let $\varphi : M \to M'$, $\psi : N \to N'$, and $\tau : P \to P'$ be maps respecting the appropriate module structure in each case. Then

$$\begin{aligned}\Phi\big(((\varphi\otimes\psi) \otimes \tau)((m \otimes n) \otimes p)\big) &= \Phi\big((\varphi \otimes \psi)(m \otimes n) \otimes \tau(p)\big)\\ &= \Phi\big((\varphi(m) \otimes \psi(n)) \otimes \tau(p)\big) = \varphi(m) \otimes (\psi(n) \otimes \tau(p))\\ &= (\varphi \otimes (\psi \otimes \tau))(m \otimes (n \otimes p)) = (\varphi \otimes (\psi \otimes \tau))(\Phi((m \otimes n) \otimes p)),\end{aligned}$$

and naturality is proved. □

Proposition 10.23. Let R and S be rings with identity, let M be a unital left R module, let N be a unital (S, R) bimodule, and let P be a unital left S module. Then

$$\mathrm{Hom}_S(N \otimes_R M, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$$

under the homomorphism Φ of abelian groups defined by $\Phi(\varphi)(m)(n) = \varphi(n \otimes m)$ for $m \in M$, $n \in N$, and $\varphi \in \mathrm{Hom}_S(M \otimes_R N, P)$. The isomorphism is natural in the variables (N, M) and P.

REMARKS. In the displayed isomorphism, $N \otimes_R M$ on the left side is automatically a left S module, and hence $\mathrm{Hom}_S(N \otimes_R M, P)$ is a well-defined abelian group. For the right side, Proposition 10.17 shows that $\mathrm{Hom}_S(N, P)$ is a left R module under the definition $(r\tau)(n) = \tau(nr)$; consequently $\mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$ is a well-defined abelian group. The naturality in the conclusion allows one to conclude, for example, that if M is in fact a unital (R, T) bimodule for a ring T with identity, then the displayed isomorphism is an isomorphism of left T modules.

PROOF. The homomorphism Φ is well defined. We construct its inverse. If ψ is in $\mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$, then the map $(n, m) \mapsto \psi(m)(n)$ sends (nr, m) to $\psi(m)(nr) = (r(\psi(m))(n) = (\psi(rm))(n)$, and this is the image of (n, rm). Hence $(n, m) \mapsto \psi(m)(n)$ is R bilinear and yields a map of $N \otimes_R M$ into P such that $n \otimes m$ maps to $\psi(m)(n)$. The latter map is an S homomorphism since $sn \otimes m$ maps to $\psi(m)(sn) = s(\psi(m)(n))$, which is s applied to the image of $n \otimes m$. We define $\Phi'(\psi)$ to be the map defined on $N \otimes_R M$ with $\Phi'(\psi)(n \otimes m) = \psi(m)(n)$.

Then $\Phi'(\Phi(\varphi))(n \otimes m) = \Phi(\varphi)(m)(n) = \varphi(n \otimes m)$ shows that $\Phi' \circ \Phi$ is the identity, and $\Phi(\Phi'(\psi))(m)(n) = \Phi'(\psi)(n \otimes m) = \psi(m)(n)$ shows that $\Phi \circ \Phi'$ is the identity. Hence Φ is an isomorphism of abelian groups.

For naturality in (N, M), let $\sigma : N' \to N$ and $\tau : M' \to M$ be given. Then

$$\begin{aligned}\Phi(\mathrm{Hom}(\sigma \otimes \tau, 1)\varphi)(m')(n') &= (\mathrm{Hom}(\sigma \otimes \tau, 1)(\varphi))(n' \otimes m')\\ &= \varphi(\sigma \otimes \tau)(n' \otimes m') = \varphi(\sigma(n') \otimes \tau(m')) = \Phi(\varphi)(\tau(m'))(\sigma(n'))\\ &= \mathrm{Hom}(\tau, \mathrm{Hom}(\sigma, 1))(\Phi(\varphi))(m')(n'),\end{aligned}$$

and naturality is proved in (N, M). For naturality in P, let $\sigma : P \to P'$ be given. Then

$$\begin{aligned}\Phi(\mathrm{Hom}(1, \sigma)\varphi)(m)(n) &= (\mathrm{Hom}(1, \sigma)\varphi)(n \otimes m) = \sigma\varphi(n \otimes m)\\ &= \sigma\big((\Phi(\varphi))(m)(n)\big) = \mathrm{Hom}(1, \mathrm{Hom}(1, \sigma))(\Phi(\varphi))(m)(n),\end{aligned}$$

and naturality is proved in P. □

Proposition 10.24. Let R be a commutative ring with identity, and let M and N be associative R algebras with identity. Then $M \otimes_R N$ is an associative R algebra with identity under the unique multiplication law satisfying

$$(m \otimes n)(m' \otimes n') = mm' \otimes nn'.$$

PROOF. What we know from Example 3 is that $M \otimes_R N$ is a unital R module. We need to define the associative-algebra multiplication in $M \otimes_R N$ and check that it satisfies the required properties.

Let $\mu(m)$ and $\nu(n)$ be the left multiplication operators in M and N defined by $\mu(m)(m') = mm'$ and $\nu(n)(n') = nn'$. The fact that R is central in M means that $\mu(m)(rm') = mrm' = rmm' = r\mu(m)(m')$ and hence that the mapping $\mu(m) : M \to M$ is a homomorphism of R modules. Similarly $\nu(n) : N \to N$ is a homomorphism of R modules. Therefore $\mu(m) \otimes \nu(n)$ is a well-defined homomorphism of abelian groups for each (m, n) in $M \times N$, and $b(m, n) = \mu(m) \otimes \nu(n)$ is a well-defined map of $M \times N$ into the abelian group $\mathrm{End}_{\mathbb{Z}}(M \otimes_R N)$. The map b is certainly additive in the M variable and in the N variable. If r is in R, then $b(mr, n) = \mu(mr) \otimes \nu(n)$. Since

$$\begin{aligned}(\mu(mr) \otimes \nu(n))(m' \otimes n') &= mrm' \otimes nn' = mm'r \otimes nn'\\ &= mm' \otimes rnn' = (\mu(m) \otimes \nu(rn))(m \otimes n'),\end{aligned}$$

we see that $b(mr, n) = b(m, rn)$. Thus b is R bilinear and extends to a homomorphism $L : M \otimes_R N \to \mathrm{End}_{\mathbb{Z}}(M \otimes_R N)$ of abelian groups.

For x and y in $M\otimes_R N$, we define a product by $xy = L(x)(y)$. Since $L(x)$ is in $\mathrm{End}_{\mathbb{Z}}(M \otimes_R N)$, we have $x(y_1 + y_2) = xy_1 + xy_2$. Since L is a homomorphism, $L(x_1 + x_2) = L(x_1) + L(x_2)$, and therefore $(x_1 + x_2)y = x_1y + x_2y$. The element $1_M \otimes 1_N$, where 1_M and 1_N are the respective identities of M and N, is a two-sided identity for $M \otimes_R N$. Since $M \otimes_R N$ is a two-sided unital R module, we have $rx = xr$, and thus $R(1_M \otimes 1_N)$ lies in the center of $M \otimes_R N$. Therefore the product operation is R linear in each variable.

Suppose that $x = m \otimes n$ and $y = m' \otimes n'$. Then we have

$$\begin{aligned} xy = L(x)(y) &= L(m \otimes n)(m' \otimes n') = b(m, n)(m' \otimes n') \\ &= (\mu(m) \otimes \nu(n))(m' \otimes n') = mm' \otimes nn' \end{aligned}$$

as asserted in the statement of the proposition. Consequently

$$\begin{aligned} (m \otimes n)\big((m' \otimes n')(m'' \otimes n'')\big) &= (m \otimes n)(m'm'' \otimes n'n'') = m(m'm'') \otimes n(n'n'') \\ &= (mm')m'' \otimes (nn')n'' = (mm' \otimes nn')(m'' \otimes n'') \\ &= \big((m \otimes n)(m' \otimes n')\big)(m'' \otimes n''). \end{aligned}$$

This proves associativity of multiplication on elements of the form $m \otimes n$. Since these elements generate the tensor product as an abelian group and since the distributive laws hold, associativity holds in general. $\square$

6. Exact Sequences

Consider a diagram of abelian groups and group homomorphisms of the form

$$\cdots \xrightarrow{\varphi_{n-1}} M_{n-1} \xrightarrow{\varphi_n} M_n \xrightarrow{\varphi_{n+1}} M_{n+1} \xrightarrow{\varphi_{n+2}} \cdots,$$

where M_{n-1}, M_n, M_{n+1}, etc., are abelian groups and φ_{n-1}, φ_n, φ_{n+1}, φ_{n+2}, etc., are homomorphisms. The diagram can be finite or infinite, and the particular kind of indexing is not important. The sequence in question is called a **complex** if all consecutive compositions are 0, i.e., if $\varphi_{k+1}\varphi_k = 0$ for all k. This condition is equivalent to having $\mathrm{image}(\varphi_k) \subseteq \ker(\varphi_{k+1})$ and is the backdrop for the traditional definitions of homology and cohomology groups, which are the various quotients $\ker(\varphi_{k+1})/\,\mathrm{image}(\varphi_k)$.

EXAMPLES OF COMPLEXES.

(1) The simplicial homology of a simplicial complex. For this situation the indexing is reversed (say by replacing n by $-n$), so that the homomorphisms lower the index. Each group M_n is a group whose elements are called "chains," and the homomorphisms are called "boundary maps." The chains in the kernel of one of the homomorphisms are said to be "closed," and those in the image

of a homomorphism are said to be "exact." The quotient of the two, taking into account the reversal of the indexing, is the system of simplicial homology groups of the simplicial complex.

(2) The de Rham cohomology of a smooth manifold. For this situation the indexing goes upward as indicated, the group M_n is the vector space of smooth differential forms of degree n, the homomorphisms are the restrictions to these spaces of the linear de Rham operator d, $\ker(\varphi_{n+1})$ is the vector subspace of "closed" forms, $\operatorname{image}(\varphi_n)$ is the vector subspace of "exact" forms, and the quotient $\ker(\varphi_{n+1})/\operatorname{image}(\varphi_n)$ is the n^{th} de Rham cohomology space of the manifold.

(3) Cohomology of groups. This was defined in Section VII.6, knowledge of which is not assumed in the present chapter. The result that shows that the appropriate sequence is a complex is Proposition 7.39, for which we gave a direct but complicated combinatorial proof.

The above sequence is said to be **exact** at M_n if $\ker(\varphi_{n+1}) = \operatorname{image}(\varphi_n)$. It is said to be an **exact sequence** if it is exact at every group in the sequence. The condition of exactness may be viewed as having two parts to it. One is the inclusion $\operatorname{image}(\varphi_n) \subseteq \ker(\varphi_{n+1})$ that enters the definition of complex. Since this condition says that $\varphi_{n+1}\varphi_n = 0$, it is often easy to check. The other condition is that $\ker(\varphi_{n+1}) \subseteq \operatorname{image}(\varphi_n)$, a condition that often is more difficult to check.

The extent to which a complex fails to be exact plays a fundamental role in the subject of homological algebra. This is a subject that for the most part is left to Chapter IV of *Advanced Algebra*. That chapter will put the examples above into a wider context, and it will develop techniques for working with homology and cohomology. In the present section we shall give the barest hint of an introduction to the subject by discussing some of the effects of the Hom functor and the tensor product functor on exact sequences.

Let us establish a setting for applying a functor F to an exact sequence or more general complex. For current purposes we have in mind that F is Hom in one of its two variables or is tensor product in one of its two variables. First we need to have two categories available so that F carries the one category to the other. These categories will have to satisfy some properties, but we shall not attempt to list such properties at this time.[5] Let us be content with some familiar examples of categories whose objects are abelian groups with additional structure and whose morphisms are group homomorphisms with additional structure. Specifically let R be a ring with identity, let $\mathcal{C}_R$ be the category of all unital left R modules, and let $\mathcal{D}_R$ be the category of all unital right R modules. We suppose that our functor

[5] The appropriate notion is that of an "abelian category," which is defined in Section IV.8 of *Advanced Algebra*.

F carries some $\mathcal{C}_R$ or $\mathcal{D}_R$ to another such category, possibly for a different ring. The functor F can be covariant or contravariant. We require also of F that it be an **additive functor**, i.e., that $F(\varphi_1+\varphi_2) = F(\varphi_1)+F(\varphi_2)$ for any maps φ_1 and φ_2 that lie in the same Hom group.

With the additional structure in place, we can now introduce the notions of **complex** and **exact sequence** for the domain and range categories of F, not just for the category of abelian groups. In this case the abelian groups in the sequence are to be objects in the category, and the group homomorphisms in the sequence are to be morphisms in the category; otherwise the definitions are unchanged. The condition that F be additive implies that F carries any 0 map to a 0 map, and that property will be key for us. In fact, we can apply F to any complex in the domain category (by applying it to each object and morphism in the sequence); after F is applied, the arrows point the same way if F is covariant, and they point the opposite way if F is contravariant. If F is covariant, it sends any consecutive composition $0 = \varphi_{k+1}\varphi_k$ to $0 = F(0) = F(\varphi_{k+1}\varphi_k) = F(\varphi_{k+1})F(\varphi_k)$; therefore the consecutive composition of F of the maps is 0, and we obtain a complex. If F is contravariant, we have $0 = F(0) = F(\varphi_{k+1}\varphi_k) = F(\varphi_k)F(\varphi_{k+1})$; the consecutive composition of F of the maps is still 0, and we still obtain a complex. Thus the additive functor F sends any complex to a complex.

However, not all additive functors invariably send exact sequences to exact sequences, as we shall see with Hom and tensor product in the category $\mathcal{C}_{\mathbb{Z}}$. Yet they each preserve some features of certain exact sequences, even when $\mathbb{Z}$ is replaced by a general ring with identity. To be precise we introduce the following definition.

A **short exact sequence** in our category is an exact sequence of the form

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0.$$

Exactness of this sequence incorporates three conditions:

(i) φ is one-one,
(ii) $\ker\psi = \operatorname{image}\varphi$,
(iii) ψ is onto.

In fact, the three conditions are precisely the conditions of exactness at M, N, and P, respectively, since the maps at either end are 0 maps. If we think of φ as an inclusion map, then the short exact sequence corresponds to the isomorphism $N/M \cong P$ obtained because ψ factors through to the quotient N/M.

Proposition 10.25. Let R be a ring with identity, let

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$$

be a short exact sequence in the category $\mathcal{C}_R$, let E be a module in $\mathcal{C}_R$, and let E' be a module in $\mathcal{D}_R$. Then the following sequences in $\mathcal{C}_{\mathbb{Z}}$ are exact:

$$E' \otimes_R M \xrightarrow{1\otimes\varphi} E' \otimes_R N \xrightarrow{1\otimes\psi} E' \otimes_R P \longrightarrow 0,$$

$$0 \longrightarrow \operatorname{Hom}_R(E, M) \xrightarrow{\operatorname{Hom}(1,\varphi)} \operatorname{Hom}_R(E, N) \xrightarrow{\operatorname{Hom}(1,\psi)} \operatorname{Hom}_R(E, P),$$

$$\operatorname{Hom}_R(M, E) \xleftarrow{\operatorname{Hom}(\varphi,1)} \operatorname{Hom}_R(N, E) \xleftarrow{\operatorname{Hom}(\psi,1)} \operatorname{Hom}_R(P, E) \longleftarrow 0.$$

REMARKS. Similarly tensor product in the first variable, which carries $\mathcal{D}_R$ to $\mathcal{C}_{\mathbb{Z}}$, retains the same exactness as in the first of these three sequences. In each case when we specialize to $R = \mathbb{Z}$, there are examples to show that exactness fails if we try to include the expected remaining 0 in the above three sequences. We give such examples after the proof of the proposition.

PROOF. For the first sequence in $\mathcal{C}_{\mathbb{Z}}$, we are to show that $1 \otimes \psi$ is onto $E' \otimes_R P$ and that every member of the kernel of $1 \otimes \psi$ is in the image of $1 \otimes \varphi$. (Recall that $\ker(1 \otimes \psi) \supseteq \operatorname{image}(1 \otimes \varphi)$ since the sequence is a automatically a complex.)

Thus let $p \in P$ be given. Since $\psi : N \to P$ is onto, choose $n \in N$ with $\psi(n) = p$. Then $(1 \otimes \psi)(e \otimes n) = e \otimes p$. The elements $e \otimes p$ generate $E' \otimes_R P$ as an abelian group, and hence $1 \otimes \psi$ is onto $E' \otimes_R P$.

To show that $\ker(1 \otimes \psi) \subseteq \operatorname{image}(1 \otimes \varphi)$, we observe from the exactness of the given sequence at N that $E' \otimes_R \ker\psi = E' \otimes_R \operatorname{image}\varphi$ is generated by all elements $e \otimes \varphi(m)$, hence by all elements $(1 \otimes \varphi)(e \otimes m)$. Therefore $E' \otimes_R \operatorname{image}\varphi = \operatorname{image}(1 \otimes \varphi)$, and it is enough to prove that

$$\ker(1 \otimes \psi) \subseteq E' \otimes_R \ker\psi. \tag{$*$}$$

To prove $(*)$, we use the fact that ψ is onto P. Define $W = E' \otimes_R \ker\psi$ as a subgroup of $E' \otimes_R N$, and let $q : E' \otimes_R N \to (E' \otimes_R N)/W$ be the quotient homomorphism. Define $b : E' \times P \to (E' \otimes_R N)/W$ by

$$b(e, p) = (e \otimes n) + W, \qquad \text{where } n \text{ is chosen such that } \psi(n) = p.$$

The expression $b(e, p)$ does not depend on the choice of the element n having $\psi(n) = p$ since another choice n' will differ from n by a member of $\ker\psi$ and will affect the definition only by a member of W. The function b is certainly additive in each variable, and it evidently has $b(er, p) = b(e, rp)$ for $r \in R$ as well. Thus b is R bilinear. Let $L : E' \otimes_R P \to (E' \otimes_R N)/W$ be the additive extension. From $b(e, \psi(n)) = (e \otimes n) + W$, we see that $L(e \otimes \psi(n)) = (e \otimes n) + W$, hence that $L \circ (1 \otimes \psi) = q$. This formula shows that $\ker(1 \otimes \psi) \subseteq \ker q = W$, and this is the inclusion $(*)$.

For the second sequence in $\mathcal{C}_{\mathbb{Z}}$, we are to show that $\operatorname{Hom}(1, \varphi)$ is one-one and that every member of the kernel of $\operatorname{Hom}(1, \psi)$ is in the image of $\operatorname{Hom}(1, \varphi)$. If

σ is in $\mathrm{Hom}_R(E, M)$ with $\mathrm{Hom}(1, \varphi)(\sigma) = 0$, then $\varphi(\sigma(e)) = 0$ for all $e \in E$. Since φ is one-one, $\sigma(e) = 0$ for all e, and $\sigma = 0$.

If τ in $\mathrm{Hom}_R(E, N)$ is in the kernel of $\mathrm{Hom}(1, \psi)$, so that $\psi(\tau(e)) = 0$ for all $e \in E$, then $\tau(e) = \varphi(m)$ for some $m \in M$ depending on e, by exactness of the given sequence at N; the element m is unique because φ is one-one. Define τ' in $\mathrm{Hom}_R(E, M)$ by $\tau'(e) =$ this m; the uniqueness of m for each e ensures that τ' is in $\mathrm{Hom}_R(E, M)$. Then we have $\tau(e) = \varphi(m) = \varphi(\tau'(e))$, and we conclude that $\tau = \mathrm{Hom}(1, \varphi)(\tau')$.

For the third sequence in $\mathcal{C}_{\mathbb{Z}}$, we are to show that $\mathrm{Hom}(\psi, 1)$ is one-one and that every member of the kernel of $\mathrm{Hom}(\varphi, 1)$ is in the image of $\mathrm{Hom}(\psi, 1)$. If σ is in $\mathrm{Hom}_R(P, E)$ with $\mathrm{Hom}(\psi, 1)(\sigma) = 0$, then $\sigma(\psi(n)) = 0$ for all n in N. Since ψ carries N onto P, $\sigma = 0$.

If τ in $\mathrm{Hom}_R(N, E)$ is in the kernel of $\mathrm{Hom}(\varphi, 1)$, then $\mathrm{Hom}(\varphi, 1)(\tau) = 0$. So $\tau(\varphi(m)) = 0$ for all $m \in M$. Thus τ vanishes on $\mathrm{image}\,\varphi = \ker\psi$, and τ descends to an R homomorphism $\overline{\tau} : N/\ker\psi \to E$. That is, τ is of the form $\tau = \overline{\tau}\psi = \mathrm{Hom}(\psi, 1)(\overline{\tau})$. $\square$

EXAMPLES OF FAILURE OF EXACTNESS IN $\mathcal{C}_{\mathbb{Z}}$. We start from the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

where φ is multiplication by 2 and ψ is the usual quotient homomorphism.

(1) We apply $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} (\,\cdot\,)$ to the given exact sequence, and the claim is that $1\otimes\varphi : (\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}) \to (\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z})$ is not one-one. In fact, $\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$, and $1 \otimes \varphi$ acts as multiplication by 2 under the isomorphism, hence is the 0 map and is not one-one.

(2) We apply $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \,\cdot\,)$ to the given exact sequence, and the claim is that $\mathrm{Hom}(1, \psi) : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ is not onto. In fact, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$, and the identity map in $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ is nonzero; therefore $\mathrm{Hom}(1, \psi)$ cannot be onto.

(3) We apply $\mathrm{Hom}_{\mathbb{Z}}(\,\cdot\,, \mathbb{Z}/2\mathbb{Z}))$ to the given exact sequence, and the claim is that $\mathrm{Hom}(\varphi, 1) : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ is not onto. In fact, $\mathrm{Hom}(\varphi, 1)$ is premultiplication by 2 and carries any σ in $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ to the homomorphism $k \mapsto \sigma(2k) = 2\sigma(k) = 0$. Since the usual quotient homomorphism $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is a nonzero member of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$, $\mathrm{Hom}(\varphi, 1)$ is not onto $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

7. Problems

1. Suppose that the commutative ring R is an integral domain. As usual, the R submodules of R are the ideals. Prove that the ideals satisfy the descending chain condition if and only if R is a field.

2. Let $\mathbb{F} = \mathbb{F}_2$ be a field with two elements.
   (a) Give an example of a representation of the cyclic group C_2 on $\mathbb{F}^2$ with the property that there is a 1-dimensional invariant subspace U but there is no invariant subspace V with $\mathbb{F}^2 = U \oplus V$.
   (b) How can one conclude from (a) that the group algebra $R = \mathbb{F}C_2$ has a unital left R module of finite length that is not semisimple? (Educational note: Compare this conclusion with Example 5 in Section 1, which shows that every unital left $\mathbb{C}G$ module is semisimple if G is a finite group.)

3. Let G be the abelian group $(\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/l\mathbb{Z})$, where k and l are nonzero integers.
   (a) Prove that G is generated by the element $1 \otimes 1$.
   (b) Prove that if k divides l, then $(\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/l\mathbb{Z}) \cong (\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/k\mathbb{Z})$.
   (c) Using multiplication as a $\mathbb{Z}$ bilinear form on $(\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$, prove that $(\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/k\mathbb{Z})$ has at least $|k|$ elements.
   (d) Conclude that $(\mathbb{Z}/k\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/l\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$, where $d = \mathrm{GCD}(k, l)$.

4. **(Fitting's Lemma)** Let R be a ring with identity, let M be a unital left R module, and suppose that M has a composition series. Let φ be a member of $\mathrm{End}_R(M)$.
   (a) Prove for the composition powers φ^n of φ that there exists an integer N such that $\ker \varphi^n = \ker \varphi^{n+1}$ and $\mathrm{image}\, \varphi^n = \mathrm{image}\, \varphi^{n+1}$ for all $n \geq N$.
   (b) Let $\mathcal{K}$ and $\mathcal{I}$ be the respective R submodules of M obtained for $n \geq N$ in (a). Prove that $\mathcal{K} \cap \mathcal{I} = 0$.
   (c) For x in M, show that there is some y in $\mathrm{image}\, \varphi^N$ with $\varphi^N(x) = \varphi^N(y)$.
   (d) Deduce from (c) that $M = \mathcal{K} + \mathcal{I}$, and conclude from (b) that $M = \mathcal{K} \oplus \mathcal{I}$.
   (e) Prove that φ carries $\mathcal{I}$ one-one onto $\mathcal{I}$ and that $(\varphi\big|_{\mathcal{K}})^n = 0$ for some n.

5. Let R be a ring with identity, and let

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$$

be an exact sequence of unital left R modules. Prove that the following conditions are equivalent:

   (i) N is a direct sum $N' \oplus \ker \psi$ of R submodules for some N',
   (ii) there exists an R homomorphism $\sigma : P \to N$ such that $\psi\sigma = 1_P$,
   (iii) there exists an R homomorphism $\tau : N \to M$ such that $\tau\varphi = 1_M$.

(Educational note: In this case one says that the exact sequence is **split**.)

6. (a) If R is the ring of quaternions, prove that $\mathrm{End}_R(R)$ is isomorphic to R as a ring.
   (b) Give an example of a noncommutative ring with identity for which $\mathrm{End}_R(R)$ is not isomorphic to R, and explain why it is not isomorphic.

7. Let R be a ring with identity, and let M be a unital left R module. Prove that M has a unique maximal semisimple R submodule N. (Educational note: The R submodule N is called the **socle** of M.)

8. Let $\mathbb{F} \subseteq \mathbb{K}$ be an inclusion of fields, and let A be an associative algebra with identity over $\mathbb{F}$. Proposition 10.24 makes $A \otimes_{\mathbb{F}} \mathbb{K}$ into an associative algebra over $\mathbb{F}$ with a multiplication such that $(a_1 \otimes k_1)(a_2 \otimes k_2) = a_1a_2 \otimes k_1k_2$. Show that $A \otimes_{\mathbb{F}} \mathbb{K}$ is in fact an associative algebra over $\mathbb{K}$ with scalar multiplication by k in $\mathbb{K}$ equal to left multiplication by $1 \otimes k$.

9. A Lie algebra $\mathfrak{g}$ over a field $\mathbb{K}$ is defined, according to Problems 31–35 at the end of Chapter VI, to be a nonassociative algebra over $\mathbb{K}$ with a multiplication written $[x, y]$ that is alternating as a function of the pair (x, y) and satisfies $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all x, y, z in $\mathfrak{g}$. If $\mathbb{L}$ is a field containing $\mathbb{K}$, prove that $\mathfrak{g}^{\mathbb{L}} = \mathfrak{g} \otimes_{\mathbb{K}} \mathbb{L}$ becomes a Lie algebra over $\mathbb{L}$ in a unique way such that its multiplication satisfies $[x \otimes c, y \otimes d] = [x, y] \otimes cd$ for x, y in $\mathfrak{g}$ and c, d in $\mathbb{L}$.

10. Let R be a ring with identity, let A be a unital right R module, and let B be a unital left R module. Since $\mathbb{Z} \subseteq R$, A and B can be considered also as $\mathbb{Z}$ modules. Form a version of $A \otimes_R B$ with associated R bilinear map $b_1 : A \times B \to A \otimes_R B$, and form a version of $A \otimes_{\mathbb{Z}} B$ with associated $\mathbb{Z}$ bilinear map $b_2 : A \times B \to A \otimes_{\mathbb{Z}} B$. Let H be the subgroup of $A \otimes_{\mathbb{Z}} B$ generated by all elements $b_2(ar, b) - b_2(a, rb)$ with $a \in A$, $b \in B$, $r \in R$, and let $q : A \otimes_{\mathbb{Z}} B \to (A \otimes_{\mathbb{Z}} B)/H$ be the quotient homomorphism. Prove that there is an abelian group isomorphism $\Phi : (A \otimes_{\mathbb{Z}} B)/H \to A \otimes_R B$ such that $\Phi(q(b_2(a, b))) = b_1(a, b)$ for all $a \in A$ and $b \in B$.

11. Let R be a commutative ring with identity, and let $\mathcal{C}$ be the category of all commutative associative R algebras with identity. Prove that if A_1 and A_2 are in $\mathrm{Obj}(\mathcal{C})$, then $(A_1 \otimes_R A_2, \{i_1, i_2\})$ is a coproduct, where $i_1 : A_1 \to A_1 \otimes_R A_2$ is given by $i_1(a_1) = a_1 \otimes 1$ and $i_2 : A_2 \to A_1 \otimes_R A_2$ is given by $i_2(a_2) = 1 \otimes a_2$.

Problems 12–20 partition simple left R modules into isomorphism types, where R is a ring with identity. For each simple left R module E and each unital left R module M, one forms the sum M_E of all simple R submodules that are isomorphic to E and calls it an **isotypic R submodule** of M. The problems introduce a calculus for working with the members of $\mathrm{End}_R(M_E)$ in terms of right vector spaces over a certain division ring. They show that if M is semisimple, then M is the direct sum of all its isotypic R submodules, each of these is mapped to itself by every member of $\mathrm{End}_R(M)$, and consequently one can understand $\mathrm{End}_R(M)$ in terms of right vector spaces over certain division rings. These problems generalize and extend Problems 47–52 at the end of Chapter VII, which in effect deal with what happens for the ring $\mathbb{C}\,G$ when G is a finite group; however, the material of Chapter VII is not prerequisite for these problems. The following notation is in force: M is any unital left R module,

E is a simple left R module, $D_E = \operatorname{Hom}_R(E, E)$ is the ring known from Proposition 10.4b to be a division ring,

$$M_E = (\text{sum of all } R \text{ submodules of } M \text{ that are } R \text{ isomorphic to } E),$$

and

$$M^E = \operatorname{Hom}_R(E, M).$$

Unital right D_E modules are right vector spaces over D_E. In Problems 18–20, $\mathcal{E}$ denotes a set of representatives of all R isomorphism classes of simple left R modules.

12. Prove that
    (a) M_E is a direct sum of simple R modules that are R isomorphic to E,
    (b) the image of every mapping in M^E belongs to M_E,
    (c) redefinition of the range from M to M_E defines an isomorphism $M^E \cong \operatorname{Hom}_R(E, M_E)$ of abelian groups.
13. Prove that
    (a) M^E is a unital right D_E module under composition of R homomorphisms,
    (b) E is a unital left D_E module under the operation of the members of D_E,
    (c) the left R module action and the left D_E module action on E commute with each other.
14. Show that $M^E \otimes_{D_E} E$ is a unital left R module in such a way that $r(m \otimes e) = m \otimes re$.
15. Prove that there is a well-defined R homomorphism $\Phi : M^E \otimes_{D_E} E \to M$ such that $\Phi(\psi \otimes e) = \psi(e)$ and such that Φ is an R isomorphism onto M_E.
16. Prove that the left R submodules N of M_E are in one-one correspondence with the right D_E vector subspaces W of M^E by the maps

$$N \mapsto \operatorname{Hom}_R(E, N) \subseteq \operatorname{Hom}_R(E, M) = M^E \quad \text{if } N \subseteq M_E$$

and

$$W \mapsto W \otimes_{D_E} E \subseteq M^E \otimes_{D_E} E \cong M_E \quad \text{if } W \subseteq M^E.$$

17. Prove for any unital left R module N that there is a canonical isomorphism

$$\operatorname{Hom}_R(M_E, N_E) \cong \operatorname{Hom}_{D_E}(M^E, N^E)$$

of abelian groups defined as follows. Suppose φ is in $\operatorname{Hom}_R(M_E, N_E)$. Composition with φ carries $\operatorname{Hom}_R(E, M)$ into $\operatorname{Hom}_R(E, N)$; this map respects the right action of D_E and hence induces a map

$$\varphi^E \in \operatorname{Hom}_{D_E}(M^E, N^E).$$

The isomorphism is given in terms of the isomorphisms Φ_M for M and Φ_N for N in Problem 15 by

$$\varphi(\Phi_M(\psi \otimes e)) = \Phi_N(\varphi^E(\psi) \otimes e) \qquad \text{for } \psi \in M^E.$$

18. If M is semisimple, prove that

$$M = \bigoplus_{E \in \mathcal{E}} M_E \cong \bigoplus_{E \in \mathcal{E}} (M^E \otimes_{D_E} E).$$

19. Still with M semisimple, prove that the left R submodules of M are in one-one correspondence with families $\{W^E \mid E \in \mathcal{E}\}$ of right D_E vector subspaces of M^E.

20. Suppose that M and N are two semisimple left R modules. Prove that there is a canonical isomorphism of abelian groups

$$\mathrm{Hom}_R(M, N) \cong \prod_{E \in \mathcal{E}} \mathrm{Hom}_{D_E}(M^E, N^E).$$

More precisely prove that an R module map from M to N is specified by giving, for a representative E of each class of simple left R modules, an arbitrary right vector-space map from M^E to N^E.