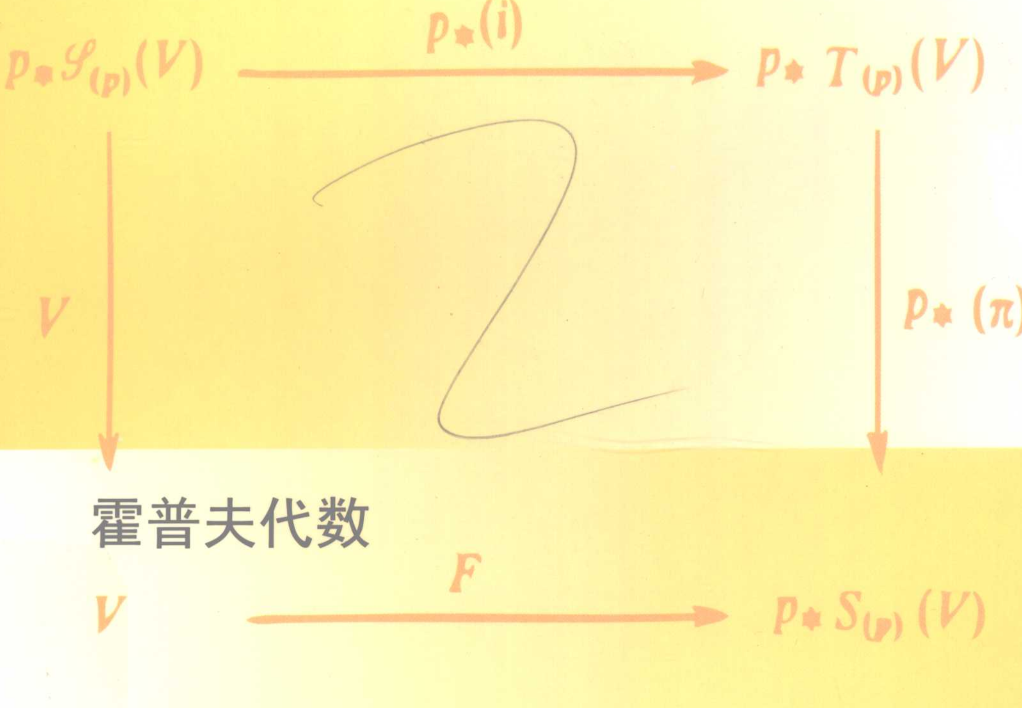
Eiichi Abe

Hopf Algebras



霍普夫代数

CAMBRIDGE

世界图书出版公司
www.wpcbj.com.cn

EIICHI ABE
Professor of Mathematics, University of Tsukuba

Hopf algebras

translated by Hisae Kinoshita and Hiroko Tanaka

CAMBRIDGE UNIVERSITY PRESS
CAMBRIDGE
LONDON NEW YORK NEW ROCHELLE
MELBOURNE SYDNEY

图书在版编目（CIP）数据

霍夫代数 = Hopf Algebras：英文/（日）英一安倍晋三著.
—北京：世界图书出版公司北京公司，2009.5
ISBN 978-7-5100-0456-8

Ⅰ.霍… Ⅱ.英… Ⅲ.代数拓扑—英文 Ⅳ.0189.2

中国版本图书馆 CIP 数据核字（2009）第 055612 号

书　　名：	Hopf Algebras
作　　者：	Eiichi Abe
中 译 名：	霍普夫代数
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街 137 号　100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@wpcbj.com.cn
开　　本：	24 开
印　　张：	12.5
版　　次：	2009 年 05 月
版权登记：	图字：01-2009-1665
书　　号：	978-7-5100-0456-8/O·671　　**定　　价：** 39.00 元

Hopf Algebras, 1st ed. (978-0-521-60489-5) by Eiichi Abe first published by Cambridge University Press 1980

Preface

Let G be a finite group and k a field. The set $A = \text{Map}(G, k)$ of all functions defined on G with values in k becomes a k-algebra when we define the scalar product and the sum and product of functions by

$$(\alpha f)(x) = \alpha f(x), \qquad (f + g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(x)g(x), \ f, g \in A, \alpha \in k, x \in G.$$

In general, a k-algebra A can be characterized as a k-linear space A together with two k-linear maps

$$\mu : A \otimes_k A \to A, \quad \eta : k \to A,$$

which satisfy axioms corresponding to the associative law and the unitary property respectively. If we identify $A \otimes_k A$ with Map $(G \times G, k)$ where $A = \text{Map}(G, k)$, and if the operations of G are employed in defining the k-linear maps

$$\Delta : A \to A \otimes_k A, \quad \varepsilon : A \to k$$

respectively by $\Delta f(x \otimes y) = f(xy)$, $\varepsilon f = f(e)$ for $x, y \in G$ and where e is the identify element of G, then Δ and ε become homomorphisms of k-algebras having properties which are dual to μ and η respectively. In general, a k-linear space A with k-linear maps μ, η, Δ, ε defined as above is called a k-bialgebra. Furthermore, we can define a k-linear endomorphism of $A = \text{Map}(G, k)$

$$S : A \to A, \quad (Sf)(x) = f(x^{-1}), \quad f \in A, \quad x \in G$$

such that the equalities

$$\mu(1 \otimes S)\Delta = \mu(S \otimes 1)\Delta = \eta \circ \varepsilon$$

hold. A k-bialgebra on which we can define a k-linear map S as above is called a k-Hopf algebra. Thus, a k-Hopf algebra is an algebraic system which simultaneously admits structures of a k-algebra as well as its dual, where these two structures are related by a certain specific law. For a finite group G, its group ring kG over a field k is the dual space of the k-linear space $A = \text{Map}(G, k)$ where its k-algebra structure is given by the dual k-linear maps of Δ and ε. Moreover, kG admits a k-Hopf algebra structure when we take the dual k-linear maps of μ, η, and S. In other words, kG is the dual k-Hopf algebra of Map (G, k).

If, for instance, we replace the finite group G in the above argument by a topological group and k by the field of real numbers or the field of complex numbers, or if we take G to be an algebraic group over an algebraically closed field k and A is replaced by the k-algebra of all continuous representative functions or of all regular functions over G, then A turns out to be a k-Hopf algebra in exactly the same manner. These algebraic systems play an important role when studying the structure of G. Similarly, a k-Hopf algebra structure can be defined naturally on the universal enveloping algebra of a k-Lie algebra. The universal enveloping algebra of the Lie algebra of a semi-simple algebraic group turns out to be (in a sense) the dual of the Hopf algebra defined above. These constitute some of the most natural examples of Hopf algebras. The general structure of such algebraic systems has recently become a focus of interest in conjunction with its applications to the theory of algebraic groups or the Galois theory of purely inseparable extensions, and a great deal of research is currently being conducted in this area.

It has only been since the late 1960s that Hopf algebras, as algebraic systems, became objects of study from an algebraic standpoint. However, beginning with the research on representation theory through the use of the representative rings of Lie groups by Hochschild–Mostow (*Ann. of Math.* **66** (1957), 495–542, **68** (1958), 295–313) and in subsequent studies (cf. references [4], [7], [8] for Chapter 3), Hopf algebras have been taken up extensively as algebraic systems and also used in applications. On the other hand, in algebraic topology, the concept of graded Hopf algebras was derived at an even earlier date from an axiomatization of the works of H. Hopf relating to topological properties of Lie groups (cf. *Ann. of Math.* **42** (1941), 22–52). Hence the name, 'Hopf algebra'. For instance, if G is a connected Lie group, the cohomology group $H^*(G)$ or the homology group $H_*(G)$ of G with coefficients in a field k has a multiplication or a dual multiplication induced by the diagonal map $d: G \to G \times G$ ($d(x) = (x, x)$, $x \in G$) and is moreover a commutative k-algebra. In addition, the map $m: G \times G \to G$ defined via the Lie group multiplication induces the maps

$$\Delta: H^*(G) \to H^*(G) \otimes H^*(G) \quad \text{or} \quad \Delta: H_*(G) \to H_*(G) \otimes H_*(G)$$

which respectively make $H^*(G)$ or $H_*(G)$ a k-Hopf algebra. These are graded Hopf algebras and such structures can be defined also for H-spaces, and have been generalized by A. Borel, J. Leary, and others (cf. A. Borel: *Ann. of Math.* **57** (1953), 115–207). For details on the algebraic properties of Hopf algebras, the reader is referred to J. Milnor–J. C. Moore: *Ann of Math.* **81** (1965), 211–64.

This book has as its main objective algebraic applications of (non-graded) Hopf algebras, and an attempt has been made to acquaint the reader with the elementary properties of Hopf algebras with a minimal amount of preliminary knowledge. There is an excellent work on the subject, *Hopf algebras* by Sweedler (Benjamin, 1969), to which this book owes a great deal. But here the central theme will revolve around applications of Hopf algebras to the representative rings of topological groups and to algebraic groups. Some recent developments on the subject have also been incorporated.

This book consists of five chapters and an appendix. Chapter 1 is preparation for the central subject of the book and deals with some basic properties of modules and algebras which become necessary in the sequel. Some simple properties of groups, fields, and topological spaces have been used without proofs. With regard to the solutions to some of the exercises and in the treatment of finitely generated commutative algebras, where I have either omitted or condensed a number of the proofs of well-known theorems, the reader is asked to refer to other texts. In Chapter 2, coalgebras, bialgebras, and Hopf algebras are defined, and their fundamental properties are outlined. Chapter 3 takes up the structure theorem of bimodules and properties of Hopf algebras similar to those of the representative rings of topological groups. The proofs of the existence and uniqueness of the integral of commutative Hopf algebras are due to J. B. Sullivan. In Chapter 4, fundamental properties of affine algebraic groups are proven through an application of the theory of Hopf algebras. The construction of factor groups, the proof of the decomposition theorem of solvable groups, and the proofs of theorems related to completely reducible groups are respectively due to Mitsuhiro Takeuchi, J. B. Sullivan, and M. E. Sweedler. Although properties pertaining to the representation of affine algebraic groups can be described satisfactorily by such an approach, there are drawbacks as well as merits in pursuing a general theory in this context. For instance, it may distort the overall view of the development of the subject matter. It should be interesting, for instance, to attempt an exposition of the theory of Borel subgroups, which is an important topic in the theory of linear algebraic groups, not touched upon in this book. Chapter 5 contains a brief glance at the Galois theory of purely inseparable extensions. Although there are numerous texts dealing with Galois theory, here I have presented a treatment of the subject by D. Winter. The appendix contains a sketch of the theory of categories, where notions such as categories, functors and, for a category $\mathscr{C}$, $\mathscr{C}$-groups and $\mathscr{C}$-cogroups, which are used throughout this book, are defined.

Since commutative Hopf algebras are precisely the commutative algebras which represent affine group schemes, applications of Hopf algebras also naturally develop along these lines. The reader will do well to refer to other texts on this matter.

The writing of this book was suggested to me by Professor Nagayoshi Iwahori of the Faculty of Science of the University of Tokyo, to whom I would like to express my most sincere gratitude. I am also very grateful to Professors Yukio Doi of Fukui University and Mitsuhiro Takeuchi of the University of Tsukuba for many valuable words of advice which they have given me in preparing the manuscript.

Eiichi Abe
Tokyo, Japan

Notations

Sets

$a \in M$ or $M \ni a$	a is an element of the set M
$M \subset N$ or $N \supset M$	$a \in M$ implies $a \in N$, namely, M is contained in N
$M \cup N$; $\bigcup_{\lambda \in \Lambda} M_\lambda$	the union of M and N; the union of M_λ $(\lambda \in \Lambda)$
$M \cap N$; $\bigcap_{\lambda \in \Lambda} M_\lambda$	the intersection of M and N; the intersection of M_λ $(\lambda \in \Lambda)$
$\emptyset$	the empty set
$\mathbb{Z}$	the set of all integers
$\mathbb{N}$	the set of all natural numbers

Maps

$f: M \to N$	a map from the set M to the set N
$x \mapsto y$	the image $f(x)$ of $x \in M$ under the map f is $y \in N$

When $f(M) = N$, f is called a surjection.
If $x, x' \in M$, $x \neq x'$ implies $f(x) \neq f(x')$, then f is called an injection.
For $M' \subseteq M$, we denote the restriction of f to M' by $f|_{M'}$.
If $f: M \to N, g: N \to P$ are two maps, the composition of f and g is written $g \circ f$, $x \mapsto g(f(x))$.

Logical symbols

$A \Rightarrow B$	If proposition A holds, then proposition B holds
$A \Leftrightarrow B$	$A \Rightarrow B$ and $B \Rightarrow A$
$\forall x \in M$	for any element x of M

Contents

		Page
	Preface	vii
	Notation	xi
1	**Modules and algebras**	
	1. Modules	1
	2. Algebras over a commutative ring	16
	3. Lie algebras	24
	4. Semi-simple algebras	40
	5. Finitely generated commutative algebras	49
2	**Hopf algebras**	
	1. Bialgebras and Hopf algebras	53
	2. The representative bialgebras of semigroups	65
	3. The duality between algebras and coalgebras	78
	4. Irreducible bialgebras	90
	5. Irreducible cocommutative bialgebras	107
3	**Hopf algebras and representations of groups**	
	1. Comodules and bimodules	122
	2. Bimodules and bialgebras	137
	3. Integrals for Hopf algebras	144
	4. The duality theorem	158
4	**Applications to algebraic groups**	
	1. Affine k-varieties	163
	2. Affine k-groups	170
	3. Lie algebras of affine algebraic k-groups	186
	4. Factor groups	201
	5. Unipotent groups and solvable groups	210
	6. Completely reducible groups	222

5 Applications to field theory
1. K/k-bialgebras 229
2. Jacobson's theorem 243
3. Modular extensions 252

Appendix: Categories and functors
A.1 Categories 264
A.2 Functors 267
A.3 Adjoint functors 271
A.4 Representable functors 271
A.5 $\mathscr{C}$-groups and $\mathscr{C}$-cogroups 274

References 278
Index 281

1

Modules and algebras

1 Modules

This section deals with direct sums, direct products, tensor products, and the projective and inductive limits of modules. Proofs of some fundamental properties of such constructions have been omitted and left as exercises. For these, the reader is asked to refer to texts such as [3] or [5].

1.1 Modules

A set A with two operations – addition and multiplication – which satisfies properties (1) to (3) below is said to be a **ring with identity**. Since this book deals exclusively with this type of ring, we will call them simply **rings**.

(1) The addition $+$ makes A an abelian group.

(2) The multiplication $\cdot$ makes A a semigroup with identity element 1.

(3) The distributive law holds. Namely, for $a, b, c \in A$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

A ring with a commutative multiplication is called a **commutative ring**. Henceforth, the product $a \cdot b$ of $a, b \in A$ will be written ab. Let A and B be rings. If a map $u : A \to B$ satisfies the properties

$$u(a + b) = u(a) + u(b), \quad u(ab) = u(a)u(b), \quad u(1) = 1, \quad a, b \in A,$$

then u is said to be a **ring morphism** from A to B. The category of rings (resp. commutative rings) will be denoted **Alg** (resp. **M**) and the set of all ring morphisms from A to B will be written **Alg** (A, B) (resp. $\mathbf{M}(A, B)$ when A, B are commutative rings).

For a ring A and an abelian group M, suppose we are given a map $\varphi : A \times M \to M$ (resp. $\psi : M \times A \to M$). We signify the group operation on M by addition $+$, and for $a \in A$, $x \in M$, we write $\varphi(a, x) = ax$ (resp. $\psi(x, a) = xa$). When conditions (1) to (4) (resp. (1′) to (4′)) below hold for $a, b \in A$ and $x, y \in M$, M is called a **left A-module** (resp. **right A-module**), and φ (resp. ψ) is said to be the **structure map** of the left (resp. right) A-module.

(1)	$a(x+y) = ax + ay$,	resp.	(1′)	$(x+y)a = xa + ya$,
(2)	$(a+b)x = ax + bx$,		(2′)	$x(a+b) = xa + xb$,
(3)	$(ab)x = a(bx)$,		(3′)	$x(ab) = (xa)b$,
(4)	$1x = x$.		(4′)	$x1 = x$.

Moreover, given rings A, B, if M is both a left A-module and a right B-module satisfying the condition

$$(ax)b = a(xb), \quad a \in A, \quad b \in B, \quad x \in M,$$

then M is called a **two-sided (A, B)-module**. A two-sided (A, A)-module is called simply a **two-sided A-module**. If A is a commutative ring, a left A-module can be regarded as a right A-module, and is often simply called an A-module. For instance, an abelian group is a $\mathbb{Z}$-module. In the case of a ring A, when the map defining the multiplication $\mu: A \times A \to A$ given by $\mu(a, b) = ab$, $a, b \in A$ is taken to be the structure map, A becomes a left A-module as well as a right A-module. Moreover, A is a two-sided A-module. For a field k, a k-module is also called a **k-linear space** or a **k-vector space**.

Let M, N be left A-modules. A map $f: M \to N$ such that

$$f(ax + by) = af(x) + bf(y), \quad a, b \in A, \quad x, y \in M,$$

is called a **left A-module morphism** from M to N. If k is a field, a k-module morphism is sometimes called a **k-linear map**. The category of left A-modules is denoted ${}_A\mathbf{Mod}$, and the set of all left A-module morphisms from M to N is denoted ${}_A\mathbf{Mod}(M, N)$. Similarly, given right A-modules M, N, we can define **right A-module morphisms** and the set of all right A-module morphisms from M to N, which we write $\mathbf{Mod}_A(M, N)$. In particular, $\mathbf{Mod}_A(M, M)$ is written $\mathrm{End}_A(M)$. If $f \in {}_A\mathbf{Mod}(M, N)$ or $f \in \mathbf{Mod}_A(M, N)$ is bijective, f is said to be an **isomorphism**. The identity map from M to M is an isomorphism, denoted by 1_M or simply by 1.

Now let $f, g \in {}_A\mathbf{Mod}(M, N)$. Defining

$$(f + g)(x) = f(x) \pm g(x), \quad x \in M,$$

$f \pm g$ becomes a left A-module morphism from M to N. Under this operation, ${}_A\mathbf{Mod}(M, N)$ becomes an abelian group. If N is also a two-sided A-module, then by defining

$$(fa)(x) = f(x)a, \quad a \in A, \quad x \in M,$$

we have $fa \in {}_A\mathbf{Mod}(M, N)$, and hence ${}_A\mathbf{Mod}(M, N)$ becomes a right A-module. When in particular $N = A$, N is a two-sided A-module, and here, the right A-module ${}_A\mathbf{Mod}(M, A)$ is called the **dual right A-module** of the left A-module M, which is denoted by M^*. If A is commutative, ${}_A\mathbf{Mod}(M, N)$ can be regarded as a left A-module.

EXERCISE 1.1 Given a left A-module morphism $f : M \to N$, f is an isomorphism $\Leftrightarrow$ there exists a left A-module morphism $g : N \to M$ such that $f \circ g = 1_N$ and $g \circ f = 1_M$.

EXERCISE 1.2 Let A be a commutative ring. Given left A-modules M, M', N, N' and left A-module morphisms $g : M \to M'$, $h : N \to N'$, the maps

$$g^* : {}_A\mathbf{Mod}(M', N) \to {}_A\mathbf{Mod}(M, N), \quad f \mapsto f \circ g,$$
$$h_* : {}_A\mathbf{Mod}(M, N) \to {}_A\mathbf{Mod}(M, N'), \quad f \mapsto h \circ f,$$

are left A-module morphisms.

We observe that if a subgroup N of a left A-module M satisfies the condition

$$x \in N, \quad a \in A \Rightarrow ax \in N,$$

then N is a left A-module. Such an N is called a **left A-submodule** of M. The factor group M/N also inherits a left A-module structure, and M/N is called a **factor left A-module**. Regarding a ring A as a left A-module (resp. right A-module; two-sided A-module), then an A-submodule of A is simply a **left ideal** (resp. **right ideal**; **two-sided ideal**).

Suppose now that the only left A-submodules of a left A-module M

are $\{0\}$ and M. In this situation, we call M a **simple** (or **irreducible**) **left A-module**. Given a left A-module morphism $f: M \to N$, the sets

$$\operatorname{Ker} f = \{x \in M;\quad f(x) = 0\},$$
$$\operatorname{Im} f = \{f(x) \in N;\quad x \in M\}$$

are left A-submodules of M and N respectively and are called the **kernel** of f and the **image** of f. The smallest left A-submodule which contains a subset S of a left A-module M is written $\langle S \rangle$ and called the left A-submodule generated by S.

Let Λ be a finite or infinite sequence of consecutive integers and let M_i $(i \in \Lambda)$ be left A-modules. Suppose we are given left A-module morphisms $f_i: M_i \to M_{i+1}$ $(i, i+1 \in \Lambda)$. When $\operatorname{Ker} f_{i+1} = \operatorname{Im} f_i$ $(i, i+1 \in \Lambda)$ for the sequence of left A-module morphisms

$$\cdots \to M_i \to M_{i+1} \to M_{i+2} \to \cdots, \tag{1.1}$$

then (1.1) is said to be an **exact sequence**. For instance, when $0 \to M \xrightarrow{f} N$ (resp. $M \xrightarrow{f} N \to 0$; $0 \to M \xrightarrow{f} N \to 0$) is an exact sequence, then f is injective (resp. surjective; bijective), and the converse also holds.

EXERCISE 1.3 Let A be a commutative ring. For a sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ of A-module morphisms to be an exact sequence, it is necessary and sufficient that, for any left A-module N, the sequence

$$0 \to {}_A\mathbf{Mod}\,(M'', N) \xrightarrow{g^*} {}_A\mathbf{Mod}\,(M, N) \xrightarrow{f^*} {}_A\mathbf{Mod}\,(M', N)$$

is exact. Furthermore, a sequence $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ of left A-module morphisms is exact if and only if, for any left A-module M, the sequence

$$0 \to {}_A\mathbf{Mod}\,(M, N') \xrightarrow{f_*} {}_A\mathbf{Mod}\,(M, N) \xrightarrow{g_*} {}_A\mathbf{Mod}\,(M, N'')$$

is exact (cf. Exercise 1.2).

1.2 Direct products and direct sums

Let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a family of left A-modules. Pick one element x_λ from each M_λ and write the resulting set $x = \{x_\lambda\}_{\lambda \in \Lambda}$, calling x_λ the λ-component of x. Let P be the set of all $x = \{x_\lambda\}_{\lambda \in \Lambda}$ constructed in the above manner. For $x=\{x_\lambda\}_{\lambda\in\Lambda}$, $y=\{y_\lambda\}_{\lambda\in\Lambda}\in P$ and $a\in A$, we define the operations

$$x+y=\{x_\lambda+y_\lambda\}_{\lambda\in\Lambda},\quad ax=\{ax_\lambda\}_{\lambda\in\Lambda},$$

which make P a left A-module. The map $p_\lambda : P\to M_\lambda$ which assigns to $x=\{x_\lambda\}_{\lambda\in\Lambda}\in P$ the λ-component x_λ of x is a left A-module morphism, and we call p_λ the canonical projection from P to M_λ. The pair $(P, \{p_\lambda\}_{\lambda\in\Lambda})$ consisting of P and the family of canonical projections p_λ $(\lambda\in\Lambda)$ is called the **direct product** of the family of left A-modules $\{M_\lambda\}_{\lambda\in\Lambda}$, and is written $P=\prod_{\lambda\in\Lambda} M_\lambda$. For $\Lambda=\{1,2,\ldots,n\}$, this is sometimes written $M_1\times\ldots\times M_n$. The direct product $(P, \{p_\lambda\}_{\lambda\in\Lambda})$ has the following property.

(P) Given a pair $(N, \{q_\lambda\}_{\lambda\in\Lambda})$ consisting of an arbitrary left A-module N and a family of left A-module morphisms $q_\lambda : N\to M_\lambda$ $(\lambda\in\Lambda)$, there exists a unique left A-module morphism $f: N\to P$ which satisfies $p_\lambda\circ f=q_\lambda$ $(\lambda\in\Lambda)$.

Hence the map which assigns to each $f\in {}_A\mathbf{Mod}(N, P)$, the element $\{p_\lambda\circ f\}_{\lambda\in\Lambda}\in\prod_{\lambda\in\Lambda} {}_A\mathbf{Mod}(N, M_\lambda)$ is a bijection. Furthermore, if A is a commutative ring, we have

$${}_A\mathbf{Mod}(N, P)\cong\prod_{\lambda\in\Lambda} {}_A\mathbf{Mod}(N, M_\lambda)$$

as left A-modules. The element of ${}_A\mathbf{Mod}(N, P)$ which corresponds to $\{f_\lambda\}_{\lambda\in\Lambda}\in\prod_{\lambda\in\Lambda} {}_A\mathbf{Mod}(N, M_\lambda)$ is written $\prod_{\lambda\in\Lambda} f_\lambda$ and is said to be the direct product of the A-module morphisms $\{f_\lambda\}_{\lambda\in\Lambda}$. A left A-module P with the above property is unique up to isomorphism, and the direct product of the family of left A-modules $\{M_\lambda\}_{\lambda\in\Lambda}$ is characterized by property (P).

Let S be the subset of P consisting of all those elements whose λ-components are zero except for a finite number of λs. Then S turns out to be a left A-submodule of P. When Λ is a finite set, we have $S=P$. Given $x_\lambda\in M_\lambda$, let $i_\lambda(x_\lambda)$ stand for the element of S whose λ-component is x_λ and all other components zero. Then the map $i_\lambda : M_\lambda\to S$ is a left A-module injection and is called the canonical embedding of M_λ into S. Identifying $i_\lambda(x_\lambda)$ with x_λ and regarding M_λ as a left A-submodule of S, the element $x=\{x_\lambda\}_{\lambda\in\Lambda}$ of S can be written