MODERN CLASSICAL ALGEBRA

John C. Moore

Lectures
Princeton University
1960-1961

Chapter 0: Preliminary remarks.

In the following chapters the standard notation of elementary set theory will be used without comment. For example, if A and B are sets the Cartesian product of A with B will be denoted by $A \times B$; it is the set of ordered pairs (a,b) such that $a \in A$ (a belongs to A) and $b \in B$. If the set A is a subset of the set B, we write either $A \subset B$ or $B \supset A$. The union of the sets A and B is denoted by $A \cup B$, and the intersection by $A \cap B$. Familiarity with all of the usual operations on sets will be presumed. Thus we assume that the reader is aware that the operation of taking the Cartesian product of sets is associative, i.e. if A,B,C are sets then $(A \times B) \times C = A \times (B \times C)$, and this set will usually be denoted by $A \times B \times C$.

If I is a set and for each element $i \in I$, A_i is a set, we will let $\cup_{i \in I} A_i$ denote the union of all of the sets A_i such that $i \in I$, and $\cap_{i \in I} A_i$ denote the intersection of these sets.

In the direction of algebra, the reader will be assumed to be familiar with the concepts of group, ring, and field at least to the extent which they usually occur in undergraduate algebra courses. As a preliminary to defining the notion of module the definition of ring will be recalled.

<u>Definitions</u>: A <u>ring</u> is an abelian group Λ together with a map $\varphi: \Lambda \times \Lambda \longrightarrow \Lambda$ and an element $1 \in \Lambda$ such that if we let $\varphi(x,y)$ be denoted by xy for $(x,y) \in \Lambda \times \Lambda$, then

i) $(xy)z = x(yz)$ for $x,y,z \in \Lambda$,

ii) $(x+y)z = xz + yz$ for $x,y,z \in \Lambda$,

iii) $x(y+z) = xy + xz$ for $x,y,z \in \Lambda$, and

iv) $1 \cdot x = x = x \cdot 1$ for $x \in \Lambda$.

The ring Λ is <u>commutative</u> if $xy = yx$ for all $x,y \in \Lambda$.

Note that the notion of ring to be used is what is sometimes called ring with a unit, and the unit is denoted by 1. For us rings without unit will not exist.

<u>Definitions</u>: If Λ is a ring, a <u>Λ-module</u> is an abelian group A together with a map $\varphi: \Lambda \times A \longrightarrow A$ such that if we let $\varphi(\lambda,a)$ be denoted by λa for $(\lambda,a) \in \Lambda \times A$, then

i) $(\lambda_1\lambda_2)a = \lambda_1(\lambda_2 a)$ for $\lambda_1,\lambda_2 \in \Lambda$, $a \in A$,

ii) $(\lambda_1 + \lambda_2)a = \lambda_1 a + \lambda_2 a$ for $\lambda_1,\lambda_2 \in \Lambda$, $a \in A$,

iii) $\lambda(a_1 + a_2) = \lambda a_1 + \lambda a_2$ for $\lambda \in \Lambda$, $a_1,a_2 \in A$, and

iv) $1 \cdot a = a$ for $a \in A$.

A <u>sub Λ-module</u> A' of A is a subgroup A' of A such that if $(\lambda,x) \in \Lambda \times A'$, then $\lambda x \in A'$.

The notion defined above is usually called left Λ-module unless the ring Λ is commutative. There exists also the notion of right Λ-module. A right Λ-module A is an abelian group A together with a map $\varphi: A \times \Lambda \longrightarrow A$ such that

i) $a(\lambda_1 \lambda_2) = (a \lambda_1) \lambda_2$ for $a \in A$, $\lambda_1, \lambda_2 \in \Lambda$,

ii) $a(\lambda_1 + \lambda_2) = a \lambda_1 + a \lambda_2$ for $a \in A$, $\lambda_1, \lambda_2 \in \Lambda$,

iii) $(a_1 + a_2) \lambda = a_1\lambda + a_2\lambda$ for $a_1, a_2 \in A$, $\lambda \in \Lambda$,

iv) $a \cdot 1 = a$ for $a \in A$.

We will usually deal with left Λ-modules, and omit the word left. In any context where both left and right Λ-modules are being considered no such omission will be made.

If Λ is a commutative ring and A is a left Λ module we may define $\psi: A \times \Lambda \longrightarrow A$ by $\psi(a,\lambda) = \lambda a$. This defines on A in a canonical way the structure of a right Λ-module, and we see that there is no distinction between the concepts of right and left Λ-module.

Definitions: If A and B are Λ-modules, then $f: A \longrightarrow B$ is a morphism of Λ-modules if it is a homomorphism of abelian groups and if $f(\lambda a) = \lambda f(a)$ for $\lambda \in \Lambda$, $a \in A$. The morphism $f: A \longrightarrow B$ is a monomorphism if $f(a) = 0$ implies $a = 0$ for $a \in A$, it is an epimorphism if for every $b \in B$ there exists $a \in A$ such that $f(a) = b$, and it is an isomorphism if it is both an epimorphism and a monomorphism.

<u>Notation</u>: The ring of integers will always be denoted by $\mathbb{Z}$.

Observe that there is no difference between the notion of $\mathbb{Z}$-module and the notion of abelian group, nor is there any difference between the notion of morphism of $\mathbb{Z}$-modules, and that of homomorphism of abelian groups.

<u>Definition</u>: If B is a Λ-module, and A is a submodule of B , then B/A is that Λ module such that as an abelian group it is the quotient of the group B by the subgroup A , and such that if $\pi: B \longrightarrow B/A$ is the canonical homorphism of B onto the quotient group B/A , then π is a morphism of Λ modules.

If $f: A \longrightarrow B$ is a morphism of Λ-modules, then the <u>kernel</u> of f is the submodule of A consisting of all those elements $a \in A$ such that $f(a) = 0$; it is denoted by $\mathrm{Ker}(f)$. The <u>image</u> of f is the submodule of B consisting of those elements of the form $f(a)$ for some $a \in A$; it is denoted by $\mathrm{Im}(f)$. The <u>coimage</u> of f is $A/\mathrm{Ker}(f)$, denoted by $\mathrm{Coim}(f)$, and the <u>cokernel</u> of f is $B/\mathrm{Im}(f)$, denoted by $\mathrm{Coker}(f)$.

Saying that f is a monomorphism is equivalent to saying that $\mathrm{Ker}(f) = 0$, and saying that f is an epimorphism is equivalent to saying that $\mathrm{Coker}(f) = 0$.

<u>Definition</u>: The sequence of morphisms of Λ-modules $A \xrightarrow{f} B \xrightarrow{g} C$ is <u>exact</u> if $\mathrm{Im}(f) = \mathrm{Ker}(g)$. A more complicated sequence of morphisms

$\cdots \longrightarrow A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} \cdots \xrightarrow{f_m} A_{m+1} \longrightarrow \cdots$ is exact if each of the subsequences $A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} A_{n+2}$ is exact.

Frequently we will consider exact sequences of the form $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$. Such a sequence is called <u>short exact</u>, and saying that we have such a short exact sequence is equivalent to saying f is a monomorphism, g is an epimorphism, and $\mathrm{Ker}(g) = \mathrm{Im}(f)$.

The ring Λ is itself a Λ-module. Submodules of Λ are just those things which are frequently called left ideals. When Λ is considered as a Λ-module, it has an important special property. Let A be any Λ-module, and let $a \in A$, then there exists a unique morphism $f_a: \Lambda \longrightarrow A$ such that $f_a(1) = a$. Clearly $f_a(\lambda) = \lambda a$. Thus the points of A correspond exactly to the morphisms of Λ into A .

<u>Definitions</u>: Let Λ be a ring and X a set. Let $F_\Lambda(X)$ be the Λ-module defined as follows: the points of $F_\Lambda(X)$ are the functions $h: X \longrightarrow \Lambda$ such that $h(x) \neq 0$ for at most a finite number of elements $x \in X$. If $h_1, h_2 \in F_\Lambda(X)$, then $h_1 + h_2$ is defined by letting $(h_1 + h_2)(x) = h_1(x) + h_2(x)$ for $x \in X$. If $\lambda \in \Lambda$, and $h \in F_\Lambda(X)$, then λh is defined by letting $(\lambda h)(x) = \lambda(h(x))$ for $x \in X$.

Let $i: X \longrightarrow F_\Lambda(X)$ be the function such that $i(x)(x) = 1$, and $i(x)(y) = 0$ for $y \neq x$.

<u>Proposition</u>: Let X be a set, A a Λ-module, and $f: X \longrightarrow A$ a function, then there exists a unique morphism $g: F_\Lambda(X) \longrightarrow A$ such that $g\,i\,(x) = f(x)$ for $x \in X$.

<u>Proof</u>: Let $h \in F_\Lambda(X)$ and suppose $x_o,\ldots,x_n$ are the points of X such that $h(x) \neq 0$. Let $g(h) = \Sigma_{k=o}^{n} h(x_k)\, f(x_k)$. Now g is a morphism having the desired property and it is unique.

<u>Definitions:</u> The Λ-module B is <u>free</u> if there exists a set X , and a function $f: X \longrightarrow B$ such that the corresponding morphism $g: F_\Lambda(X) \longrightarrow B$ is an isomorphism.

Using the function $i: X \longrightarrow F_\Lambda(X)$ we consider that X is a subset of $F_\Lambda(X)$, and we call $F_\Lambda(X)$ the free Λ-module generated by X for any set X . When $g: F_\Lambda(X) \longrightarrow B$ is an isomorphism the image of the set X under g is called a basis for B , and every element of B can be expressed uniquely as a linear combination of the elements of the basis.

<u>Definitions</u>: If B is a Λ-module, <u>a set of generators for B</u> is a subset X of B such that the morphism $g: F_\Lambda(X) \longrightarrow B$ which has the property that $g(x) = x$ for $x \in X$ is an epimorphism. We say that B is <u>finitely generated</u> if there exists a finite set of generators for B .

Exercises

1. Let Λ be a ring, and A a Λ-module. Let $\mathcal{E}_\Lambda(A)$ be the set of morphisms $f: A \longrightarrow A$. If $f, g \in \mathcal{E}_\Lambda(A)$ define $f + g$ by letting $(f+g)(a) = f(a) + g(a)$ and $f \cdot g$ by letting $(fg)(a) = f(g(a))$. Show that $\mathcal{E}_\Lambda(A)$ is a ring. If Λ is commutative show that the function $g: \Lambda \longrightarrow \mathcal{E}_\Lambda(A)$ defined by $g(\lambda)(a) = \lambda a$ is a morphism of rings, i.e. $g(1) = 1$, $g(\lambda_1 + \lambda_2) = g(\lambda_1) + g(\lambda_2)$ and $g(\lambda_1 \lambda_2) = g(\lambda_1)\, g(\lambda_2)$ for $\lambda_1, \lambda_2 \in \Lambda$. Show that if Λ is not commutative the preceding statement is not always true.

2. Let Λ be a ring, and A an abelian group. Show that any morphism of rings $g: \Lambda \longrightarrow \mathcal{E}_Z(A)$ gives A the structure of a Λ-module. Conversely show that if A is a Λ-module the function $g: \Lambda \longrightarrow \mathcal{E}_Z(A)$ such that $g(\lambda)(a) = \lambda a$ is a morphism of rings.

3. If B is a Λ-module show that there exists a free Λ-module F and an epimorphism $f: F \longrightarrow B$.

4. Show that if $f: A \longrightarrow B$ is an epimorphism of Λ-modules, and B is free, then there exists a morphism $h: B \longrightarrow A$ such that $hf: B \longrightarrow B$ is the identity.

5. Show that if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is a short exact sequence of Λ-modules, and A and C are free then B is free.

6. Show that if $f: A \longrightarrow B$ is an epimorphism of Λ-modules and A is finitely generated, then B is finitely generated.

7. Show that if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is a short exact sequence of Λ-modules, and both A and C are finitely generated, then B is finitely generated.

8. Show that if I is a set, and for each $i \in I$, A_i is a Λ-module, then there exists a Λ-module $\oplus_{i \in I} A_i = A$ and morphisms $f_i: A_i \longrightarrow A$ such that if B is any Λ-module and for each $i \in I$, $g_i: A_i \longrightarrow B$ is a morphism there is a unique morphism $g: A \longrightarrow B$ such that for each $i \in I$, $gf_i = g_i$.

9. Show that I is a set, and for each $i \in I$ A_i is a Λ-module, then there exists a Λ-module $\times_{i \in I} A_i = A$ and morphisms $\pi_i: A \longrightarrow A_i$ such that if B is any Λ-module and for each $i \in I$, $g_i: B \longrightarrow A_i$ is a morphism there is a unique morphism $g: B \longrightarrow A$ such that for each $i \in I$, $\pi_i g = g_i$.

10. Show that if I is a set, and for each $i \in I$, A_i is a Λ-module, then there is a unique morphism $h: \oplus_{i \in I} A_i \longrightarrow \times_{i \in I} A_i$ such that $\pi_i h f_i : A_i \longrightarrow A_i$ is the identity, and show further that h is an isomorphism if and only if $\{i \mid i \in I \text{ and } A_i \neq 0\}$ is a finite set.