2.1 Modules and Module Homomorphisms

The notion of a **module** arises out of attempts to do classical linear algebra (vector spaces over fields) using arbitrary rings of coefficients.

Let A be a ring. An A-**module** is an abelian group $(M, +)$ together with a map (**scalar multiplication**)

$$\mu : A \times M \ \rightarrow \ M \ , \quad (a, m) \ \mapsto \ am \equiv \mu(a, m)$$

satisfying the following axioms:

(i) $(\forall a \in A)(\forall x, y \in M) \qquad a(x+y) \;=\; ax+ay$;

(ii) $(\forall a, b \in A)(\forall x \in M) \qquad (a+b)x \;=\; ax+bx$;

(iii) $(\forall a, b \in A)(\forall x \in M) \qquad (ab)x \;=\; a(bx)$;

(iv) $(\forall x \in M) \qquad 1x \;=\; x$.

The notion of a module is closely related to endomorphism rings of abelian groups:

Consider an abelian group M and put

$$\text{End}\,(M) = \{\, \phi : M \to M \;\mid\; \phi \text{ is a group homomorphism} \,\}\,,$$

elements of which are called **endomorphisms**.

Easy to check:

End (M) is a (noncommutative) ring with respect to **pointwise addition**, that is, for $\phi, \psi \in$ End (M) ,

$$(\phi + \psi)(x) \;=\; \phi(x) + \psi(x) \qquad\qquad (\forall x \in M) \ ,$$

and **multiplication** being composition of mappings.

Suppose also that M is an A-module.

Define

$$\theta \ : \ A \ \longrightarrow \ \text{End}\,(M)$$

by, for $a \in A$,

$$\theta(a) \ : \ M \ \longrightarrow \ M \quad \text{where} \quad m \mapsto am \quad (\forall m \in M) \ .$$

By Axiom (i), each $\theta(a)$ is indeed a group homomorphism,

and by Axioms (ii), (iii), (iv), θ preserves addition, multiplication and identity elements respectively.

Thus $\theta \ : \ A \ \longrightarrow \ \text{End}\,(M)$ is a ring homomorphism.

Conversely, let $\theta : A \longrightarrow \text{End}\,(M)$ be a ring homomorphism.

Define $\mu : A \times M \to M$ by

$$(a, m) \;\mapsto\; [\theta(a)](m) \qquad (\forall a \in A, m \in M)\ .$$

Then Axiom (i) holds, because each $\theta(a)$ is a group homomorphism,

and Axioms (ii), (iii), (iv) hold because θ preserves addition, multiplication and identity elements respectively.

Thus

> A-modules correspond to ring homomorphisms from A into endomorphism rings of abelian groups.

Examples:

(1) If $I \lhd A$ then I becomes an A-module by regarding the ring multiplication, of elements of A with elements of I, as scalar multiplication.

In particular, A is an A-module.

(2) If A is a field then A-modules are precisely vector spaces over A .

(3) All abelian groups are $\mathbb{Z}$-modules (mentioned in the Overview).

(4) Let $A = F[x]$ where F is a field, and let M be an A-module.

Since F is a subring of A, M is also a vector space over F.

Define

$$\alpha \; : \; M \to M \qquad \text{by} \qquad m \mapsto xm \quad (\forall m \in M) \,.$$

By Axioms (i) and (iii),

α is a linear transformation of M as a vector space over F.

Further, consider

$$f(x) \;=\; \lambda_0 + \lambda_1 x \;+\; \ldots \;+ \lambda_n x^n \quad \in \quad F[x]\,.$$

Then, by Axioms (ii) and (iii), for each $m \in M$,

$$\begin{aligned} f(x)\,m &= \lambda_0\,m + \lambda_1 x\,m + \ldots + \lambda_n x^n\,m \\ &= \lambda_0\,m + \lambda_1 \alpha(m) + \ldots + \lambda_n \alpha^n(m) \\ &= \bigl(\lambda_0\,\mathrm{id} \;+ \lambda_1 \alpha + \ldots + \lambda_n \alpha^n\bigr)(m) \\ &= \bigl[f(\alpha)\bigr](m)\,. \end{aligned}$$

Thus

scalar multiplication by $f(x)$ is application of the linear transformation

$$f(\alpha) : M \to M \ .$$

Conversely, given any vector space M over a field F and any linear transformation $\alpha : M \to M$, one can make M into an $F[x]$-module by defining

$$f(x)\, m \ = \ \big[f(\alpha)\big](m)$$

for $m \in M$ and $f(x) \in F[x]$.

(5) Let G be any group and F any field. Form the (not necessarily commutative) group ring

$$F[G] \;=\; \Big\{ \, \sum \alpha_g \, g \;\Big|\; g \in G\,, \;\; \alpha_g \in F\,, \quad \text{of finite support} \;\; \Big\} \, .$$

Consider an $F[G]$-module M .

In particular, M is a vector space over F

$\Big[$ because F can be identified with a subring of $F[G]$ under the injection $\lambda \;\mapsto\; \lambda\,1 \qquad (\forall \lambda \in F)\, \Big]$.

If $g \in G$ then define

$$\theta(g) : M \rightarrow M \qquad \text{by} \qquad m \mapsto gm \ .$$

Easy to check that

$$\theta \ : \ G \ \longrightarrow \ \text{Aut}_{\,F}(M)$$

where $\text{Aut}_{\,F}(M)$ is the group of invertible linear transformations from M to M , regarded as a vector space over F ,

and, moreover,

θ is a group homomorphism, that is, a **group representation**.

Conversely, if M is a vector space over a field F, G is a group and

$$\theta : G \to \text{Aut}_F(M)$$

is a group representation, then the following is easy to check:

by defining

$$gm = \left[\theta(g)\right](m) \qquad (\forall g \in G)(\forall m \in M)$$

and extending by linearity to arbitrary elements of $F[G]$, we obtain a scalar multiplication, with respect to which M becomes an $F[G]$-module.

Thus, $F[G]$-modules correspond to representations of a group G by invertible linear transformations of a vector space over a field F .