IV. Modules

IV.A. Definition and examples

Modules over a ring arose from algebraic number theory and representation theory. The definition we use now, a simultaneous generalization of vector spaces over a field and the action of a group on a set, is another contribution of E. Noether. The main immediate applications will be to the structure theory of finitely generated abelian groups and to the canonical forms of a linear transformation on a vector space.

IV.A.1. DEFINITION. Let R be a ring.
A **left** (resp. **right**) ***R*-module** is

- an abelian group M

together with a "scalar multiplication" map

- $\underset{(r,m)}{R} \times \underset{\longmapsto}{M \to} \underset{rm}{M}$ resp. $\underset{(m,r)}{M} \times \underset{\longmapsto}{R \to} \underset{mr}{M}$

satisfying the axioms ($\forall\ m, m' \in M$ and $r, r' \in R$)

$$\left.\begin{array}{ll} \text{(i)} & r(m+m') = rm + rm' \\ \text{(ii)} & (r+r')m = rm + r'm \\ \text{(iii)} & (rr')m = r(r'm) \\ \text{(iv)} & 1_R m = m \end{array}\right\} \quad \text{resp.} \quad \begin{cases} (m+m')r = mr + m'r \\ m(r+r') = mr + mr' \\ m(rr') = (mr)r' \\ m1_R = m. \end{cases}$$

If R is commutative, then we use the terminology "R-module" as left vs. right turn out to yield equivalent structures.

IV.A.2. EXAMPLES. (a) Given a field $\mathbb{F}$, an $\mathbb{F}$-module is the same thing as an **$\mathbb{F}$-vector space** (we can take this as the definition).

(b) A $\mathbb{Z}$-module is the same thing as an abelian group.

(c) Any ring R is a (left and right) module over itself. Any left [resp. right] ideal $I \subset R$ is a left [resp. right] R-module.

(c′) Given any subring $R_0 \subset R$, R is a (left and right) R_0-module, and any R-module M has the structure of an R_0-module.

(c″) Given a ring homomorphism $\theta\colon S \to R$, an R-module M has the structure of an S-module via $sm := \theta(s)m$.

(d) Given a ring R, the map $R \times R^n \to R^n$ sending $(r, (r_1, \ldots, r_n)) \mapsto (rr_1, \ldots, rr_n)$ makes R^n into a (left) R-module. This is the prototype for **free** R-modules. ("Direct summands" of R^n will be the prototype for **projective** R-modules, and "quotients" of R^n for **finitely generated** R-modules.)

(e) For those who are familiar with manifolds, a finitely generated projective $C^\infty(\mathcal{M})$-module is the same thing as a smooth vector bundle over $\mathcal{M}$.

(f) $\mathbb{R}^n$ is a left $M_n(\mathbb{R})$-module.

(g) Let G be a finite group. A **representation of G** on an $\mathbb{F}$-vector space V is a map

$$G \times V \overset{\rho}{\to} V$$
$$(g, v) \mapsto \rho(g)v \quad (\text{or } "g.v")$$

$$\text{satisfying} \quad \begin{cases} g.(v + v') = g.v + g.v' \\ g.(fv) = f(g.v) \quad (f \in \mathbb{F}) \\ (gg').v = g.(g'.v), \quad 1_G.v = v. \end{cases}$$

We can "linearize" this action to get a left-module: let $\mathbb{F}[G]$ be the ring consisting of elements $\sum_i f_i[g_i]$ with multiplication law generated by $[g][g'] := [gg']$, the so-called **group ring of G over** $\mathbb{F}$. Then we define

$$(\textstyle\sum_i f_i[g_i])v := \sum_i f_i(g_i.v)$$

and check axioms (i)-(iv). So a representation of G has the structure of an $\mathbb{F}[G]$-module.

(h) Given an $\mathbb{F}$-vector space V, an **endomorphism**

$$T\colon V \to V$$

is an $\mathbb{F}$-*linear* homomorphism of abelian groups; that is, we have $T(fv) = fT(v)$ and $T(v+v') = T(v)+T(v')$ ($\forall\ f \in \mathbb{F},\ v, v' \in V$). Denoting the collection of all such by $\mathbf{End}_{\mathbb{F}}(\mathbf{V})$, we consider the evaluation map

$$\begin{aligned} \mathbb{F}[\lambda] &\xrightarrow{\theta} \mathrm{End}_{\mathbb{F}}(V) \\ P(\lambda) &\longmapsto P(T), \end{aligned}$$

where λ is an indeterminate.

Now, we can *add* and *compose* endomorphisms, making $\mathrm{End}_{\mathbb{F}}(V)$ into a ring and V into an $\mathrm{End}_{\mathbb{F}}(V)$-module. It also makes θ a ring homomorphism, with image

$$\mathrm{im}(\theta) =: \mathbb{F}[T].$$

By (c″), this gives V the structure of an $\mathbb{F}[\lambda]$-module, which leads to the theory of canonical forms for T.

(i) Let F be a number field, and $\mathfrak{a} \subset F$ be a fractional ideal. Then $\mathfrak{a}$ has the structure of $\mathcal{O}_F$-module. Indeed, F is also an $\mathcal{O}_F$-module; but it is not finitely generated as an abelian group (why?), whereas $\mathfrak{a}$ is.

Conversely, we claim that any finitely generated abelian subgroup of F with $\mathcal{O}_F$-module structure is a fractional ideal. Let $\mathfrak{a} \leq F$ be f.g. and closed under multiplication by $\mathcal{O}_F$; then we ask: *does there exist an element $f \in F$ such that $f\mathfrak{a} \subset \mathcal{O}_F$?* If this is true, then $f\mathfrak{a} =: I$ is an ideal of $\mathcal{O}_F$, and $\mathfrak{a} = f^{-1}I$ a fractional ideal.

To see this, let $\alpha_1, \ldots, \alpha_k$ be a generating set for $\mathfrak{a}$ (as abelian group), and write $\alpha_i = \frac{a_i}{b_i}$, $a_i, b_i \in \mathcal{O}_F$, using the fact that F is the fraction field of $\mathcal{O}_F$. Then $(\prod_j b_j)\alpha_i \in \mathcal{O}_F\ (\forall i) \implies (\prod_j b_j)\mathfrak{a} \subset \mathcal{O}_F$.

Now consider the

IV.A.3. DEFINITION. A module M over a ring R is **finitely generated** (as an R-module) if there exists a finite subset $\mathcal{S} \subseteq M$ such that $M = \{\sum_{s \in \mathcal{S}} r_s s \mid r_s \in R\}$.

Since $\mathcal{O}_F$ is f.g. as an abelian group, $\mathfrak{a}$ is f.g. as an abelian group iff $\mathfrak{a}$ is f.g. as an $\mathcal{O}_F$-module, and so we have the

IV.A.4. PROPOSITION. *The fractional ideals of F are precisely the finitely generated $\mathcal{O}_F$-submodules of F.*

(I'll discuss submodules at greater length later.)

The similarities between Defn. IV.A.1 ((iii) and (iv) in particular) and the definition of a monoid G acting on a set X,[1] suggest recasting the definition of module as a homomorphism of rings — just as we can recast the monoid action as a homomorphism of monoids $G \to \mathfrak{T}_X$ (where $\mathfrak{T}_X$ is the monoid of transformations). In the remainder of the section we work this out.

IV.A.5. DEFINITION. Given an abelian group $(M, +, 0)$, the set of **endomorphisms** $\text{End}(M)$ is the set of homomorphisms $\eta\colon M \to M$. (The defining properties are $\eta(x+y) = \eta(x) + \eta(y)$ and $\eta(0) = 0$, consequences of which include $\eta(-x) = -\eta(x)$, $\eta(nx) = n\eta(x)$, and the determination of η by its behavior on a generating set for M.)

IV.A.6. PROPOSITION. $\text{End}(M)$ *is a ring under addition and composition of endomorphisms.*

SKETCH. I'll summarize some key points:

- $1_{\text{End}(M)} = \text{id}_M$
- $0_{\text{End}(M)} =$ zero-map (sending everything to 0)
- $\text{End}(M)$ is closed under addition since

$$\begin{aligned}(\eta+\zeta)(x+y) &= \eta(x+y) + \zeta(x+y) \\ &= \eta(x) + \eta(y) + \zeta(x) + \zeta(y) \\ [M \text{ abelian } \implies] &= \eta(x) + \zeta(x) + \eta(y) + \zeta(y) \\ &= (\eta+\zeta)(x) + (\eta+\zeta)(y).\end{aligned}$$

[1]Same as Defn. II.F.1, with G only taken to be a monoid.

- Distributivity properties hold, e.g.

$$\begin{aligned}((\eta+\zeta)\rho)(x) &= (\eta+\zeta)(\rho(x)) = \eta(\rho(x)) + \zeta(\rho(x)) \\ &= (\eta\rho)(x) + (\zeta\rho)(x) = (\eta\rho+\zeta\rho)(x).\end{aligned} \qquad \square$$

What is the group of units $(\mathrm{End}(M))^*$? These are, naturally, the invertible endomorphisms — the automorphisms $\mathrm{Aut}(M)$. Note that this is a *subgroup of the multiplicative monoid* of $\mathrm{End}(M)$ and is *not* usually closed under addition.

IV.A.7. EXAMPLE. (i) Let $M = (\mathbb{Z}, +, 0)$. Then we have $\mathrm{End}(M) = (\mathbb{Z}, +, \bullet, 0, 1)$. Why? M is generated by 1, so any endomorphism is determined by where 1 is sent. Of course, $\mathrm{Aut}(M) = \{\pm 1\} \cong \mathbb{Z}_2$ (as a ring).

(ii) Let $M = (\mathbb{Z}_n, +, 0)$. Again (for the same reason) $\mathrm{End}(M) = (\mathbb{Z}_n, +, \bullet, 0, 1)$, but $\mathrm{Aut}(M) \cong \mathbb{Z}_n^*$.

(iii) Let $M = \mathbb{Z}^n$. I claim that $\mathrm{End}(M) \cong M_n(\mathbb{Z})$:

PROOF. Write $\mathbf{e}_1, \ldots, \mathbf{e}_n$ for the standard basis (column) vectors in $\mathbb{Z}^n$. We define $\phi\colon \mathrm{End}(\mathbb{Z}^n) \to M_n(\mathbb{Z})$ by $\phi(\mu) := (\mu(\mathbf{e}_1) \mid \cdots \mid \mu(\mathbf{e}_n))$, so $\phi(\mathrm{id}_{\mathbb{Z}^n}) = \mathbb{1}_n$ and $\phi(0) = \mathbf{0}_n$; ϕ clearly respects "$+$". As for "$\bullet$": for any $\mu \in \mathrm{End}(\mathbb{Z}^n)$ and $v \in \mathbb{Z}^n$, matrix-vector multiplication yields

$$\begin{aligned}\phi(\mu)v = (\mu(\mathbf{e}_1) \mid \cdots \mid \mu(\mathbf{e}_n)) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} &= \sum_{i=1}^{n} v_i \mu(\mathbf{e}_i) = \mu\left(\textstyle\sum_{i=1}^n v_i \mathbf{e}_i\right) \\ &= \mu(v).\end{aligned}$$

So for $\eta, \zeta \in \mathrm{End}(\mathbb{Z}^n)$, we have $\phi(\eta)\zeta(\mathbf{e}_i) = \eta\zeta(\mathbf{e}_i)$ hence

$$\begin{aligned}\phi(\eta\zeta) = (\eta\zeta(\mathbf{e}_1) \mid \cdots \mid \eta\zeta(\mathbf{e}_n)) &= \phi(\eta) \cdot (\zeta(\mathbf{e}_1) \mid \cdots \mid \zeta(\mathbf{e}_n)) \\ &= \phi(\eta) \cdot \phi(\zeta),\end{aligned}$$

where the dot is matrix multiplication. Injectivity and surjectivity are clear, since the $\{\mathbf{e}_i\}$ freely generate $\mathbb{Z}^n$. $\square$

One should compare the following to "Cayley for monoids":[2]

IV.A.8. THEOREM. *Any ring R is isomorphic to a ring of endomorphisms of an abelian group, i.e. to a subring of* $\mathrm{End}(M)$ *for some abelian group M.*

PROOF. Let $M = (R, +, 0)$, and denote by $\ell_r \colon \underset{m \longmapsto rm}{M \to M}$ the group homomorphism given by left-multiplication by an element $r \in R$. We obtain a homomorphism of *rings* by

$$\begin{aligned} \ell \colon R &\to \mathrm{End}(M) \\ r &\mapsto \ell_r \\ (\text{since} \quad rs &\mapsto \ell_{rs} = \ell_r \ell_s \\ \text{and} \;\; r+s &\mapsto \ell_{r+s} = \ell_r + \ell_s). \end{aligned}$$

We only need to show that $\ell(R) \cong R$, i.e. that ℓ presents R as a subring of $\mathrm{End}(R)$. That is, we must check injectivity. If $\ell_r = 0_{\mathrm{End}(M)}$, then $rm = 0$ ($\forall m \in M$) $\implies$ $r = r1 = 0$, done. □

If we try the same thing for *right* multiplication, we run into the problem

$$\mathfrak{r}_{rs}(m) = m(rs) = (mr)s = (\mathfrak{r}_r(m))s = \mathfrak{r}_s(\mathfrak{r}_r(m)) = (\mathfrak{r}_s \mathfrak{r}_r)(m).$$

IV.A.9. DEFINITION. The **opposite ring** of R is $(R, +, \bullet^{\mathrm{op}}, 0, 1) =: R^{\mathrm{op}}$, where $r \cdot^{\mathrm{op}} s := sr$.

So $\mathfrak{r}$ gives a homomorphism $\mathfrak{r} \colon R^{\mathrm{op}} \to \mathrm{End}(M)$, where M continues to denote the abelian group $(R, +, 0)$. We can write (with **[Jacobson]**)

$$R_{\mathfrak{r}} := \mathrm{im}(\mathfrak{r}) \subseteq \mathrm{End}(M)\,, \quad R_{\ell} := \mathrm{im}(\ell) \subseteq \mathrm{End}(M).$$

Recalling that $C_A(B)$ denotes the centralizer of B in A, we have

IV.A.10. PROPOSITION. $R_{\mathfrak{r}} = C_{\mathrm{End}(M)}(R_\ell)$, *and* $R_\ell = C_{\mathrm{End}(M)}(R_{\mathfrak{r}})$.

[2] i.e. the statement that every monoid G is a submonoid of a monoid of transformations of a set (in particular, G itself).

PROOF. $\ell_r \mathfrak{r}_s = \mathfrak{r}_s \ell_r$ is clear, so $R_{\mathfrak{r}} \subset C_{\mathrm{End}(M)}(R_\ell)$ etc. Conversely, suppose $\eta \in \mathrm{End}(M)$ is such that $\eta \ell_r = \ell_r \eta$ for every $r \in R$. Then

$$\eta(m) = \eta(m1) = \eta(\ell_m(1)) = \ell_m(\eta(1)) = m \cdot \eta(1) = \mathfrak{r}_{\eta(1)}(m) \quad (\forall m)$$

$\implies \eta = \mathfrak{r}_{\eta(1)} \in R_{\mathfrak{r}}$. (Note that $\eta(1)$ need not be 1 since η is merely a homomorphism of abelian groups.) $\square$

The basis of the discussion above is viewing R as left and right R-module. If we instead let M be an arbitrary left R-module, we see that

$$\begin{aligned} \mathfrak{L}\colon R &\longrightarrow \mathrm{End}(M) \\ r &\longmapsto \{m \mapsto rm\} \end{aligned}$$

yields a ring homomorphism. Conversely, given a ring homomorphism

$$\theta\colon R \to \mathrm{End}(M),$$

with M an abelian group, one verifies IV.A.1(i)-(iv) as follows:

- θ lands in $\mathrm{End}(M) \implies$ (i): $r(m+m') = rm + rm'$;
- θ sends $r+s$ to $\theta(r)+\theta(s) \implies$ (ii): $(r+s)m = rm + sm$;
- θ sends rs to $\theta(r)\circ\theta(s) \implies$ (iii): $(rs)m = r(sm)$; and
- θ sends 1_R to $1_{\mathrm{End}(M)} \implies$ (iv): $1_R m = m$.

Similarly, if M is a right R-module, then

$$\begin{aligned} \mathfrak{R}\colon R^{\mathrm{op}} &\longrightarrow \mathrm{End}(M) \\ r &\longmapsto \{m \mapsto mr\} \end{aligned}$$

produces a ring homomorphism; and the converse is left to the reader. This proves the

IV.A.11. THEOREM. *Let R be a ring, M an abelian group. A left R-module structure on M is equivalent to a ring homomorphism $R \to$ $\mathrm{End}(M)$. A right R-module structure on M is equivalent to a ring homomorphism $R^{op} \to \mathrm{End}(M)$.*

From this point of view, the two notions are "the same" for a commutative ring R because $R = R^{\mathrm{op}}$.

For representations of G (cf. IV.A.2(g)), the homomorphism in IV.A.11 takes the specific form of a ring homomorphism

$$\mathbb{F}[G] \longrightarrow \mathrm{End}_{\mathbb{F}}(V)$$

which is induced by linearizing a group homomorphism

$$G \to \mathrm{Aut}_{\mathbb{F}}(V).$$

The right-hand sides here denote $\mathbb{F}$-*linear* endo/auto-morphisms; this constraint on the $\mathbb{F}[G]$-module structure/G-action comes from the assumption that $g.(fv) = f(g.v)$ in IV.A.2(g). If V is finite (say, n) dimensional, then $\mathrm{Aut}_{\mathbb{F}}(V) \cong \mathrm{GL}(n, \mathbb{F})$.