Module Theory

Anamitro Biswas

September 6, 2024

Before we begin

I am a big fan of category theoretic notation, and hence abhor a mosaic of concrete examples in the text beyond the point of clarification of the abstract ideas presented thereof. So, I have tried to make the first part of the text clean of specific known cases, except for the purpose of citing them as counterexamples. And if the reader is familiar with one or two basic examples to begin with, this, I think, will rather help him/her imagine around the abstract pillar of clouds rather than restrciting them to the dimensions of an iron pillar.

Amples examples are provided later: those that in themselves prove to be interesting enough to be worth studying.

Same goes with rigour. Ramakrishna Paramahamsa, a spiritual mystic of Bengal, was of the opinion that the *thorn of knowledge* should act as a tool to surgically remove the *thorn of ignorance*; and then both should be discarded altogether, just in the same way we do not carry along surgical instruments after we are cured. Same goes for mathematical *rigour*. It is acceptable only to the extent it does not undermine the learner's imagination, only to the purpose it helps to present a clearer idea or convince something otherwise unbelievable. So, I have kept it concise and free of such irritating rigour. However, if need be, that can be step-by-step worked out pretty much without any external help by a reader who is informed with standard undergraduate abstract algebra, and just follows the text clearly.

1 Group action

Let A be any set and G a group written here in a multiplicative way. We define a *group action* as a function $G \times A \to A;\ (g, a) \mapsto g.a \in A$ such that

(i) $g_1.\left(g_2.a\right) = \left(g_1 g_2\right).a$ for all $g_1, g_2 \in G$ and all $a \in A$;

(ii) $1_G.a = a$ for all $a \in A$.

We informally say that the group G "acts on" the set A; $G \curvearrowright A$.

For some $g \in G$, define $\sigma_g : A \to A;\ \sigma_g(A) = g.a$. Then, $\sigma_g \in S_A$, i.e., σ_g is essentially a permutation of A. This is because, we can similarly have a $\sigma_{g^{-1}}$ that acts as both left and right inverse of σ_g, making σ_g a bijective map. Indeed, $\left(\sigma_{g^{-1}} \circ \sigma_g\right)(a) = g^{-1}.(g.a) = \left(g^{-1}g\right).a = a$. Also, $\varphi : G \to S_A;\ g \mapsto \sigma_g$ is a homomorphism, i.e., $\varphi\left(g_1 g_2\right)(a) = \sigma_{g_1 g_2}(a) = \left(g_1 g_2\right).a = g_1.\left(g_2.a\right) = \sigma_{g_1}\left(\sigma_{g_2}(a)\right) = \varphi\left(g_1\right) \circ \varphi\left(g_2\right)(a)$.

2 Ring Module

A *module* M over a ring R is an action of R on M in the multiplicative way, subject to the following conditions:

(i) $(r+s)\,m = rm + sm$;

(ii) $(rs)\,m = r(sm)$;

(iii) $r\,(m+n) = rm + rn$;

(iv) if $1 \in R$, $1m = m$ (in this case, the module is said to be *unital*)

for all $r, s \in R$ and all $m, n \in M$. It follows that $(-r)m = -rm$ and $0m = 0$. A *submodule* is a subset that is a module in itself, and it's trivial that an equivalent condition is that $\phi \neq N \subseteq M$ is a submodule if and only if $x, y \in N \Rightarrow x + \alpha y \in N$ for all $\alpha \in R$.

2.1 Module homomorphism

A *module homomorphism* $\varphi : M \to N$ where M and N are modules over a ring R is a mapping that keeps the module structure of $\varphi(M)$ intact, i.e.,

(i) $\varphi\left(m_1 + m_2\right) = \varphi\left(m_1\right) + \varphi\left(m_2\right)$ for all $m_1, m_2 \in M$;

(ii) $\varphi(rm) = r\varphi(m)$ where $r \in R$ and $m \in M, \varphi(m) \in N$.

This can alternatively stated that $\varphi\left(m_1 + rm_2\right) = \varphi\left(m_1\right) + r\varphi\left(m_2\right)$ for all $m_1, m_2 \in M$ and all $r \in R$. The *kernel* $\ker\varphi = \{m \in M \mid \varphi(m) = 0 \in N\}$ and *image* $\varphi(M) = \{n \in N \mid \exists\, m \in M \ni n = \varphi(m)\}$ are submodules of M and N respectively. An *isomorphism* $\varphi : M \cong N$ is a homomorphism which is bijective. The set of homomorphisms from a module M to a module N is denoted by $\mathrm{Hom}_R(M, N)$. For $\varphi, \psi \in \mathrm{Hom}_R(M, N)$, we define $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$ for all $m \in M$. $\mathrm{Hom}_R(M, N)$ is an abelian group with this addition. Further, if the acting ring R is commutative, we can establish $\mathrm{Hom}_R(M, N)$ as an R-module. If we let $(r\varphi)(m) = r(\varphi(m))$ for $r \in R, m \in M$, we have, for $s \in R$, $(r\varphi)(\beta m) = r(\varphi(\beta m)) = r(\beta\varphi(m)) = \beta(r\varphi)(m)$ since M is an R-module and φ is a module homomorphism. Now, if $\varphi_1 \in \mathrm{Hom}_R(L, M)$ and $\varphi_2 \in \mathrm{Hom}_R(M, N)$, we have the $\varphi_2 \circ \varphi_1 \in \mathrm{Hom}_R(L, N)$. With all these, in a special case, $\mathrm{Hom}_R(M, M)$ is a ring with multiplicative identity $I : m \mapsto m\ \forall\, m \in M$. This ring is called the *ring of endomorphisms* of M over R, denoted by $\mathrm{End}_R(M)$.

We have the natural map $f : R \to \mathrm{End}_R(M);\ r \mapsto rI$, which is not always an injective map. There might be zero divisors in the ring. But no unit belongs to $\ker f$ for sure. Otherwise, take for example, $M = \mathbb{Z}/7\mathbb{Z}, R = \mathbb{Z}$. Then $7m = 0$ for all $m \in M$. But if R is a field, this map is injective and we call $\mathrm{Im}\, f$ (the isomorphic copy of R) as the subring of scalar transformations in $\mathrm{End}_R(M)$.

Now, a module is an abelian group with some extra condition imposed with respect to a ring R. $\mathbb{Z}$ being the most primitive model of a ring (except the fact that it is an integral domain; well, the most primitive example of an integral domain), $\mathbb{Z}$-modules are just those abelian groups with no other extra condition. Thus module homomorphisms are necessarily group homomorphisms but the reverse need not be true. Also, if the underlying ring is $\mathbb{Z}$, the module homomorphisms are just the homomorphisms between abelian groups.

2.2 Quotient module

Let N be a submodule of M. As abelian groups N is a normal subgroup, and we try to impose a module structure, naturally, on the quotient group M/N by defining for $r \in R$, $r(m+N) := rm + N$. This is well-defined since if $m_1 + N = m_2 + N$, then $m_1 - m_2 \in N \Rightarrow r\left(m_1 - m_2\right) \in N \Rightarrow r\left(m_1 + N\right) = r\left(m_2 + N\right)$. In fact $\pi : M \to M/N$ is a module homomorphism, since it is a homomorphism of abelian groups anyway, and $r\pi(m) = r(m+N) = rm + N = \pi(rm)$. Futher, the kernel of the module homomorphism is the same as the kernel of the group homomorphism over the same sets with the same group operation, so $\ker \pi = N$.

2.3 Annihilator

If we have an ideal I of R such that $rm = 0$ for all $r \in I$ and $m \in M$, then I is called an *annihilator* of M. In that case we can visualize M as a ring module over the quotient ring R/I where $(r+I).m := rm$ where $r \in R$, $m \in M$. In particular, if I is maximal, then R/I is a field and hence M shall be a vector space.

Take for example a $\mathbb{Z}$-module G. This means that for some element x in the module, $nx \in G$. Thus G consists of distinct cycles of finite or infinite length and so is an abelian group. On the other hand, any abelian group is a $\mathbb{Z}$-module. Now, if there exists some $m \in \mathbb{N}$ such that $mx = 0$ for all $m \in G$, then $m\mathbb{Z}$ is an annihilator of G. Even otherwise, simply G is a $\mathbb{Z}/m\mathbb{Z}$-module. In particular for $m = p \in \mathbb{P}$ a prime, $\mathbb{Z}/m\mathbb{Z}$ has the structure of $\mathbb{F}_p$ and so G is a vector space over $\mathbb{F}_p$.

We shall denote by $\operatorname{Ann}_M(I)$ the annihilator of right ideal I of R in module M as $\operatorname{Ann}_M(I) := \{m \in M \mid am = 0 \,\forall\; a \in I\}$. One can see that $\operatorname{Ann}_M(I)$ is a submodule of M, because if $m_1, m_2 \in \operatorname{Ann}_M(I)$, then $m_1 + \alpha m_2 \in \operatorname{Ann}_M(I)$ for all $\alpha \in R$.

On the other hand, for a submodule N of M, the *annihilator* of N in R consists of those $r \in R$ for which $rn = 0$ for all $n \in N$, denoted by $\operatorname{Ann}_R(N)$. One can see that this is a two-sided ideal of R as it absorbs any other element r_1 of R this way: $r_1 rn = r_1 0 = 0$, or $rr_1 n = rn_1$ for some $n_1 \in N$ and $rn_1 = 0$ for $r \in \operatorname{Ann}_R(N)$. The annihilator of a submodule of M is contained in M, and might be a proper subset as well, e.g.,

2.4 Field

If the ring is actually a field (i.e., commutative and without any zero divisors), then the module is essentially a vector space over the field. For commutaive rings a right module is also a left module. Now, if V is a vector space over a field F, then V is also a module over the polynomial ring $F[x]$. We can assign a linear operator (field-module homomorphism) $T : V \to V$ and with respect to that define for $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$,

$$p(x).v = a_n T^n v + a_{n-1} T^{n-1} v + \ldots a_1 T v + a_0 v$$

which is consistent with its restriction on F, where $v \mapsto a_0 v$. Note that this extended action depends upon the linear operator T chosen. If T is identically 0, we have the same module structure with no more information about the elements other than those of F. On the other hand, if T is the shift operator, $\left(v_1, \ldots, v_r\right) \mapsto \left(v_2, v_3, \ldots, v_r, 0\right)$, we get a different $F[x]$-module structure of V.

Thus, essentially we arrive at a bijection

$$\left\{\begin{array}{r} \text{a module structure of} \\ V \text{ over } F[x] \end{array}\right\} \longleftrightarrow \left\{\begin{array}{r} \text{a vector space } V \text{ over } F \\ \text{and a linear operator } T : V \to V \end{array}\right\}$$

Now we call a subspace W of V, *T-invariant* or *T-stable* for a linear operator $T : V \to V$ if $T(W) \subseteq W$. Thus, for W to be a submodule of V with respect to $F[x]$ we need, necessarily and sufficiently, W to be *T-stable* in V, because for W to be T-stable means W to be T^k-stable for $k \in \mathbb{N}$ and closed with respect to sums as a module (abelian group). An example might be the shift operator mentioned earlier, where $T^k e_i = \begin{cases} e^{i-k} \text{ if } k < i; \\ 0 \text{ else.} \end{cases}$ for $e_i = \underbrace{(0, 0, \ldots, 0, 1, 0, \ldots, 0)}_{r}$ with 1 in the i^{th} position. Thus if $W = \left\{\left(v_1, \ldots, v_t, 0, \ldots 0\right)\right\}$ be a t-dimensional subspace of V, then $T^k \left(v_1, \ldots, v_\ell, 0, \ldots, 0\right) \in W$ for all $\ell \leq t$ and so W is T-stable, i.e., submodule.