Abstract Algebra. Math 6310. Bertram/Utah 2022-23.

Modules

Let R be a commutative ring with 1.

Definition. An R-*module* is an abelian group $(M,+)$ with a multiplication map:

$$\cdot : R \times M \to M$$

that satisfies the following properties:

(i) Multiplication by $a \in R$ is an abelian group homomorphism:

$$a(m_1 + m_2) = am_1 + am_2 \text{ and } a \cdot 0 = 0$$

(ii) Multiplication associates and distributes with the ring operations:

$$a_1(a_2m) = (a_1a_2)m \text{ and } (a_1 + a_2)m = a_1m + a_2m$$

(iii) Ring identities act as identities:

$$1 \cdot m = m, \ 0 \cdot m = 0$$

Definition. A map $f : M \to N$ of R-modules is an R-*module homomorphism* if:

(i) f is a homomorphism of the underlying abelian groups, and:

(ii) $f(am) = af(m)$ for all $a \in R$ and $m \in M$.

Examples. (a) Vector spaces over a field k.

(b) All abelian groups are $\mathbb{Z}$-modules with repeated addition as multiplication.

(c) The product abelian group $R^n = Re_1 \oplus \cdots \oplus Re_n$ with scalar multiplication. These are the *free* R-modules.

(d) An ideal $I \subset R$ is an R-module.

(e) If $f : R \to S$ is a ring homomorphism, then S is an R-module where the multiplication is inherited from multiplication in the ring S.

Proposition 1. When R is viewed as an R-module, then the homomorphisms:

$$f : R \to R$$

are multiplication by $a = f(1)$. As a consequence, the R-module homomorphisms of free R-modules are given by multiplication by matrices with entries in R.

Proof. By definition (ii), $f(b) = f(b \cdot 1) = b \cdot f(1) = b \cdot a$ for all $b \in R$. The assembly of the matrix is exactly as in the case of vector spaces. $\square$

Definition. An R-*sub-module* of an R-module M is a subgroup $S \subset M$ that is also closed under multiplication by elements of R.

Example. (a) An ideal $I \subset R$ is a sub-module of R itself, thought of as an R-module.

(b) The kernel and image of an R-module homomorphism are sub-modules.

Proposition 2. Given a sub-R-module $S \subset M$, the quotient abelian group:

$$M/S = \{m + S \mid m \in M\}/\sim$$

is an R-module with product $a(m + S) = am + S$. This is the *quotient module*. Moreover, if $f : M \to N$ is an R-module homomorphism, then the map

$$\overline{f} : M/\ker(f) \to f(M) \text{ given by } \overline{f}(m + K) = f(m) \text{ is an isomorphism}$$

Remark. The *cokernel* f is the quotient module $q : N \to N/f(M)$.

Example. For the $\mathbb{Z}$-module homomorphsm $n : \mathbb{Z} \to \mathbb{Z}$, we have the modules: $\ker(n) = 0 \subset \mathbb{Z}, \mathrm{im}(n) = n\mathbb{Z} \subset \mathbb{Z}$ and $q = \mathrm{coker}(n) : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Remark. This is a first isomorphism theorem for R-modules, but since sub-modules and kernels are the same thing (unlike subrings and ideals), we are able construct the cokernel module. This will be systematized in the notion of an *abelian category.*

Definition. M is *finitely generated* if there is a surjective homomorphism:

$$f : R^n \to M, \text{ of } R\text{-modules, in which case } M = R^n/\ker(f) \text{ by Proposition 2.}$$

Remark. Recall that in the case of vector spaces, being finitely generated means having a finite spanning set of vectors. We learned in linear algebra that every spanning set of vectors has a subset that spans **and** are linearly independent. We call such a set a *basis* of V. The big difference between vector spaces and R-modules is the non-existence (in general) of bases in the latter case. Note that when a basis does exist, then by definition, the associated map:

$$f : R^n \to M \text{ is an isomorphism}$$

so R-modules with a basis are (isomorphic to) free R-modules, and the novel aspect of finitely generated R-modules is that they need not be free.

Definition. An element $t \in M$ of an R-module M is *torsion* if it is non-zero and:

$$at = 0 \text{ for some non-zero } a \in R$$

Remark. A torsion element in an R-module is analogous to a zero-divisor in R. In fact, it **is** a zero-divisor when $M = R$. Thus, a ring R is a domain if and only if it has no torsion elements as a module over itself. More broadly, the free modules D^n over a domain have no torsion elements, and neither do the submodules of free modules over a domain. It is important, however, to keep in mind that the ring R needs to be specified when trying to decide whether M has torsion elements or not.

Examples. (i) Every element of $\mathbb{Z}/n\mathbb{Z}$ is torsion when it is viewed as a $\mathbb{Z}$-module.

(ii) Every non-zero element of the field $\mathbb{Z}/p\mathbb{Z}$ is **not** torsion, when viewed as a module over itself, since with this interpretation, $\mathbb{Z}/p\mathbb{Z}$ is a domain.

(ii) Only the elements $2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}$ and $4 + 6\mathbb{Z}$ (and 0) are torsion when $\mathbb{Z}/6\mathbb{Z}$ is viewed as a module over itself. Note that this set is not closed under addition.

Proposition 3. If M is an R-module and R is a domain, then the set:

$$T = \{t \in M \mid t \text{ is a torsion element}\} \cup \{0\} \subset T$$

is a sub-module. It is called the *torsion submodule* of M.

Proof. Because a domain has no zero-divisors, we can conclude that:

$$a_1t_1 = 0 \text{ and } a_2t_2 = 0 \text{ implies } a_1a_2(t_1 + t_2) = 0 \text{ and } a_1, a_2 \neq 0 \text{ implies } a_1a_2 \neq 0$$

Thus a sum of torsion elements is torsion, and similarly the product of a torsion element by a (non-zero) element $a \in R$ is torsion. $\square$

We will assume R is a domain until otherwise indicated.

Definition. (a) An R-module $M = T$ of only torsion elements is a *torsion* module.

(b) An R-module with no torsion elements is *torsion-free.*

Proposition 4. (a) Any quotient T/S of a torsion module T is torsion.

(b) Any sub-module $S \subset F$ of a torsion-free module F is torsion-free.

(c) The quotient M/T of any module by its torsion sub-module is torsion-free.

Proof. (a) and (b) are easy to see. As for (c), consider:

$$a(m+T) = 0 + T \text{ implies that } am \in T$$

which implies that $m \in T$, so $m + T = 0 + T$. □

Remark. Thus in particular an R-module with non-zero torsion is not free, and not a sub-module of a free R-module (assuming always that R is a domain). We will see that when R is a PID, torsion is the only "obstruction" to freedom.

We turn now to finitely generated modules and the special role of Noetherianness. For this we may drop the assumption that R is a domain.

Proposition 5. If R is Noetherian and M is a finitely generated R-module, then:

(a) Every increasing chain $S_0 \subset S_1 \subset \cdots \subset M$ of sub-modules of M reaches its maximum $S_n = S_\infty (= \cup_{k=0}^{\infty} S_k)$.

(b) Every submodule of M is finitely generated.

Proof. Since submodules of R (viewed as an R-module) are exactly the ideals in R, this is a generalization of the definition of a Noetherian ring. The equivalence of (a) and (b) is exactly as in the case of ideals. Let $S_\bullet$ be a chain of submodules of M and consider the string of surjections of quotients:

$$Q_0 = M/S_0 \to Q_1 = M/S_1 \to \cdots$$

Then (a) holds if and only if every such string of surjections of quotients of M terminates; i.e. $Q_n = Q_{n+1} = \cdots = Q_\infty$ for some n. It follows immediately that if M has property (a) and $q : M \to N$ is a surjection, then N has property (a).

We have assumed M is finitely generated, i.e. there is a surjection $q : R^n \to M$ from some n. So it suffices to prove (a) for the free modules R^n. Now suppose:

$$K \subset M \text{ and } q : M \to M/K$$

and property (a) holds for both K and M/K. Then:

(i) The images $q(S_i)$ form an increasing chain of submodules of M/K, so:

$$q(S_d) = q(S_{d+1}) = \cdots = q(S_\infty) \text{ for some } d, \text{ and then}$$

(ii) $(S_d \cap K) \subset (S_{d+1} \cap K) \subset ...$ are an increasing chain of submodules of K, so

$$S_e \cap K = S_{e+1} \cap K = \cdots = S_\infty \cap K \text{ for some } e \geq d$$

Suppose $s \in S_\infty$. Then some $s_e \in S_e$ satisfies $q(s) = q(s_e)$ (since $e \geq d$), and then some $k_e \in S_e \cap K$ satisfies $k_e = s - s_e \in S_\infty \cap K$. So:

$$s = k_e + s_e \in S_e$$

and we have shown that $S_e = S_\infty$. We apply this to the inclusion of the first factor:

$$R \subset R^n \text{ and the projection } q : R^n \to R^n/R = R^{n-1}$$

onto the remaining factors to conclude that if R^{n-1} satisfies (a), then R^n does too. But then we're done by induction! □

Corollary. If R is Noetherian, then every finitely generated module M is *finitely presented*, i.e. there is a sequence of R-modules:

$$R^m \xrightarrow{f} R^n \xrightarrow{q} M \to 0$$

such that q is surjective, and the image of f is the kernel of q and therefore:

Every finitely presented R-module is (by definition) the cokernel of a matrix:

$$A = (a_{ij}) : R^m \to R^n;\ a_{ij} \in R$$

Notice that in the case of a Noetherian ring, we can repeat the generations:

$$R^n \to M \text{ is surjective, with kernel } M'$$
$$R^{n_1} \to M' \text{ is surjective, with kernel } M''$$
$$R^{n_2} \to M'' \text{ is surjective, with kernel } M'''$$
$$\text{etc}$$

and we can ask whether these modules "improve" in some measurable way with each successive iteration. We've already seen one instance of this, namely, the fact that M', M'',... are submodules of a free module, and therefore have no torsion.

Example. Let $k[x_0]$ be the polynomial ring, and consider:

$$\mathrm{ev}_0 : k[x_0] \to k \text{ the evaluation at } x_0 = 0$$

Then the kernel is the ideal module $x_0 k[x_0] \subset k[x_0]$, which is free (of rank one).

Next, consider the polynomial ring $k[x_0, x_1]$ in two variables, and:

$$\mathrm{ev}_{(0,0)} : k[x_0, x_1] \to k \text{ the evaluation at } (x_0, x_1) = (0, 0)$$

Then the kernel ideal is generated by x_0 and x_1, which is the image:

$$k[x_0, x_1]^2 \to k[x_0, x_1];\ A = (x_0, x_1)^T$$

and the kernel of **this** matrix is free, generated by:

$$k[x_0, x_1] \to k[x_0, x_1]^2;\ B = (-x_1, x_0)$$

In other words, every pair $f, g \in k[x_0, x_1]$ such that $x_0 f + x_1 g = 0$ satisfies:

$$f = -x_1 h \text{ and } g = x_0 h$$

for a polynomial h (this follows from the fact that $k[x_0, x_1]$ is a UFD!

These are the first two cases of the *Koszul complex* for the $k[x_0, ..., x_n]$-module k.