

1. PRELIMINARIES

Let R be a commutative ring. (This is the notion obtained by removing the multiplicative-inverse axiom in the definition of a field.) A *module* M over R is defined exactly like a vector space over a field except that we use R in the role of the field. (The lack of multiplicative inverses implies that if $rm = 0$ for some $m \in M$ and $r \in R$ then it need not happen that $r = 0$ or $m = 0$. Consider $R = \mathbf{Z}$ and M the integers modulo 10, with $r = 5$ and $m = 2 \pmod{10}$. The structure theory of modules over commutative rings is an enormous active branch of modern mathematics.) A slightly peculiar example of a ring is the *zero ring* 0 ; this is the only ring in which $0 = 1$ (since if $0 = 1$ in a commutative ring then for any element r we have $r = r \cdot 1 = r \cdot 0$ and this vanishes by the usual argument with axiomatics for addition and multiplication). When we consider $M = R$ as an R -module, it is understood that we do so by using multiplication and addition from the ring structure of R (just as we consider a field as a vector space over itself).

The notions of *R -linear map*, *direct sum* (of finitely many R -modules), *R -submodule*, and *quotient of an R -module by an R -submodule* are defined exactly as in the case of vector spaces over fields (though we no longer have bases, so matrices play no role in general and there is no concept of dimension!); direct sums and quotients have the same mapping properties as for vector spaces (with the same proofs). The aim of this handout is to explore the algebraic side of modules and derivations, to put in perspective some of our later considerations with vector bundles (especially the tangent bundle).

2. MODULES

An *ideal* J in R is an R -submodule of R (i.e., J is an additive subgroup of R and $am \in J$ for all $a \in R$ and $m \in J$).

Example 2.1. It is easy to check that $J = 10\mathbf{Z}$ is an ideal inside of $R = \mathbf{Z}$. For the local ring \mathcal{O}_x at a point x on a C^p premanifold with corners (X, \mathcal{O}) , the kernel \mathfrak{m}_x of the evaluation map $e_x : \mathcal{O}_x \rightarrow \mathbf{R}$ is an ideal.

If M is an R -module and J is an ideal in R , we define $JM \subseteq M$ to be the set of finite sums $\sum r_i m_i$ with $m_i \in M$ and $r_i \in J$. This is *not* the set of multiples rm with $r \in J$ and $m \in M$, as this set is usually not preserved under addition. For example, if $R = \mathbf{R}[x, y]$, $M = R \oplus R$, and J is the set of polynomials with vanishing constant term, then J is an ideal in R (check!) and the set of multiples $rm \in M$ with $r \in J$ and $m \in M$ contains elements such as $(x, 0), (0, y) \in M$, but their sum $(x, 0) + (0, y) = x \cdot (1, 0) + y \cdot (0, 1)$ is *not* of the form rm with $r \in J$ and $m \in M$. Indeed, if $m = (f, g)$ then $rm = (rf, rg)$ and hence we would have $rf = x$ and $rg = y$ for some polynomials $r, f, g \in \mathbf{R}[x, y]$ with $r(0) = 0$. But consideration of least-degree terms in r, f , and g readily gives a contradiction.

Lemma 2.2. *For an ideal J in R , JM is an R -submodule of M . Moreover, R/J admits a natural structure of commutative ring making $R \rightarrow R/J$ a ring homomorphism, and M/JM is thereby naturally a module over R/J .*

Proof. The stability of $JM \subseteq M$ under addition follows from the definition of JM as a collection of certain finite sums, and for $r \in R$ and $\sum r_i m_i \in JM$ with $r_i \in J$ and $m_i \in M$ we have $r \cdot (\sum r_i m_i) = \sum (rr_i) m_i$ with $rr_i \in J$ because J is an ideal of R .

We make R/J into a ring by using addition and multiplication of representatives. This must be proved to be well-defined (and then the ring axioms are inherited from R). The case of addition goes exactly as in the case of quotient vector spaces, and for multiplication we have to check that

if $r, r' \in R$ and $x, x' \in J$ then $(r+x)(r'+x') - rr' \in J$. This difference is $rx' + xr' + xx'$, with each term in J since $x, x' \in J$ and J is an ideal. We make M/JM an R/J -module by using the R -module structure on representatives, and the well-definedness goes in the same way as for the ring structure on R/J . ■

We now apply the notion of quotient M/JM of a R -module M modulo an ideal J of R in order to show how linear algebra is a helpful device in the study of modules over general commutative rings. A nonzero module M over R is *finite free of rank $n > 0$* over R if there exists a finite R -basis of size n ; that is, elements $m_1, \dots, m_n \in M$ such that every $m \in M$ has a unique expression $m = \sum r_i m_i$ with $r_i \in R$. It is a fact of life (that makes commutative algebra interesting) that most modules are *not* free:

Example 2.3. Let $R = \mathbf{R}[x, y]$ and J be the ideal of polynomials with vanishing constant term. This is “finitely generated” in the sense that $x, y \in J$ and J is the set of R -linear combinations of x and y : each $r \in J$ has the form $fx + gy$ for $f, g \in R$ (such f, g are rather non-unique; for example, $xy + yx^2 - y = (y + yx)x + (-1)y = (y)x + (x^2 - 1)y$ and so on). But it can be proved with a tiny bit of knowledge of commutative algebra (or by hand, if you try) that J does not have an R -basis.

There are some very important theorems that provide criteria to ensure that certain kinds of nonzero modules do have R -bases, and such freeness results are extremely powerful. A natural question on the theme of modules with R -bases is this: if a nonzero M has R -bases with sizes n and n' , does n necessarily equal n' ? We now show how to give an affirmative answer by reducing the question to the known case when R is a field (i.e., the theory of dimension in linear algebra)!

Lemma 2.4. *If M is a nonzero R -module that is finite free of rank $n > 0$ over R then M/JM is finite free of rank n over R/J for every ideal $J \subseteq R$ with $J \neq R$.*

Proof. Assume that M is R -free with a basis of m_i 's. Let $\bar{m}_i \in M/JM$ be the image of m_i , so we need to prove that there are an R/J -basis of M/JM . Each element $\bar{m} \in M/JM$ is the image of some $m \in M$, so $m = \sum a_i m_i$ and hence (by the definition of the R/J -module structure on M/JM) we have $\bar{m} = \sum \bar{a}_i \bar{m}_i$ with $\bar{a}_i \in R/J$ the image of a_i . This gives the spanning property, and for uniqueness we must prove that if $\bar{a}_i \in R/J$ with $\sum \bar{a}_i \bar{m}_i = 0$ in M/JM then $\bar{a}_i = 0$ for all i . If we pick $a_i \in R$ lifting \bar{a}_i , then the vanishing hypothesis says $\sum a_i m_i \in JM$. Thus, by the *basis* property of the m_i 's, to infer $a_i \in J$ for all i (and hence $\bar{a}_i = 0$ in R/J for all i) we just need to prove that every element of JM has its unique basis expansion $\sum b_i m_i$ with all $b_i \in J$. By definition, elements of JM as finite sums $\sum r_k \mu_k$ with $r_k \in J$ and $\mu_k \in M$. Writing $\mu_k = \sum c_{ik} m_i$ with $c_{ik} \in R$, we get $\sum_k r_k \mu_k = \sum_i (\sum_k c_{ik} r_k) m_i$, and $\sum_k c_{ik} r_k \in J$ for all i because $r_k \in J$ for all k and J is an ideal. This completes the proof that M/JM is R -free on the set of \bar{m}_i 's. ■

Now we suppose M is R -free and nonzero with ranks n and n' , and we want to prove that necessarily $n = n'$. Suppose for a moment that there exists an ideal J in R such that R/J is a field. (e.g., $R = \mathcal{O}_x$ and $J = \mathfrak{m}_x$, with $R/J \simeq \mathbf{R}$ for a C^p premanifold (X, \mathcal{O}) and a point $x \in X$). Thus, M/JM is a vector space over this field, so it a well-defined notion of dimension, which is to say that all of its bases have the same size. The preceding lemma shows that there are bases of sizes n and n' , so indeed $n = n'$. But why does such an ideal J exist?

The cases of relevance to us are local rings $R = \mathcal{O}_x$ at points on premanifolds with corners, so there is no problem there (take $J = \mathfrak{m}_x$). For most rings that arise “in nature” it turns out to not be too difficult to prove the existence of such so-called “maximal ideals” (the rings I have in mind are noetherian rings, for which there is a very well-developed theory). By using Zorn’s Lemma, one can prove by the magic of far-out logic that such an ideal J exists in any nonzero ring R . But if M is a nonzero module over a ring R then R has to be nonzero (since if $0 = 1$ in R then for all $m \in M$

we have $m = 1 \cdot m = 0 \cdot m$ and this vanishes by the usual axiomatics as in the case of vector spaces over a field). Hence, we are done.

3. DERIVATIONS OVER A RING

A *derivation* from R into an R -module M is an additive mapping $D : R \rightarrow M$ that satisfies $D(rr') = rD(r) + r'D(r')$ for all $r, r' \in R$.

Lemma 3.1. *For any derivation $D : R \rightarrow M$ to an R -module, $D(1) = 0$ and if $D, D' : R \rightarrow M$ are two derivations then so is $aD + a'D' : R \rightarrow M$ for any $a, a' \in R$.*

Proof. Since $D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = D(1) + D(1)$ in M , we have $D(1) = 0$. It is a trivial calculation to check that R -linear combinations of derivations are derivations. ■

Example 3.2. Taking $M = R$ and $R = \mathbf{R}[x_1, \dots, x_n]$, the standard partials $\partial_{x_j} : R \rightarrow R$ are \mathbf{R} -linear derivations. This amounts to the Leibnitz rule. Thus, for any $f_j \in \mathbf{R}[x_1, \dots, x_n]$, the operator $D = \sum f_j \partial_{x_j}$ carrying h to $\sum f_j (\partial h / \partial x_j)$ is an \mathbf{R} -linear derivation (and such f_j 's are uniquely determined: $D(x_j) = f_j$ for all j). Somewhat more amusingly, this gives *all* \mathbf{R} -linear derivations of $\mathbf{R}[x_1, \dots, x_n]$ viewed as an $\mathbf{R}[x_1, \dots, x_n]$ in the natural way. More specifically, if D is an \mathbf{R} -linear self-derivation of $\mathbf{R}[x_1, \dots, x_n]$, then we claim $D - \sum D(x_j) \partial_{x_j} = 0$.

Let ∂ denote this difference, so it is an \mathbf{R} -linear self-derivation. Since ∂ is \mathbf{R} -linear we have $\partial(c) = \partial(c \cdot 1) = c \cdot \partial(1) = 0$ for all $c \in \mathbf{R}$. Also, by construction $\partial(x_j) = 0$ for all j . Thus, by \mathbf{R} -linearity, ∂ kills all polynomials with top degree at most 1. Now we argue by induction to show it kills all polynomials f with top degree at most n for $n \geq 2$. By expressing f as an \mathbf{R} -linear combination of monomials, it suffices to prove that the \mathbf{R} -linear ∂ kills all monomials with degree at most n . Any such monomial has the form $x_i h$ with h of degree at most $n - 1$, and

$$\partial(x_i h) = h \partial(x_i) + x_i \partial(h) = x_i \partial(h)$$

since $\partial(x_i) = 0$. But by induction $\partial(h) = 0$. Hence, we conclude $\partial = 0$. This establishes the desired expression for D .

Theorem 3.3. *If $D, D' : R \rightarrow M$ are two derivations, the Lie bracket $[D, D'] \stackrel{\text{def}}{=} D \circ D' - D' \circ D$ is also a derivation of R into M , and the (cyclic) Jacobi identity*

$$[D, [D', D'']] + [D', [D'', D]] + [D'', [D, D']] = 0$$

holds for any three derivations from R into M . Moreover,

$$[rD, r'D'] = rr'[D, D'] + rD(r')D' - r'D'(r)D$$

for all $r, r' \in R$.

Proof. The additivity of $[D, D']$ is clear, and for the Leibnitz identity we just compute:

$$[D, D'](rr') = D(D'(rr')) - D'D(rr') = D(rD'(r') + r'D'(r)) - D'(rD(r') + r'D(r)),$$

and this is

$$D(r)D'(r') + rDD'(r') + D(r')D'(r)r'DD'(r) - D'(r)D(r') + rD'D(r') + D'(r')D(r) + r'D'D(r).$$

Cancellation leaves us with $r[D, D'](r') + r'[D, D'](r)$. The Jacobi identity is a direct calculation with the associative law and cancellations (no need to even evaluate on specific elements), and the proposed formula for $[rD, r'D']$ is given by evaluation of both sides on an arbitrary $r'' \in R$. ■