

LECTURE 2 : FREE MODULES

In the next few lectures we will establish basic properties of the modules which form the building blocks of homological algebra. These are : free modules, projective modules and injective modules. Roughly speaking, modules are to rings as vector spaces are to fields. You'll recall, that over a field K , all modules (vector spaces) are essentially the same – they are (up to isomorphism) simply a direct sum of (possibly infinitely many) copies of K . This is an immediate consequence of the fact that any vector space has a basis. Of course, this no longer holds over rings which may not be fields. From an algebraic view, one may regard homological algebra as an attempt to do linear algebra over rings more complicated than fields, and to a large degree, the objects studied are the obstructions encountered in an attempt to imitate classical linear algebra.

For the time being, R will denote an associative ring with identity and all modules will be unitary left R -modules. In the next several lectures, nothing we do will require that the ring be commutative. Consequently we will hold out for maximum generality until no longer possible (or bearable). However, if you are uncomfortable with modules over a non-commutative ring or have little background in algebra, feel free to assume that the underlying ring is commutative.

A few words about the non-commutative situation. Everything we do will work just as well for unitary right R -modules, but we will refrain from mentioning the “right” analogue of every “left” theorem given. However, just because every left theorem has a right analogue does not mean that a particular module which may be both a left and right R -module satisfies the same properties on the left as it does on the right.

Examples 2.1. (i) Suppose that R is a field and M is a vector space over R . Then M is an abelian group and there exists a map (scalar multiplication) $\phi : R \times M \rightarrow M$ satisfying the following properties :

- (a) $\phi(\lambda, m_1 + m_2) = \phi(\lambda, m_1) + \phi(\lambda, m_2)$, for all $\lambda \in R$ and $m_1, m_2 \in M$. In other words, $\lambda(m_1 + m_2) = \lambda m_1 + \lambda m_2$.
- (b) $\phi(\lambda_1 + \lambda_2, m) = \phi(\lambda_1, m) + \phi(\lambda_2, m)$, for all $\lambda_1, \lambda_2 \in R$ and $m \in M$. In other words, $(\lambda_1 + \lambda_2)m = \lambda_1 m + \lambda_2 m$.
- (c) $\phi(\lambda, \phi(\gamma, m)) = \phi(\lambda\gamma, m)$, for all $\lambda, \gamma \in R$ and $m \in M$. I.e., $\lambda(\gamma m) = (\lambda\gamma)m$.

LECTURE 2

(d) $\phi(1, m) = m$, for all $m \in M$. I.e., $1 \cdot m = m$.

Notice that there is no reference to any field property in the definition above. The only thing required is that R be a ring with identity. Hence, the foregoing is precisely the definition for M to be an R -module.

(ii) If R is a division ring, i.e., every element has a multiplicative inverse, then modules are called vector spaces, since any module has a basis. The proof of this fact is *exactly* the same as for fields. The crucial point in each case is the following : A set of vectors is linearly dependent if and only if one of them is in the span of the remaining ones. This is precisely where the property of divisibility in division rings (or fields) comes in.

(iii) If $R \subseteq S$ are rings, then S may be regarded as an R -module. In particular, any ring may be regarded as a module over itself.

(iv) If $\{M_\alpha\}$ is any collection of R -modules, then $\bigoplus M_\alpha$ and $\prod M_\alpha$ are R -modules in a natural way.

(v) If R is commutative and M and N are R -modules, then $\text{Hom}_R(M, N)$, the set of R -module homomorphisms from M to N , is an R -module.

Homomorphisms. If R is a field and M and N are vector spaces, then a map $\phi : M \rightarrow N$ is a vector space homomorphism (“linear transformation”) if the following conditions hold

- (i) $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$, for all $m_1, m_2 \in M$.
- (ii) $\phi(\lambda m) = \lambda \phi(m)$, for all $\lambda \in R$ and $m \in M$.

For general R , a map $\phi : M \rightarrow N$ is an R -module homomorphism, if it satisfies exactly the same two conditions.

Submodules and Quotients. If R is a field, M a vector space over R , then a subset $N \subseteq M$ is a subspace if it is closed under addition and scalar multiplication. Exactly the same conditions for general R yield that N is a *submodule* of M . Just as for vector spaces, the set of (left) cosets M/N forms an R -module in a natural way : Addition is the same as for abelian groups and scalar multiplication is the obvious $r \cdot (m + N) = r \cdot m + N$.

If $\phi : M \rightarrow N$ is an R -module homomorphism, then $\ker(\phi)$ and $\text{im}(\phi)$ are submodules of M and N respectively. A sequence $L \xrightarrow{\psi} M \xrightarrow{\phi} N$ of R -modules and R -module homomorphisms

FREE MODULES

is said to be *exact* if $\text{im}(\psi) = \text{ker}(\phi)$. A *short exact sequence* is a sequence

$$0 \rightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N \rightarrow 0$$

exact at each term. Thus, ψ is one-to-one, $\text{im}(\psi) = \text{ker}(\phi)$ and ϕ is onto.

Isomorphism Theorems. The standard isomorphism theorems hold for modules. Let $\phi : M \rightarrow N$ be an R module homomorphism and let $L \subseteq K \subseteq M$ be submodules. Then

- (i) $M/\text{ker}(\phi) \cong \text{im}(\phi)$. In particular, if ϕ is onto, then $M/\text{ker}(\phi) \cong N$.
- (ii) K/L is a submodule of M/L and $(M/L)/(K/L) \cong M/K$.
- (iii) $A + B/B$ is canonically isomorphic to $A/A \cap B$ for all submodules $A, B \subseteq M$.

The proofs of the results concerning submodules, quotients and homomorphisms are exactly the same as the proofs of the corresponding results for vector spaces. The results are all formal consequences of the definition. Thus, in some regards, modules over a ring behave like vector spaces over a field. That every vector space has a basis is *not* a formal consequence of the definition, but rather a property of the underlying ring. Free modules are precisely those R -modules admitting a basis.

Definition 2.2. Let M be an R -module. A subset $X \subseteq M$ is said to be a *basis* for M if every element of M can be written uniquely as a finite linear combination of elements from X . Equivalently, the following two conditions must hold :

- (i) Given $m \in M$, there exist $\lambda_1, \dots, \lambda_n \in R$ and $x_1, \dots, x_n \in X$ such that $m = \lambda_1 x_1 + \dots + \lambda_n x_n$. In other words, the x 's generate ("span") M .
- (ii) For $\lambda_1, \dots, \lambda_n \in R$ and $x_1, \dots, x_n \in X$, if $\lambda_1 x_1 + \dots + \lambda_n x_n = 0$, then $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$. In other words, the x 's are linearly independent.

An R -module F is said to be a *free* R -module if it has a basis. We adopt the convention that the zero module is free with empty basis.

Examples 2.3. (i) If $R = \mathbb{Z}$, any finitely generated torsion-free abelian group is a free abelian group, i.e., a free \mathbb{Z} -module.

(ii) $F = R \oplus R \oplus \dots \oplus R$, with "standard basis" $(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots$

(iii) $R[X]$ is a free R -module with basis $1, X, X^2, \dots$

The next Proposition is a module analogue of the basic structure theorem for vector spaces.

LECTURE 2

Proposition 2.4. *Let F be an R -module. Then F is a free R -module if and only if F is isomorphic to a direct sum of copies of R .*

Proof. Suppose that F is a free module with basis $X = \{x_\alpha\}_{\alpha \in A}$. Given an element $f \in F$, it can be uniquely written $f = \lambda_{\alpha_1}x_{\alpha_1} + \cdots + \lambda_{\alpha_n}x_{\alpha_n}$, with $\lambda_{\alpha_i} \in R$ and $x_{\alpha_i} \in X$. The map $\phi : F \rightarrow \bigoplus R_\alpha$ which sends f to the A -tuple with coordinates $\lambda_{\alpha_1}, \dots, \lambda_{\alpha_n}$ is easily seen to be an R -module isomorphism. The converse is similar.

Recall that for vector spaces over a field, any two bases have the same cardinality. The same is true for vector spaces over a division ring (with exactly the same proof). Unfortunately, this no longer holds for free modules over an arbitrary ring. It does hold, however, for free modules over many rings, including all commutative rings. To make this precise, we will say that a ring R satisfies the *invariant basis property* if for all free modules F and bases X and Y of F , it holds that $|X| = |Y|$.

The next proposition provides a useful test to tell if a ring satisfies the invariant basis property. In the proof we will use the following construction. If $I \subseteq R$ is a left ideal and M an R -module, we let IM denote the subset of M consisting of all finite linear combinations of elements of M with coefficients from I . Thus a typical element of IM has the form $i_1m_1 + \cdots + i_km_k$, with the i 's from I and the m 's from M . It is easy to check that IM is a submodule and that, if I is two-sided, M/IM is an R/I -module under the natural scalar multiplication $(r + I) \cdot (m + IM) = r \cdot m + IM$.

Proposition 2.5. *Let $\phi : R \rightarrow S$ be a surjective ring homomorphism. If S satisfies the invariant basis property, then R satisfies the invariant basis property.*

Proof. Let F be a free R -module and $X \subseteq F$ a basis for F . Set $I := \ker(\phi)$, so $R/I = S$. It suffices to show that $\{x + IF\}_{x \in X}$ is a basis for F/IF over R/I and that $|X| = |\{x + IF\}_{x \in X}|$. Clearly, the elements $\{x + IF\}_{x \in X}$ span F/IF over R/I . Suppose

$$(*) \quad (r_1 + I)(x_{j_1} + IF) + \cdots + (r_n + I)(x_{j_n} + IF) = 0$$

in F/IF . Then over R , we may write

$$r_1x_{j_1} + \cdots + r_nx_{j_n} = i_1x_{k_1} + \cdots + i_mx_{k_m},$$

FREE MODULES

with i 's in I and x_{k_t} 's in X . Since the x 's form a basis for F , $r_1, \dots, r_n \in I$. It follows that the coefficients in (*) are zero (over R/I), so the set $\{x + IF\}_{x \in X}$ is linearly independent and therefore forms a basis for F/IF .

The set map $x \rightarrow x + I$ from X to $\{x + IF\}_{x \in X}$ is clearly onto. Suppose it is not one-to-one. Then there exist $x_1, x_2 \in X$ such that $x_1 - x_2 \in IF$. Therefore, we may write $x_1 - x_2 = i_1 x_{j_1} + \dots + i_t x_{j_t}$ for i_j 's in I . But this clearly contradicts uniqueness of expression for basis elements. Thus the set map is one-to-one and we have $|X| = |\{x + IF\}_{x \in X}|$.

Corollary 2.6. *Let R be a ring which maps onto a division ring. Then R has the invariant basis property. In particular, any commutative ring has the invariant basis property.*

Proof. The first statement follows from Proposition 2.5 and the fact that any division ring has the invariant basis property. For the second statement, if R is commutative and $M \subseteq R$ is a maximal ideal, then R/M is a field. By Zorn's lemma, such an M always exists.

Example 2.7. Let K be a field and V be any K -vector space having a countably infinite basis, e.g., $K \oplus K \oplus \dots$. Consider $R := \text{Hom}_K(V, V)$, the set of K -vector space homomorphisms from V to itself. Then R is an associative non-commutative ring (under composition of homomorphisms and "point-wise" addition.) One can show that as R -modules, $R \cong R \oplus R$. Thus, by the proof of Proposition 2.4, the module $F := R = R \oplus R$ has a basis consisting of one element and another basis consisting of two elements. It follows by iteration that for all $n \geq 1$, F has a basis consisting of n elements. For a proof, see Exercise 5. It turns out that this anomaly can only occur in the finite case. That is, no matter the ring, if F is a free module with an infinite basis, then all bases have the same cardinality.

A final comment. We've noted that if R is a division ring, then every R -module is free. Any ring having this property is necessarily a division ring. To see this, we must show that every non-zero element $a \in R$ is a unit. Let $M \subseteq R$ be a maximal left ideal. Then R/M is a left R -module having no proper left R -submodules. Hence, if R/M is free, it must be free on a single element, say $x + M$. Since $x \notin M$, $R = R \cdot x + M$. If $r \cdot x \in M$, then $r = 0$, since $x + M$ is a basis for R/M . Thus, $R = Rx \oplus M$, so $R/M = Rx$. Therefore, Rx is a free R -module having no proper submodules. Clearly x is a basis for Rx (since $r \cdot x = 0 \in M$, implies $r = 0$). Let $0 \neq a \in R$. Since $ax \neq 0$, $Rx = Rax$, so $x = uax$ for some $u \in R$. Thus,

LECTURE 2

$(1 - ua) \cdot x = 0$, so $1 - ua = 0$. Hence $1 = ua$ and a is left invertible. Similarly, if every right R -module is free, then every non-zero element is right invertible. Therefore, if every R -module (left or right) is free, every non-zero element is both left and right invertible and it follows from this that every non-zero element is a unit (i.e., has a two-sided inverse).