Math 210B Lecture 1 Notes

Daniel Raban

January 7, 2019

1 Free Modules

1.1 Free modules over rings

Let R be a commutative ring.

Definition 1.1. An R-module M is **free** on a subset X if for any R-module N and map $f : X \to N$, there exists a unique R-module homomorphism $\phi_f : M \to N$ such that $\phi_f|_X = f$.

Example 1.1. If X is a set, we can construct the free module on X: $F_X = \bigoplus_{x \in X} R \cdot x$.

We can think of this as a functor F from Set to R-mod. With this viewpoint, if $f : X \to Y$, then $F(f) : F_X \to F_Y$ is given by $F(f)(\sum_{i=1}^n a_i x_i) = \sum_{i=1}^n a_i f(x_i)$. So for $F : \text{Set} \to \text{R-mod}$,

$$\mathrm{Hom}_{\mathrm{Set}}(X, N) \cong \mathrm{Hom}_{\text{R-mod}}(F_X, N),$$

where this isomorphism is natural. That is, F is left-adjoint to the forgetful functor from R-mod to Set.

Lemma 1.1. *An R-module M is free on X if and only if*

1. *X generates M as an R-module (i.e. for all $m \in M$, there exist $x_1, \dots, x_n \in X$ and $a_1, \dots, a_n \in R$ such that $m = \sum a_i x_i$)*
2. *X is R-linearly independent (i.e. if $\sum_{i=1}^n a_i x_i = 0$ with $s_1, \dots, x_n \in X$ distinct, then $a_i = 0$ for all i).*

Proof. If M is free on X¡ then there exists a unique isomorphism from M to F_X, induced by the identity on X. F_X satisfies these two properties, so M does.

If M satisfies the two properties, then there exists a unique $\phi : F_X \to M$ sending $x \mapsto X$ (since $X \subseteq M$). Property 1 implies that ϕ is surjective, and property 2 implies that ϕ is injective. $\square$

1.2 Bases and vector spaces

Definition 1.2. If X generates the R-module M and is linearly independent, we call it a **basis** of the M.

Theorem 1.1. *Every vector space V over a field has a basis. In fact, every linearly independent set in V is contained in a basis, and every spanning set contains a basis.*

Proof. We will prove the first statement; the other two statements follow by a similar argument. Let V be an F-vector space, where F is a field. Conide the set S of subsets X of V that are F-linearly independent. $(S, \subseteq)$ is a partially ordered set (poset). If C is a chain, $\bigcup_{X \in C} X$ is linearly independent, so it is an upper bound on C. By Zorn's lemma, S has a maximal element B. Let $W = \operatorname{span}(B)$. If $v \in V \setminus W$, then $B \cup \{v\}$ is linearly independent, contradicting the maximality of B. Then $V = W$, so B is a basis. $\square$

Example 1.2. The field condition is very important; here are counterexamples for general rings. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}$. Then $2 \in \mathbb{Z}$, but 2 is not contained in a basis of $\mathbb{Z}$. The set $\{2, 3\}$ spans $\mathbb{Z}$, but does not contain a basis.

Proposition 1.1. *Let V be an F-vector space with a basis of n elements. Let $Y \subseteq W$.*

1. *If Y spans V, then $|Y| \geq n$.*

2. *If Y is linearly independent, then $|Y| \leq n$.*

3. *If $|Y| = n$, then Y is linearly independent iff Y spans V.*

Remark 1.1. The first two properties hold for free modules with a basis of n elements as well, but the 2nd property becomes harder to prove. For the third property, in the general case, we just have that if Y spans and $|Y| = n$, then Y is linearly independent.

Corollary 1.1. *If $\varphi : V \to W$ is an F-linear transformation of finite-dimensional vector spaces over F, then $\dim_F(V) = \dim_F(\ker(\varphi)) + \dim_F(\operatorname{im}(\varphi))$. In particular, if $\dim V = \dim W$, then φ is injective iff φ is surjective iff φ is an isomorphism.*

1.3 Cardinality of bases

Theorem 1.2. *If X and Y are sets and $F_X \cong F_Y$, then X and Y have the same cardinality.*

Proof. Suppose $|Y| \geq |X|$ and first suppose that X is infinite. It suffices to show F_X has no basis of cardinality $> |X|$. Suppose $B \subseteq F_X$ is a basis of F_X. Every $x \in X$ is a finite linear combination of some elements in B; let B_x be the set of these. Then $|\coprod_{x \in X} B_x| \geq |\bigcup_{x \in X} B|$ and it generates F_X, so we can get the upper bound on cardinality $|B| \leq |\mathbb{Z} \times X| = |X|$. Therefore, F_X has no basis of cardinality $> |X|$.

If Y is finite, let $\mathfrak{m}$ be a maximal ideal of R. Then $F = R/\mathfrak{m}$ is a field, and

$$F_X/\mathfrak{m}F_X \cong \left(\bigoplus_{x\in X} R\right)/\mathfrak{m}\left(\bigoplus_{x\in X} R\right) \cong \bigoplus_{x\in X} F.$$

The same is try for F_Y. The isomorphism $F_X \cong F_Y$ induces the isomorphism of F-vector spaces $F_X/\mathfrak{m}F_X \cong F_Y/\mathfrak{m}F_Y$, which then have bases of cardinality $|X|$ and $|Y|$. Y is finite, so X is finite and has cardinality $|X| = |Y|$. $\square$