Lecture 29: Free modules, finite generation, and bases for vector spaces

1. Universal property of free modules

Recall:

Definition 29.1. Let R be a ring. Then the direct sum module

$$R^n := R \oplus \ldots \oplus R$$

is called the *free R-module of rank n.*

Chit-chat 29.2. Why is this called a free R-module? Behold:

Proposition 29.3. Let M be an R-module. Then any ordered n-tuple of elements $x_1, \ldots, x_n \in M$ uniquely determines an R-module homomorphism

$$X : R^n \to M$$

given by

$$(0, \ldots, 0, 1, 0, \ldots, 0) \mapsto x_i$$

where the 1 is in the ith coordinate.

Remark 29.4. This is the same property as for the free group on n generators: Any ordered n-tuple of elements of a group G determines a unique map from F_n to G.

Proof. Given $(x_1, \ldots, x_n)$, define $X : R^n \to M$ by

$$X(a_1, \ldots, a_n) := a_1 x_1 + \ldots + a_n x_n \in M.$$

This is a group homomorphism because

$$\begin{aligned} X((a_1, \ldots, a_n) + (b_1, \ldots, b_n)) &= (a_1 + b_1)x_1 + \ldots (a_n + b_n)x_n \\ &= (a_1 x_1 + \ldots + a_n x_n) + (b_1 x_1 + \ldots b_n x_n) \\ &= X(a_1, \ldots, a_n) + X(b_1, \ldots, b_n). \end{aligned}$$

where the middle equality is using the property of M being an R-module. This is also an R-module homomorphism because

$$\begin{aligned} X(r(a_1,\ldots,a_n)) &= X((ra_1,\ldots,ra_n)) \\ &= (ra_1)x_1+\ldots+(ra_n)x_n \\ &= r(a_1x_1+\ldots a_nx_n) \\ &= rX((a_1,\ldots,a_n)) \end{aligned}$$

Again, the penultimate equality is using the fact that M is an R-module. □

2. Spans and linear independence and bases

Definition 29.5. Fix $x_1,\ldots,x_n \in M$.

(1) We say this collection *spans* M if the map $X : R^n \to M$ is a surjection.
(2) We say that this collection is *linearly independent* in M if the map $X : R^n \to M$ is an injection.
(3) We say this collection is a *basis* for M if X is both an injection and a surjection.

Chit-chat 29.6. You'll recognize these terms from linear algebra. And in terms of equations, these definitions mean exactly what you'd imagine:

Proposition 29.7. Let M be a left R-module, and let $x_1,\ldots,x_n \in M$ be an ordered collection.

(1) The collection spans M if and only if for every $y \in M$, there exists a collection $a_1,\ldots,a_n \in R$ so that
$$y = a_1x_1+\ldots+a_nx_n.$$
(2) The collection is linearly independent if and only if the equation
$$0 = a_1x_1+\ldots+a_nx_n$$
has one and only one solution: $(a_1,\ldots,a_n)=(0,\ldots,0)$.
(3) The collection is a basis if and only if for any $y \in M$, the equation
$$y = a_1x_1+\ldots+a_nx_n$$
has one and only one collection $(a_1,\ldots,a_n)$ solving it.

Proof. The first is the definition of surjection. The latter claim follows because a homomorphism is injective if and only if the kernel is trivial, and $(0,\ldots,0)\in R^n$ is the additive identity of R^n. The last claim is the definition of a bijection. □

Definition 29.8. We say that a module is *finitely generated* if there is some number $n \in \mathbb{Z}_{\geq 0}$ and a surjective R-module homomoprhism $R^n \to M$.

Chit-chat 29.9. This is also in analogy to groups. A group G is finitely generated if and only if there is some finite collection of elements g_i such that all other elements can be expressed as products of g_i and their inverses. Likewise, M is finitely generated if there is a finite collection x_i such that every element of M can be obtained by taking linear combinations of x_i.

Non-example 29.10. *Not* every module over R admits a basis. This is in contrast to vector spaces. For example, if $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, then for any $x \in M$, the equation

$$ax = 0$$

has many solutions—a could equal $n, 2n, \ldots$.

Take-away: Not every finitely generated R-module admits a basis.

3. Vector spaces and subspaces

Recall:

Definition 29.11. A commutative ring is called a *field* if $R - \{0\}$ is a group under multiplication.

Definition 29.12. Let F be a field. A module over F is called a *vector space over F*.

Definition 29.13. Let V be a vector space. Then a submodule of V is called a *linear subspace* of V.

4. Spanning sets are bigger than independent sets

The following is the most importance consequences of being a field, as opposed to a ring:

Theorem 29.14. Let F be a field, and let M be a vector space over F. If $v_1, \ldots, v_n$ span and $w_1, \ldots, w_m$ are linearly independent, then $n \geq m$.

Proof of the Theorem. Let $y_1, \ldots, y_m$ be linearly independent, and let $v_1, \ldots, v_n$ be spanning. By re-ordering v_i if necessary, we can assume that

$$y_1 = a_1 v_1 + \ldots + a_n v_n$$

for $a_1 \neq 0$. Then $y_1, v_2, \ldots, v_n$ is also spanning, for we can obtain v_1 as a linear combination of the y_1 and the v_i—just divide the above equation by $a_1 \neq 0$ and rearrange terms.

Let $M_1 \subset M$ be the submodule generated by y_1—i.e., the image of $R \to M$ defined by $1 \mapsto y_1$—and consider the quotient

$$M/M_1.$$

(You'll prove this is also an R-module—i.e., a vector space—in your homework.) Then $\overline{y_2}, \ldots, \overline{y_m}$ are still linearly independent, for a linear combination of them equals zero if and only if

$$a_1 y_1 = a_2 y_2 + \ldots + a_m y_m$$

for some $a_1 \in F$, and such an equation can hold only when all the $a_i = 0$, since the y_i are assumed linearly independent. Note $\overline{y_1} = 0, \overline{v_2}, \ldots, \overline{v_n}$ are still spanning, so $\overline{v_2}, \ldots, \overline{v_n}$ is spanning. So we have $n-1$ vectors spanning M/M_1, and we have $m-1$ linearly independent vectors in it.

By repeating the trick above, if we have m linearly independent elements in a vector space spanned by n elements, we can obtain $m-k$ linearly independent elements in a quotient vector space spanned by $n-k$ elements. So which of these numbers will hit 0 first? If $n-k=0$ first, we are in a quotient vector space spanned by 0 elements—i.e., the zero vector space—so we must conclude $m-k=0$ as well, for there are no linearly independent vectors in the zero vector space. And in this case, $m=n$. If $m-k$ reaches zero before $n-k$ does, we have that $m \leq n$. $\square$

5. Corollaries

Corollary 29.15. If M is a finitely generated vector space, then any two bases of M have the same number of elements in it.

Proof. If the $\{v_i\}$ and $\{w_i\}$ above are both spanning and linearly independent, we have $n \geq m$ and $m \geq n$. Hence $m=n$. $\square$

Definition 29.16. Let M be a finitely generated vector space over F. Then the number of elements in a basis for M is called the *dimension* of M over F.

Remark 29.17. This is the single most important fact in linear algebra: That we have a notion of dimension. It took us thousands of years to know what we mean by an n-dimensional space, so don't take this lightly!

Corollary 29.18. If M is a finitely generated vector space, any linearly independent collection $w_1, \ldots, w_m$ can be completed to a basis—that is, we can find $w_{m+1}, \ldots, w_n$ so that the resulting collection $w_1, \ldots, w_n$ is both linearly independent and spanning.

Proof. Since M is finitely generated, there is some N for which we have a surjection $F^N \to M$. So any set of linearly independent vectors must have size $\leq N$ by the theorem. If $X_m : F^m \to M$ is the map determined by $w_1, \ldots, w_m$, and if X_m is not surjective, choose an element w_{m+1} not in $\operatorname{im}(X_m)$. Note the resulting collection $w_1, \ldots, w_{m+1}$ is still linearly independent, for if

$$a_1 w_1 + \ldots + a_{m+1} w_{m+1} = 0$$

then we have

$$a_1 w_1 + \ldots + a_m w_m = -a_{m+1} w_{m+1}.$$

If $a_{m+1} = 0$, by linear independence of the w_i, we know all $a_i = 0$. On the other hand, if $a_{m+1} \neq 0$ we arrive at a contradiction by dividing:

$$\frac{a_1}{-a_{m+1}} w_1 + \ldots + \frac{a_m}{-a_{m+1}} w_m = w_{m+1}.$$

The lefthand side is in the image of X_m, but w_{m+1} was chosen not to be.

So we have an injective homomorphism $X_{m+1} : F^{m+1} \to M$. If X_{m+1} is not surjective, we repeat the argument. It must become a surjective map at some $m + k \leq N$ by the theorem. So let k be the integer at which X_{m+k} first becomes a surjection. By the above argument, it is still an injection, so we have a basis determined by the generators $w_1, \ldots, w_{m+k}$. $\square$

Corollary 29.19. Any finitely generated module over a field F is isomorphic to F^n for some n.

PROOF. Begin with the linearly independent set 0 and complete to a basis. A basis defines an isomorphism from F^n to your module. $\square$

Remark 29.20. This is definitely not true for R-modules if R is not a field—after all, any finite abelian group is a $\mathbb{Z}$-module, but any free $\mathbb{Z}$-module is the zero module or an infinite module.

Corollary 29.21. Let $V' \subset V$ be a subspace. Then $\dim V' + \dim V/V' = \dim V$.

PROOF. Let $v_1, \ldots, v_{\dim V'}$ be a basis for V'. Let $\overline{u_1}, \ldots, \overline{u_{\dim V/V'}}$ be a bsis for V/V'. Then choosing representatives u_i for $\overline{u_i}$, the set

$$v_1, \ldots, v_{\dim V'}, u_1, \ldots, u_{\dim V/V'}$$

is a basis for V. It obviously spans since for each $a \in V$, $\overline{a}$ is a linear combination of $\overline{u_i}$, hence a is in the V'-orbit of some linear combination of the u_i. It is linearly independent because if we have that

$$0 = a_1 v_1 + \ldots a_{\dim V'} v_{\dim V'} + b_1 u_1 + \ldots + b_{\dim V/V'} u_{\dim V/V'}$$

then

$$\overline{0} = a_1 \overline{v}_1 + \ldots a_{\dim V'} \overline{v_{\dim V'}} + b_1 \overline{u_1} + \ldots b_{\dim V/V'} \overline{u_{\dim V/V'}}.$$

The a_i terms go to zero since $\overline{v}_i = 0$, hence we get an equation saying a linear combination of the $\overline{u}_i$ is zero. This means each b_i must be zero by linear independence of the $\overline{u}_i$. The original equation then says that $0 = \sum a_i v_i$, so by linear independence of the v_i, the a_i must be zero. $\square$

Corollary 29.22 (Rank-nullity theorem)**.** Let $f : V \to W$ be a map of F-modules and assume V is finitely generated. Then $\dim \ker f + \dim \operatorname{im} f = \dim V$.

PROOF. By the first isomorphism theorem, we know there is a group isomorphism $V/\ker f \cong \operatorname{im} f$. But this homomorphism is also an F-module map, as you can check by hand. Thus $\operatorname{im} f \cong V/\ker f$. $\square$