

The primary text for Algebra II is Dummit and Foote's *Abstract Algebra*, and will cover the following topics:

- modules and advanced linear algebra;
- representation theory of finite groups;
- field theory and Galois theory.

## Contents

<b>Modules and Advanced Linear Algebra</b>	<b>1</b>
Tensor Products of Modules . . . . .	1
Introduction and Basic Definitions . . . . .	1
Universal Property . . . . .	3
Module Structure on Tensor Products . . . . .	5
Finitely Generated Modules over PIDs . . . . .	6
Smith Normal Form . . . . .	6
Structure of Finitely-Generated Modules over PIDs . . . . .	8

## Modules and Advanced Linear Algebra

### Tensor Products of Modules

The first major topic in Modules and Advanced Linear Algebra is tensor products.

#### Introduction and Basic Definitions

To motivate tensor products, we recall a basic fact from linear algebra. If we assume that  $R$  is a field, and  $M, N$  are finite-dimensional  $R$ -vector spaces, then the following equation necessarily holds:

$$\dim(M \oplus N) = \dim(M) + \dim(N).$$

We want to construct a similar operation on vector spaces,  $M \otimes N$ , that satisfies

$$\dim(M \otimes N) = \dim(M) \dim(N).$$

For now, we will label this by  $M \bar{\otimes} N$ , where we use the  $\bar{\otimes}$  to refer to the fact that this is a temporary definition. Naively, we might seek to define  $M \bar{\otimes} N$  as follows. If we let  $\{x_1, \dots, x_k\}$  be a basis for  $M$  and  $\{y_1, \dots, y_\ell\}$  a basis for  $N$ , then we will define  $M \bar{\otimes} N$  to be all the formal  $R$ -linear combinations over the basis

$$B = \{x_i \otimes y_j \mid 1 \leq i \leq k, 1 \leq j \leq \ell\}.$$

While this is technically correct — as in, this does yield a vector space with

$$\dim(M \bar{\otimes} N) = \dim(M) \dim(N),$$

the issue is that this definition is not canonical, in that it depends on chosen bases for  $M$  and  $N$ . Furthermore, it is not clear how one may generalize from this definition to modules over arbitrary rings, which do not necessarily have bases. To resolve this issue, we will go about defining a construction that “extends,” in a sense, this definition of  $M \bar{\otimes} N$ .

To start, we define the simple tensor  $m \otimes n$  for any  $m \in M$  and  $n \in N$ . If we let

$$m = \sum_{i=1}^k \lambda_i x_i$$

$$n = \sum_{j=1}^{\ell} \mu_j y_j,$$

then we will define

$$m \otimes n = \sum_{i=1}^k \sum_{j=1}^{\ell} \lambda_i \mu_j (x_i \otimes y_j).$$

We observe that every element of  $M \bar{\otimes} N$  is a sum (i.e., an *integral* linear combination) of simple tensors, as by regrouping we may take

$$\sum_{i=1}^k \sum_{j=1}^{\ell} \lambda_{ij} (x_i \otimes y_j) = \sum_{i=1}^k \sum_{j=1}^{\ell} (\lambda_{ij} x_i) \otimes y_j.$$

The simple tensors satisfy the following relations:

$$(R1) \quad (m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n;$$

$$(R2) \quad m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2;$$

$$(R3) \quad (\alpha m) \otimes n = m \otimes (\alpha n)$$

for  $m, m_1, m_2 \in M$ ,  $n, n_1, n_2 \in N$ , and  $\alpha \in R$ .

**Proposition:** These are the defining relations for  $M \bar{\otimes} N$  in the category of abelian groups.

We will simply take this proposition as fact.

Now, let

$$\begin{aligned} Q &= M \times N \\ &= \{(m, n) \mid m \in M, n \in N\} \end{aligned}$$

be the Cartesian product of  $M$  and  $N$  as sets. We will then take  $\mathbb{Z}[Q]$  to be the standard free  $\mathbb{Z}$ -module (i.e., free abelian group) on  $Q$ . That is,  $\mathbb{Z}[Q]$  is the set of formal linear combinations

$$v = \sum_{q \in Q} \lambda_q q,$$

where  $\lambda_q \in \mathbb{Z}$  and only finitely many coefficients are nonzero. By the universal property of free abelian groups, the map  $(m, n) \mapsto m \otimes n$  descends to a unique homomorphism  $\varphi: \mathbb{Z}[Q] \rightarrow M \bar{\otimes} N$ . Such a homomorphism is necessarily surjective as every element of  $M \bar{\otimes} N$  is an integral linear combination of simple tensors, meaning that we have

$$M \bar{\otimes} N \cong \mathbb{Z}[Q] / \ker(\varphi)$$

as abelian groups.

Now, consider the subgroup of  $\mathbb{Z}[Q]$ , which we denote  $\langle K \rangle$ , that is generated by the following elements:

$$(I) \quad (m_1 + m_2, n) - (m_1, n) - (m_2, n);$$

$$(II) \quad (m, n_1 + n_2) - (m, n_1) - (m, n_2);$$

$$(III) \quad (\alpha m, n) - (m, \alpha n)$$

for  $m_1, m_2, m \in M$ ,  $n_1, n_2, n \in N$ , and  $\alpha \in R$ . Then, from proposition that the relations (R1) through (R3) define  $M \bar{\otimes} N$ , it follows that  $\langle K \rangle = \ker(\varphi)$ . Thus, we may define the tensor product canonically as follows.

**Definition:** Letting  $M, N, Q, K$  be as above, we define

$$M \otimes N := \mathbb{Z}[Q]/\langle K \rangle, \quad (\dagger)$$

and define  $m \otimes n = (m, n) + K$ .

So far, this has only given us an abelian group. We may ask how to define  $\mathbb{Z}[Q]/\langle K \rangle$  as an  $R$ -vector space, which naturally seems to be defined by

$$r \left( \sum_{i=1}^n m_i \otimes n_i \right) = \sum_{i=1}^n (rm_i) \otimes n_i \quad (*)$$

To show that the right-hand side of  $(*)$  is well-defined is a very difficult task. We will not do it here.

Now, we can actually quite easily generalize  $(\dagger)$  to modules over non-fields.

- If  $R$  is a commutative ring with 1, and  $M$  and  $N$  are left  $R$ -modules, the definition in  $(\dagger)$  copies over exactly.
- If  $R$  is non-commutative with 1, then the definition in  $(\dagger)$  makes sense, but the scalar multiplication in  $(*)$  does *not* hold.

In fact, we need to change the assumptions for  $M$  and  $N$  as  $R$ -modules. In particular, we need  $M$  to be a *right*  $R$ -module, and  $N$  to be a left  $R$ -module, and take the generators of type (III) for  $K$  to be defined by

$$(III') \quad (mr, n) - (m, rn)$$

for  $m \in M$ ,  $n \in N$ , and  $r \in R$ . This gives the tensor product  $M \otimes_R N$  an abelian group structure, but does not endow it with a  $R$ -module structure.

We may now consider some simple examples computing tensor products.

**Example:** Let  $R = \mathbb{Z}$ . We will show that  $\mathbb{Z}/n\mathbb{Z} \otimes_R \mathbb{Q} = 0$ .

As a general strategy, in order to show that a tensor product is the zero module, it suffices to show for every simple tensor. Observe that  $0 \otimes y = 0$  for any tensor product, since we may take

$$\begin{aligned} 0 \otimes y &= (0 + 0) \otimes y \\ &= 0 \otimes y + 0 \otimes y. \end{aligned}$$

Therefore, we may write

$$\begin{aligned} [a] \otimes b &= (n[a]) \otimes \left( \frac{b}{n} \right) \\ &= [na] \otimes \frac{b}{n} \\ &= 0 \otimes \frac{b}{n} \\ &= 0. \end{aligned}$$

### Universal Property

We may now work towards understanding one of the defining properties of tensor products in general. This requires a discussion of a weakened version of  $R$ -bilinear maps.

**Definition:** Let  $R$  be a ring,  $M$  a right  $R$ -module,  $N$  a left  $R$ -module, and  $L$  an abelian group written additively. A map  $\varphi: M \times N \rightarrow L$  is called  *$R$ -balanced* if

$$(BM1) \quad \varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$$

$$(BM2) \quad \varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$$

$$(BM3) \quad \varphi(mr, n) = \varphi(m, rn)$$

for all  $r \in R$ ,  $m, m_1, m_2 \in M$ , and  $n, n_1, n_2 \in N$ .

**Theorem:** Let  $R, M, N, L$  be as above. Let

$$\begin{aligned} \Omega &= \{ \Phi: M \otimes N \rightarrow L \mid \Phi \text{ a group homomorphism} \} \\ \Delta &= \{ \varphi: M \times N \rightarrow L \mid \varphi \text{ } R\text{-balanced} \}. \end{aligned}$$

Define the map  $J: \Omega \rightarrow \Delta$  by

$$(J\Phi)(m, n) = \Phi(m \otimes n).$$

Then,  $J$  is bijective.

*Proof.* We have that  $J$  is injective since  $J\Phi$  captures the value of  $\Phi$  on simple tensors, and  $\Phi$  is completely determined by its value on simple tensors since  $\Phi$  is a group homomorphism, and elements of  $M \otimes N$  are sums of simple tensors.

To prove surjectivity, we recall that

$$M \otimes N = \mathbb{Z}[M \times N] / \langle K \rangle.$$

Let  $\varphi: M \times N \rightarrow L$  be an  $R$ -balanced map. By the universal property for free modules, there is a homomorphism  $\tilde{\varphi}: \mathbb{Z}[M \times N] \rightarrow L$  taking  $(m, n) \mapsto \varphi(m, n)$ .

We only need to show now that  $\tilde{\varphi}$  kills the elements of  $K$  that generate  $\langle K \rangle$ , but this follows from the fact that  $\varphi$  is  $R$ -balanced. Therefore, we get an induced map

$$\begin{aligned} \Phi: M \otimes N &\rightarrow L \\ m \otimes n &\mapsto \varphi(m, n), \end{aligned}$$

so we are done.  $\square$

**Definition:** Let  $R$  be a commutative ring,  $M, N, L$  left  $R$ -modules. A map  $\varphi: M \times N \rightarrow L$  is called  $R$ -bilinear if it satisfies (BM1), (BM2), and

$$(BM3') \quad \varphi(m, rn) = \varphi(rm, n) = r\varphi(m, n)$$

**Theorem:** If  $R, M, N, L$  are as above, then there exists a natural bijection between  $\text{hom}_R(M \otimes N, L)$  and  $\text{hom}_R(M \times N, L)$ .

The proof is the same as the proof in the case of  $R$ -balanced maps, mutatis mutandis.

**Proposition:** Let  $R$  be a commutative ring, and  $M, N$  free left  $R$ -modules with respective bases  $X$  and  $Y$ . Then,  $M \otimes N$  is a free module with basis

$$Z = \{ x \otimes y \mid x \in X, y \in Y \}.$$

*Proof.* We have that  $Z$  generates  $M \otimes N$  as a  $R$ -module, so we only need to show that  $Z$  is linearly independent.

Let

$$v = \sum_{i=1}^t r_i x_i \otimes y_i.$$

Without loss of generality, we assume that  $r_1 \neq 0$ . It is enough to find a homomorphism  $\varphi: M \otimes N \rightarrow R$  such that  $\varphi(v) \neq 0$ .

Toward this end, we construct an  $R$ -bilinear map, which we only need to specify on the basis. Define

$$\alpha: M \rightarrow R$$

$$\begin{aligned}
x_i &\mapsto \begin{cases} 0 & x_i \neq x_1 \\ 1 & x_i = x_1 \end{cases} \\
\beta: N &\rightarrow R \\
y_i &\mapsto \begin{cases} 0 & y_i \neq y_1 \\ 1 & y_i = y_1 \end{cases}.
\end{aligned}$$

The map  $\varphi: M \times N \rightarrow R$  given by  $\varphi(x_i, y_i) = \alpha(x_i)\beta(y_i)$  is thus  $R$ -bilinear and induces a map on the tensor product that is nonzero at  $v$ . Thus,  $v$  is not the zero vector.  $\square$

### Module Structure on Tensor Products

Thus far, we have only shown that there is a module structure on the tensor product whenever we are considering modules over commutative rings. Else, we only have an abelian group. We will specify the case when there is a module structure on the tensor product.

**Definition:** Let  $R$  and  $S$  be unital rings. An  $(S, R)$ -bimodule is an abelian group  $(M, +)$  that is both a left  $S$ -module and right  $R$ -module satisfying the compatibility condition

$$(sm)r = s(mr)$$

for all  $m \in M$ ,  $r \in R$ , and  $s \in S$ .

**Example:**

- (i) If  $R$  and  $S$  are both subrings of the same ring  $T$  with  $1_R = 1_S = 1_T$ , then  $T$  is an  $(S, R)$  bimodule, where  $S$  acts by left-multiplication and  $R$  acts by right-multiplication.
- (ii) If  $R$  is commutative,  $M$  a left  $R$ -module, then  $M$  can be considered as an  $(R, R)$ -bimodule by setting  $m \cdot r = rm$ .

**Proposition:** Let  $R$  and  $S$  be rings,  $M$  an  $(S, R)$ -bimodule, and  $N$  a right  $R$ -module. Then,  $M \otimes N$  can be endowed with a unique  $S$ -module structure by taking  $s(m \otimes n) = sm \otimes n$ .

*Proof.* Fix  $s \in S$ . Define the map  $\varphi_s: M \times N \rightarrow M \otimes_R N$  by taking  $\varphi_s(m, n) = sm \otimes n$ .

This map is  $R$ -balanced; we will verify (BM3) for this purpose:

$$\begin{aligned}
\varphi_s(mr, n) &= s(mr) \otimes n \\
&= (sm)r \otimes n \\
&= sm \otimes rn \\
&= \varphi_s(m, rn).
\end{aligned}$$

Thus, by the universal property, there is a homomorphism of abelian groups  $\overline{\varphi}_s: M \otimes N \rightarrow M \otimes N$  such that  $\overline{\varphi}_s(m \otimes n) = sm \otimes n$ . We will then define the action of  $s$  on  $M \otimes N$  by taking  $s \cdot u = \overline{\varphi}_s(u)$  for any  $u \in M \otimes N$ .  $\square$

The most useful case for this proposition is the *extension of scalars*. If  $R \subseteq S$  is a unital subring, then we may view  $S$  as an  $(S, R)$ -bimodule; for any left  $R$ -module  $N$ , we have that  $S \otimes_R N$  may be endowed with the structure of an  $S$ -module. We call this module the extension of scalars of  $N$  from  $R$  to  $S$ .

**Definition:** Let  $R$  be a commutative ring with 1. An  $R$ -algebra is a ring  $A$  which is also an  $R$ -module such that multiplication  $\mu: A \times A \rightarrow A$ ,  $\mu(a, b) = ab$  is an  $R$ -bilinear map.

**Example** (Some  $R$ -algebras): The following are  $R$ -algebras:

- (i) the polynomial ring  $R[x_1, \dots, x_n]$  in commuting variables;
- (ii) the ring of noncommutative polynomials  $R\langle x_1, \dots, x_n \rangle$ ;
- (iii) the matrices  $\text{Mat}_n(R)$  of  $n \times n$  matrices over  $R$ .

**Theorem:** Let  $A$  and  $B$  be  $R$ -algebras, where  $R$  is commutative. Then,  $A \otimes B$  has a unique  $R$ -algebra structure such that

$$(a \otimes b)(c \otimes d) = ac \otimes bd.$$

*Proof.* See Proposition 1.4.3 in [this document](#). □

**Lemma:** If  $R \subseteq S$  is a unital subring, with  $S$  commutative, and  $M$  is an  $R$ -algebra, then  $S \otimes_R M$  is an  $S$ -algebra.

**Lemma:** With the same assumptions as above, we have isomorphisms

$$\begin{aligned} S \otimes_R \text{Mat}_n(R) &\cong \text{Mat}_n(S) \\ S \otimes_R R[x_1, \dots, x_n] &\cong S[x_1, \dots, x_n] \\ S \otimes_R R[x]/(f(x)) &\cong S[x]/(f(x)). \end{aligned}$$

The general proof approach for these types of problems is to use the universal properties to construct an isomorphism of abelian groups, then prove that the isomorphism is compatible with the  $S$ -action and products of elements.

## Finitely Generated Modules over PIDs

We will now turn our focus towards proving the structure theorem for finitely generated modules over a PID. For this, we will use the Smith Normal Form.

### Smith Normal Form

**Definition:** Let  $R$  be a PID, and  $A \in \text{Mat}_n(R)$ . We say  $A$  is in Smith normal form if there exists  $m \leq \min(k, n)$  and elements  $d_1, \dots, d_m$  such that

$$A = \begin{pmatrix} d_1 & \cdots & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_m & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

where  $d_i \neq 0$  for all  $i$  and  $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_m)$ .

**Theorem:** If  $R$  is a PID with  $A \in \text{Mat}_n(R)$ , then there are  $U \in \text{GL}_k(R)$  and  $V \in \text{GL}_n(R)$  such that  $UAV$  is in Smith normal form.

This decomposition is essentially unique, in that if we have two Smith normal forms

$$\begin{aligned} D &= \begin{pmatrix} d'_1 & \cdots & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_m & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \\ D' &= \begin{pmatrix} d'_1 & \cdots & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d'_s & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \end{aligned}$$

then  $s = m$  and  $d_i$  and  $d'_i$  are associates for each  $i$ .

To show existence, we consider the elementary row (and column) operations, viewed as elementary matrices. Given  $\lambda \in R$ , we consider  $E_{ij}(\lambda)$  with  $i < j$  to be a square matrix of size to be determined size that has 1 along the diagonal,  $\lambda$  in position  $(i, j)$ , and 0 everywhere else. Furthermore, for any  $i \neq j$ , we let  $F_{ij}$  be the matrix obtained from an identity matrix of a certain size by swapping rows  $i$  and  $j$ .<sup>1</sup> Then, we have the following table of correspondences.

Elementary Row Operation	Interpretation as Matrix Multiplication
$R_i(A) \mapsto R_i(A) + \lambda R_j(A)$	$A \mapsto A_{ij}(\lambda)A$
$C_i(A) \mapsto C_i(A) + \lambda C_j(A)$	$A \mapsto AE_{ji}(\lambda)$
$R_i(A) \leftrightarrow R_j(A)$	$A \mapsto F_{ij}A$
$C_i(A) \leftrightarrow C_j(A)$	$A \mapsto AF_{ij}$

Thus, it suffices to show that every  $A$  can be replaced via these elementary row operations to a matrix in Smith normal form.

We will prove the special case where  $R$  is a Euclidean domain, since the primary applications we will be using are for the cases of  $\mathbb{Z}$  and  $F[x]$  for some field  $F$ , and both of these rings are Euclidean domains. If  $N$  is the Euclidean norm for  $R$ , then we will let  $N(A) = \min_{a_{ij} \neq 0} N(a_{ij})$  denote the norm of the matrix.

*Proof of Existence.* By induction, we may assume that existence holds for any matrices with smaller values of  $k+n$ . Starting with an arbitrary matrix with dimensions  $k \times n$ , we claim that we can reduce any nonzero matrix to either

- (i) a matrix  $A'$  with smaller norm
- (ii) a matrix of the block diagonal form

$$\begin{pmatrix} d_1 & 0 \\ 0 & B \end{pmatrix}, \quad (\dagger)$$

where  $d_1$  divides all the entries of  $B$ .

To see that this suffices to prove existence of Smith normal form, we start by seeing that if case 1 occurs, we apply the reduction until case 2 occurs, which necessarily happens by the well-ordering principle. Then, if  $A$  is reduced to a matrix of the block diagonal form  $(\dagger)$ , then by the induction hypothesis we may reduce  $B$  to Smith normal form using the elementary operations. We may then apply these same operations to  $A$  to yield  $A$  to have  $d_2|d_3|\cdots|d_m$  and the block  $d_1$  on the upper left hand corner, so since these elementary row operations yield  $R$ -linear combinations of the original element, with  $d_1$  dividing all the entries of  $B$ , we have that  $d_1|d_2$ .

Now, we will show that this is satisfactory. Using column and row flips, we may assume that  $N(A) = N(a_{11})$ . Write

$$\begin{aligned} a_{1j} &= a_{11}q_{1j} + r_{1j} \\ a_{i1} &= a_{11}q_{i1} + r_{i1} \end{aligned}$$

for all  $2 \leq i, j \leq n$ . Then, for any  $i$  and  $j$ , we have  $N(r_{i1}) < N(a_{11})$  and  $N(r_{1j}) \leq N(a_{11})$ , or we have  $N(r_{i1}) = 0$  or  $N(r_{1j}) = 0$ . By applying the operations  $C_j(A) \mapsto C_j(A) - q_{1j}C_1(A)$  and  $R_i(A) \mapsto R_i(A) - q_{i1}R_1(A)$ , we may perform the replacements  $a_{i1} \mapsto r_{i1}$  and  $a_{1j} \mapsto r_{1j}$ . If there is at least one such nonzero remainder, then we have  $N(A') < N(A)$ , and this shows case (i).

If all the remainders are 0, then we have the block diagonal form  $(\dagger)$ , and split into two subcases. If we had  $a_{11}|b_{ij}$  for all  $b_{ij} \in B$ , then we would be done. Else, suppose there were some  $s, t \geq 2$  with  $a_{11} \nmid a_{st}$ . In this case, we may first perform the operation  $R_1(A') \mapsto R_1(A') + R_s(A')$ , write  $a_{st} = a_{11}q + r$  with  $r \neq 0$ , and then perform  $C_t(A) = C_t(A) - qC_1(A)$  to find that  $N(A')$  is not minimal, so we may perform the process further. This gives existence.  $\square$

<sup>1</sup>One may recognize this as the matrix corresponding to the permutation  $\tau = (i, j)$ .

### Structure of Finitely-Generated Modules over PIDs

**Theorem** (Uniqueness of Rank): Let  $R \neq \{0\}$  be a commutative ring. If  $R^n \cong R^m$ , then  $n = m$ .

*Proof.* The theorem holds for the case of  $R$  as a field, and otherwise, pass to a quotient by a maximal ideal.  $\square$

**Corollary:** If  $M$  is a finitely generated free module over a commutative ring  $R$ , then if we define  $\text{rk}(M)$  to be the value of  $n \in \mathbb{Z}_{\geq 0}$  such that  $M \cong R^n$ , such a value is then unique.

**Theorem** (Compatible Basis Theorem): Let  $R$  be a PID, and  $M$  a finitely generated free module with rank  $n$ . Let  $N$  be a submodule of  $M$ . Then,  $N$  is free with rank  $m \leq n$ , and there is a basis  $\{y_1, \dots, y_n\}$  for  $M$  and elements  $(d_1) \supseteq \dots \supseteq (d_m)$  in  $R$  such that  $\{d_1 y_1, \dots, d_m y_m\}$  is a basis for  $N$ .

Moreover,  $m$  is unique, and  $d_1, \dots, d_m$  are unique up to associates.

*Proof.* Let  $\{x_1, \dots, x_n\}$  be a basis for  $M$ , and let  $N$  be generated by  $\{u_1, \dots, u_k\}$ . We may write

$$u_i = \sum_{j=1}^n a_{ij} x_j$$

for some  $a_{ij} \in R$ . Writing the system of equations as a matrix

$$\begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} = (a_{ij})_{i,j} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

we may then put the matrix  $A = (a_{ij})_{i,j}$  in Smith normal form, giving  $A = PDQ$  for some diagonal matrix  $D = \text{diag}_{k,n}(d_1, \dots, d_m)$ ,  $P \in \text{GL}_k(R)$ , and  $Q \in \text{GL}_n(R)$ . Write

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = Q \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = P^{-1} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}.$$

Then,  $\{y_1, \dots, y_n\}$  form a basis for  $M$ , and  $\{v_1, \dots, v_k\}$  generate  $N$ ; since we may write

$$\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = D \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

it follows that  $k = m$ ,  $v_i = d_i y_i$ , and we are done. Linear independence follows from the fact that  $R$  is an integral domain and that  $\{y_1, \dots, y_n\}$  is a basis.  $\square$