Some notes on modules
Hjalmar Rosengren, 9 September 2015

1 Bases of free modules

To understand the following discussion you must be familiar with the notions of *free module*, *finitely generated module* and *basis*, see the course literature.

It's easy to see that if two R-modules have bases with the same cardinality, then they are isomorphic. However, the converse is *not* true; a module can have two bases with different cardinalities. We give a concrete example of this phenomenon.

Consider infinite matrices $(a_{jk})_{j,k=1}^{\infty}$ with entries $a_{jk} \in \mathbb{R}$ (we could replace $\mathbb{R}$ by any ring). We assume that only finitely many elements in each column are non-zero. Thanks to this restriction, we can add and multiply matrices as usual, obtaining a ring R. Consider R as an R-module. Obviously, the identity matrix

$$e = \begin{bmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \\ \vdots & & & \ddots \end{bmatrix}$$

forms a basis of R with one element. Now consider the two matrices

$$f_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 1 & \\ \vdots & & & & & \ddots \end{bmatrix}, \qquad f_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0 & 1 & \\ \vdots & & & & & & \ddots \end{bmatrix}.$$

It is then easy to see that any $A \in R$ can be written uniquely as $A = A_1 f_1 + A_2 f_2$, where A_1 and A_2 are obtained from A by deleting all even and odd columns, respectively. Thus, f_1 and f_2 form a basis for R with two elements. For this ring, $R \simeq R^2$ as R-modules, an explicit isomorphism being $A \mapsto (A_1, A_2)$. By a variation of the same argument, $R \simeq R^n$ for any n.

For modules over *commutative* rings, one cannot construct such examples. Any two bases for a free module over a commutative ring have the same cardinality. This is (partially) proved by Brzezinski but we prefer to give a more pedestrian proof in the finite-dimensional case.

Proposition 1. *For a finitely generated free module M over a commutative ring R, any two bases have the same number of elements.*

Proof. First note that any basis of a finitely generated free module is finite. To see this, let $x_1, \dots, x_n$ be generators and $(e_i)_{i\in\Lambda}$ a basis. Expressing each x_j in terms of the basis elements, all coefficients outside a finite subset $\Lambda_j \subseteq \Lambda$ vanish. Consequently, taking $x \in M$ arbitrary, x can be expressed as a combination of basis elements indexed by the finite set $\Lambda_1 \cup \dots \cup \Lambda_n$. By the definition of basis, this set must be all of Λ.

Assume now that we have two bases $(e_j)_{j=1}^m$ and $(f_k)_{k=1}^n$ for M. We can write

$$e_j = \sum_{k=1}^{n} a_{jk} f_k, \qquad f_j = \sum_{k=1}^{m} b_{jk} e_k, \quad a_{jk},\ b_{jk} \in R.$$

If we plug one of these expressions into the other one, we find that the matrices $A = (a_{jk})$ and $B = (b_{jk})$ necessarily satisfy $AB = I_m$ and $BA = I_n$, where I_k is the identity matrix of order k. We want to prove that $m = n$. For a contradiction, assume $m > n$. We then create $(m \times m)$-matrices A' and B' by filling out the matrices A and B by zeroes, that is,

$$A' = \begin{bmatrix} A & 0 \end{bmatrix}, \qquad B' = \begin{bmatrix} B \\ 0 \end{bmatrix}.$$

It is now easy to compute

$$A'B' = I_m, \qquad B'A' = \begin{bmatrix} I_n & 0 \\ 0 & 0 \end{bmatrix}.$$

Taking determinants we get

$$\det(A')\det(B') = 1, \qquad \det(B')\det(A') = 0,$$

which is a contradiction (if we assume $1 \neq 0$ as part of our ring axioms). □

In the proof we used that

$$\det(AB) = \det(A)\det(B)$$

for matrices over commutative rings. Indeed, looking at the proof for real matrices found in any linear algebra textbook, it should be clear that it only uses general properties of commutative rings.

2 Direct sums and summands

We will now discuss direct sums of modules. Throughout, all modules will be over a fixed ring R.

Lemma 2. *Let M_1, M_2 be submodules of some module M. Then, the following are equivalent:*

(A) *Any element $x \in M$ can be written uniquely as $x = m_1 + m_2$, $m_i \in M_i$.*

(B) $M_1 + M_2 = M$ *and* $M_1 \cap M_2 = \{0\}$.

(C) *The map $(m_1, m_2) \mapsto m_1 + m_2$ is an isomorphism $M_1 \times M_2 \to M$.*

The proof is very easy and left to the reader. If these conditions are satisfied, we call M the (internal) *direct sum* of M_1 and M_2 and write $M = M_1 \oplus M_2$.

If K and L are R-modules, then $K \times L$ contains submodules $K' = K \times \{0\} \simeq K$ and $L' = \{0\} \times L \simeq L$ such that $K \times L = K' \oplus L'$. For this reason, $K \oplus L$ is often used as an alternative notation for $K \times L$ (external direct sum).

If K is a submodule of M, it is natural to ask whether there is a submodule L of M such that $M = K \oplus L$. If that is the case, we call K a *direct summand* of M and L a *complement* of M.

Not all submodules are direct summands; for instance, you may check that the $\mathbb{Z}$-module $\mathbb{Z}/4\mathbb{Z}$ contains a submodule isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is not a direct summand.

We will now give criteria for determining whether a submodule is a direct summand. We need some terminology. An *exact sequence* is a finite or infinite sequence of modules and homomorphisms

$$\cdots \to L \xrightarrow{f} M \xrightarrow{g} N \to \cdots$$

such that $\mathrm{Im}(f) = \mathrm{Ker}(g)$ at each step. A *short* exact sequence has the form

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0, \tag{1}$$

where $0 = \{0\}$ is the trivial R-module. This means that f is injective, $\mathrm{Im}(f) = \mathrm{Ker}(g)$ and g is surjective. Then, L is isomorphic to a submodule of M and N is isomorphic to M/L. Thus, up to isomorphisms, a short exact sequence has the form

$$0 \to L \to M \to M/L \to 0 \tag{2}$$

where L is a submodule of M.

Lemma 3. *Given a short exact sequence* (1)*, the following are equivalent:*

(A) *There is a homomorphism* $\phi : M \to L$ *with* $\phi \circ f = \mathrm{id}$.

(B) *There is a homomorphism* $\psi : N \to M$ *with* $g \circ \psi = \mathrm{id}$.

(C) *The submodule* $\mathrm{Im}(f) = \mathrm{Ker}(g)$ *in* M *is a direct summand.*

Proof. We prove the equivalence of (B) and (C). The equivalence of (A) and (C) is similar and left as an exercise.

Assuming (B), we show that $M = \mathrm{Im}(f) \oplus \mathrm{Im}(\psi)$. By Lemma 2, it is enough to check that $M = \mathrm{Im}(f) + \mathrm{Im}(\psi)$ and $\mathrm{Im}(f) \cap \mathrm{Im}(\psi) = \{0\}$. For the first part, we write $x = x_1 + x_2$, where $x_1 = x - \psi(g(x))$ and $x_2 = \psi(g(x))$. It is then easy to check that $x_1 \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ and, obviously, $x_2 \in \mathrm{Im}(\psi)$. For the second part, suppose $y \in \mathrm{Im}(f) \cap \mathrm{Im}(\psi)$, so $y = f(a) = \psi(b)$. Then $b = g(\psi(b)) = g(f(a)) = 0$ so $y = \psi(0) = 0$.

To show that (C) implies (B), let $M_1 = \mathrm{Ker}(g)$ and suppose there exists M_2 with $M = M_1 \oplus M_2$. Let h be the restriction of g to M_2. We claim that $h : M_2 \to N$ is an isomorphism. Indeed, it is injective since $\mathrm{Ker}(h) = \mathrm{Ker}(g) \cap M_2 = M_1 \cap M_2 = \{0\}$. To see that h is surjective, take $y \in N$ arbitrary and choose $x \in M$ with $g(x) = y$. Decomposing $x = x_1 + x_2$, $x_i \in M_i$, we have $y = g(x_1) + g(x_2) = 0 + h(x_2)$ so $y \in \mathrm{Im}(h)$. Since h is an isomorphism, so is $\psi = h^{-1}$, and it is clear that $g \circ \psi = \mathrm{id}$. □

We can now prove the following result, which will be the starting point for classifying finitely generated modules over a PID.

Lemma 4. *If $L \subseteq M$ is a submodule such that M/L is free, then L is a direct summand of M.*

Proof. Consider the exact sequence (2). We will apply criterion (B) in Lemma 3. Take a basis $e_1, \dots, e_n$ for M/L and pick for each j a representative $f_j \in M$ of the coset e_j. Define $\psi : M/L \to M$ by

$$\psi(x_1 e_1 + \cdots + x_n e_n) = x_1 f_1 + \cdots + x_n f_n, \qquad x_1, \dots, x_n \in R.$$

It is then easy to check that ψ satisfies the appropriate condition. □