NOTES ON LINEAR ALGEBRA OVER INTEGRAL DOMAINS

Contents

1. Introduction

These notes establish the classification of finitely generated modules over a principal ideal domain. We begin with several introductory sections on rank and basis, proving proving our main theorem. We follow essentially Samuel, "Algebraic Theory of Numbers", section 1.5, for our main result. Samuel's book on algebraic number theory. These notes were prepared for Basic Algebra, 60210, discussion on modules in December 2018.

2. Rank and basis

Let R be a ring and let M be a R-module with submodules M_1 and M_2. Consider the R-module homomorphism,

$f : M_1 \oplus M_2 \to M$, given by $f(x, y) = x + y$, for $x \in M_1$, $y \in M_2$.

We set $M_1 + M_2 = f(M_1 \oplus M_2) = \{x_1 + x_2 : x_1 \in M_1, x_2 \in M_2\}$. Since the image of R-module homomorphism is a submodule, it follows that $M_1 + M_2$ is a submodule of M.

By Theorem 4.3.3 in Ash, $f : M_1 \oplus M_2 \to M$ is a R-module isomorphism if and only if:

(1) $M = M_1 + M_2$, and

(2) $M_1 \cap M_2 = 0$.

When f is an isomorphism, we say $M = M_1 \oplus M_2$, or $M = M_1 + M_2$ is direct.

Let S be a subset of a R-module M.

Definition 2.1. *(i) We say S is R-linearly independent over if for any subset $v_1, \ldots, v_n$ of S, then $\sum_{i=1}^n a_i v_i = 0$ with $a_i \in R$ implies that $a_1 = a_2 = \cdots = a_n = 0$.*

(ii) We say S spans M if for any $v \in M$, there is $m \geq 0$ and $v_1, \ldots, v_m \in S$ and $a_1, \ldots, a_m \in R$ so that $v = \sum_{i=1}^m a_i v_i$.

(iii) We say S is a basis of M if S spans M and is R-linearly independent.

Recall that a R-module M is called *free* if M has a basis. The next result asserts that if M is a direct sum of two free modules, then M is free.

Lemma 2.2. *Let $M = M_1 + M_2$ be direct. Suppose $S_1 = \{v_1, \ldots, v_t\}$ is a basis of M_1 and $S_2 = \{w_1, \ldots, w_u\}$ is a basis of M_2. Then $T := S_1 \cup S_2$ is a basis of M.*

Proof : We first show that T is linearly independent, so suppose that
$\sum_{i=1}^{t} a_i v_i + \sum_{j=1}^{u} b_j w_j = 0$, $a_i, b_j \in R$.
Set $v = \sum_{i=1}^{t} a_i v_i$ and set $w = \sum_{j=1}^{u} b_j w_j = 0$. Note that $v \in M_1$ and $w \in M_2$.

Then by assumption, $v + w = 0$, so $v = -w \in M_1 \cap M_2 = 0$. Since $v = 0$, $\sum_{i=1}^{t} a_i v_i = 0$, so $a_i = 0, i = 1, \ldots, t$, since S_1 is a basis, and hence linearly independent. Since $w = 0$, $\sum_{j=1}^{u} b_j w_j = 0$, so $b_j = 0, j = 1, \ldots, u$, since S_2 is linearly independent. Hence T is linearly independent.

We now show that T generates M. Since $M = M_1 + M_2$, if $m \in M$, then $m = v + w$, with $v \in M_1$, and $w \in M_2$. Since S_1 generates M_1, $v = \sum_{i=1}^{t} a_i v_i$ for some $a_i \in R$. Since S_2 generates M_2, $w = \sum_{j=1}^{u} b_j w_j$, for some $b_j \in R$.

Then $m = v + w = \sum_{i=1}^{t} a_i v_i + \sum_{j=1}^{u} b_j w_j$, so T generates M.

Q.E.D.

Definition 2.3. *We say a R-module M is finitely generated if there exists a finite generating set S of M, or equivalently, if there is a finite subset $S \subset M$ such that if $v \in M$, then $v = \sum_{v_i \in S} a_i v_i$, with $a_i \in R$.*

By convention, the 0-submodule $\{0\}$ is generated by the empty set, and an empty sum $\sum_{i=1}^{0} r_i v_i = 0$..

Let R be an integral domain and let $F = Frac(R)$ be its fraction field. We regard $R \subset F$ via the injective map $a \mapsto \frac{a}{1}$. Then it follows that
$R^n = \{(a_1, \ldots, a_n) : a_i \in R\} \subset F^n = \{(\alpha_1, \ldots, \alpha_n) : \alpha_i \in F\}$.

Let $V \subset R^n$ be a R-submodule.

Let $FV := \{\alpha v : \alpha \in F, v \in V\} \subset F^n$.

Lemma 2.4. *FV is a F-subspace of F^n.*

Proof : It suffices to show that if $u_1, u_2 \in FV$ and $\lambda \in F$, then $u_1 + u_2 \in FV$ and $\lambda u_1 \in FV$.

We set $u_1 = \alpha_1 v_1$ and $u_2 = \alpha_2 v_2 \in FV$, with $v_1, v_2 \in V$, and $\alpha_1 = \frac{a_1}{b_1}, \alpha_2 = \frac{a_2}{b_2} \in F$, so $a_1, a_2, b_1, b_2 \in R$, and b_1, b_2 are both nonzero. Then

$$\alpha_1 v_1 + \alpha_2 v_2 = \frac{a_1}{b_1} v_1 + \frac{a_2}{b_2} v_2 = \frac{1}{b_1 b_2}(a_1 b_2 v_1 + b_1 a_2 v_2) \in FV,$$

since $a_1b_2v_1+b_1a_2v_2 \in V$ by definition of submodule. If $\lambda \in F$, then $\lambda \cdot \alpha_1 v_1 = (\lambda \cdot \alpha_1) \cdot v_1 \in FV$. Thus, FV is a F-subspace.

Q.E.D.

Definition 2.5. *Let V be a R-module. We define $rk_R(V)$ to be the maximum cardinality of a R-linearly independent subset S of V, provided one exists, and if none exists, we say $rk_R(V) = \infty$.*

Lemma 2.6. *Let $V \subset R^n$ be a R-submodule. Then $rk_R(V) = \dim_F(FV)$.*

Proof: Let S be a maximal R-linearly independent subset of V. We showed that FV is a finite dimensional subspace of F^n. Since $V \subset FV$, we may regard S as a subset of FV, and we first claim that S is linearly independent over F. Indeed, suppose there are $v_i \in S$ and $\alpha_i \in F$ with $\sum_{i=1}^n \alpha_i v_i = 0$. Let $\alpha_i = \frac{a_i}{b_i}$ with $a_i, b_i \in R$ and all $b_i \neq 0$. Let $b = b_1 \cdots b_n$ and let $c_i = \frac{b}{b_i}$ for $i = 1, \ldots, n$. Then $\sum_{i=1}^n \frac{1}{b} c_i a_i v_i = 0$, so that $\sum_{i=1}^n c_i a_i v_i = 0$. Since S is R-linearly independent, it follows that each $c_i a_i = 0$. Since each $c_i \neq 0$, we conclude that each $a_i = 0$, so each $\alpha_i = 0$, and our first claim follows. Since S is linearly independent over F, it follows that $|S| = k \leq n$, so S is finite, and we label $S = \{v_1, \ldots, v_k\}$. We now show that S is a maximal F-linearly independent subset of FV. Suppose by contradiction that $S \cup \{v\}$ is a F-linearly independent subset of FV. Then $v = \frac{a}{b} v_0$ for some $v_0 \in V$ and $a, b \in R$ with b nonzero, so that $bv = av_0$. Since S is a maximal R-linearly independent subset, we see that $\{av_0, v_1, \ldots, v_k\}$ is a R-linearly dependent subset of V. Hence, there exist $c, c_1, \ldots, c_k \in R$ so that $cav_0 + \sum_{i=1}^k c_i v_i = 0$ with at least one of $c, c_1, \ldots, c_k$ nonzero. Multiplying by $\frac{1}{b}$, we obtain $cv + \sum_{i=1}^k \frac{c_i}{b} v_i = 0$, and at least one of $c, c_1/b, \ldots, c_k/b$ is nonzero, and this contradicts the assumption that $S \cup \{v\}$ is F-linearly independent. We have now shown that S is a maximal F-linearly independent subset of FV, and hence S is a basis of FV, so that $\dim_F(FV) = |S| = rk_R(V)$.

Q.E.D.

Note that the lemma implies that the cardinality of a maximal R-linearly independent subset S of V is independent of the choice of S.

Proposition 2.7. *Let R be an integral domain, and let $V \subset R^n$ be a R-submodule.*

(1) $0 \leq rk_R(V) \leq n$.

(2) $rk_R(R^n) = n$.

(3) Let M_1, M_2 be R-submodules of R^n and suppose $M = M_1 + M_2$ is direct. Then $FM_1 \cap FM_2 = 0$, $FM_1 + FM_2 = F(M_1 + M_2)$, and $rk_R(M) = rk_R(M_1) + rk_R(M_2)$.

(4) Let $v_1, \ldots, v_r$ be a basis of a submodule M of R^n. Then $v_1, \ldots, v_r$ is a basis of FM, so $rk_R(M) = r$.

(5) Let $v \in M$ be nonzero. Then $\{v\}$ is a basis of $R \cdot v$, so $rk_R(R \cdot v) = 1$.

Proof : (1) and (2): Since $V \subset R^n$, it follows from definitions that $FV \subset FR^n = F^n$. Hence, by linear algebra over fields and the previous lemma,

$0 \leq rk_R(V) = \dim_F(FV) \leq \dim_F(F^n) = n$.

For (3), we first show that $FM_1 \cap FM_2 = 0$. For this, let $\alpha_1 v_1 \in FM_1$, and $\alpha_2 v_2 \in FM_2$, with

(*) $\alpha_1 = \frac{a_1}{b_1}$, $\alpha_2 = \frac{a_2}{b_2}$, for $v_i \in M_1$, $v_2 \in M_2$, $a_1, a_2 \in R$, and b_1, b_2 nonzero elements of R.

If $\alpha_1 v_1 = \alpha_2 v_2 \in FM_1 \cap FM_2$, then

$\frac{a_1}{b_1} v_1 = \frac{a_2}{b_2} v_2$, so $\frac{a_1 b_2}{b_1 b_2} v_1 = \frac{a_2 b_1}{b_1 b_2} v_2$.

Since $b_1 b_2 \neq 0$, then $a_1 b_2 v_1 = a_2 b_1 v_2 \in M_1 \cap M_2 = 0$. Since $b_2 \neq 0$,

$a_1 v_1 = {b_2}^{-1} a_2 b_1 v_2 = 0$, so $\alpha_1 v_1 = 0$. It follows that $FM_1 \cap FM_2 = 0$.

We next show that $FM_1 + FM_2 = F(M_1 + M_2)$. Indeed, let $v_1 \in M_1$ and $v_2 \in M_2$. Then if $\alpha \in F$, then $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2 \in FM_1 + FM_2$, so $F(M_1 + M_2) \subset FM_1 + FM_2$. Conversely, let $\alpha_1 v_1 \in FM_1$ and $\alpha_2 v_2 \in FM_2$ with α_1, α_2 as in (*) above. Then

$\alpha_1 v_1 + \alpha_2 v_2 = \frac{1}{b_1 b_2}(a_1 b_2 v_1 + a_2 b_1 v_2) \in F(M_1 + M_2)$, since $\frac{1}{b_1 b_2} \in F$ and $a_1 b_2 v_1 + a_2 b_1 v_2 \in M_1 + M_2$.

Given these observations,

$rk_R(M) = rk_R(M_1 + M_2) = \dim_F(F(M_1 + M_2)) = \dim_F(FM_1 + FM_2)$.

But from linear algebra over fields, if V_1 and V_2 are F-subspaces of F^n, then

$\dim_F(V_1 + V_2) = \dim_F(V_1) + \dim_F(V_2) - \dim_F(V_1 \cap V_2)$.

Applying this with $V_1 = FM_1$ and $V_2 = FM_2$ gives assertion (3), since $FM_1 \cap FM_2 = 0$.

We now prove assertion (5). It is clear from the definition of $R \cdot v$ that $\{v\}$ generates $R \cdot v$. Let $v \in R^n$ is nonzero, then $v = r_1 e_1 + \cdots + r_n e_n$ for some $r_1, \ldots, r_n \in R$ (here $e_1, \ldots, e_n$ are standard basis vectors of R^n.) Since $v \neq 0$, some $r_i \neq 0$. If $a \cdot v = 0$ for $a \in R$, then $a r_1 e_1 + \cdots + a r_n e_n = 0$, so since $\{e_1, \ldots, e_n\}$ is a basis of R^n, $a r_i = 0$. Since $r_i \neq 0$, it follows that $a = 0$. Hence, the set $\{v\}$ is linearly independent. It follows easily that $\{v\}$ is a basis of $F \cdot v = FR \cdot v$, so $\dim_F(F \cdot v) = 1$, and this completes the proof of (5).

We prove assertion (4) by induction on r, and note that the case $r = 0$ is trivial and the case $r = 1$ was proved as part of assertion (5). Let $M_1 = Rv_1 + \cdots + Rv_{r-1}$. Then it follows easily that $S_1 = \{v_1, \ldots, v_{r-1}\}$ is a basis of M_1. By induction, S_1 is a basis of FM_1 and $rk_R(M_1) = r - 1$. Let $M_2 = R \cdot v_r$. By (5), $\{v_r\}$ is a basis of M_2, and $rk_R(M_2) = 1$. By Lemma 2.2, it follows that $v_1, \ldots, v_r$ is a basis of $M = M_1 + M_2$. Note that $M_1 \cap M_2 = 0$ since $\{v_1, \ldots, v_r\}$ is a basis. Hence, $FM_1 \cap FM_2 = 0$ by assertion (3), and

$FM = F(M_1 + M_2) = FM_1 + FM_2 = \sum F \cdot v_i$ by induction. This proves (4).

Q.E.D.

Let M be a free finitely generated R-module with R-module isomorphism $\phi : M \to R^n$. Let $M_1 \subset M$ be a R-submodule. It follows that $\phi : M_1 \to \phi(M_1)$ is a R-module isomorphism. Hence, $rk_R(M_1) = rk_R(\phi(M_1))$.

Proposition 2.8. *Let M be a free finitely generated R-module with R-module isomorphism $\phi : M \to R^n$. Then*

(1) Let $M_1, M_2 \subset M$ be submodules. If $M_1 \cap M_2 = 0$, then $rk_R(M_1) + rk_R(M_2) = rk_R(M_1 + M_2)$.

(2) Let $M_1 \subset M$ be a free submodule with basis $v_1, \ldots, v_r$. Then $rk_R(M_1) = r$.

(3) If $M_1 \subset M$ is a submodule, then $0 \leq rk_R(M) \leq n$.

(4) If $v \in M$ is nonzero, then $rk_R(R \cdot v) = 1$.

Proof : For (1), note that $\phi(M_1) \cap \phi(M_2) = \phi(M_1 \cap M_2) = 0$. Thus, by (3) of Proposition 2.7,

$rk_R(\phi(M_1 + M_2)) = rk_R(\phi(M_1) + \phi(M_2)) = rk_R(\phi(M_1)) + rk_R(\phi(M_2))$, and this implies (1). For (2), it follows easily from definitions that $\phi(v_1), \ldots, \phi(v_r)$ is a basis of $\phi(M_1)$, and now (2) follows from (4) of Proposition 2.7. Assertion (3) is clear by (1) of Proposition 2.7, and Assertion (4) is clear by (5) of Proposition 2.7.

Q.E.D.

Note that a R-submodule M_1 of a free module M may not be generated by one element, but may still have $rk_R(M_1) = 1$. For example, let $R = F[x, y]$, the polynomial ring in two variables, and let $M = R$, which is free with basis $\{1\}$. Let $M_1 = (x, y)$. Then $M_1 \neq R \cdot v$ for any $v \in M_1$ since (x, y) is not a principal ideal. But $FM_1 = Fx + Fy = F$, so $rk_R(M_1) = 1$.

3. Linear forms

We discuss the R-linear maps from a R-module M to R. As before, R is a commutative ring.

Definition 3.1. *Let R be a ring and let M, N be R-modules. Then*

$\mathrm{Hom}_R(M, N) = \{\phi : M \to N : \phi \text{ is a } R - \text{module homomorphism}\}$.

For $f_1, f_2 \in \mathrm{Hom}_R(M, N)$, let $f_1 + f_2 : M \to N$ be defined by $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ for $x \in M$. For $r \in R$, let $r \cdot f_1 : M \to N$ be defined by $(r \cdot f_1)(x) = r \cdot (f_1(x))$. Note that $f_1 + f_2, r \cdot f_1 \in \mathrm{Hom}_R(M, N)$. Indeed, for the second assertion, let $a \in R$ and $x \in M$, and compute

$(r \cdot f_1)(a \cdot x) = r \cdot (f_1(a \cdot x)) = f_1(ra \cdot x) = f_1(ar \cdot x) = ar \cdot (f_1(x)) = a \cdot (r \cdot f_1)(x)$.

This requires that R is commutative, but $f_1 + f_2 \in \mathrm{Hom}_R(M, N)$ even when R is noncommutative, and we leave the easy verification to the reader.

Lemma 3.2. $\mathrm{Hom}_R(M, N)$ *is a R-module.*

We leave these assertions to the reader. They are quite easy.

We consider the special case when $N = R$, viewed as a R-module using multiplication in R. We let $M = R^n$, and for $i = 1, \ldots, n$, we define $p_i : R^n \to R$ by the formula $p_i(r_1, \ldots, r_n) = r_i$. It is routine to verify that $p_i \in \mathrm{Hom}_R(R^n, R)$.

Remark 3.3. *If R is a commutative ring, then $\mathrm{Hom}_R(R^n, R)$ has basis $p_1, \ldots, p_n$ as an R-module. In particular, $\mathrm{Hom}_R(R^n, R) \cong R^n$ is a free module, and the map $\phi \mapsto (\phi(e_1), \ldots, \phi(e_n))$ is a R-module isomorphism.*

4. Main theorem

In this section, R is a PID with fraction field F.

Theorem 4.1. *Let M be a free R-module of rank n and let N be a submodule of M. Then*

(i) N is free of rank q with $0 \leq q \leq n$,

(ii) If $N \neq 0$, then there is a basis $v_1, \ldots, v_n$ of M and nonzero elements $a_1, \ldots a_q$ of R such that $a_1 v_1, \ldots, a_q v_q$ is a basis of N and $a_i \mid a_{i+1}$ for $i = 1, \ldots, q-1$.

Proof. First note that if $N = 0$, then N is free of rank 0, and the assertion (ii) is vacuously satisfied. Thus, we may assume $N \neq 0$. Let $\phi \in \mathrm{Hom}_R(M, R)$. Then $\phi(N)$ is a submodule of R, and hence is an ideal I_ϕ. Since R is a PID, $I_\phi = (a_\phi)$, the principal ideal generated by a_ϕ. Let S be the collection of all principal ideals (a_ϕ) as ϕ ranges over elements of $\mathrm{Hom}_R(M, R)$. Let $u_1, \ldots, u_n$ be a basis of M, so that each $v \in M$ can be written uniquely as $v = r_1 u_1 + \cdots + r_n u_n$ with $r_1, \ldots, r_n \in R$. Then the map $p_i : M \to R$ given by $p_i(\sum_{j=1}^n r_j v_j) = r_i$ is easily to seen to be a R-module homomorphism. Since $N \neq 0$, there is $v \in N$ and an index i such that $p_i(v) \neq 0$. By definition, $p_i(v) \in p_i(N) = I_{p_i}$, so we see that $I_{p_i} \neq (0)$. Thus S contains a nonzero ideal. Since R is a PID, R is Noetherian by Proposition 3.2 of the notes on Ash, section 2.6, and thus, the collection S of ideals has a maximal element by Lemma 3.3 of the above referenced notes, which is necessarily nonzero. Choose $\phi \in \mathrm{Hom}_R(M, R)$ such that (a_ϕ) is maximal in S, so that $a_\phi \neq 0$, and if $(a_\phi) \subset (a_\tau)$ for $\tau \in \mathrm{Hom}_R(M, R)$, then $(a_\phi) = (a_\tau)$. By definition, there is $w \in N$ such that $\phi(w) = a_\phi$.

We claim that for every $\tau \in \mathrm{Hom}_R(M, R)$, $a_\phi \mid \tau(w)$. Indeed, consider the ideal $(a_\phi, \tau(w))$ of R generated by a_ϕ and $\tau(w)$. Since R is a PID, $(a_\phi, \tau(w)) = (d)$ for some $d \in R$, and by definition, $(a_\phi) \subset (d)$, and $d = r a_\phi + s\tau(w)$ for some $r, s \in R$. Since $\mathrm{Hom}_R(M, R)$ is a R-module, $\phi_{r,s} := r\phi + s\tau \in \mathrm{Hom}_R(M, R)$. By construction, $\phi_{r,s}(w) = r\phi(w) + s\tau(w) = r a_\phi + s\tau(w) = d$. Hence, $d \in (a_{\phi_{r,s}})$, so $(d) \subset (a_{\phi_{r,s}})$, and $(a_\phi) \subset (a_{\phi_{r,s}})$, and the latter is an ideal of S. Hence, by maximality of a_ϕ, we conclude from $(a_\phi) \subset (d) \subset (a_{\phi_{r,s}})$ that $(a_\phi) = (d)$, so that $\tau(w) \in (d)$ implies that a_ϕ divides $\tau(w)$.

In particular, $a_\phi \mid p_i(w)$ for $i = 1, \ldots, n$. We write $w = \sum_{i=1}^n r_i u_i$ in terms of our chosen basis of M. Since $r_i = p_i(w)$, we conclude that $a_\phi \mid r_i$ for all i, so that $r_i = b_i \cdot a_\phi$ for some

$b_i \in R$. Hence,

$$w = \sum_{i=1}^{n} a_\phi b_i u_i = a_\phi v_1, \text{ where } v_1 := \sum_{i=1}^{n} b_i u_i.$$

Thus, $a_\phi = \phi(w) = \phi(a_\phi v_1) = a_\phi \phi(v_1)$, and since R is an integral domain, we conclude that $\phi(v_1) = 1$. We now use this last assertion to decompose M and N as direct sums.

More precisely, we claim that

(1) $M = \ker(\phi) + R \cdot v_1$

(2) $N = (N \cap \ker(\phi)) + R \cdot w$, and both of these sums are direct.

To show that $M = \ker(\phi) + R \cdot v_1$, we observe that if $v \in M$, then $v = (v - \phi(v)v_1) + \phi(v)v_1$, and $\phi(v - \phi(v)v_1) = \phi(v) - \phi(v)\phi(v_1) = \phi(v) - \phi(v) = 0$. To show that the sum in (1) is direct, let $u = av_1 \in \ker(\phi)$ be an element of $\ker(\phi) \cap R \cdot v_1$. Then $0 = \phi(u) = a\phi(v_1) = a$, so that $a = 0$, and thus $u = 0$, so the intersection is zero. To show (2), let $y \in N$. Since $\phi(N) = (a_\phi)$, $\phi(y) = b \cdot a_\phi$ for some $b \in R$. Thus,

$$y = (y - bw) + bw = (y - ba_\phi v_1) + ba_\phi v_1,$$

and $\phi(y - ba_\phi v_1) = ba_\phi - ba_\phi = 0$ so $y - bw \in \ker(\phi)$. Since $R \cdot w \subset R \cdot v_1$, we see that $\ker(\phi) \cap R \cdot w = 0$ from the proof of directness of (1), so that the sum in (2) is direct.

We now prove assertion (i) by induction on the rank q of N, and note that $q \leq n$ by Proposition 2.8 (3). If $q = 0$, then $FN = 0$, so since $N \subset FN$, we conclude that $N = 0$, so N is free with empty basis. Now suppose $q > 0$ so $N \neq 0$. By (2) above, we know $N \cong (N \cap \ker(\phi)) + R \cdot w$ with the sum direct. Since $w \neq 0$, $R \cdot w$ has rank one by Proposition 2.8 (4). Hence, by Proposition 2.8 (1), it follows that the rank of $N \cap \ker(\phi) = q - 1$. Hence, by induction on q, $N \cap \ker(\phi)$ is free, and by Proposition 2.8 (3), it has a basis with $q - 1$ elements, which we denote by $w_2, \ldots, w_q$. By Lemma 2.2, it follows that $w = w_1, w_2, \ldots, w_q$ is a basis of N, so that N is free of rank q by Proposition 2.8 (3).

We prove assertion (ii) by induction on n. When $n = 0$, $M = 0$ and there is nothing to prove. If $n > 0$, we use the directness of (1) and the steps in the above paragraph to deduce that the rank of $\ker(\phi)$ is $n - 1$. By assertion (i), we know that the submodule $\ker(\phi)$ of M is free, and thus has a basis with $n - 1$ elements by Proposition 2.8 (3). We now apply induction on n to the pair $N \cap \ker(\phi) \subset \ker(\phi)$ to deduce that $\ker(\phi)$ has a basis $v_2, \ldots, v_n$ and there are elements $a_2, \ldots, a_q \in R$ such that $a_2 v_2, \ldots, a_q v_q$ is a basis of $N \cap \ker(\phi)$ and $a_i \mid a_{i+1}$ for $i = 2, \ldots, q - 1$. We let $a_1 = a_\phi$. Then $v_1, v_2, \ldots, v_n$ is a basis of M and $a_1 v_1, \ldots, a_q v_q$ is a basis of N using Lemma 2.2. It remains to show that $a_1 \mid a_2$. Since $v_1, \ldots, v_n$ is a basis of M, each $v \in M$ can be uniquely written $v = \sum_{j=1}^{n} r_j v_j$, and it is routine to check that if $q_i(v) = r_i$, then $q_i \in \mathrm{Hom}_R(M, R$. Let $\tau = q_1 + q_2 \in \mathrm{Hom}_R(M, R)$, so that $\tau(v_i) = 1$ if $i \in \{1, 2\}$ and $\tau(v_i) = 0$ if $i \geq 2$.. Then $a_1 = \tau(a_1 v_1) \in \tau(N) = (a_\tau)$ and $a_2 = \tau(a_2 v_2) \in \tau(N) = (a_\tau)$. Thus, $a_\phi = a_1 \in (a_\tau)$ so $(a_\phi) \subset (a_\tau)$. Since (a_ϕ) is maximal from the set S, we deduce that $(a_\phi) = (a_\tau)$, so that $a_2 \in (a_\phi) = (a_1)$ and $a_1 \mid \alpha_2$.

Q.E.D.