

NOTES ON LINEAR ALGEBRA OVER INTEGRAL DOMAINS

CONTENTS

1. Introduction	1
2. Rank and basis	1
3. Linear forms	4

1. INTRODUCTION

These notes establish some basic results about linear algebra over integral domains that are used in the classification of finitely generated modules over a principal ideal domain in Samuel's book on algebraic number theory. The assertions are very easy. They were prepared for Basic Algebra, 60210, discussion on modules in December 2009.

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,

$f : M_1 \oplus M_2 \rightarrow M$, 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, $f : M_1 \oplus M_2 \rightarrow M$ 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.

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 2.1. *Let $M = M_1 + M_2$ be direct. Suppose $S_1 = \{v_1, \dots, v_t\}$ is a basis of M_1 and $S_2 = \{w_1, \dots, w_u\}$ 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

$$\sum_{i=1}^t a_i v_i + \sum_{j=1}^u b_j w_j = 0, \quad a_i, b_j \in R.$$

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 $a_i = 0, i = 1, \dots, t$, since S_1 is a basis, and hence linearly independent. Since $w = 0$, $\sum_{j=1}^u b_j w_j = 0$, so $b_j = 0, j = 1, \dots, u$, 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 2.2. 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 $F = \text{Frac}(R)$ be its fraction field. We regard $R \subset F$ via the injective map $a \mapsto \frac{a}{1}$. Then it follows that

$$R^n = \{(a_1, \dots, a_n) : a_i \in R\} \subset F^n = \{(\alpha_1, \dots, \alpha_n) : \alpha_i \in F\}.$$

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

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

Lemma 2.3. 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 $a_1 b_2 v_1 + b_1 a_2 v_2 \in V$ 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 2.4. Let $V \subset R^n$ be a R -submodule. Then $\text{rk}_R(V) = \dim_F(FV)$.

Proposition 2.5. Let R be an integral domain, and let $V \subset R^n$ be a R -submodule.

(1) $0 \leq \text{rk}_R(V) \leq n$.

(2) $\text{rk}_R(R^n) = n$.

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

(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,

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

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 $v_1 \in M_1$, $v_2 \in M_2$, $a_1, a_2 \in R$, 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

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

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 $v = r_1 e_1 + \dots + r_n e_n$ for some $r_1, \dots, r_n \in R$ (here e_1, \dots, 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 $ar_1 e_1 + \dots + ar_n e_n = 0$, so since $\{e_1, \dots, e_n\}$ is a basis of R^n , $ar_i = 0$. 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 $M_1 = Rv_1 + \dots + Rv_{r-1}$. Then it follows easily that $S_1 = \{v_1, \dots, v_{r-1}\}$ 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 2.1, it follows that v_1, \dots, v_r is a basis of $M = M_1 + M_2$. Note that $M_1 \cap M_2 = 0$ since $\{v_1, \dots, v_r\}$ 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.

Definition 2.6. Let M be a free finitely generated R -module with R -module isomorphism $\phi : M \rightarrow R^n$. Let $M_1 \subset M$ be a R -submodule. Then $rk_R(M_1) = rk_R(\phi(M_1))$.

Proposition 2.7. Let M be a free finitely generated R -module with R -module isomorphism $\phi : M \rightarrow R^n$. 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, \dots, 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 2.5,

$rk_R(\phi(M_1 + M_2)) = rk_R(\phi(M_1) + \phi(M_2)) = rk_R(\phi(M_1)) + rk_R(\phi(M_2))$, and this implies (1). For (2), it follows easily from definitions that $\phi(v_1), \dots, \phi(v_r)$ is a basis of $\phi(M_1)$, and now (2) follows from (4) of Proposition 2.5. Assertion (3) is clear by (1) of Proposition 2.5, and Assertion (4) is clear by (5) of Proposition 2.5.

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

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

For $f_1, f_2 \in \text{Hom}_R(M, N)$, let $f_1 + f_2 : M \rightarrow N$ be defined by $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ for $x \in M$. For $r \in R$, let $r \cdot f_1 : M \rightarrow N$ be defined by $(r \cdot f_1)(x) = r \cdot (f_1(x))$. Note that $f_1 + f_2, r \cdot f_1 \in \text{Hom}_R(M, N)$. 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 $f_1 + f_2 \in \text{Hom}_R(M, N)$ even when R is noncommutative, and we leave the easy verification to the reader.

Lemma 3.2. $\text{Hom}_R(M, N)$ 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 $i = 1, \dots, n$, we define $p_i : R^n \rightarrow R$ by the formula $p_i(r_1, \dots, r_n) = r_i$. It is routine to verify that $p_i \in \text{Hom}_R(R^n, R)$.

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

We establish one further result concerning principal ideal domains.

Lemma 3.4. Let R be a principal ideal domain, and let $S = \{I_j\}_{j \in J}$ be a collection of ideals of R . Then S has a maximal element N ; i.e., $N \in S$ is an ideal, and if $I_j \in S$, and $N \subset I_j$, then $N = I_j$.

Proof : We suppose that there does not exist a maximal element N . Then for every $K \in S$, there exists $L \in S$ such that $K \subset L$ and $K \neq L$. Pick an ideal $I_1 \in S$. By assumption, there exists an ideal $I_2 \in S$ such that $I_1 \subset I_2$, but $I_1 \neq I_2$. Similarly, for each $j \geq 1$, there exists an ideal $I_{j+1} \in S$ such that $I_j \subset I_{j+1}$, but $I_j \neq I_{j+1}$. Thus,

$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$ is an infinite ascending chain of proper inclusions of ideals. But R is a PID, so it satisfies the ascending chain condition on ideals by the PID theorem proved in class (or Ash, Theorem 2.6.6 and Theorem 2.6.9).

Q.E.D.