7 Modules Over PIDs

2/24: **7.1. Uniqueness of the rational canonical form.** Let $I_1 \subset I_2 \subset \cdots$ be a sequence of ideals in a PID R. Assume that there is some natural number N such that $I_N = R$. Thus, if $I_i = (a_i)$, we have $a_{i+1} \mid a_i$ for all i and $1 = a_N = a_{N+1} = \cdots$. Let $M_i = R/I_i$, and let $M = M_1 \oplus M_2 \oplus \cdots$. For a prime p of R and for $k \geq 0$, we see that $p^k M/p^{k+1}M$ is a module over the *field* $R/(p)$, and is therefore a vector space over $R/(p)$. Denote by $d(p,k)$ its dimension. Define $n_i(p)$ to be the greatest nonnegative integer such that $I_i \subset (p^{n_i})$ — equivalently, $n_i(p)$ is the power of p that occurs in the factorization of a_i. However, $a_i = 0$ (equivalently $I_i = 0$) is a possibility, in which case we put $n_i(p) = \infty$.

(i) Prove that the sequence $d(p,0), d(p,1), \dots$ determines the sequence $n_1(p), n_2(p), \dots$.

Proof. We begin with some preliminary results.

We first exhibit an alternate form for M. For all $i \geq N$, we have that $1 = a_i$ and hence

$$M_i = R/I_i = R/(a_i) = R/(1) = R/R \cong 0$$

It follows if we let $\alpha = N - 1$ that

$$M = M_1 \oplus M_2 \oplus \cdots \cong M_1 \oplus \cdots \oplus M_\alpha = R/(a_1) \oplus \cdots \oplus R/(a_\alpha)$$

Since R is a PID (hence a UFD) and $a_1 \in R$, we know that a_1 has a unique factorization

$$a_1 = u p_1^{e_{1,1}} \cdots p_n^{e_{1,n}}$$

It follows by the Chinese Remainder Theorem (CRT) that

$$R/(a_1) \cong R/(p_1^{e_{1,1}}) \oplus \cdots \oplus R/(p_n^{e_{1,n}})$$

Additionally, since $a_\alpha \mid a_{\alpha-1} \mid \cdots \mid a_1$, we know that the unique factorization of *every* a_i will be expressed in terms of the same primes and lesser or equal (and possibly zero) exponents. Essentially, if $i < j$, then

$$a_i = u' p_1^{e_{i,1}} \cdots p_n^{e_{i,n}} \qquad\qquad a_j = u'' p_1^{e_{j,1}} \cdots p_n^{e_{j,n}}$$

where $e_{i,\ell} \geq e_{j,\ell}$ ($\ell = 1, \dots, n$). Thus, by combining the last several results, we have that

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_\alpha) \cong \left(\bigoplus_{\ell=1}^{n} R/(p_\ell^{e_{1,\ell}}) \right) \oplus \cdots \oplus \left(\bigoplus_{\ell=1}^{n} R/(p_\ell^{e_{\alpha,\ell}}) \right)$$

This will be useful later.

Next, we investigate some properties of the individual quotient modules. Let $j \in \{1, \dots, n\}$ be arbitrary. Consider the ideal $pR/(p_j^{e_{i,j}})$, first where $p = p_j$. In this case, we have that

$$p_j R/(p_j^{e_{i,j}}) \cong R/(p_j^{\max\{0, e_{i,j}-1\}})$$

Now consider the case where $p \neq p_j$. In this case, we can show that

$$pR/(p_j^{e_{i,j}}) \cong R/(p_j^{e_{i,j}})$$

Both of these results will be useful later.

We now begin the proof in earnest.

Let p be an arbitrary prime of R. We divide into two cases ($p \in \{p_1, \dots, p_n\}$ and $p \notin \{p_1, \dots, p_n\}$). First, suppose that $p \in \{p_1, \dots, p_n\}$. For the sake of simplicity, let $p = p_j$. To begin, rewrite the CRT expansion of $R/(a_i)$ to

$$R/(a_i) \cong \bigoplus_{\ell=1}^{n} R/(p_\ell^{e_{i,\ell}}) \cong \underbrace{\left(\bigoplus_{\substack{\ell=1 \\ \ell \neq j}}^{n} R/(p_\ell^{e_{i,\ell}}) \right)}_{N_{i,j}} \oplus R/(p_j^{e_{i,j}}) = N_{i,j} \oplus R/(p_j^{e_{i,j}})$$

for each $i \in \{1, \dots, \alpha\}$. Thus, we have that

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_\alpha) \cong [N_{1,j} \oplus R/(p_j^{e_{1,j}})] \oplus \cdots \oplus [N_{\alpha,j} \oplus R/(p_j^{e_{\alpha,j}})]$$

Let $\beta_j = \max\{i \in \{1, \dots, \alpha\} : e_{i,j} > 0\}$. Then combining several previous results, we have that

$$p^k M \cong [N_{1,j} \oplus R/(p_j^{\max\{0, e_{1,j} - k\}})] \oplus \cdots \oplus [N_{\beta_j,j} \oplus R/(p_j^{\max\{0, e_{\beta_j,j} - k\}})] \oplus N_{\beta_j+1,j} \oplus \cdots \oplus N_{\alpha,j}$$

and similarly for $k+1$. Note that each $N_{i,j}$ is unchanged under left multiplication by p^k because all of its component $R/(p_\ell^{e_{i,\ell}})$'s are unchanged under left multiplication by the coprime element p_j, as discussed above. It follows that

$$\begin{aligned} p^k M / p^{k+1} M \cong (R/(p_j^{\max\{0, e_{1,j} - k\}}))/(R/(p_j^{\max\{0, e_{1,j} - k - 1\}})) \\ \oplus \cdots \oplus (R/(p_j^{\max\{0, e_{\beta_j,j} - k\}}))/(R/(p_j^{\max\{0, e_{\beta_j,j} - k - 1\}})) \end{aligned}$$

since quotients of identical submodules in a direct sum are equal to zero, and these can be isomorphismed out of the quotient direct sum. Additionally, we have that

$$(R/(p_j^{\max\{0, e_{i,j} - k\}}))/(R/(p_j^{\max\{0, e_{i,j} - k - 1\}})) \cong R/(p_j)$$

for $k < e_{i,j}$ and

$$(R/(p_j^{\max\{0, e_{i,j} - k\}}))/(R/(p^{\max\{0, e_{i,j} - k - 1\}})) \cong (R/R)/(R/R) \cong 0/0 \cong 0$$

for $k \geq e_{i,j}$ ($i = 1, \dots, \beta_j$).

We are now prepared to count dimensions in $p^k M / p^{k+1} M$, i.e., to describe the desired relationship between the d's and n_i's. By the above and the assumption that $e_{i,j} \geq 1$, $p^0 M / p^{0+1} M$ is a β_j-dimensional vector space over the field $R/(p)$. As we increase k, eventually k will equal $e_{\beta_j,j}$. At this point, we will have $d(p, k-1) > d(p, k)$. In particular, suppose $d(p, k) = d(p, k-1) - \gamma$. Then $e_{\beta_j,j} = \cdots = e_{\beta_j - \gamma + 1, j}$ and $n_{\beta_j}(p) = \cdots = n_{\beta_j - \gamma + 1}(p) = e_{\beta_j,j} = k$. Continuing on, eventually we will get to $k = e_{\beta_j - \gamma, j}$. The change in the dimension d here will reveal the values of $n_{\beta_j - \gamma}(p)$ and possibly some $n_{\beta_j - \gamma - 1}(p), n_{\beta_j - \gamma - 2}(p), \dots$. Once we are past $e_{1,j}$, we could raise k infinitely high and still not alter the identity of the vector space any more (specifically as pertains to $i \in \{\beta_j + 1, \dots, \alpha\}$). Thus, we relate $n_i(p)$ and $d(p, k)$ by stating that

$$\boxed{n_i(p) = \min\{k : d(p, k) < i\}}$$

Note that for $i \in \{\beta_j + 1, \dots, \alpha\}$, this definition has an interpretation that may still make some sense. If $i > \beta_j$, then $\{k : d(p, k) < i\} = \emptyset$ since $d(p, k) \geq 0$ for all k by definition. In particular, since it would be incorrect to say that such an empty set has minimum equal to any integer, we may as well adopt the convention that $\min \emptyset$ is greater than all of the integers, i.e., $\min \emptyset = \infty$.

Now suppose that $p \notin \{p_1, \dots, p_n\}$, then we have by the above that

$$pM = \left(\bigoplus_{j=1}^{n} pR/(p_j^{e_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} pR/(p_j^{e_{\alpha,j}}) \right) \cong \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{\alpha,j}}) \right)$$

It follows inductively that

$$p^k M \cong \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{\alpha,j}}) \right)$$
$$p^{k+1} M \cong \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{\alpha,j}}) \right)$$

Thus, since $p^k M = p^{k+1} M$, we have that $p^k M / p^{k+1} M = 0$ for all $k \in \mathbb{Z}_{\geq 0}$. Therefore, $d(p,k) = 0$ for all $k \in \mathbb{Z}_{\geq 0}$ and thus, consistent with the above (under the convention $\beta_j = 0$), we may take $n_i(p) = \infty$ $(i = 1, \ldots, \alpha)$. ☐

(ii) Deduce that if $M \cong N$ where $N = N_1 \oplus N_2 \oplus \cdots$ and $N_i = R/J_i$ for an increasing sequence of ideals $J_1 \subset J_2 \subset \cdots$, then $I_n = J_n$ for all $n \in \mathbb{N}$.

Proof. Since R is a PID, each $J_i = (b_i)$ for some $b_i \in R$. Moreover, the increasing sequence condition implies the divisibility condition $b_2 \mid b_1$, $b_3 \mid b_2$, etc. Since

$$N = R/(b_1) \oplus R/(b_2) \oplus \cdots$$

this divisibility condition implies that b_1 annihilates each $R/(b_i)$ and, hence, N itself. Moreover, any factor of b_1 would miss some part of $R/(b_1)$, so b_1 is minimal. Thus, $\mathrm{Ann}(N) = (b_1)$. We can show in an analogous manner using the analogous conditions on M that $\mathrm{Ann}(M) = (a_1)$. But since $M \cong N$, we have that

$$(b_1) = \mathrm{Ann}(N) = \mathrm{Ann}(M) = (a_1)$$
$$b_1 = a_1$$

In particular, this proves that $I_1 = J_1$. More importantly, however, it pairs with the divisibility condition to demonstrate that the prime factorization of each b_i is a product of the same n primes $p_1, \ldots, p_n$. These primes in the factorizations will be raised to certain powers that are bounded by $e_{1,1}, \ldots, e_{1,n}$, respectively.

We can determine the exact values of the primes' exponents via comparison of the sequences $d(p_j, 0), d(p_j, 1), \ldots$ from part (i) in both M and N. In particular, since $M \cong N$, $p_j^k N / p_j^{k+1} N$ will follow the same dimension sequence $d(p_j, 0), d(p_j, 1), \ldots$ as that generated by $p_j^k M / p_j^{k+1} M$. Note that this observation justifies using a notation for the sequence that does not distinguish between N and M. To conclude, we can apply part (i) to learn that the sequences $d(p_j, 0), d(p_j, 1), \ldots$ as applied to N generate the exponents $e_{1,1}, \ldots, e_{\alpha,n}$. In particular, these exponents that match the corresponding ones in M. ☐

7.2. Let K be the fraction field of the PID R. We regard K as an R-module and regard $R \subset K$ as an R-submodule.

(i) Show that K/R is a torsion R-module.

Proof. To prove that K/R is a torsion R-module, it will suffice to show that for all $m + R \in K/R$, there exists a nonzero $a \in R$ such that $a(m + R) = 0 + R$. Let $m + R \in K/R$ be arbitrary. Pick any $a \in R$. Then since $am \in Rm \subset R = 0 + R$, $a(m + R) = am + R = 0 + R$, as desired. ☐

(ii) We have shown that every torsion R-module is the direct sum of its p-primary components. The p-primary component of K/R is S/R, where S is an R-submodule of K. Do you recognize S? *Hint*: You encountered it in fourth week.

Proof. Let $p \in R$ be a prime. By definition, the p-primary component S/R of the R-module K/R is the set of all $a/b + R \in K/R$ such that $p^k(a/b + R) = 0 + R$ for some $k \in \mathbb{Z}_{\geq 0}$. The last expression in the previous sentence is equivalent to $p^k a/b \in R$. But this will be true iff

$b \mid p^k$, i.e., if $b = p^\ell$ for some nonnegative integer $\ell \leq k$. Thus, S/R is equivalently the set of all $a/p^\ell + R \in K/R$ for $\ell \in \mathbb{Z}_{\geq 0}$. Evidently, this is the image of R_p under the canonical surjection, so

$$\boxed{S = R_p}$$

□

7.3. Given subrings A, B of a ring C, it is not true that $A + B$ is a subring in general. But here is an example where it is indeed a subring: Let $C = F(X)$ where F is a field, let $A = F[X]$, let $a \in F$, and let B be the image of the unique ring homomorphism $\phi : F[T] \to F(X)$ such that $\phi(c) = c$ for all $c \in F$ and $\phi(T) = (X - a)^{-1}$. Prove that...

(i) $A \cap B = F$;

Proof. We proceed via a bidirectional inclusion proof.

Suppose first that $c \in F$. Then $c \in F[X] = A$ by definition. Additionally, since $c \in F[T]$ by definition and $\phi(c) = c$ by the definition of ϕ, we have that $c \in \text{im}(\phi) = B$. Therefore, since $c \in A$ and $c \in B$, $c \in A \cap B$, as desired.

Now suppose that $c \in A \cap B$. Since $c \in A$, we know that c is a polynomial in X with coefficients in F. Additionally, by the universal property of the polynomial ring, we know that $\phi = \text{ev}_{(X-a)^{-1}}$. Consequently, $B = \text{im}(\phi) = F[(X - a)^{-1}]$. It follows that if c is the image of any nonconstant polynomial in $F[T]$, a has a nontrivial denominator. But this would contradict our earlier statement that $c \in F[X]$. Thus, c must be the image of some constant. In particular, it follows by the definition of ϕ that $c \in F$, as desired. □

(ii) $A + B$ equals the subring S of the previous problem, where $R = F[X]$ and $p = (X - a)$.

Proof. Analogy to previous: $C = K$ and $A = R$. So $S = R_p = F[X]_{(X-a)}$.

$F[X] + F[(X - a)^{-1}] = F[X]_{(X-a)}$. Invoke the Euclidean algorithm on elements in the right set. Divide by $(X - a)^n$.

The subring S of the previous problem, rephrased in terms of this problem, is

$$S = R_p = F[X]_{(X-a)}$$

Thus, to prove that $A + B = S$, it will suffice to show that $F[X] + F[(X - a)^{-1}] = F[X]_{(X-a)}$. We proceed once again via a bidirectional inclusion proof.

Suppose first that $p/(X - a)^n \in F[X]_{(X-a)}$, where $n \in \mathbb{N}$. By the Euclidean algorithm for monic polynomials, we know that

$$p(X) = q(X) \cdot (X - a)^n + r(X)$$
$$\frac{p(X)}{(X - a)^n} = q(X) + \frac{r(X)}{(X - a)^n}$$

for some $q, r \in F[X]$ with $\deg(r) < n$. From here, we cam resolve $r(X)/(X - a)^n$ into a polynomial in $(X - a)^{-1}$ using the method of partial fractions. Therefore, as the sum of a term in $F[X]$ and a term in $F[(X - a)^{-1}]$, $p/(X - a)^n \in F[X] + F[(X - a)^{-1}]$, as desired.

Now suppose that $p + q \in F[X] + F[(X - a)^{-1}]$. Add all terms together with least common denominator $(X - a)^n$, where n is the degree of $f \in F[T]$ whose image under ϕ is q. This yields a rational function equal to $p + q$ in $F[X]_{(X-a)}$, as desired. □

7.4. Let R be a commutative ring. The **derivative** (of $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$), denoted by f', is defined by $f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$. Assume that R is a subring of a commutative ring A. Let M be an A-module. An ***R*-derivation** (of A with values in M) is a function $D : A \to M$ that satisfies...

(1) $D(a + b) = D(a) + D(b)$ for all $a, b \in A$;

(2) $D(ab) = aD(b) + bD(a)$ for all $a, b \in A$;

(3) $D(c) = 0$ for all $c \in R$.

Prove that $D(f) = f'$ is an R-derivation D of $R[X]$ with values in $R[X]$ that satisfies $D(X) = 1$.

Proof. To prove that D is an R-derivation, it will suffice to check Properties 1-3.

Property 1: Let $a, b \in R[X]$ be arbitrary. Suppose $a = a_0 + \cdots + a_nX^n$ and $b = b_0 + \cdots + b_mX^m$. WLOG let $n \leq m$. Then

$$\begin{aligned}
D(a+b) &= (a+b)' \\
&= [(a_0+b_0) + \cdots + (a_n+b_n)X^n + b_{n+1}X^{n+1} + \cdots + b_mX^m]' \\
&= (a_1+b_1) + \cdots + n(a_n+b_n)X^{n-1} + (n+1)b_{n+1}X^n + \cdots + mb_mX^{m-1} \\
&= (a_1 + \cdots + na_nX^{n-1}) + (b_1 + \cdots + mb_mX^{m-1}) \\
&= a' + b' \\
&= D(a) + D(b)
\end{aligned}$$

as desired.

Property 2: Let $a, b \in R[X]$ be arbitrary. Suppose $a = a_0 + \cdots + a_nX^n$ and $b = b_0 + \cdots + b_mX^m$.

WLOG let $n \leq m$. Then

$$\begin{aligned}
aD(b) + bD(a) &= aD(b) + D(a)b \\
&= [a_0 + \cdots + a_nX^n] \cdot [b_0 + \cdots + b_mX^m]' \\
&\quad + [a_0 + \cdots + a_nX^n]' \cdot [b_0 + \cdots + b_mX^m] \\
&= [a_0 + \cdots + a_nX^n] \cdot [b_1 + \cdots + mb_mX^{m-1}] \\
&\quad + [a_1 + \cdots + na_nX^{n-1}] \cdot [b_0 + \cdots + b_mX^m] \\
&= \sum_{r=0}^{m+n-1} \left(\sum_{p=0}^{r} a_p(r-p+1)b_{r-p+1} \right) X^r + \sum_{r=0}^{m+n-1} \left(\sum_{p=0}^{r} (p+1)a_{p+1}b_{r-p} \right) X^r \\
&= \sum_{r=0}^{m+n-1} \left(\sum_{p=0}^{r} a_p(r-p+1)b_{r-p+1} + \sum_{p=0}^{r} (p+1)a_{p+1}b_{r-p} \right) X^r \\
&= \sum_{r=1}^{m+n} \left(\sum_{p=0}^{r-1} a_p(r-p)b_{r-p} + \sum_{p=0}^{r-1} (p+1)a_{p+1}b_{r-p-1} \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} \left(\sum_{p=0}^{r-1} (r-p)a_pb_{r-p} + \sum_{p=1}^{r} pa_pb_{r-p} \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} \left(ra_0b_r + \sum_{p=1}^{r-1} (r-p)a_pb_{r-p} + \sum_{p=1}^{r-1} pa_pb_{r-p} + ra_rb_0 \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} \left(ra_0b_r + \sum_{p=1}^{r-1} ra_pb_{r-p} + ra_rb_0 \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} r \left(a_0b_r + \sum_{p=1}^{r-1} a_pb_{r-p} + a_rb_0 \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} r \left(\sum_{p=0}^{r} a_pb_{r-p} \right) X^{r-1} \\
&= \left[\sum_{r=0}^{m+n} \left(\sum_{p=0}^{r} a_pb_{r-p} \right) X^r \right]' \\
&= (ab)' \\
&= D(ab)
\end{aligned}$$

as desired.

<u>Property 3</u>: Let $c \in R$ be arbitrary. Then

$$D(c) = c' = 0$$

as desired.

Lastly, we have by that

$$D(X) = X' = 1$$

as desired. □

7.5. (i) Let $a \in R$ and let $f \in R[X]$, where R is a commutative ring. a is said to be a **root** (resp. **repeated root**) of f if f is a multiple of $(X - a)$ (resp. $(X - a)^2$). Prove that $f(a) = f'(a) = 0$ iff f is a multiple of $(X - a)^2$.

Proof. Suppose first that f is a multiple of $(X-a)^2$. Then $f(X) = q(X)\cdot(X-a)^2$ for some $q \in R[X]$. It follows that
$$f(a) = q(a)\cdot(a-a)^2 = q(a)\cdot 0 = 0$$
Additionally, Problem 7.4 tells us that the normal product rule of differentiation applies even when the R in $R[X]$ is an arbitrary commutative ring, not just when $R = \mathbb{R}$. Thus,
$$f'(X) = q'(X)\cdot(X-a)^2 + q(a)\cdot(X^2 - 2aX + a^2)' = q'(X)\cdot(X-a)^2 + q(a)\cdot(2X-2a)$$
It follows that
$$f'(a) = q'(a)\cdot(a-a)^2 + q(a)\cdot(2a-2a) = q'(a)\cdot 0 + q(a)\cdot 0 = 0+0 = 0$$
as desired.

Now suppose that $f(a) = f'(a) = 0$. Since $f(a) = 0$, we have by the application of the Euclidean algorithm in Lecture 3.1 that
$$f(X) = q(X)\cdot(X-a)$$
for some $q \in R[X]$. Similarly, $f'(a) = 0$ implies that
$$f'(X) = \tilde{q}(X)\cdot(X-a)$$
for some $\tilde{q} \in R[X]$. To relate these two equations, we'll differentiate the first one. This yields
$$f'(X) = q(X)\cdot(X-a)' + q'(X)\cdot(X-a) = q(X)\cdot 1 + q'(X)\cdot(X-a) = q(X) + q'(X)\cdot(X-a)$$
This implies that
$$\begin{aligned} q(X) + q'(X)\cdot(X-a) &= \tilde{q}(X)\cdot(X-a) \\ q(X) &= [\tilde{q}(X) - q'(X)]\cdot(X-a) \end{aligned}$$
i.e., that $q(X)$ is a multiple of $X-a$, itself. Define $r(X) = \tilde{q}(X) - q'(X)$. Then
$$f(X) = q(X)\cdot(X-a) = r(X)\cdot(X-a)\cdot(X-a) = r(X)\cdot(X-a)^2$$
Therefore, f is a multiple of $(X-a)^2$, as desired. □

(ii) Let F be a subfield of a field E. Let $a \in E$ and let $f \in F[X]$. Show that if a is a repeated root of f, then there is some $g \in F[X]$ such that...
 (1) $\deg(g) > 0$;
 (2) Both f and f' are multiples of g in $F[X]$.

Proof. Consider the ring homomorphism $\mathrm{ev}_a : F[X] \to E$. More specifically, consider $\ker(\mathrm{ev}_a)$. Since $F[X]$ is a PID and kernels are ideals, we know that $\ker(\mathrm{ev}_a) = (g)$ for some $g \in F[X]$. Since a is a repeated root of f, part (i) implies that $f(a) = f'(a) = 0$. Thus, $f, f' \in \ker(\mathrm{ev}_a) = (g)$, so both f and f' are multiples of g. Additionally, we know that $\deg(g) > 0$ since the only constant polynomial that "maps" a to 0 is the zero polynomial, and f nonzero an element of (g) implies that 0 is not the generator of the kernel. □

7.6. This is essentially a repetition of the last problem from HW6 but by a slightly different method.

Let $F[X]_{<m}$ be the collection of $a \in F[X]$ such that $\deg(a) < m$. Let $f, g \in F[X]$ be polynomials of degrees d and e, respectively. Define $T : F[X]_{<e} \oplus F[X]_{<d} \to F[X]_{<d+e}$ by $T(a,b) = af + bg$. Note that T is a linear transformation of F-vector spaces, with domain and target of the same dimension.

(i) Deduce that $\gcd(f,g) = 1$ iff every $h \in F[X]$ with $\deg(h) < d+e$ can be expressed as $af + bg$ for some $a, b \in F[X]$ satisfying $\deg(a) < e$ and $\deg(b) < d$.

Proof. Suppose first that $\gcd(f, g) = 1$. Then there exist $\tilde{a}, \tilde{b} \in F[X]$ such that $\tilde{a}f + \tilde{b}g = 1$. Proving the desired claim is equivalent to proving that T is surjective. Since T maps like-dimensional vector spaces, it will suffice to show that T is injective. Suppose $T(a, b) = T(a', b')$. Then $af + bg = a'f + b'g$. Equivalently,

$$\begin{aligned}(a - a')f + (b - b')g &= 0\\ a &= a' - \frac{b - b'}{f}g\\ a &\in a' + (g)\end{aligned}$$

Since g has degree e and $F[X]/(g) \cong \{h \in F[X] : \deg(h) < e\}$ by Lecture 3.1, there is a unique $\tilde{a} \in F[X]_{<e}$ such that $\tilde{a} + (g) = a + (g) = a' + (g)$. It follows that we must have $a = \tilde{a}$ and $a' = \tilde{a}$, thereby proving that $a = a'$ by transitivity. An analogous argument can show that $b = b'$. Thus $(a, b) = (a', b')$ as desired.

Now suppose that every $h \in F[X]$ with $\deg(h) < d + e$ can be expressed as $af + bg$ for some $a, b \in F[X]$ satisfying $\deg(a) < e$ and $\deg(b) < d$. Let $h = 1$. Clearly $\deg(h) = 0 < d + e$ in this case. It follows by the supposition that $h = af + bg$ for some $a, b \in F[X]$ satisfying $\deg(a) < e$ and $\deg(b) < d$. Thus, $1 = h = af + bg \in (f, g)$, so we must have $\gcd(f, g) = 1$, as desired. □

(ii) The **resultant** (of f, g), denoted by $\mathrm{Res}(f, g)$, is the determinant of T. To define the latter, one requires a basis for the source and target. In particular,

$$(1, 0), (X, 0), \dots, (X^{e-1}, 0), (0, 1), (0, X), \dots, (0, X^{d-1})$$

is the basis for $F[X]_{<e} \oplus F[X]_{<d}$ and

$$1, X, \dots, X^{d+e-1}$$

is the basis for $F[X]_{<d+e}$.

Deduce that $\gcd(f, g) = 1$ iff $\mathrm{Res}(f, g) \neq 0$.

Proof. Suppose first that $\gcd(f, g) = 1$. Then by part (i), every $h \in F[X]$ with $\deg(h) < d + e$ can be expressed as $af + bg$ for some $a, b \in F[X]$ satisfying $\deg(a) < e$ and $\deg(b) < d$. It follows that T is surjective. Thus, since its domain and range have the same dimension, it is invertible as well. Therefore, it is nonsingular and hence $\mathrm{Res}(f, g) \neq 0$.

Now suppose that $\mathrm{Res}(f, g) \neq 0$. Then T is nonsingular and hence it is invertible. Thus, for the same reason as above, T is surjective. In particular, 1 is in the range of T, so there must exist $a, b \in F[X]$ such that $af + bg = T(a, b) = 1$. It follows that $1 = af + bg \in (f, g)$. Therefore, $\gcd(f, g) = 1$. □

7.7. Given an R-module M and $a \in R$, denote by $a_M : M \to M$ the function $a_M(m) = am$ for all $m \in M$. Now consider $M = R/(p^2) \oplus R/(p)$ where R is a PID and $p \in R$ is a prime. Let N be a submodule of M which has the property that $T(N) \subset N$ for every R-module self-isomorphism $T : M \to M$. Prove that N is one of the following four submodules: $0, M, pM, \ker(p_M)$. *Note*: The above problem is also valid for $(R/(p^2))^m \oplus (R/(p))^n$.

Proof. If $N = 0, M$, then the statement obviously holds. Thus, we concern ourselves with the case where $N \notin \{0, M\}$. In this case, we want to show that $N = pM$ or $N = \ker(p_M)$. We know that

$$pM = pR/(p^2) \oplus 0 \qquad \ker(p_M) = pR/(p^2) \oplus R/(p)$$

$\ker(p_M)$ is a 2D vector space over $R/(p)$. We want to show that $N \cap \ker(p_M) \neq 0$ iff $N \neq 0$. We know that $pN \subset N$ by the definition of N as a submodule. Let $n \in N$ be nonzero. Suppose $n \notin \ker(p_M)$. Then $pn \in \ker(p_M)$. We know that $pn \in N$ as well. Thus, $pn \in N \cap \ker(p_M)$.

$N \cap \ker(p_M) \subset \ker(p_M)$. Thus, $N \cap \ker(p_M)$ is either a 1D or a 2D vector space over $R/(p)$. We want to show that if it's 2D, then it equals $\ker(p_M)$, and if it's 1D, then it equals pM. 2D case: We know that

$N \cap \ker(p_M) \subset \ker(p_M)$. 2D implies that $N \subsetneq \ker(p_M)$. Thus, either $N = \ker(p_M)$ or $N \supsetneq \ker(p_M)$. In the first case, we are done. In the second case, we can show that this implies that $N = M$. 1D case: We know that $pM \cap \ker(p_M) = p_M$. Assume $N \neq pM$. Then $N \cap \ker(p_M) = \langle (pa, 1) \rangle$. But T exists, where $T : M \to M$ sends $T(1, 0) = (1, 0)$ and $T(0, 1) = (p, 1)$. Therefore we must have $N \cap \ker(p_M) = pM$.

Suppose that $N \supsetneq pM$. $N/pM \subset M/pM$. Then use $T(1, 0) = (1, 1)$ and $T(0, 1) = (0, 1)$. $\square$