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 $d(p,0), d(p,1), \dots$ determine the sequence $n_1(p), n_2(p), \dots$.

(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 $n \in \mathbb{N}$.

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.

(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.

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 $\alpha \in F$, 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) $A \cap B = F$;

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

7.4. Let R be a commutative ring. The **derivative** (of $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$), denoted by f', is defined by $f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$. 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 $D(X) = 1$.

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. $(X - a)^n$ for some $n \in \mathbb{N}$). Prove that $f(a) = f'(a) = 0$ iff f is a multiple of $(X - a)$.

(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 $F[X]$.

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 $\deg(b) < d$.

(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,

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

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

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

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

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

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 $T(N) \subset M$ 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 $(R/(p^2))^m \oplus (R/(p))^n$.