Day 4: Modules over a PID

Tom Gannon

August 17, 2017

1 Introduction

Today we'll show that given any principal ideal domain R, any torsion free R module M is isomorphic to a the free module R^m for some m. This comes up a lot in working over *Discrete Valuation Rings*, the natural setting where a lot of number theory occurs.

1.1 Primer on Principal Ideal Domains

Recall that a *Principal Ideal Domain* R is an integral domain R such that any ideal $I \subset R$ can be written $I = Ra$ for some element $a \in R$. One of the reasons we like to work with principal ideal domains is that is that if we can show that the set of all elements of an ring that satisfy a property $\mathscr{P}$ is an ideal, then we are guaranteed an element $a \in R$ such that a given $r \in R$ has property $\mathscr{P}$ if and only if $a|r$. The other reason we work with PIDs are that we have a *Bézout Identity*:

Exercise 1.1. *(PIDs Satisfy Bézout Identity): Assume $a_1, ..., a_n$ are elements of a PID R. Determine a notion of a greatest common divisor of $\{a_1, ..., a_n\}$, and let d denote this greatest common divisor. Show that if $e \in R$ such that $e|a_i$ for all i, $e|d$. Moreover, show that the **Bézout Identity** holds, that is, there exist $r_i \in R$ such that $r_1a_1 + ... + r_na_n = d$.*

Exercise 1.2. *(UFDs Don't Satisfy Bézout Identity) Determine the notion of a greatest common divisor in a unique factorization domain. Let $S := k[x, y]$ where k is some field. Then S is a UFD. Show that for all $r, s \in S, rx + sy \neq gcd(x, y)$.*

1.2 Primer on Modules

Recall that a *module* M over a ring R is a definition you can Google, and that we say M is *torsion free* if $r \in R, m \in M$ and $rm = 0$ implies either $r = 0$ or $m = 0$.

Exercise 1.3. *(Torsion Free Hypothesis is Necessary) Show that if M is a non torsion free module over a principal ideal domain R, then for all $k \in \mathbb{N}, M \ncong R^k$.*

2 Primer on Modules over a Principal Ideal Domain

Theorem 2.1. *Let M be a torsion free module over a principal ideal domain R that can be generated with n elements and cannot be generated by any fewer number of elements. Then $M \cong R^k$.*

Proof. Induction on n. For the inductive step, assume $n > 1$ and that if N is a torsion free module over a R that can be generated with $n - 1$ elements and cannot be generated by any fewer number of elements, $N \cong R^{n-1}$. Let $m_1, ..., m_n$ be a set of minimal generators for M. Then there is a "natural" map $\phi : R^n \to M$.

Exercise 2.2. *Determine what ϕ should be, and argue why this immediately implies that ϕ is a module morphism (i.e. an $R-$"linear" map) and that ϕ is surjective. Conclude $M \cong R^n/ker(\phi)$.*

Thus is suffices to show that $W := ker(\phi)$ is trivial. Assume it isn't.

Let's set up some notation. Let $\pi_i : R^n \to R$ be projection onto the i^{th} coordinate, and $\zeta_i : W \to R$ defined to be the composite of inclusion $W \hookrightarrow R^n$ with π_i. We claim that $W = Rm$ for some $m \in M$.

Exercise 2.3. *(Kernel Has Rank $\leq$ 1) Show there exists an i such that ζ_i is not the zero map. Swapping generators if necessary, we assume that $\zeta := \zeta_n \neq 0$. Show there exists a nonzero $x \in R^n$ such that $W = Rx$. (Hint: Show that if the last coordinate of two elements of W agree, then the vectors themselves agree. Then let I denote the set of all elements $r_n \in R$ with $r_1e_1 + ... + r_ne_n \in W$.)*

Exercise 2.4. *(Almost basis completion) Show that given any element nonzero*[1] $x \in M$*, there exists a* $b \in R$ *and a basis of* R^n*, say,* $\{y_1, ..., y_n\}$ *such that* $by_1 = x$*. (Hint: Let* $x = (x_i)$ *componentwise and let* $b := gcd(x_1, ..., x_n), y_1 = \frac{1}{b}x$*. Then there exists* r_i *such that* $r_1\frac{x_1}{d} + ... + r_n\frac{x_n}{d} = 1$*. Let* $\Phi : R^n \to R$ *via* $\Phi(b_1, ..., b_n) = r_1b_1 + ... + r_nb_n$*. Then* $x = \Phi(x)y_1 + (x - \Phi(x)y_1)$ *to show* $R^n \cong Ry_1 \oplus ker(\Phi)$*.)*

Exercise 2.5. *Combine the last two exercises to contradict the assumption that our generating set was minimal. (Hint: What assumption haven't we used yet?)*

□

This result is the result that is used a lot in the specific applications of Discrete Valuation Rings and the like, which will be covered on like, day one of the course. But in the meantime, know that there's a stronger version of the theorem that gives a lot more power, whose proof isn't that much harder than this proof and can be found in Dummit and Foote:

Theorem 2.6. *(Fundamental Theorem of Modules over a Principal Ideal Domain) Let* M *be a finitely generated module over a principal ideal domain* R*. Then there exists a unique* $n \in \mathbb{N}$ *(including the possibility of* $n = 0$*) such that* $M \cong R^n \oplus R/(a_1) \oplus ... \oplus R/(a_m)$ *for some* $a_1|a_2|...|a_m$ *in* R*.*

Exercise 2.7. *(Finite Generation Hypothesis is Necessary) Determine a torsion free* R *module that is not a direct sum (even of infinite index!) of copies of* R*. (Hint: You learned the specific example you need in high school or before).*

Exercise 2.8. *(Finite Fields Are Cyclic) Assuming the Fundamental Theorem of Modules over a Principal Ideal Domain, show that the multiplicative group of a finite field is a cyclic group.*

[1] This also trivially holds for $x = 0$, but a hint is that the proof is different if x is nonzero.