Lecture 3

Domenico Valloni

1 Finitely generated modules over P.I.D

The aim of this lecture is to show how to classify finitely generated modules over PID. For instance, if we choose $R = \mathbb{Z}$, we know that finitely generated modules are finitely generated abelian groups. By the structure theorem of abelian groups, we can then writen any such module M uniquely as

$$M \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

where $\alpha_i \geq 1$ and the p_i are primes of $\mathbb{Z}$, not necessarily distinct. We shall prove a similar result when $\mathbb{Z}$ is replaced by any PID.

Let us begin with some general ideas which work over any Noetherian commutative ring R. Let M be a finitely generated R-module. By definition, we can find a surjection $R^s \xrightarrow{f} M$. Now, $\ker(f)$ is a submodule of R^s, hence finitely generated because R is Noetherian. In particular, we can find another surjection $R^t \to \ker(f)$. In this way we get an exact sequence (which we call a presentation of M)

$$R^t \xrightarrow{g} R^s \xrightarrow{f} M$$

and the first isomorphism theorem tells us that $M \cong R^s/\ker(f)$ and since $\ker(f) = \operatorname{Im}(g)$ we also have $M \cong R^s/\operatorname{Im}(g)$. This means that M is generated by s elements with t relations between them. So our first observation: given any map of modules $g\colon R^s \to R^t$ we can associate a module $M = R^t/\operatorname{Im}(f)$, and any finitely generated module M can be constructed in this way.

Now, we notice that two maps $g, g'\colon R^t \to R^s$ may yield the same module M (same = isomorphic). For instance, let $\phi \in \operatorname{Aut}(R^s)$ be a module automorphism and consider $g' = \phi \circ g$. Then we clearly have an isomorphism

$$R^s/\operatorname{Im}(g) \cong R^s/\operatorname{Im}(g'),$$

and the automorphism is induced by ϕ. Similarly, if $\psi \in \operatorname{Aut}(R^t)$ then one easily checks that both g and $g \circ \psi$ yield isomorphism R-modules. Thus, we come to the following realization:

To classify finitely generated modules over a noetherian ring R, it is enought to classify elements of $\operatorname{Hom}_R(R^t, R^s)$ up to pre- and post-composition by elements of $\operatorname{Aut}(R^t)$ and $\operatorname{Aut}(R^s)$ (with varying s and t).

This is useful, because we can now interpret elements of $\operatorname{Hom}_R(R^t, R^s)$ as matrices. Let $e_1, e_2, \cdots, e_t$ be the canonical basis of R^t and $e_1, e_2, \cdots, e_s$ be the canonical basis of R^s. For any $f \in \operatorname{Hom}_R(R^t, R^s)$ we can write

$$f(e_i) = \sum_{j=1}^{s} a_{ji} e_j$$

and we associate to any f the matrix

$$(f(e_1), f(e_2), \cdots, f(e_t)) = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1t} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & a_{s3} & \dots & a_{st} \end{bmatrix}.$$

It is easy to see that this defines a bijection

$$\operatorname{Hom}_R(R^t, R^s) \xleftrightarrow{1:1} M_{s\times t}(R).$$

Now, let $f \in \operatorname{Hom}_R(R^t, R^s)$ with associated matrix $A \in M_{s\times t}(R)$ and let $\phi \in \operatorname{Aut}(R^s)$. What is the matrix associated to $\phi \circ f \in \operatorname{Hom}_R(R^t, R^s)$? Again, this is simple: as $\phi \in \operatorname{Aut}(R^s)$, we can associate to it a matrix $B \in M_{s\times s}(R)$ by the same reasoning. Then, under the above correspondence, one sees that the matrix associated to $\phi \circ f$ is nothing but $B \cdot A$ (usual matrix multiplication).

Lemma 1. *A matrix $A \in M_{s\times s}(R)$ is invertible if and only if $\det(A)$ is a unit in R.*

Proof. If A is invertible, then there is a matrix B such that $AB = 1$, hence $\det(A)\det(B) = 1$, which shows that first direction.

To show the other direction, let $\operatorname{adj}(A)$ be the adjoint matrix of A. By the Cramer rule we then have

$$\operatorname{adj}(A) \cdot A = \det(A)\,\mathrm{Id}_s\,.$$

Therefore, if $\det(A)$ is invertible in R, $\det(A)^{-1}\operatorname{adj}(A)$ gives the inverse of A. □

So, we have come to the following fact:

To classify finitely generated modules over a noetherian ring R, it is enought to classify matrices of $M_{s\times t}(R)$ up to multiplication by invertible matrices on both sides.

As it turns out, we can do this rather easily when R is a PID, thanks to Smith's normal form.

Theorem 2 (Smith normal form). *Let R be a PID and let $A \in M_{s\times t}(R)$. Then, there are two invertible matrices $S \in M_{s\times s}(R)$ and $T \in M_{t\times t}(R)$ and $r \leq \min\{s,t\}$ such that*

$$SAT = \left[\begin{array}{ccccc|cc} d_1 & 0 & 0 & \dots & 0 & 0 & \cdots \\ 0 & d_2 & 0 & \dots & 0 & 0 & \cdots \\ 0 & 0 & d_3 & \dots & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 0 & 0 & 0 & \dots & d_r & 0 & \cdots \\ \hline 0 & 0 & 0 & \dots & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}\right]$$

with $d_1 \mid d_2 \mid d_3 \cdots$ uniquely determined up to units of R.

Proof. Recall that if R is a PID and if $a, b \in R$ we can define the greatest common divisor $\gcd(a,b)$ as a generator of the ideal (a,b). This is well-defined up to units. For $a \in R$ write a prime decomposition $a = p_1p_2\cdots p_k$, where each p_i is prime. We define $\mu(a) = k$. This is well defined, moreover, if a divides b then $\mu(a) \leq \mu(b)$ and if a divides b and $\mu(a) = \mu(b)$ then $a = ub$ with u a unit. Consider the following set:

$$\mathcal{A} = \{B = SAT \colon S \in \mathrm{GL}_s(R) \text{ and } T \in \mathrm{GL}_t(R)\}.$$

Note that if A' is obtained from A by switching rows or columns, or by adding to one row/column a multiplie of another, then $A' \in \mathcal{A}$. Now, pick $A' = (a'_{ij}) \in \mathcal{A}$ such that $\mu(a'_{11})$ is minimal (i.e., for any $A'' = (a''_{ij}) \in \mathcal{A}$ we have $\mu(a''_{11}) \geq \mu(a'_{11})$).

I claim that a'_{11} divides every other entry of the form a'_{1i} and a'_{i1} for every possible i. Since we can switch rows and columns, we can simply show that a'_{11} divides a'_{12}. Now, let d be a gcd of a'_{11} and a'_{12} and write $\alpha_{11} = a'_{11}/d$ and $\alpha_{12} = a'_{12}/d$. If $x, y \in R$ are such that $xa'_{11} + ya'_{12} = d$ then $x\alpha_{11} + y\alpha_{12} = 1$. Now, consider the $t \times t$ matrix

$$C' = \left[\begin{array}{cc|ccc} x & -\alpha_{12} & 0 & \dots & 0 \\ y & \alpha_{11} & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right]$$

it is easy to see that $\det(C') = 1$ and hence that $A'C' \in \mathcal{A}$. But the first entry of $A'C'$ is d. By the minimality of A' we hence must have $\mu(d) \geq \mu(a_{11})$ and since $d \mid a'_{11}$ by construction, we deduce that$a'_{11} = \gcd(a'_{11}, a'_{12})$. This shows that a'_{11} divides all the first row and first column entries. But then, by performing elementary operations, and calling $d_1 = a'_{11}$, we can easily bring the matrix A' to the form

$$C' = \left[\begin{array}{c|cccc} d_1 & 0 & 0 & \dots & 0 \\ \hline 0 & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \dots & * \end{array}\right]$$

We now procede as before, but only modifying the smaller matrix inside. After having found in this way d_2, we notice that by adding the first row of the matrix above to its second row (where there is d_2) we must have that $d_1 \mid d_2$ by what we have shown before. An iteration of this proves the theorem. We do not prove that the various d_i are unique up to unit, but this follows e.g. from their intrinsic description using minors of the matrix. □

What does this tell us about the structure of modules?

Corollary 3. *Let R be a PID and let M be a finitely generated R-module. Then,*

$$M \cong R^n \oplus \bigoplus_i R/(d_i)$$

with $d_{i+1} \mid d_i$ (note that I have reversed the order of divisibility from the Smith's normal form theorem).

If $d = p_1^{a_1} p_2^{a_2} \cdots$ is a prime decomposition (which always exist because R is a PID) we get by the chinese remainder theorem

$$R/(d) = \oplus_i R/(p_i)^{a_i}.$$

In particular, we have

Corollary 4 (Second form)**.** *Let R be a PID and let M be a finitely generated R-module. Then,*

$$M \cong R^n \oplus \bigoplus_i R/(p_i)^{a_i}$$

where p_i are (not necessarily distint) primes of R.

Note that the integer n is uniquely determined, and can be characterized as the maximal number of R-linearly independent elements of M. That is

$$n = \max\{k \geq 0 \colon \exists m_1, m_2, \cdots m_k \in M \colon \sum_{i=1}^{k} a_i m_i = 0 \text{ then } a_1 = a_2 = \cdots = a_k = 0\}.$$

We shall show now that the sequence of integers d_i appearing in Corollary 3 is unique (up to units). The are called the *elementary divisors* of M. Thus, we can summarize the structure theorem in this form:

Theorem 5. *If R is a PID and M is a finitely generated module, then*

$$M \cong R^n \oplus \bigoplus_i R/(d_i)$$

for a unique n and uniquely determined $d_i \in R$ (up to unit) such that $d_{i+1} \mid d_i$.

An immediate corollary of the structure theorem is the following

Definition 6. Let M be a left R-module, with R any ring. Define:

1. $\mathrm{Ann}(M) = \{a \in R\colon am = 0 \text{ for every } m \in M\}$;
2. $\mathrm{Ann}(m) = \{a \in R\colon am = 0\}$ for $m \in M$;
3. $\mathrm{Tor}(M) = \{m \in M\colon am = 0 \text{ for } a \in R, a \text{ not a zero divisor}\}$;
4. for $a \in R$ put $\mathrm{Tors}_a(M) = M[a] = \{m \in M\colon am = 0\}$.

One easily shows that

1. $\mathrm{Ann}(M)$ is a left and right ideal of R;
2. $\mathrm{Ann}(m)$ is an ideal if R is commutative;
3. $\mathrm{Tor}(M)$ is a submodule of M if R is commutative;
4. $M[a]$ is a submodule of M if R is commutative.

For instance, let us show the third point. Clearly $\mathrm{Tor}(M)$ is closed under scalar multiplication if R is commutative. If now $m_1, m_2 \in \mathrm{Tor}(M)$ then there are two non-zero divisors $a_1, a_2 \in R$ such that $a_1 m_1 = a_2 m_2 = 0$. Hence, $a_1 a_2$ is not a zero divisor either, and $a_1 a_2 (m_1 + m_2) = 0$. One easily proves:

Lemma 7. *We have* $\mathrm{Ann}(R/(d)) = (d)$ *and* $R/(d)[a] \cong R/\mathrm{gcd}(a, d)$. *Moreover,*

$$\mathrm{Tor}(R^n \oplus \bigoplus_i R/(d_i)) = \bigoplus_i R/(d_i).$$

Proof. If $a \in \mathrm{Ann}(R/(d))$ when $a \cdot (1 + (d)) \subset (d)$ which means that $a \in (d)$. Then since $d \in \mathrm{Ann}(R/(d))$ we conclude. For the second point, assume there is $x + (d) \in R/(d)$ with $x \in R$ such that $ax + (d) = (d)$. This means that $ax \in (d)$. Using the prime decomposition we see that $x \in (d/\gcd(a, d))$ necessarily. Put $d' = d/\gcd(a, d)$. Then

$$R/(d)[a] = (d')/(d) \subset R/(d)$$

note that $(d) \subset (d')$ so we can form the quotient. We then conclude since the map

$$R/\gcd(a, d) \xrightarrow{d'} (d')/(d)$$

given by $x + (\gcd(a, d)) \mapsto d'x + (d)$ is a R-module isomorphism. □

In order to get the uniqueness of the d_i in the theorem, we need to consider the primary decomposition of torsion modules:

Definition 8. Let M be a R-module, with R a PID. For a prime p of R, let $M_p \subset M$ be the submodule given by

$$M_p = \{m \in M\colon \text{ there is } n \in \mathbb{N} \text{ such that } p^n \cdot m = 0\}.$$

Lemma 9. *Let M be a (not necessarily finitely generated) R-module, with R a PID, then* $\mathrm{Tors}(M) = \oplus_p M_p$, *where the direct sum ranges over all the primes of R (up to multiplication by a unit).*

Proof. To show that the sum is direct, we need to show that if p and q are coprime primes of R then $M_p \cap M_q = 0$. By coprimality, and since R is a PID, for any $a, b \geq 0$ we can write $1 = xp^a + yq^b$ with $x, y \in R$. Now, if $m \in M$ satisfies both $p^a m = q^b m = 0$ it means that $m = (xp^a + yq^b)m = 0$. Hence, the submodule of M generated by the various M_p is isomorphic to $\oplus_p M_p$. Now, pick any $m \in \mathrm{Tors}(M)$, and consider the map $R \to M$ sending $a \mapsto am$. Let d be a generator of the kernel, so that $Rm \cong R/(d) \subset M$ (note that d cannot be a unit since m is torsion). Consider the prime factorization

$$d = \prod_i p_i^{\alpha_i}.$$

By the Chinese reminder theorem we have that

$$R/(d) \cong \bigoplus_o R/(p_i)^{\alpha_i}$$

and that $R/(p_i)^{\alpha_i} \subset M_{p_i}$. Thus, we that $Rm \subset \oplus_p M_p$ hence $\mathrm{Tor}(M) = \oplus_p M_p$. $\square$

Now we classify the various possible M_p:

Proposition 10. *Assume that M is finitely generated and that $M_p = M$. Then, there is a unique sequence of integers $a_1 \geq a_2 \geq \cdots \geq a_k$ such that*

$$M = \oplus_{i=1}^k R/(p^{a_i}).$$

Proof. We need to show that if for two sequences $a_1 \geq a_2 \geq \cdots \geq a_k$ and $b_1 \geq b_2 \geq \cdots \geq b_l$ yield isomorphic modules then $k = l$ and $a_i = b_i$ for every i. We prove this by induction on the length k. So, if $k = 1$, then $R/(p^{a_1})$ is a cyclic module (generated by the image of 1). On the other hand, if

$$\oplus_{j=1}^l R/(p^{b_i})$$

is cyclic, then necessarily $l = 1$. Now, we only need to prove that $R/(p^n) \cong R/(p^m)$ if and only if $n = m$. But $\mathrm{Ann}(R/(p^n)) = (p^n)$ and $\mathrm{Ann}(R/(p^m)) = (p^m)$, hence the statement.

Assume now that we know the statement for all lengths $\leq k - 1$ and we want to prove it for k. So assume that

$$\oplus_{i=1}^k R/(p^{a_i}) \cong \oplus_{j=1}^l R/(p^{b_j}).$$

For a finitely module M such that $M_p = M$ define its exponent as the minimal $n \geq 0$ such that $p^n M = 0$. Note that this exist because M is finitely generated. Then the exponent of $\oplus_{i=1}^k R/(p^{a_i})$ is easily seen to be a_1 (the greated power appearing). Hence, since isomorphic modules have the same exponent, we deduce that $a_1 = b_1 = e$. In particular both decompositions contain a factor of the form $R/(p^e)$. Now consider $M/(R/(p^e))$. This has two decomposition

$$M/(R/(p^e)) = \oplus_{i=2}^k R/(p^{a_i}) \cong \oplus_{j=2}^l R/(p^{b_j})$$

and we conclude by induction. $\square$

Now, it is easy to construct the various d_i. Explicitely, choose a finitely generated torsion module M, and let M_p be the module

$$M_p = \oplus_i^k R/(p^{a_{p,i}})$$

with $a_{p,1} \geq a_{p,2} \geq a_{p,2} \geq a_{p,k}$ and we put $a_{p,i} = 0$ for $i > k$. The, define $d_i = \prod_p p^{a_{p,i}}$. It is easy to show that $d_i \mid d_{i+1}$.

1.1 Application: Jordan normal form

Let k be an algebraically closed field and let V be a finitely dimensional vector space. Let $F\colon V \to V$ be an endomorphism. As an application of the previous result, we show how to obtain the existence of the Jordan decomposition for F. The first key observation is to note that there is a one-to-one correspondence (which work over any field K)

$$\{\text{f.g. torsion } K[x]-\text{modules}\} \leftrightarrow \{(V, F) \text{ with } V \text{ f.d. } K-\text{vector space}, F \in \operatorname{End}(V)\} \tag{1.1}$$

The correspondence is constructed as follows. Let M be a finitely generated, torsion $K[x]-$module. Then we know by the structure theorem that M is a finite direct sum of modules of the form $K[x]/(f)$ with $\deg(f) > 0$ and hence in particular that M is a finite dimensional vector space over K. Let now $x \in K[x]$. Since M is a module, we have a multiplication map $x\colon M \to M$ which sends $m \mapsto xm$. So multiplication by x induces an element $F \in \operatorname{End}_K(V)$. This defines a pair (V, F) of a finite dimensional K-vector space with an endomorphism.

On the other hand, let (V, F) be as above. We want to define a $K[x]$-module structure on V. But this is done by letting $g(x) \in K[x]$ act on V as $g(F) \in \operatorname{End}_K(V)$. In this way, we see V as a $K[x]$-module. To show that it is torsion, we consider for instance the characteristic polynomial $P(X) = \det(x \operatorname{Id} - F) \in K[x]$. We know that $P(F) = 0$ by the Cayley–Hamilton theorem and hence that $(P) \subset \operatorname{Ann}(M)$. This shows that M is torsion. Finally, it is clearly finitely generated, e.g., by a K-basis of V.

Remark 1. This correspondence also preserves direct sums. In fact, it is an equivalence of categories.

Now, assume K is algebraically closed and consider a pair (V, F). This corresponds to a module M over $K[x]$. But the only primes of $K[x]$ are of the form $(x - c)$ for $c \in K$ since K is algebraically closed. The primary decomposition $M = \oplus_p M_p$ yields a decomposition

$$(V, F) = \oplus_p (V_p, F_p)$$

and the further decomposition $M_p = \oplus_{i=1}^k R/(p^{a_i})$ as in the preveious section yields a decomposition

$$(V_p, F_p) = \oplus_{i=1}^k (V_{p,i}, F_{p,i}).$$

There are the Jordan blocks. Now, write $p = (x - c)$ and consider the block $V_{p,i}$. This corresponds to the module $K[x]/(x - c)^{a_i}$. A basis of the vector space $K[x]/(x-c)^{a_i}$

is given by $1, x-c, (x-c)^2, \cdots, (x-c)^{a_i-1}$. With respect to this basis, the action of x is $x(x-c)^i = (x-c)^{i+1} + c(x-c)^i$ if $i < a_i - 1$ and $x(x-c)^{a_i-1} = c(x-c)^{a_i-1}$. This means that on the block $V_{p,i}$ F acts in the Jordan form

$$\begin{bmatrix} c & 1 & 0 & \dots & 0 \\ 0 & c & 1 & \dots & 0 \\ 0 & 0 & c & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & 1 \\ 0 & 0 & 0 & \dots & c \end{bmatrix}$$

with respect to the basis above.