Modules over a PID

Nicolas Mascot

TCD

March 20, 2020

Submodules of free modules

Theorem

Let R be a PID, and let M be an R-module. If M is free, then every submodule of M is also free.

Submodules of free modules

Theorem

Let R be a commutative domain. TFAE:

1. *R is a PID,*
2. *If M is a free R-module, then all the submodules of M are also free.*

Proof: necessity of PID

Proof.

R is a free R-module of rank 1, whose submodules are the ideals of R. Let $I \neq 0$ be such an ideal.
If I is free of rank $\geqslant 2$, let $i_1, i_2, \cdots$ be an R-basis of I. Then

$$\lambda i_1 + \mu i_2 = 0 \quad \text{for} \quad \lambda = i_2 \in R, \mu = -i_1 \in R,$$

contradition. So if I is free, it must be of rank 1. Let i_1 be a basis; then

$$I = \{\lambda i_1, \ \lambda \in R\} = (i_1)$$

is principal.

Proof: sufficiency of PID

Proof.

Conversely, let M be free of rank n. Then $M \simeq R^n$, so WLOG we suppose $M = R^n$.
Let $S \subset R^n$ be a sub-R-module, we prove by induction on n that S is free.
If $n = 0$, then $R^n = \{0\}$, so $S = \{0\}$ is free of rank 0.

Suppose true for $n - 1$. Define

$$\pi : \begin{array}{ccc} S & \longrightarrow & R \\ (x_1, \cdots, x_n) & \longmapsto & x_n \end{array}$$

and

$$S_0 = \operatorname{Ker} \pi = \{(x_1, \cdots, x_n) \in S \mid x_n = 0\}.$$

Proof: sufficiency of PID

Proof.

By induction hypothesis, $S_0 \subset R^{n-1}$ is free; let $s_1, \cdots, s_m$ be a basis. Besides, $\operatorname{Im} \pi \subset R$ is a submodule, hence an ideal, so of the form gR for some $g \in R$.

If $g = 0$, then $\operatorname{Im} \pi = \{0\}$, so $S = S_0$, done.

Else, we have $g \neq 0$. Let $s = (\cdots, g) \in S$.
Claim: $s_1, \cdots, s_m, s$ is an R-basis of S.

Generating: Let $x = (x_1, \cdots, x_n) \in S$. Then $x_n \in \operatorname{Im} \pi = gR$, so $x_n = gy$ for some $y \in R$. Then $x - ys \in S_0$, so is of the form $\sum_i \lambda_i s_i$ for some $\lambda_i \in R$. Thus $x = \sum_i \lambda_i s_i + ys$.

Linearly independent: Suppose $\sum_i \lambda_i s_i + ys = 0$ for some $\lambda_i, y \in R$. Look at the last coordinate: $\sum_i \lambda_i 0 + yg = 0$, whence $yg = 0$, whence $y = 0$. So $\sum_i \lambda_i s_i = 0$. □

The Smith normal form

Theorem

Let R be a PID, and let A be a matrix with entries in R. It is possible to turn A into a diagonal matrix with entries

$$d_1 \mid d_2 \mid \cdots$$

using a succession of the following operations:

- *Add a multiple of a row of A to another row,*
- *Swap two rows of A,*
- *Add a multiple of a column of A to another column,*
- *Swap two columns of A.*

The d_i are called the *<u>invariant factors</u>* *of A; they are unique up to associates.*

SNF: proof, case R Euclidean

Proof.

1. Swap rows and columns until one of the nonzero entries of A of the smallest size is at the top-left corner.
2. Use the top-left entry λ as a pivot so as to replace all the terms in the first row and in the first column by their reminders by a.
3. If $A = \left(\begin{array}{c|ccc} \lambda & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$ with λ dividing all the entries of A', iterate on the block A'. Else, swap rows and columns again and go to step 2.

□

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 8 & 4 & 8 \\ 16 & 14 & 10 \\ 12 & 12 & 6 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 8 & 4 & 8 \\ 16 & 14 & 10 \\ 12 & 12 & 6 \end{pmatrix} \qquad C_2 \leftrightarrow C_1$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 4 & 8 & 8 \\ 14 & 16 & 10 \\ 12 & 12 & 6 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 4 & 8 & 8 \\ 14 & 16 & 10 \\ 12 & 12 & 6 \end{pmatrix} \qquad \begin{array}{l} R_2 \leftarrow R_2 - 3R_1, \\ R_3 \leftarrow R_3 - 3R_1 \end{array}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 4 & 8 & 8 \\ 2 & -8 & -14 \\ 0 & -12 & -18 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 4 & 8 & 8 \\ 2 & -8 & -14 \\ 0 & -12 & -18 \end{pmatrix} \qquad \begin{array}{l} C_2 \leftarrow C_2 - 2C_1, \\ C_3 \leftarrow C_3 - 2C_1 \end{array}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 4 & 0 & 0 \\ 2 & -12 & -18 \\ 0 & -12 & -18 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 4 & 0 & 0 \\ 2 & -12 & -18 \\ 0 & -12 & -18 \end{pmatrix} \qquad R_2 \leftrightarrow R_1$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & -12 & -18 \\ 4 & 0 & 0 \\ 0 & -12 & -18 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & -12 & -18 \\ 4 & 0 & 0 \\ 0 & -12 & -18 \end{pmatrix} \qquad R_2 \leftarrow R_2 - 2R_1$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & -12 & -18 \\ 0 & 24 & 36 \\ 0 & -12 & -18 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & -12 & -18 \\ 0 & 24 & 36 \\ 0 & -12 & -18 \end{pmatrix} \qquad \begin{aligned} C_2 &\leftarrow C_2 + 6C_1, \\ C_3 &\leftarrow C_3 + 9C_1 \end{aligned}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 24 & 36 \\ 0 & -12 & -18 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 24 & 36 \\ 0 & -12 & -18 \end{pmatrix} \qquad R_3 \leftrightarrow R_2$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & -18 \\ 0 & 24 & 36 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & -18 \\ 0 & 24 & 36 \end{pmatrix} \qquad R_3 \leftarrow R_3 + 2R_2$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & -18 \\ 0 & 0 & 0 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & -18 \\ 0 & 0 & 0 \end{pmatrix} \qquad C_3 \leftarrow C_3 - 2C_2$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & 6 \\ 0 & 0 & 0 \end{pmatrix} \qquad C_3 \leftrightarrow C_2$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & -12 \\ 0 & 0 & 0 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & -12 \\ 0 & 0 & 0 \end{pmatrix} \qquad C_3 \leftarrow C_3 + 2C_2$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Example: SNF over $\mathbb{Z}$

Example

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Invariant factors: $d_1 = 2 \mid d_2 = 6 \mid d_3 = 0$.

Application: Finitely generated modules over a PID

Theorem

Let R be a PID, and let M be a finitely generated R-module. There exist <u>*invariant factors*</u>

$$d_1 \mid d_2 \mid \cdots \in R$$

such that

$$M \simeq (R/d_1 R) \times (R/d_2 R) \times \cdots$$

These invariant factors are unique up to associates.

Remark

$R/0R = R$, and $R/uR = \{0\}$ for all $u \in R^\times$.

Finitely generated modules over a PID: proof

Proof.

Let $m_1, \cdots, m_p \in M$ generate M; then the morphism

$$f : \begin{array}{ccc} R^p & \longrightarrow & M \\ (\lambda_1, \cdots, \lambda_p) & \longmapsto & \sum_i \lambda_i m_i \end{array}$$

is surjective, so $M \simeq R^p / \operatorname{Ker} f$ by the isomorphism theorem. Let

$$N = \operatorname{Ker} f \subset R^p;$$

then N is a free R-module, let $n_1, \cdots, n_q$ be a basis. Express the $n_i \in R^p$ as a $p \times q$ matrix A. Operations on the columns of A amount to changing the basis $n_1, \cdots, n_q$, and operations on the rows amount to changing the generators $m_1, \cdots, m_p$. So taking the SNF of A, we get generators $m_1', m_2', \cdots$ of M satisfying the relations $d_i m_i' = 0 \in M$. □

Application: Finitely generated Abelian groups

Corollary

Let G be a finitely generated Abelian group. There exist invariant factors

$$d_1 \mid d_2 \mid \cdots \in \mathbb{Z}_{\geqslant 0}$$

such that

$$G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots$$

These invariant factors are unique.

Finitely generated Abelian groups: example

Example

Let G be the Abelian group with generators g_1, g_2, g_3 and relations

$$\begin{cases} 8g_1 + 16g_2 + 12g_3 = 0, \\ 4g_1 + 14g_2 + 12g_3 = 0, \\ 8g_1 + 10g_2 + 6g_3 = 0. \end{cases}$$

Then $A = \begin{pmatrix} 8 & 4 & 8 \\ 16 & 14 & 10 \\ 12 & 12 & 6 \end{pmatrix}$ has SNF with invariant factors

$$2 \mid 6 \mid 0,$$

so

$$G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times \mathbb{Z}.$$

Application: The rational canonical form (1/6)

Definition

Let K be a field, and let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x].$$

The <u>companion matrix</u> of f is

$$C_f = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix} \in M_n(K).$$

Application: The rational canonical form (2/6)

Lemma

Let $V = K[x]/f(x)K[x]$ seen as a K-vector space. Then $1, x, x^2, \cdots, x^{\deg f - 1}$ is a K-basis of V, and the matrix of multiplication by x is C_f.

Remark

The characteristic polynomial

$$\det(x1_n - C_f)$$

of C_f and the minimal polynomial of C_f are both $f \in K[x]$.

Application: The rational canonical form (3/6)

Corollary

Let K be a field, V a finite-dimensional K-vector space, and $T \in \mathrm{End}(V)$. There exist unique monic polynomials

$$f_1(x) \mid f_2(x) \mid \cdots \mid f_k(x) \in K[x]$$

such that there exists a basis of V such that the matrix of T is

$$\begin{pmatrix} C_{f_1} & & & \\ & C_{f_2} & & \\ & & \ddots & \\ & & & C_{f_k} \end{pmatrix}.$$

The minimal polynomial of T is $f_k(x)$, and it characteristic polynomial is $f_1(x)f_2(x)\cdots f_k(x)$.

Application: The rational canonical form (4/6)

Proof.

Put a $K[x]$-module structure on V by letting $xv = T(v)$ for all $v \in V$. For instance,

$$(x^2 - 1)v = T(T(v)) - v.$$

Since V has finite dimension over K, it is a finitely generated $K[x]$-module. As $K[x]$ is a PID,

$$V \simeq (K[x]/f_1(x)K[x]) \times \cdots \times (K[x]/f_k(x)K[x])$$

for some unique monic $f_1(x) \mid f_2(x) \mid \cdots \mid f_k(x) \in K[x]$. □

Application: The rational canonical form (5/6)

Example

Take $V = K^3$ and $T \in \mathrm{End}(V)$ having matrix $A = \begin{pmatrix} 7 & -5 & -5 \\ 5 & -3 & -5 \\ 5 & -5 & -3 \end{pmatrix}$ with respect to the standard basis e_1, e_2, e_3 of V. Then the $K[x]$-module V is generated by e_1, e_2, e_3 with relations

$$\begin{cases} xe_1 - (7e_1 + 5e_2 + 5e_3) = 0, \\ xe_2 + (5e_1 + 3e_2 + 5e_3) = 0, \\ xe_3 + (5e_1 + 5e_2 + 5e_3) = 0, \end{cases}$$

so we take the SNF of

$$\begin{pmatrix} x-7 & 5 & 5 \\ -5 & x+3 & 5 \\ -5 & 5 & x+3 \end{pmatrix} \in M_3(K[x]).$$

Application: The rational canonical form (6/6)

Example

We find the invariant factors

$$1 \mid (x-2) \mid (x-2)(x+3) = x^2 + x - 6,$$

so

$$V \simeq (K[x]/(1)) \times (K[x]/(x-2)) \times (K[x]/(x^2+x-6))$$

and the rational canonical form of A is

$$\left(\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 0 & 6 \\ 0 & 1 & -1 \end{array}\right).$$

In particular, A has minimal polynomial $(x-2)(x+3)$ and characteristic polynomial $(x-2)^2(x+3)$.