# MAU22102
# Rings, Fields, and Modules
# 4 - Modules over a ring


Nicolas Mascot

mascotn@tcd.ie


Module web page

Hilary 2020–2021

Version: March 29, 2021


Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

# Modules vs. vector spaces

# Reminder: vector spaces

## Definition (Vector space over a field)

*Let $K$ be a field. A <u>$K$-vector space</u> is a set $V$ equipped with two composition laws*

$$\begin{array}{ccc} V \times V & \longrightarrow & V \\ (v, w) & \longmapsto & v + w, \end{array} \qquad \begin{array}{ccc} K \times V & \longrightarrow & V \\ (\lambda, v) & \longmapsto & \lambda v \end{array}$$

*such that $(V, +)$ is an Abelian group, and that for all $\lambda, \mu \in K$ and $v, w \in V$, we have*

$$\lambda(\mu v) = (\lambda\mu)v, \qquad 1v = v,$$

$$(\lambda + \mu)v = (\lambda v) + (\mu v), \qquad \lambda(v + w) = (\lambda v) + (\lambda w).$$

# Modules

## Definition (Module over a ring)

*Let $R$ be a (not necessarily commutative) ring. An <u>$R$-module</u> is a set $M$ equipped with two composition laws*

$$\begin{array}{rcl} M \times M & \longrightarrow & M \\ (m,n) & \longmapsto & m+n, \end{array} \qquad \begin{array}{rcl} R \times M & \longrightarrow & M \\ (\lambda,m) & \longmapsto & \lambda m \end{array}$$

*such that $(M,+)$ is an Abelian group, and that for all $\lambda, \mu \in R$ and $m, n \in M$, we have*

$$\lambda(\mu m) = (\lambda\mu)m, \qquad 1m = m,$$

$$(\lambda+\mu)m = (\lambda m) + (\mu m), \qquad \lambda(m+n) = (\lambda m) + (\lambda n).$$

# Modules: examples

**Example**

Let $R$ be a ring, and let $n \in \mathbb{N}$. Then

$$R^n = \{(x_1, \cdots, x_n) \mid x_i \in R\}$$

is an $R$-module.

**Example**

Let $(G, +)$ be an Abelian group. Then $G$ is actually a $\mathbb{Z}$-module:

$$ng = \underbrace{g + \cdots + g}_{n \text{ times}} \qquad (n \in \mathbb{Z}, g \in G).$$

# Submodules

## Definition (Submodule)

*Let $M$ be an $R$-module. A submodule of $M$ is a subset of $M$ which is nonempty and closed under $+$ and under multiplication by $R$.*

## Example

Let $M = R$, viewed as an $R$-module. Then the submodules of $M$ are the ideals of $R$.

# Generating sets of a module

## Definition (Generating set, finitely generated)

*Let $M$ be an $R$-module. Elements $m_1, \cdots, m_n \in M$ form a generating set if every $m \in M$ can be expressed in the form*

$$m = \sum_{i=1}^{n} \lambda_i m_i$$

*for some (not necessarily unique) $\lambda_i \in R$.*
*If such a finite generating set exists, then we say that $M$ is finitely generated.*

## Counter-example

Let $R$ be a commutative ring. Then $R[x]$ is an $R$-module, which is not finitely generated.

# Linear independence, free modules

## Definition (Linearly independent, free)

*Let $M$ be an $R$-module. Elements $m_1, \cdots, m_n \in M$ are linearly independent if the only $\lambda_1, \cdots, \lambda_n \in R$ satisfying*

$$\sum_{i=1}^{n} \lambda_i m_i = 0$$

*are $\lambda_1 = \cdots = \lambda_n = 0$.*

*If furthermore $m_1, \cdots, m_n$ form a generating set of $M$, we say that $M$ is a free $R$-module of rank $n$, and that the $m_i$ form a basis of $M$. In this case, every $m \in M$ can be expressed as*

$$m = \sum_{i=1}^{n} \lambda_i m_i$$

*for some unique $\lambda_i \in R$.*

# Free modules: examples

**Example**

$R^n$ is a free $R$-module of rank $n$, with basis

$$e_1 = (1, 0, \cdots, 0),\ e_2 = (0, 1, 0, \cdots, 0),\ \cdots, e_n = (0, \cdots, 0, 1).$$

**Counter-example**

The $\mathbb{Z}$-module $M = \mathbb{Z}/2\mathbb{Z}$ is finitely generated, but it is <u>not</u> a free module.

# Modules vs. vector spaces

In a vector space, one can extract a basis out of any generating set, and every linearly independent family can be extended into a basis.

### Counter-example

$\{2, 3\}$ is a generating family of the $\mathbb{Z}$-module $M = \mathbb{Z}$, because $n = (-n)2 + (n)3$ for all $n \in \mathbb{Z}$. But one cannot extract a basis out of it.

### Counter-example

In the $\mathbb{Z}$-module $M = \mathbb{Z}$, the linearly independent family $\{2\}$ cannot be extended into a basis.

# Module morphisms

# Morphisms

**Definition (Module morphism)**

*Let $M$ and $N$ be two $R$-modules. A map $f : M \longrightarrow N$ is a morphism if it is $R$-linear, meaning*

$$f(m + m') = f(m) + f(m') \text{ and } f(\lambda m) = \lambda f(m)$$

*for all $m, m' \in M$ and $\lambda \in R$.*
*A morphism is an isomorphism if it is bijective, in which case its inverse is automatically a morphism.*

# Morphisms: examples

**Example**

An $R$-module $M$ is finitely generated iff. there exits $n \in \mathbb{N}$ and a surjective morphism $R^n \longrightarrow M$. It is free of rank $n$ iff. it is isomorphic to $R^n$.

**Remark**

Let $I \subset R$ be a maximal ideal, and let $k = R/I$ be the corresponding field. Then

$$R^n \simeq R^m \Longrightarrow k^n \simeq k^m \Longrightarrow n = m,$$

so the rank of a free module is well-defined.

# Kernels and images

**Theorem (Kernel and image are submodules)**

*Let $M$ and $N$ be two $R$-modules, and $f : M \longrightarrow N$ be a morphism. Then*

$$\operatorname{Ker} f = \{m \in M \mid f(m) = 0\} \subseteq M$$

*is a submodule of $M$, and*

$$\operatorname{Im} f = \{f(m) \mid m \in M\} \subseteq N$$

*is a submodule of $N$.*

*$f$ is injective iff. $\operatorname{Ker} f = \{0\}$, surjective iff. $\operatorname{Im} f = N$, and an isomorphism iff. it is both.*

# Kernels and images: example

**Example**

Let

$$f : \begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ (x,y) & \longmapsto & x - y \bmod 2. \end{array}$$

Then

$$\operatorname{Im} f = \mathbb{Z}/2\mathbb{Z},$$

and

$$\operatorname{Ker} f = \{(x,y) \in \mathbb{Z}^2 \mid x \equiv y \bmod 2\}$$

is a free submodule of rank 2 of $\mathbb{Z}^2$ with basis $\{(1,1),(1,-1)\}$.

# Morphisms between free modules

Let $M$ be a free $R$-module with basis $m_1, m_2, \cdots$. Every $m \in M$ can be expressed uniquely as $m = \lambda_1 m_1 + \lambda_2 m_2 + \cdots$, and can thus be represented by its coordinates $\lambda_1, \lambda_2, \cdots \in R$.

Likewise, if $N$ is another free $R$-module with basis $n_1, n_2, \cdots$, then each morphism from $M$ to $N$ may be represented by it matrix with respect to these bases. Conversely, each matrix (of the appropriate size) corresponds to a morphism from $M$ to $N$.

Composition of morphisms corresponds to multiplication of matrices. In particular, a morphism from $M$ to $N$ is an isomorphism if and only if its matrix is invertible.

# $\mathrm{GL}_n(R)$: statement

Let $R$ be a commutative ring and $n \in \mathbb{N}$ be n integer. Write

$$M_n(R) = \{n \times n \text{ matrices with coefficients in } R\}$$

and

$$\mathrm{GL}_n(R) = M_n(R)^\times.$$

**Theorem (Invertible matrices over a ring)**

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det A \in R^\times\}.$$

# $\mathrm{GL}_n(R)$: proof and example

**Proof.**

If $A, B \in M_n(R)$ satisfy $AB = I_n$, then

$$1 = \det(I_n) = \det(AB) = \det(A)\det(B)$$

so $\det(A) \in R^\times$.
Conversely, every $A \in M_n(R)$ satisfies

$$AA' = \det(A) I_n$$

where $A'$ is the adjugate matrix of $A$. □

**Example**

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}.$$

# Quotient modules

**Theorem (Construction of quotient modules)**

*Let $M$ be an $R$-module, and $S \subseteq M$ be a submodule. Then the quotient set*

$$M/S = M/\sim, \quad \text{where } m \sim m' \iff m - m' \in S,$$

*inherits an $R$-module structure. The projection map*

$$M \longrightarrow M/S$$

*is a surjective morphism whose kernel is $S$.*

# The isomorphism theorem for modules

**Theorem (Isomorphism theorem for modules)**

*Let $M$ and $N$ be two $R$-modules, $S \subseteq M$ a submodule, and $f : M \longrightarrow N$ be a morphism. Then $f$ factors as*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d] & N \\ M/S \arrow[ur, dashed] & \end{tikzcd}$$

*iff.* $S \subseteq \operatorname{Ker} f$.

*In particular, $f$ induces an isomorphism $M/\operatorname{Ker} f \simeq \operatorname{Im} f$.*

# Modules over a PID: theorems

# Submodules of free modules

**Theorem (Freeness over a PID)**

*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 (Freeness over PID)**

*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

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

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 $S$.

<ins>Generating:</ins> 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 $x = \sum_i \lambda_i s_i + ys$.

<ins>Linearly independent:</ins> 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 $\sum_i \lambda_i s_i = 0$. $\square$

# The Smith normal form

**Theorem (SNF & invariant factors)**

*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 invariant factors 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 $\lambda$ 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 $\lambda$ dividing all the entries of $A'$, iterate on the block $A'$. Else, swap rows and columns again and go to step 2.

$\square$

# 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

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

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

# Modules over a PID: applications

# Application: Finitely generated modules over a PID

**Theorem**

*Let $R$ be a PID, and let $M$ be a finitely generated $R$-module. There exist invariant factors*

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

*such that*

$$M \simeq (R/d_1R) \times (R/d_2R) \times \cdots$$

*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

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

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 $d_i m'_i = 0 \in M$. $\square$

# Application: Finitely generated Abelian groups

**Corollary (Classification of finitely generated Abelian groups)**

*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 $A = \left(\begin{smallmatrix} 8 & 4 & 8 \\ 16 & 14 & 10 \\ 12 & 12 & 6 \end{smallmatrix}\right)$ 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)

**From this point on, all the material is non-examinable.**

## Definition (Companion matrix)

*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 companion matrix 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 (Rational canonical form)

*Let $K$ be a field, $V$ a finite-dimensional $K$-vector space, and $T \in \operatorname{End}(V)$. 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*

$$\begin{pmatrix} C_{f_1} & & & 0 \\ & C_{f_2} & & \\ & & \ddots & \\ 0 & & & C_{f_k} \end{pmatrix}.$$

*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 $V = K^3$ with basis $e_1, e_2, e_3$, and $T \in \operatorname{End}(V)$ having matrix $B = \begin{pmatrix} 7 & -5 & -5 \\ 5 & -3 & -5 \\ 5 & -5 & -3 \end{pmatrix}$.

The $e_i$ generate $V$ over $K$ and hence over $K[x]$, whence a surjective $K[x]$-module morphism $f : K[x]^3 \longrightarrow V$ taking the basis $E_1, E_2, E_3$ of $K[x]^3$ to $e_1, e_2, e_3$.

The $xE_i - T(E_i)$ lie in $\operatorname{Ker} f$, and actually form a basis of it; so we take the SNF of

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

# 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 as a $K[x]$-module,

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

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 $(x-2)^2(x+3)$.