# 10. Modules over PIDs



The structure theorem for finitely-generated abelian groups and Jordan canonical form for endomorphisms of finite-dimensional vector spaces are example corollaries of a common idea.

---

## 1. *The structure theorem*

Let $R$ be a **principal ideal domain**, that is, a commutative ring with identity such that every ideal $I$ in $R$ is **principal**, that is, the ideal can be expressed as

$$I = R \cdot x = \{r \cdot x : r \in R\}$$

for some $x \in R$. An $R$-module $M$ is **finitely-generated** if there are finitely-many $m_1, \ldots, m_n$ in $M$ such that every element $m$ in $M$ is expressible in at least one way as

$$m = r_1 \cdot m_1 + \ldots + r_n \cdot m_n$$

with $r_i \in R$.

A basic construction of new $R$-modules from old is as **direct sums**: given $R$-modules $M_1, \ldots, M_n$, the direct sum $R$-module

$$M_1 \oplus \ldots \oplus M_n$$

is the collection of $n$-tuples $(m_1, \ldots, m_n)$ with $m_i \in M_i$, with component-wise operation [1]

$$(m_1, \ldots, m_n) + (m'_1, \ldots, m'_n) = (m_1 + m'_1, \ldots, m_n + m'_n)$$

[1] This certainly is the obvious generalization, to modules, of vector addition in vector spaces written as ordered $n$-tuples.

and the multiplication [2] by elements $r \in R$ by

$$r \cdot (m_1, \ldots, m_n) = (rm_1, \ldots, rm_n)$$

**[1.0.1] Theorem:** Let $M$ be a finitely-generated module over a PID $R$. Then there are uniquely determined ideals

$$I_1 \supset I_2 \supset \ldots \supset I_t$$

such that

$$M \approx R/I_1 \oplus R/I_2 \oplus \ldots \oplus R/I_t$$

The ideals $I_i$ are the **elementary divisors** of $M$, and this expression is the **elementary divisor form** of $M$. [3]

*Proof:* (next chapter) ///

---

# 2. *Variations*

The following proposition (which holds in more general circumstances) suggests variations on the form of the structure theorem above.

**[2.0.1] Proposition:** [4] Let $I$ and $J$ be ideals of a commutative ring $R$ with identity 1 such that

$$I + J = R$$

Take $r \in I$ and $s \in J$ such that $r + s = 1$. Then

$$R/I \oplus R/J \approx R/IJ$$

by [5]

$$(x + I, y + J) \longrightarrow sx + ry + IJ$$

*Proof:* First, prove well-definedness. Note that $r + s = 1$ implies that $1 - r = s \in J$, and, similarly, $1 - s = r \in I$. If $x - x' \in I$ and $y - y' \in I$, then

$$(sx + ry) - (sx' + ry') = s(x - x') + r(y - y') \in JI + IJ = IJ$$

This proves well-definedness. [6] Next, show that the kernel is trivial. Indeed, if $sx + ry \in IJ$, then $(1 - r)x = sx \in I$. Thus, as $rx \in I$, $x \in I$. Similarly $y \in J$, and we have injectivity. For surjectivity, take any $z \in R$, and compute that

$$(z + I,\ z + J) \longrightarrow sz + rz + IJ = (r + s)z + IJ = z + IJ$$

---

[2] Obviously generalizing the scalar multiplication in vector spaces.

[3] Other sources call the $I_i$'s the **invariant factors** of the module.

[4] Yes, this is simply an abstracted form of Sun-Ze's theorem. The proof is exactly the same.

[5] Yes, the element $s \in J$ is the coefficient of $x$, and the element $r \in I$ is the coefficient of $y$.

[6] Keep in mind that in this context $IJ$ is not merely the collection of product $xy$ with $x \in I$ and $y \in J$, but is the set of finite sums $\sum_i x_i y_i$ with $x_i \in I$, $y_i \in J$.

since $r + s = 1$. ///

Returning to the situation that $R$ is a PID, let $I = R \cdot x$. Factor the generator $x$ into prime element powers $p_i^{e_i}$ and a unit $u$ in $R$

$$x = u \cdot p_1^{e_1} \dots p_t^{e_t}$$

Then, iterating the result of the previous proposition,

$$R/I = R/\langle x \rangle = R/\langle p_1^{e_1} \rangle \oplus \dots \oplus R/\langle p_t^{e_t} \rangle$$

[2.0.2] **Remark:** Depending on the circumstances, it may be interesting that the left-hand side is expressible as the right-hand side, or, at other moments, that the right-hand side is expressible as the left-hand side.

Now if we have a direct sum

$$R/I_1 \oplus \dots \oplus R/I_n$$

we can do the same further prime-wise decomposition, if we want. That is, let

$$I_i = \langle p_1^{e_{i1}} \dots p_t^{e_{it}} \rangle$$

(with a common set of primes $p_j$ in $R$), with non-negative integer exponents, [7] the divisibility condition is

$$e_{1j} \le e_{2j} \le \dots \le e_{nj}$$

and

$$R/I_1 \oplus \dots \oplus R/I_n \approx (R/\langle p_1^{e_{11}} \rangle \oplus \dots \oplus R/\langle p_1^{e_{n1}} \rangle) \oplus \dots \oplus (R/\langle p_t^{e_{1t}} \rangle \oplus \dots \oplus R/\langle p_t^{e_{nt}} \rangle)$$

That is, for each prime $p_i$, we can extract a summand in elementary divisor form whose elementary divisor ideals are generated simply by powers of $p_i$. (If some $e_{ij} = 0$, then $R/\langle p_j^{e_{ij}} \rangle = \{0\}$.)

Conversely, a direct sum of direct sums corresponding to distinct (non-associate) primes in $R$ can be reassembled in a *unique* manner to fit the conclusion of the structure theorem.

As an example of the re-assembly into canonical form, taking $R = \mathbb{Z}$, let

$$M = \Big(\mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/8\Big) \oplus \Big(\mathbb{Z}/9 \oplus \mathbb{Z}/27\Big)$$

It is important to realize that there is *unique* choice of how to put the summands together in the form of the conclusion of the Structure Theorem, here

$$M \approx \mathbb{Z}/2 \oplus \mathbb{Z}/36 \oplus \mathbb{Z}/216$$

It is *true* that this is *also* isomorphic (for example) to

$$\mathbb{Z}/18 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/216$$

but this is not in canonical form, and mere permutation of the summands is insufficient to put it into canonical form.

[2.0.3] **Remark:** Even *without* the condition

$$e_1 \le \dots \le e_n$$

[7] Allowing non-negative integer exponents keeps the notation from becoming even more ridiculous than it is, though, at the same time, it creates some potential for confusion.

for prime $p$ in $R$ any direct sum

$$R/\langle p^{e_1}\rangle \oplus \ldots \oplus R/\langle p^{e_t}\rangle$$

involving just the prime $p$ at worst needs merely a permutation of its factors to be put into elementary divisor form.

---

# 3. *Finitely-generated abelian groups*

Surely a very popular choice of PID is the ring of integers $\mathbb{Z}$. Finitely-generated $\mathbb{Z}$-modules are exactly *abelian groups*, since any abelian group is a $\mathbb{Z}$-module with structure given as usual by

$$n \cdot m = \begin{cases} \underbrace{m + \ldots + m}_{n} & (n \geq 0) \\ -(\underbrace{m + \ldots + m}_{|n|}) & (n \leq 0) \end{cases}$$

Any ideal $I$ in $\mathbb{Z}$ has a unique non-negative generator. Thus, the Structure Theorem becomes

[3.0.1] **Corollary:** Let $M$ be a finitely-generated $\mathbb{Z}$-module (that is, a finitely-generated abelian group). Then there are uniquely determined non-negative integers $d_1, \ldots, d_n$ such that [8]

$$d_1 | d_2 | \ldots | d_n$$

and

$$M \approx \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2 \oplus \ldots \oplus \mathbb{Z}/d_n$$

[3.0.2] **Corollary:** Let $n = p_1^{e_1} \ldots p_t^{e_t}$ with $p_1$, ..., $p_t$ distinct primes in $\mathbb{Z}$. Then every abelian group of order $n$ is uniquely expressible as a direct sum

$$A_{p_1^{e_1}} \oplus \ldots \oplus A_{p_t^{e_t}}$$

of abelian groups $A_{p_i^{e_i}}$ of orders $p_i^{e_i}$.

---

[8] Keep in mind that any integer divides 0, so it may happen that some of the $d_i$ are 0. Of course, if $d_i = 0$, then $d_j = 0$ for $j \geq i$.

*Proof:* This second corollary comes from the observations on variations of the Structure Theorem that we can obtain by thinking in terms of Sun-Ze's theorem. ///

[3.0.3] **Corollary:** The finite abelian groups of order $p^n$ for prime $p$ are

$$\mathbb{Z}/p^{e_1} \oplus \ldots \oplus \mathbb{Z}/p^{e_t}$$

for all sets of positive integers $e_1, \ldots, e_t$ (for varying $t$) with

$$e_1 \leq \ldots \leq e_t$$

and

$$e_1 + \ldots + e_t = n$$

*Proof:* The inequalities on the exponents are the conditions organizing the elementary divisors, and the last equality reflects the condition that the order of the whole group be as required. ///

[3.0.4] **Example:** Count the number of abelian groups of order 1000.

A finite abelian group is certainly finitely generated. Since $100000 = 2^5 \cdot 5^5$ (and 2 and 5 are distinct primes in $\mathbb{Z}$), by observations above, every abelian group of order 100000 is uniquely expressible as a direct sum of an abelian group of order $2^5$ and an abelian group of order $5^5$. From the last corollary, the number of abelian groups of order $p^5$ for any prime $p$ is the number of sums of non-decreasing sequences of positive integers which sum to the exponent, here 5. [9] For 5 the possibilities are

$$\begin{aligned} 1+1+1+1+1 &= 5 \\ 1+1+1+2 &= 5 \\ 1+2+2 &= 5 \\ 1+1+3 &= 5 \\ 2+3 &= 5 \\ 1+4 &= 5 \\ 5 &= 5 \end{aligned}$$

That is, the abelian groups of order $p^5$ for prime $p$ are

$$\mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p$$

$$\mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p^2$$

$$\mathbb{Z}/p \oplus \mathbb{Z}/p^2 \oplus \mathbb{Z}/p^2$$

$$\mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p^3$$

$$\mathbb{Z}/p^2 \oplus \mathbb{Z}/p^3$$

$$\mathbb{Z}/p \oplus \mathbb{Z}/p^4$$

$$\mathbb{Z}/p^5$$

Thus, there are 7 abelian groups of order $2^5$, and 7 of order $5^5$, and $7 \cdot 7 = 49$ abelian groups of order $2^5 \cdot 5^5 = 100000$.

[9] The number of non-decreasing sequences of positive integers summing to $n$ is the number of **partitions** of $n$. This number grows rapidly with $n$, and seems not to be expressible by any simple computationally useful formula.

A useful and commonly occurring manner of describing a finitely-generated $\mathbb{Z}$-module is as a *quotient* of

$$M = \mathbb{Z}^t = \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{t}$$

by a submodule $N$, which itself can be described as the image of some $\mathbb{Z}^r$. The **standard basis** of $\mathbb{Z}^t$ is the set of generators given by

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \quad (1 \text{ at } i^{th} \text{ place})$$

In the following chapter we will prove a result giving as a special case

[3.0.5] **Corollary:** Let $M$ be a $\mathbb{Z}$-module generated by $m_1, \ldots, m_t$. Then there is a unique $\mathbb{Z}$-module homomorphism $f : \mathbb{Z}^t \longrightarrow M$ such that $f(e_i) = m_i$. The kernel of $f$ is finitely generated on at most $t$ generators, and in fact is isomorphic to $\mathbb{Z}^r$ for some $r \leq t$.

///

---

# 4. *Jordan canonical form*

In this section we make the other popular choice of PID, namely $k[x]$ for a field $k$.

Let $k$ be a field, $V$ a finite-dimensional vector space over $k$, and $T$ a $k$-linear endomorphism of $V$. Let $k[x] \longrightarrow \mathrm{End}_k(V)$ be the unique $k$-algebra homomorphism which sends $x \longrightarrow T$. This makes $V$ into a $k[x]$-module. To say that $V$ is finite-dimensional is to say that it is finitely-generated as a $k$-module, so certainly is finitely-generated as a $k[x]$-module. Thus, by the Structure Theorem, and by the prime-wise further decompositions,

[4.0.1] **Corollary:** Given $k$-vectorspace $V$ and $k$-linear endomorphism $T$ of $V$, there is a sequence of monic polynomials $d_1, \ldots, d_t$ with [10]

$$d_1 | d_2 | \ldots | d_t$$

such that, as a $k[x]$-module,

$$V \approx k[x]/\langle d_1 \rangle \oplus \ldots \oplus k[x]/\langle d_t \rangle$$

where $x$ acts on $V$ by $T$, and $x$ acts on the right-hand side by multiplication by $x$. [11] Further, taking monic irreducibles $f_1, \ldots, f_r$ and exponents $e_{ij}$ such that $d_i = \prod_j f_j^{e_{ij}}$, we have

$$V \approx \left( k[x]/\langle f_1^{e_{11}} \rangle \oplus \ldots \oplus k[x]/\langle f_1^{e_{t1}} \rangle \right) \oplus \ldots \oplus \left( k[x]/\langle f_r^{e_{1r}} \rangle \oplus \ldots \oplus k[x]/\langle f_r^{e_{tr}} \rangle \right)$$

Though we have not chosen a basis nor written matrices, this $k[x]$-module decomposition of the original $k$-vectorspace with endomorphism $T$ is a **Jordan canonical form** of $V$ with respect to $T$. [12] The monic polynomials $d_i$ that occur are the **elementary divisors** of $T$ on $V$. [13]

---

[10] One must remember that divisibility of elements and inclusion of the corresponding principal ideals run in opposite directions, namely, $a|b$ if and only if $Ra \supset Rb$.

[11] What else could the action be on a sum of $k[x]$-modules of the form $k[x]/I$?

[12] It is only *a* canonical form because there are typically many different $k[x]$-isomorphisms of $V$ to such a direct sum.

[13] It is not hard to see that the *minimal polynomial* of $T$ (that is, the monic generator for the kernel of the map $k[x] \longrightarrow \mathrm{End}_k(V)$ that sends $x \longrightarrow T$) is the largest $d_t$ of the elementary divisors $d_i$ of $T$.

Breaking $V$ up into $k[x]$-module summands of the form

$$N = k[x]/\langle f^e \rangle \quad (f \text{ irreducible monic in } k[x])$$

is the finest reasonable decomposition to expect. Each such $N$ is a $k$-vectorspace of dimension $\deg f$. [14]

**[4.0.2] Example:** Let

$$V = k[x]/\langle (x-\lambda)^e \rangle$$

be a $k$-vectorspace with with operator $T$ given by multiplication by $x$ (on the quotient), with $\lambda \in k$. Then

$$x \cdot (x-\lambda)^{e-1} = (x-\lambda)(x-\lambda)^{e-1} + \lambda(x-\lambda)^{e-1} = \lambda \cdot (x-\lambda)^{e-1} \bmod (x-\lambda)^e$$

That is, $(x-\lambda)^{e-1}$ modulo $(x-\lambda)^e$ is a $\lambda$-**eigenvector** with **eigenvalue** $\lambda$ for the operator $T$. [15]

**[4.0.3] Example:** A $k[x]$-module of the form

$$V = k[x]/\langle F \rangle$$

with (not necessarily irreducible) monic

$$F(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + xa_2x^2 + a_1x + a_0$$

in $k[x]$ of degree $n$ is called a **cyclic module** for $k[x]$, since it can be generated by a single element, as we shall see here. A reasonable choice of $k$-basis is

$$1,\ x,\ x^2,\ \ldots,\ x^{n-1}$$

Then the endomorphism $T$ on $V$ given by multiplication by $x$ is, with respect to this basis,

$$T \cdot x^i = \begin{cases} x^{i+1} & (i < n-1) \\ -(a_0 + a_1x + \ldots + a_{n-1}x^{n-1}) & (i = n-1) \end{cases}$$

That is, with respect to this basis, $T$ has the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \ldots & -a_0 \\ 1 & 0 & 0 & 0 & 0 & & -a_1 \\ 0 & 1 & 0 & 0 & 0 & & -a_2 \\ \vdots & & \ddots & \ddots & & & \vdots \\ & & & 1 & 0 & & -a_{n-3} \\ & & & 0 & 1 & 0 & -a_{n-2} \\ 0 & & & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

This is the **rational canonical form** of $T$. [16]

---

[14] If the exponent $e$ is strictly larger than 1, then there are yet smaller $k[x]$ submodules, but they will not appear in a direct sum decomposition. This is clarified in examples below.

[15] As usual, for a $k$-linear endomorphism $T$ of a $k$-vectorspace $V$, a non-zero vector $v \in V$ is a $T$-eigenvector with eigenvalue $\lambda \in k$ if $Tv = \lambda v$. In some sources these are called *proper values* rather than eigenvalues, but this terminology seems to be no longer in use.

[16] Note that only on a *cyclic* $k[x]$-module (where $x$ acts by a $k$-linear endomorphism $T$) is there such a rational canonical form of the endomorphism $T$. And, yes, the question of whether or not a $k$-vectorspace with distinguished endomorphism $T$ is cyclic or not certainly does depend on the endomorphism $T$. If there is a vector such that $v, Tv, T^2v, \ldots$ form a basis, the module is cyclic, and $v$ is a **cyclic vector**.

**[4.0.4] Remark:** If we want to make a matrix $T$ (viewed as an endomorphism of $k^n$, viewed as column vectors) such that with the $k[x]$-module structure on $k^n$ created by $k[x] \longrightarrow \mathrm{End}_k k^n$ given by $x \longrightarrow T$,

$$k^n \approx k[x]/\langle F\rangle$$

as $k[x]$-modules, we simply take the matrix $T$ as above, namely with sub-diagonal 1s and the coefficients of the desired polynomial arranged in the right column. [17]

**[4.0.5] Example:** To make a 3-by-3 matrix $T$ so that the associated $k[x]$-structure on $k^3$ gives a module isomorphic to

$$k[x]/\langle x^3 + 2x^2 + 5x + 7\rangle$$

we take

$$T = \begin{pmatrix} 0 & 0 & -7 \\ 1 & 0 & -5 \\ 0 & 1 & -2 \end{pmatrix}$$

If $k$ happens to be *algebraically closed*, then a monic irreducible is of the form $x - \lambda$ for some $\lambda \in k$. Thus, the simplest $k[x]$-modules we're looking at in the context of the Structure Theorem are $k$-vectorspaces $V$ of the form

$$V = k[x]/\langle (x-\lambda)^e\rangle$$

The endomorphism $T$ of $V$ is multiplication by $x$. [18] At this point we can choose $k$-bases with respect to which the matrix of $T$ (multiplication by $x$) is of various simple sorts. One obvious choice [19] is to take $k$-basis consisting of (the *images* of, in the quotient)

$$1,\ x,\ x^2,\ \ldots,\ x^{e-1}$$

We have

$$T \cdot x^i = \begin{cases} x^{i+1} & (\text{for } i < e-1) \\ x^e - (x-\lambda)^e & (\text{for } i = e-1) \end{cases}$$

The slightly peculiar expression in the case $i = e-1$ is designed to be a polynomial of degree $< e$, hence, a linear combination of the specified basis elements $1, x, \ldots, x^{e-1}$. [20] The other obvious choice is

$$1,\ x-\lambda,\ (x-\lambda)^2,\ \ldots,\ (x-\lambda)^{e-1}$$

In this case, since

$$x(x-\lambda)^i = (x-\lambda)^{i+1} + \lambda(x-\lambda)^i$$

we have

$$T \cdot (x-\lambda)^i = \begin{cases} \lambda(x-\lambda)^i + (x-\lambda)^{i+1} & (\text{for } i < e-1) \\ \lambda(x-\lambda)^i & (\text{for } i = e-1) \end{cases}$$

The latter choice shows that (the image in the quotient of)

$$(x-\lambda)^{e-1} = \lambda - \text{eigenvalue of } T$$

[17] No, this sort of construction does not give any idea about eigenvalues or eigenvectors. But, on some occasions, this is not the issue.

[18] Now that we've forgotten the original $T$ above, having replaced it by multiplication by $x$ on a quotient of $k[x]$!

[19] Which might have the appeal of not depending upon $\lambda$.

[20] The matrix arising from this choice of basis is, in some circumstances, for example as just above, called the *rational canonical form*, though one should not depend upon this.

Indeed, the matrix for $T$ with respect to the latter basis is the **Jordan block**

$$\begin{pmatrix} \lambda & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & \lambda & 0 & 0 & 0 & & \\ 0 & 1 & \lambda & 0 & 0 & & \\ \vdots & & & \ddots & & & \vdots \\ & & & 1 & \lambda & 0 & 0 \\ & & & 0 & 1 & \lambda & 0 \\ 0 & & \dots & & 0 & 1 & \lambda \end{pmatrix}$$

Thus, concerning matrices, the Structure Theorem says

[4.0.6] **Corollary:** For algebraically closed fields $k$, given an endomorphism $T$ of a finite-dimensional $k$-vectorspace, there is a choice of basis such that the associated matrix is of the form

$$\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_t \end{pmatrix}$$

where each $B_i$ on the diagonal is a **Jordan block**, and all other entries are 0. ///

[4.0.7] **Example:** When $k$ is not necessarily algebraically closed, there may be irreducibles in $k[x]$ of higher degree. For monic irreducible $f$ in $k[x]$ consider the $k[x]$-module

$$V = k[x]/\langle f^e \rangle$$

with endomorphism $T$ being multiplication by $x$ (on the quotient). Choice of $k$-basis that illuminates the action of $T$ is more ambiguous now. Still, there are not very many plausible natural choices. Let $d = \deg f$. Then take $k$-basis consisting of (the images in the quotient of)

$$1, x, x^2, \dots, x^{d-1},\ f,\ f \cdot x,\ f \cdot x^2 \dots, f \cdot x^{d-1},\ \dots,\ f^{e-1},\ f^{e-1}x,\ \dots,\ f^{e-1} \cdot x^{d-1}$$

That is, we choose a basis $1, x, x^2, \dots, x^{d-1}$ for (images of) polynomials of degrees less than $f$, and then multiply those by powers of $f$ below the power $f^e$ that is (by definition) 0 in the quotient. [21] The endomorphism $T$ is still multiplication by $x$ in the quotient. For certain of the basis elements the effect is easy to describe in terms of the basis: [22]

$$T \cdot f^i \cdot x^j = f^i \cdot x^{j+1} \quad (\text{for } j < d-1)$$

However the other cases are somewhat messier than before. Namely,

$$T \cdot f^i \cdot x^{d-1} = \begin{cases} f^i \cdot x^d &= f^i \cdot (x^d - f) + f^{i+1} \quad (i < e-1) \\ f^i \cdot x^d &= f^i \cdot (x^d - f) \quad (i = e-1) \end{cases}$$

Note that $x^d - f$ is a linear combination of monomials $x^j$ with $0 \le j \le d-1$. This is still called a **Jordan canonical form**.

[4.0.8] **Example:** Let $k = \mathbb{R}$, $f(x) = x^2 + 1$, and consider

$$V = \mathbb{R}[x]/\langle (x^2+1)^3 \rangle$$

[21] Note that there is no obvious choice to replace $1, x, x^2, \dots, x^{d-1}$.

[22] Note that this easy case did not occur at all when the monic irreducible $f$ was *linear*.

According to the prescription just given, we take basis

$$1,\ x,\ x^2+1,\ (x^2+1)x,\ (x^2+1)^2,\ (x^2+1)^2x$$

Then the endomorphism $T$ which is multiplication by $x$ is, in terms of this basis,

$$\begin{array}{lcccl} T\cdot 1 & & & = & x \\ T\cdot x & = & x^2 & = & -1+(x^2+1) \\ T\cdot x^2+1 & & & = & (x^2+1)x \\ T\cdot (x^2+1)x & = & (x^2+1)x^2 & = & -(x^2+1)+(x^2+1)^2 \\ T\cdot (x^2+1)^2 & & & = & (x^2+1)^2x \\ T\cdot (x^2+1)^2x & = & (x^2+1)^2x^2 & = & -(x^2+1)^2 \end{array}$$

since $(x^2+1)^3=0$ in the quotient. That is, with respect to this basis, the matrix is

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Notice that there is no eigenvector or eigenvalue in the usual more elementary sense. But we still do have some understanding of what the endomorphism does.

[4.0.9] **Remark:** Note that the latter more complicated (because $k$ need not be algebraically closed) version of Jordan canonical form incorporates both the simpler version of Jordan canonical form as well as the rational canonical form.

---

# 5. *Conjugacy versus $k[x]$-module isomorphism*

First, it is important to realize that conjugation of matrices

$$A \longrightarrow gAg^{-1}$$

(for invertible $g$) is exactly changing the basis with respect to which one computes the matrix of the underlying endomorphism.

Two $n$-by-$n$ matrices $A$ and $B$ with entries in a field $k$ are **conjugate** if there is an invertible $n$-by-$n$ matrix $g$ with entries in $k$ such that

$$B = gAg^{-1}$$

Conjugacy is obviously an equivalence relation. The **conjugacy classes** of $n$-by-$n$ matrices with entries in $k$ are the corresponding equivalence classes with respect to this equivalence relation.

But it is somewhat misguided to fix upon matrices as descriptive apparatus for linear endomorphisms, [23] since, in effect, a matrix specifies not only the endomorphism but also a *basis* for the vector space, and a whimsically or accidentally chosen basis will not illuminate the structure of the endomorphism.

[23] Though, certainly, a matrix-oriented version of linear algebra is a reasonable developmental stage, probably *necessary*. And writing out a small numerical matrix is a compellingly direct description of an endomorphism, entirely adequate for many purposes.

Thus, we will take the viewpoint that, yes, the set $V = k^n$ of size $n$ column matrices with entries in $k$ is a $k$-vectorspace, and, yes, $n$-by-$n$ matrices give $k$-linear endomorphisms[24] of $V$ by matrix multiplication, *but*, no, this is only one of several possible descriptions, and admittedly sub-optimal for certain purposes.

Thus, more properly, given two $k$-linear endomorphisms $S$ and $T$ of a finite-dimensional $k$-vectorspace $V$, say that $S$ and $T$ are **conjugate** if there is an *automorphism*[25] $g : V \longrightarrow V$ such that

$$g \circ S \circ g^{-1} = T$$

Emphatically, this includes conjugation of matrices if or when we write endomorphisms as matrices.

The following proposition, which is trivial to prove once laid out clearly, illustrates (among other things) that conjugacy of matrices is a special example of a more meaningful structural property.

[5.0.1] **Proposition:** Let $V$ be a finite-dimensional $k$-vectorspace. Let $S$ and $T$ be two $k$-linear endomorphisms of $V$. Let $V_S$ be $V$ with the $k[x]$-module structure in which $x$ acts on $v \in V$ by $xv = Sv$, and let $V_T$ be $V$ with the $k[x]$-module structure in which $x$ acts on $v \in V$ by $xv = Tv$. Then $S$ and $T$ are conjugate if and only if $V_S \approx V_T$ as $k[x]$-modules.

*Proof:* First, suppose that $V_S \approx V_T$ as $k[x]$-modules. Let $g : V_S \longrightarrow V_T$ be the $k$-vectorspace isomorphism that is also a $k[x]$-module isomorphism. The latter condition means exactly that (in addition to the vectorspace isomorphism aspect) for all $v$ in $V$

$$g(x \cdot v) = x \cdot g(v)$$

That is, since in $V_S$ the action of $x$ is $xv = Sv$ and in $V_T$ is $xv = Tv$

$$g(Sv) = T\, g(v)$$

Since this is true for all $v \in V$, we have an equality of endomorphisms

$$g \circ S = T \circ g$$

Since $g$ is invertible,

$$g \circ S \circ g^{-1} = T$$

as claimed. It is clear that this argument is reversible, giving the opposite inclusion as well. ///

[5.0.2] **Remark:** The uniqueness part of the Structure Theorem says that the elementary divisors (ideals) $I_1 \supset \ldots \supset I_t$ in an expression

$$M \approx R/I_1 \oplus \ldots \oplus R/I_t$$

(with $M$ a finitely-generated module over a PID $R$) are uniquely determined by the $R$-module isomorphism class of $M$, and, conversely, that choice of such ideals uniquely determines the isomorphism class. Thus,

---

[24] At least once in one's life one should check that matrix multiplication and composition of endomorphisms are compatible. Given a $k$-vectorspace $V$ with $k$-basis $e_1, \ldots, e_n$, define a map $\varphi$ from the ring $\mathrm{End}_k(V)$ of $k$-linear endomorphisms to the ring of $n$-by-$n$ matrices with entries in $k$, by defining the $ij^{th}$ entry $\varphi(T)_{ij}$ of $\varphi(T)$ (for endomorphism $T$) by $Te_j = \sum_i \varphi(T)_{ij} e_i$. (Yes, there is another obvious possibility for indexing, but the present choice is what we want. One should check this, too.) Then $\varphi$ is a ring homomorphism. The main point is multiplication: On one hand, for two endomorphisms $S$ and $T$, $(S \circ T)e_k = \sum_j \varphi(S \circ T)_{ik} e_i$. On the other hand, using the linearity of $S$, $S(Te_k) = S(\sum_k \varphi(T)_{jk} e_j) = \sum_k \varphi(T)_{jk} \sum_k \varphi(S)_{ij} e_i$. Since a matrix product has $ij^{th}$ entry $(\varphi(S)\varphi(T))_{ij} = \sum_\ell \varphi(S)_{i\ell}\varphi(T)_{\ell j}$, the two expressions are the same thing.

[25] As usual, an automorphism is an endomorphism that is an isomorphism of the thing to itself.

[5.0.3] **Corollary:** Conjugacy classes of endomorphisms of a finite-dimensional $k$-vectorspace $V$ are in bijection with choices of (monic) elementary divisors $d_1|\dots|d_t$ in an expression

$$V \approx k[x]/\langle d_1\rangle \oplus \dots \oplus k[x]/\langle d_t\rangle$$

as $k[x]$-module. ///

[5.0.4] **Remark:** Further, using the unique factorization in the PID $k[x]$, one finds that in prime-wise decompositions (via Sun-Ze)

$$k[x]/\langle f_1^{e_1}\dots f_r^{e_r}\rangle \approx k[x]/\langle f_1^{e_1}\rangle \oplus \dots \oplus k[x]/\langle f_r^{e_r}\rangle$$

with $f_i$s irreducible, the exponents $e_i$ are uniquely determined by the isomorphism class, and vice-versa. Combining this uniqueness with the Structure Theorem's uniqueness gives the corresponding uniqueness for the general prime-wise expression of a module as a direct sum.

[5.0.5] **Remark:** The extent to which different-appearing Jordan forms of *matrices* can be conjugate is (likewise) answered by the uniqueness assertion of the Structure Theorem. For example, in the case of algebraically closed field, two Jordan forms are conjugate if and only if the collection (counting repeats) of Jordan blocks of one is equal to that of the other, allowing only permutations among the blocks. That is, in matrix form, the only mutually conjugate Jordan forms are visually obvious.

[5.0.6] **Example:** The following two Jordan forms are conjugate

$$\begin{pmatrix} 3 & 0 & 0 & 0 & 0\\ 1 & 3 & 0 & 0 & 0\\ 0 & 1 & 3 & 0 & 0\\ 0 & 0 & 0 & 7 & 0\\ 0 & 0 & 0 & 1 & 7 \end{pmatrix} \quad \text{is conjugate to} \quad \begin{pmatrix} 7 & 0 & 0 & 0 & 0\\ 1 & 7 & 0 & 0 & 0\\ 0 & 0 & 3 & 0 & 0\\ 0 & 0 & 1 & 3 & 0\\ 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

by

$$\begin{pmatrix} 3 & 0 & 0 & 0 & 0\\ 1 & 3 & 0 & 0 & 0\\ 0 & 1 & 3 & 0 & 0\\ 0 & 0 & 0 & 7 & 0\\ 0 & 0 & 0 & 1 & 7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 7 & 0 & 0 & 0 & 0\\ 1 & 7 & 0 & 0 & 0\\ 0 & 0 & 3 & 0 & 0\\ 0 & 0 & 1 & 3 & 0\\ 0 & 0 & 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}^{-1}$$

[5.0.7] **Remark:** Without further indications from context, it is not clear whether one would want to parametrize conjugacy classes by the decomposition given immediately by the Structure Theorem, namely sums of rational canonical forms, or by the further prime-wise decomposition (as in the Jordan decomposition), which do still involve some sort of rational canonical forms when the underlying field is not algebraically closed.

Generally, for a commutative ring $R$ with identity 1, let

$$GL(n,R) = \{ \text{ invertible } n\text{-by-}n \text{ matrices, entries in } R \}$$

This is the **general linear group** of size $n$ over $R$.

[5.0.8] **Example:** Determine the conjugacy classes in $GL(2,k)$ for a field $k$. Note that $GL(2,k)$ is the set (group) of *invertible* endomorphisms of the two-dimensional $k$-vectorspace $k^2$. From the Structure Theorem, and from the observation above that conjugacy classes are in bijection with batches of elementary divisors, we can immediately say that $k[x]$-module structures

$$V \approx k[x]/\langle d_1\rangle \oplus \dots \oplus k[x]/\langle d_t\rangle$$

with $d_1|\dots|d_t$ and

$$\deg d_1 + \dots + \deg d_t = 2 = \dim_k V$$

specify the conjugacy classes. [26] Since the dimension is just 2, there are only two cases

$$V \approx \begin{cases} k[x]/\langle d_1\rangle & (d_1 \text{ monic quadratic}) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\lambda\rangle & (\text{monic linear case}) \end{cases}$$

Yes, in the second case the linear monic is repeated, due to the divisibility requirement. Using rational canonical forms in the first case, and (in a degenerate sense) in the second case as well, we have corresponding irredundant conjugacy class representatives

$$\begin{pmatrix} 0 & -a_2 \\ 1 & -a_1 \end{pmatrix} \quad (a_1 \in k,\ a_2 \in k^\times)$$
$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \qquad (\lambda \in k^\times)$$

One might object that in the first of the two cases we have no indication of eigenvalues/eigenvectors. Thus, we might consider the two cases of quadratic monics, namely, irreducible and not. In the irreducible case nothing further happens, but with reducible $d_1(x) = (x-\lambda)(x-\mu)$ if $\lambda \neq \mu$ we have

$$k[x]/\langle (x-\lambda)(x-\mu)\rangle \approx k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\mu\rangle$$

We still have no real recourse but to use a rational canonical form for the quadratic irreducible case, but the reducible case with distinct zeros is diagonalized, and the *repeated factor* (reducible) case gives a non-trivial Jordan block. The $k[x]$-module structures are, respectively,

$$V \approx \begin{cases} k[x]/\langle d_1\rangle & (d_1 \text{ irreducible monic quadratic}) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\mu\rangle & (\lambda \neq \mu, \text{ both in } k^\times) \\ k[x]/\langle (x-\lambda)^2\rangle & (\text{repeated root case, } \lambda \in k^\times) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\lambda\rangle & (\text{monic linear case}) \end{cases}$$

In matrix form, the irredundant representatives are, respectively,

$$\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \quad (x^2 + a_1 x + a_0 \text{ irreducible})$$
$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \qquad (\lambda \neq \mu, \text{ both in } k^\times)$$
$$\begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix} \qquad (\lambda \in k^\times)$$
$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \qquad (\lambda \in k^\times)$$

[5.0.9] **Example:** Determine the conjugacy classes in $GL(3,k)$ for a field $k$. From the Structure Theorem and the fact that conjugacy classes are in bijection with batches of elementary divisors, the $k[x]$-module structures

$$V \approx k[x]/\langle d_1\rangle \oplus \dots \oplus k[x]/\langle d_t\rangle$$

[26] Again, the endomorphism $T$ representing the conjugacy class is the one given by multiplication by $x$ on the right-hand side. It is *transported* back to $V$ via the $k$-vectorspace isomorphism.

with $d_1|\dots|d_t$ and

$$\deg d_1 + \dots + \deg d_t = \dim_k V = 3$$

specify the conjugacy classes. Since the dimension is 3, there are 3 cases

$$V \approx \begin{cases} k[x]/\langle C\rangle & (C \text{ monic cubic}) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle (x-\lambda)(x-\mu)\rangle & (\lambda,\mu \in k^\times) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\lambda\rangle & (\lambda \in k^\times) \end{cases}$$

Yes, in the second case the linear monic is repeated, as even more so in the third, by the divisibility requirement. We can still use a rational canonical form in each of the cases, to write matrix versions of these

$$\begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix} \qquad (a_0 \in k^\times)$$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & -\lambda\mu \\ 0 & 1 & -\lambda-\mu \end{pmatrix} \qquad (\lambda,\mu \in k^\times)$$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \qquad (\lambda \in k^\times)$$

In the first two cases the eigenvalues/eigenvectors are not delineated. It breaks up into 3 subcases, namely, irreducible cubic, linear and irreducible quadratic, and three linear factors. The $k[x]$-module structures are, respectively,

$$V \approx \begin{cases} k[x]/\langle C\rangle & (C \text{ irred monic cubic}) \\ k[x]/\langle (x-\lambda)Q(x)\rangle & (\lambda \in k^\times,\ Q \text{ irred monic quadratic}) \\ k[x]/\langle (x-\lambda)(x-\mu)(x-\nu)\rangle & (\lambda,\mu,\nu \in k^\times) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle (x-\lambda)(x-\mu)\rangle & (\lambda,\mu \in k^\times) \\ k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\lambda\rangle & (\lambda \in k^\times) \end{cases}$$

The third and fourth cases break up into subcases depending upon the confluence (or not) of the parameters. That is, in the third case there are three subcases, where all the $\lambda, \mu\, nu$ are the same, only two are the same, or all different. The fourth case has two subcases, $\lambda = \mu$ or not. [27] In the following display, it is assumed that $\lambda, \mu, \nu$ are distinct and non-zero. The last-mentioned subcases are presented on the same line. And $Q$ is an irreducible monic quadratic, $C$ an irreducible monic cubic.

$$\frac{k[x]}{\langle C\rangle}$$

$$\frac{k[x]}{\langle (x-\lambda)Q(x)\rangle}$$

$$\frac{k[x]}{\langle x-\lambda\rangle} \oplus \frac{k[x]}{\langle x-\mu\rangle} \oplus \frac{k[x]}{\langle x-\nu\rangle} \qquad \frac{k[x]}{\langle (x-\lambda)^2\rangle} \oplus \frac{k[x]}{\langle x-\mu\rangle} \qquad \frac{k[x]}{\langle (x-\lambda)^3\rangle}$$

$$\frac{k[x]}{\langle x-\lambda\rangle} \oplus \frac{k[x]}{\langle x-\lambda\rangle} \oplus \frac{k[x]}{\langle x-\mu\rangle} \qquad \frac{k[x]}{\langle x-\lambda\rangle} \oplus \frac{k[x]}{\langle (x-\lambda)^2\rangle}$$

$$\frac{k[x]}{\langle x-\lambda\rangle} \oplus \frac{k[x]}{\langle x-\lambda\rangle} \oplus \frac{k[x]}{\langle x-\lambda\rangle}$$

[27] If the field $k$ is $\mathbb{F}_2$, then non-zero parameters in the ground field cannot be distinct.

In matrix form, the irredundant representatives are, respectively, (with $\lambda, \mu, \nu$ distinct and non-zero)

$$\begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix} \quad (x^3 + a_2x^2 + a_1x + a_2 \text{ irreducible})$$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & -a_0 \\ 0 & 1 & -a_1 \end{pmatrix} \qquad (x^2 + a_1x + a_0 \text{ irreducible})$$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 1 \\ 0 & 0 & \nu \end{pmatrix} \qquad \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix} \qquad \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}$$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix} \qquad \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}$$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

[5.0.10] **Example:** Determine the conjugacy classes in $GL(5, k)$ for field $k$. Use the Structure Theorem and the bijection of conjugacy classes with batches of elementary divisors. There are seven different patterns of degrees of elementary divisors, with $\lambda, \mu, \nu \in k^\times$, and all polynomials *monic*

(1) $$\frac{k[x]}{\langle Q \rangle} \qquad (Q \text{ quintic})$$

(2) $$\frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle (x-\lambda)C(x) \rangle} \qquad (C \text{ cubic})$$

(3) $$\frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle (x-\lambda)Q(x) \rangle} \qquad (Q \text{ quadratic})$$

(4) $$\frac{k[x]}{\langle Q(x) \rangle} \oplus \frac{k[x]}{\langle (x-\lambda)Q(x) \rangle} \qquad (Q \text{ quadratic})$$

(5) $$\frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle (x-\lambda)(x-\mu) \rangle}$$

(6) $$\frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle} \oplus \frac{k[x]}{\langle x-\lambda \rangle}$$

There is no obvious graceful way to write rational canonical forms that indicate divisibility. Listing the

divisors to save space, the reducibility subcases are (with $\lambda, \mu, \nu, \sigma, \tau$ non-zero)

| | | |
|---|---|---|
| $(1a)$ | $Q(x)$ | ($Q$ irred quintic) |
| $(1b)$ | $Q(x)C(x)$ | ($Q$ irred quadratic, $C$ irred cubic) |
| $(1c)$ | $(x-\lambda)Q_1(x)Q_2(2)$ | ($Q_1, Q_2$ irred quadratic) |
| $(1d)$ | $(x-\lambda)(x-\mu)(x-\nu)Q(2)$ | ($Q$ irred quadratic) |
| $(1e)$ | $(x-\lambda)(x-\mu)(x-\nu)(x-\sigma)(x-\tau)$ | |
| $(2a)$ | $(x-\lambda),\ (x-\lambda)C(x)$ | ($C$ irred cubic) |
| $(2b)$ | $(x-\lambda),\ (x-\lambda)(x-\mu)Q(x)$ | ($Q$ irred quadratic) |
| $(2c)$ | $(x-\lambda),\ (x-\lambda)(x-\mu)(x-\nu)(x-\tau)$ | |
| $(3a)$ | $(x-\lambda),\ (x-\lambda),\ (x-\lambda)Q(x)$ | ($Q$ irred quadratic) |
| $(3b)$ | $(x-\lambda),\ (x-\lambda),\ (x-\lambda)(x-\mu)(x-\nu)$ | |
| $(3c)$ | $Q(x),\ (x-\lambda)Q(x)$ | ($Q$ irred quadratic) |
| $(3d)$ | $(x-\mu)(x-\nu),\ (x-\lambda)(x-\mu)(x-\nu)$ | |
| $(4)$ | $(x-\lambda),\ (x-\lambda),\ (x-\lambda),\ (x-\lambda)(x-\mu)$ | |
| $(5)$ | $(x-\lambda),\ (x-\lambda),\ (x-\lambda),\ (x-\lambda),\ (x-\lambda)$ | |

There still remains the sorting into subcases, depending upon confluence of parameters. The most novel case is the case denoted $1c$ above, where there is a single elementary divisor $(x-\lambda)Q_1(x)Q_2(x)$, with irreducible monic quadratics[28] $Q_i$. If $Q_1 \neq Q_2$, the canonical form is merely a direct sum of previous (smaller) cases. But if $Q_1 = Q_2$, a new thing happens in the direct summand $k[x]/\langle Q(x)^2\rangle$ in

$$k[x]/\langle (x-\lambda)\,Q(x)^2\rangle \approx k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle Q(x)^2\rangle$$

As earlier, letting $Q(x) = x^2 + a_1x + a_2$, we can choose a basis

$$1,\ x,\ Q(x),\ xQ(x) \mod Q(x)^2$$

for $k[x]/\langle Q(x)^2\rangle$. Then the endomorphism given by multiplication by $x$ has matrix

$$\begin{pmatrix} 0 & -a_0 & 0 & 0 \\ 1 & -a_1 & 0 & 0 \\ 0 & 1 & 0 & -a_0 \\ 0 & 0 & 1 & -a_1 \end{pmatrix}$$

**[5.0.11] Example:** Determine the matrix canonical form for an endomorphism $T$ of a 6-dimensional $k$-vectorspace $V$, where $T$ has the single elementary divisor $C(x)^2$m where $C$ is an irreducible monic cubic

$$C(x) = x^3 + a_2x^2 + a_1x + a_0$$

[28] If the underlying field $k$ is algebraically closed, this and more complicated situations do not arise.

Take basis

$$1,\ x,\ x^2,\ C(x),\ xC(x),\ x^2C(x) \mod C(x)^2$$

for $k[x]/\langle C(x)^2\rangle$. Then the endomorphism $T$ given by multiplication by $x$ has matrix

$$\begin{pmatrix} 0 & 0 & -a_0 & 0 & 0 & 0 \\ 1 & 0 & -a_1 & 0 & 0 & 0 \\ 0 & 1 & -a_2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -a_0 \\ 0 & 0 & 0 & 1 & 0 & -a_1 \\ 0 & 0 & 0 & 0 & 1 & -a_2 \end{pmatrix}$$

[5.0.12] **Example:** If the single elementary divisor were $C(x)^3$ with a monic cubic $C(x) = x^3 + a^2x^2 + a_1x + a_0$, then the basis

$$1,\ x,\ x^2,\ C(x),\ xC(x),\ x^2C(x),\ C(x)^{@},\ xC(x)^2,\ x^2C(x)^2 \mod C(x)^3$$

gives matrix

$$\begin{pmatrix} 0 & 0 & -a_0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -a_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -a_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -a_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -a_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -a_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -a_2 \end{pmatrix}$$

---

# 6. *Worked examples*

[10.1] Given a 3-by-3 matrix $M$ with integer entries, find $A, B$ integer 3-by-3 matrices with determinant $\pm 1$ such that $AMB$ is diagonal.

Let's give an *algorithmic*, rather than *existential*, argument this time, saving the existential argument for later.

First, note that given two integers $x, y$, not both 0, there are integers $r, s$ such that $g = \gcd(x, y)$ is expressible as $g = rx + sy$. That is,

$$(\ x \quad y\ ) \begin{pmatrix} r & * \\ s & * \end{pmatrix} = (\ g \quad *\ )$$

What we want, further, is to figure out what other two entries will make the second entry 0, *and* will make that 2-by-2 matrix invertible (in $GL_2(\mathbb{Z})$). It's not hard to guess:

$$(\ x \quad y\ ) \begin{pmatrix} r & -y/g \\ s & x/g \end{pmatrix} = (\ g \quad 0\ )$$

Thus, given $(x\ y\ z)$, there is an invertible 2-by-2 integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$(\ y \quad z\ ) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\ \gcd(y, z) \quad 0\ )$$

That is,

$$(\,x \quad y \quad z\,)\begin{pmatrix}1&0&0\\0&a&b\\0&c&d\end{pmatrix} = (\,x \quad \gcd(y,z) \quad 0\,)$$

Repeat this procedure, now applied to $x$ and $\gcd(y,z)$: there is an invertible 2-by-2 integer matrix $\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}$ such that

$$(\,x \quad \gcd(y,z)\,)\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix} = (\,\gcd(x,\gcd(y,z)) \quad 0\,)$$

That is,

$$(\,x \quad \gcd(y,z) \quad 0\,)\begin{pmatrix}a'&b'&0\\c'&d'&0\\0&0&1\end{pmatrix} = (\,\gcd(x,y,z) \quad 0 \quad 0\,)$$

since *gcd*s can be computed iteratively. That is,

$$(\,x \quad y \quad z\,)\begin{pmatrix}1&0&0\\0&a&b\\0&c&d\end{pmatrix}\begin{pmatrix}a'&b'&0\\c'&d'&0\\0&0&1\end{pmatrix} = (\,\gcd(x,y,z) \quad 0 \quad 0\,)$$

Given a 3-by-3 matrix $M$, *right*-multiply by an element $A_1$ of $GL_3(\mathbb{Z})$ to put $M$ into the form

$$MA_1 = \begin{pmatrix}g_1&0&0\\*&*&*\\*&*&*\end{pmatrix}$$

where (necessarily!) $g_1$ is the *gcd* of the top row. Then *left*-multiply by an element $B_2 \in GL_3(\mathbb{Z})$ to put $MA$ into the form

$$B_2 \cdot MA_1 = \begin{pmatrix}g_2&*&*\\0&*&*\\0&*&*\end{pmatrix}$$

where (necessarily!) $g_2$ is the *gcd* of the left column entries of $MA_1$. Then right multiply by $A_3 \in GL_3(\mathbb{Z})$ such that

$$B_2MA_1 \cdot A_3 = \begin{pmatrix}g_3&0&0\\*&*&*\\*&*&*\end{pmatrix}$$

where $g_3$ is the *gcd* of the top row of $B_2MA_1$. Continue. Since these *gcd*s divide each other successively

$$\ldots |g_3|g_2|g_1 \neq 0$$

and since any such chain must be finite, after finitely-many iterations of this the upper-left entry ceases to change. That is, for some $A, B \in GL_3(\mathbb{Z})$ we have

$$BMA = \begin{pmatrix}g&*&*\\0&x&y\\0&*&*\end{pmatrix}$$

and also $g$ divides the top row. That is,

$$u = \begin{pmatrix}1&-x/g&-y/g\\0&1&0\\0&0&1\end{pmatrix} \in GL_3(\mathbb{Z})$$

Then

$$BMA \cdot u = \begin{pmatrix} g & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

Continue in the same fashion, operating on the lower right 2-by-2 block, to obtain a form

$$\begin{pmatrix} g & 0 & 0 \\ 0 & g_2 & 0 \\ 0 & 0 & g_3 \end{pmatrix}$$

Note that since the $r, s$ such that $\gcd(x, y) = rx + sy$ can be found via Euclid, this whole procedure is *effective*. And it certainly applies to larger matrices, not necessarily square.

[10.2] Given a row vector $x = (x_1, \ldots, x_n)$ of integers whose *gcd* is 1, prove that there exists an $n$-by-$n$ integer matrix $M$ with determinant $\pm 1$ such that $xM = (0, \ldots, 0, 1)$.

(*The iterative/algorithmic idea of the previous solution applies here, moving the gcd to the right end instead of the left.*)

[10.3] Given a row vector $x = (x_1, \ldots, x_n)$ of integers whose *gcd* is 1, prove that there exists an $n$-by-$n$ integer matrix $M$ with determinant $\pm 1$ whose bottom row is $x$.

This is a corollary of the previous exercise. Given $A$ such that

$$xA = (\, 0 \quad \ldots \quad 0 \quad \gcd(x_1, \ldots, x_n) \,) = (\, 0 \quad \ldots \quad 0 \quad 1 \,)$$

note that this is saying

$$\begin{pmatrix} * & \ldots & * \\ \vdots & & \vdots \\ * & \ldots & * \\ x_1 & \ldots & x_n \end{pmatrix} \cdot A = \begin{pmatrix} * & \ldots & * & * \\ \vdots & & \vdots & \vdots \\ * & \ldots & * & * \\ 0 & \ldots & 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} * & \ldots & * \\ \vdots & & \vdots \\ * & \ldots & * \\ x_1 & \ldots & x_n \end{pmatrix} = \begin{pmatrix} * & \ldots & * & * \\ \vdots & & \vdots & \vdots \\ * & \ldots & * & * \\ 0 & \ldots & 0 & 1 \end{pmatrix} \cdot A^{-1}$$

This says that $x$ is the bottom row of the invertible $A^{-1}$, as desired.

[10.4] Show that $GL(2, \mathbb{F}_2)$ is isomorphic to the permutation group $S_3$ on three letters.

There are exactly 3 non-zero vectors in the space $\mathbb{F}_2^2$ of column vectors of size 2 with entries in $\mathbb{F}_2$. Left multiplication by elements of $GL_2(\mathbb{F}_2)$ permutes them, since the invertibility assures that no non-zero vector is mapped to zero. If $g \in GL_2(\mathbb{F}_2)$ is such that $gv = v$ for all non-zero vectors $v$, then $g = 1_2$. Thus, the map

$$\varphi : GL_2(\mathbb{F}_2) \longrightarrow \text{permutations of the set } N \text{ of non-zero vectors in } \mathbb{F}_2^2$$

is *injective*. It is a group homomorphism because of the associativity of matrix multiplication:

$$\varphi(gh)(v) = (gh)v = g(hv) = \varphi(g)(\varphi(h)(v))$$

Last, we can confirm that the injective group homomorphism $\varphi$ is also surjective by showing that the order of $GL_2(\mathbb{F}_2)$ is the order of $S_3$, namely, 6, as follows. An element of $GL_2(\mathbb{F}_2)$ can send any basis for $\mathbb{F}_2^2$ to any other basis, and, conversely, is completely determined by telling what it does to a basis. Thus, for example, taking the first basis to be the standard basis $\{e_1, e_2\}$ (where $e_i$ has a 1 at the $i^{th}$ position and 0s

elsewhere), an element $g$ can map $e_1$ to any non-zero vector, for which there are $2^2-1$ choices, counting *all* less 1 for the zero-vector. The image of $e_2$ under $g$ must be linearly independent of $e_1$ for $g$ to be invertible, and conversely, so there are $2^2-2$ choices for $ge_2$ (*all* less 1 for 0 and less 1 for $ge_1$). Thus,

$$|GL_2(\mathbb{F}_2)| = (2^2-1)(2^2-2) = 6$$

Thus, the map of $GL_2(\mathbb{F}_2)$ to permutations of non-zero vectors gives an isomorphism to $S_3$.

[10.5] Determine all conjugacy classes in $GL(2,\mathbb{F}_3)$.

First, $GL_2(\mathbb{F}_3)$ is simply the group of *invertible* $k$-linear endomorphisms of the $\mathbb{F}_3$-vectorspace $\mathbb{F}_3^2$. As observed earlier, conjugacy classes of endomorphisms are in bijection with $\mathbb{F}_3[x]$-module structures on $\mathbb{F}_3^2$, which we know are given by *elementary divisors*, from the Structure Theorem. That is, all the possible structures are parametrized by monic polynomials $d_1|\dots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_3^2$, namely 2. Thus, we have a list of irredundant representatives

$$\begin{cases} \mathbb{F}_3[x]/\langle Q\rangle & Q \text{ monic quadratic in } \mathbb{F}_3[x] \\ \mathbb{F}_3[x]/\langle x-\lambda\rangle \oplus \mathbb{F}_3[x]/\langle x-\lambda\rangle & \lambda \in \mathbb{F}_3^\times \end{cases}$$

We *can* write the first case in a so-called rational canonical form, that is, choosing basis $1, x \bmod Q$, so we have two families

$$\begin{cases} (1) & \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} & b \in \mathbb{F}_3,\ a \in \mathbb{F}_3^\times \\ (2) & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} & \lambda\mathbb{F}_3^\times \end{cases}$$

But the first family can be usefully broken into three subcases, namely, depending upon the reducibility of the quadratic, and whether or not there are repeated roots: there are 3 cases

$$\begin{array}{rcll} Q(x) & = & \text{irreducible} & \\ Q(x) & = & (x-\lambda)(x-\mu) & (\text{with } \lambda \neq \mu) \\ Q(x) & = & (x-\lambda)^2 & \end{array}$$

And note that if $\lambda \neq \mu$ then (for a field $k$)

$$k[x]/\langle (x-\lambda)(x-\mu)\rangle \approx k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\mu\rangle$$

Thus, we have

$$\begin{cases} (1a) & \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} & x^2+ax+b \text{ irreducible in } \mathbb{F}_3[x] & \\ (1b) & \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} & \lambda \neq \mu \text{ both nonzero} & (\text{modulo interchange of } \lambda,\mu) \\ (1b) & \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} & \lambda \in \mathbb{F}_3^2 & \\ (2) & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} & \lambda \in \mathbb{F}_3^\times & \end{cases}$$

One might, further, list the irreducible quadratics in $\mathbb{F}_3[x]$. By counting, we know there are $(3^2-3)/2 = 3$ irreducible quadratics, and, thus, the guesses $x^2-2$, $x^2+x+1$, and $x^2-x+1$ (the latter two being cyclotomic, the first using the fact that 2 is not a square mod 3) are all of them.

[10.6] Determine all conjugacy classes in $GL(3,\mathbb{F}_2)$.

Again, $GL_3(\mathbb{F}_2)$ is the group of *invertible* $k$-linear endomorphisms of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_2^3$, and conjugacy classes of endomorphisms are in bijection with $\mathbb{F}_2[x]$-module structures on $\mathbb{F}_2^3$, which are given by *elementary divisors*. So all possibilities are parametrized by monic polynomials $d_1|\dots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_2^3$, namely 3. Thus, we have a list of irredundant representatives

$$\begin{cases} (1) & \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic cubic in } \mathbb{F}_2[x] \\ (2) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle & \\ (3) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle & \end{cases}$$

since the only non-zero element of $\mathbb{F}_2$ is $\lambda = 1$. We *can* write the first case in a so-called rational canonical form, that is, choosing basis $1, x, x^2 \bmod Q$, there are three families

$$\begin{cases} (1) & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix} & x^3 + ax^2 + bx + 1 \text{ in } \mathbb{F}_2[x] \\ (2) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} & \\ (3) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \end{cases}$$

It is useful to look in detail at the possible factorizations in case 1, breaking up the single summand into more summands according to relatively prime factors, giving cases

$$\begin{cases} (1a) & \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle \\ (1a') & \mathbb{F}_2[x]/\langle x^3 + x^2 + 1\rangle \\ (1b) & \mathbb{F}_2[x]/\langle (x-1)(x^2 + x + 1)\rangle \\ (1c) & \mathbb{F}_2[x]/\langle (x-1)^3\rangle \end{cases}$$

since there are just two irreducible cubics $x^3 + x + 1$ and $x^3 + x^2 + 1$, and a unique irreducible quadratic, $x^2 + x + 1$. (The counting above tells the number, so, after any sort of guessing provides us with the right number of verifiable irreducibles, we can stop.) Thus, the 6 conjugacy classes have irredundant matrix representatives

$$(1a)\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad (1a')\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad (1b)\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad (1c)\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$(2)\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad (3)\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

[10.7] Determine all conjugacy classes in $GL(4, \mathbb{F}_2)$.

Again, $GL_4(\mathbb{F}_2)$ is *invertible* $k$-linear endomorphisms of $\mathbb{F}_2^4$, and conjugacy classes are in bijection with $\mathbb{F}_2[x]$-module structures on $\mathbb{F}_2^4$, given by *elementary divisors*. So all possibilities are parametrized by monic polynomials $d_1|\dots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_2^4$, namely 4. Thus,

we have a list of irredundant representatives

$$\begin{cases} \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic quartic} \\ \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)Q(x)\rangle & Q \text{ monic quadratic} \\ \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle & \\ \mathbb{F}_2[x]/\langle Q\rangle \oplus \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic quadratic} \\ \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle & \end{cases}$$

since the only non-zero element of $\mathbb{F}_2$ is $\lambda = 1$. We could write all cases using rational canonical form, but will not, deferring matrix forms till we've further decomposed the modules. Consider possible factorizations into irreducibles, giving cases

$$\begin{cases} (1a) & \mathbb{F}_2[x]/\langle x^4+x+1\rangle \\ (1a') & \mathbb{F}_2[x]/\langle x^4+x^3+1\rangle \\ (1a'') & \mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle \\ (1b) & \mathbb{F}_2[x]/\langle (x-1)(x^3+x+1)\rangle \\ (1b') & \mathbb{F}_2[x]/\langle (x-1)(x^3+x^2+1)\rangle \\ (1c) & \mathbb{F}_2[x]/\langle (x-1)^2(x^2+x+1)\rangle \\ (1d) & \mathbb{F}_2[x]/\langle (x^2+x+1)^2\rangle \\ (1e) & \mathbb{F}_2[x]/\langle (x-1)^4\rangle \\ (2a) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)(x^2+x+1)\rangle \\ (2b) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^3\rangle \\ (3) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\ (4a) & \mathbb{F}_2[x]/\langle x^2+x+1\rangle \oplus \mathbb{F}_2[x]/\langle x^2+x+1\rangle \\ (4b) & \mathbb{F}_2[x]/\langle (x-1)^2\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\ (5) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \end{cases}$$

since there are exactly three irreducible quartics (as indicated), two irreducible cubics, and a single irreducible

quadratic. Matrices are, respectively, and unilluminatingly,

$$\begin{bmatrix} 0&0&0&1\\ 1&0&0&1\\ 0&1&0&0\\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 0&0&0&1\\ 1&0&0&1\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&1\\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&0\\ 0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 0&1&0&0\\ 1&1&0&0\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&1&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 0&1&0&0\\ 1&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 0&0&1&0\\ 0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}$$

[10.8] Tell a $p$-Sylow subgroup in $GL(3, \mathbb{F}_p)$.

To compute the order of this group in the first place, observe that an automorphism (invertible endomorphism) can take any basis to any other. Thus, letting $e_1, e_2, e_3$ be the standard basis, for an automorphism $g$ the image $ge_1$ can be any non-zero vector, of which there are $p^3 - 1$. The image $ge_2$ can be anything not in the span of $ge_1$, of which there are $p^3 = p$. The image $ge_3$ can be anything not in the span of $ge_1$ and $ge_2$, of which, because those first two were already linearly independent, there are $p^3 - p^2$. Thus, the order is

$$|GL_3(\mathbb{F}_p)| = (p^3 - 1)(p^3 - p)(p^3 - p^2)$$

The power of $p$ that divides this is $p^3$. Upon reflection, a person might hit upon considering the subgroup of upper triangular *unipotent* (eigenvalues all 1) matrices

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

where the super-diagonal entries are all in $\mathbb{F}_p$. Thus, there would be $p^3$ choices for super-diagonal entries, the right number. By luck, we are done.

[10.9] Tell a 3-Sylow subgroup in $GL(3, \mathbb{F}_7)$.

As earlier, the order of the group is

$$(7^3 - 1)(7^3 - 7)(7^3 - 7^2) = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$$

Of course, since $\mathbb{F}_7^\times$ is cyclic, for example, it has a subgroup $T$ of order 3. Thus, one might hit upon the subgroup

$$H = \{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} : a, b, c \in T \}$$

is a subgroup of order $3^3$. Missing a factor of 3. But all the permutation matrices (with exactly one non-zero entry in each row, and in each column, and that non-zero entry is 1)

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

These normalize *all* diagonal matrices, and also the subgroup $H$ of diagonal matrices with entries in $T$. The group of permutation matrices consisting of the identity and the two 3-cycles is order 3, and putting it together with $H$ (as a semi-direct product whose structure is already described for us) gives the order $3^4$ subgroup.

[10.10] Tell a 19-Sylow subgroup in $GL(3, \mathbb{F}_7)$.

Among the Stucture Theorem canonical forms for endomorphisms of $V = \mathbb{F}_7^3$, there are $\mathbb{F}_7[x]$-module structures

$$V \approx \mathbb{F}_7[x]/\langle \text{ irreducible cubic } C \rangle$$

which are *invertible* because of the irreducibility. Let $\alpha$ be the image of $x$ in $\mathbb{F}_7[x]/\langle C \rangle$. Note that $\mathbb{F}_7[\alpha] = \mathbb{F}_7[x]/C$ also has a natural ring structure. Then the action of any $P(x)$ in $k[x]$ on $V$ (via this isomorphism) is, of course,

$$P(x) \cdot Q(\alpha) = P(\alpha) \cdot Q(\alpha) = (P \cdot Q)(x) \bmod C(x)$$

for any $Q(x) \in \mathbb{F}_7[x]$. Since $C$ is irreducible, there are no non-trivial zero divisors in the ring $\mathbb{F}_7[\alpha]$. Indeed, it's a field. Thus, $\mathbb{F}_7[\alpha]^\times$ *injects* to $\mathrm{End}_{\mathbb{F}_7} V$. The point of saying this is that, therefore, if we can find an element of $\mathbb{F}_7[\alpha]^\times$ of order 19 then we have an *endomorphism* of order 19, as well. And it is arguably simpler to hunt around inside $\mathbb{F}_{7^3} = \mathbb{F}_7[\alpha]$ than in groups of matrices.

To compute anything explicitly in $\mathbb{F}_{7^3}$ we need an irreducible cubic. Luckily, $7 = 1 \bmod 3$, so there are many non-cubes mod 7. In particular, there are only two non-zero cubes mod 7, $\pm 1$. Thus, $x^3 - 2$ has no linear factor in $\mathbb{F}_7[x]$, so is irreducible. The *sparseness* (having not so many non-zero coefficients) of this polynomial will be convenient when computing, subsequently.

Now we must find an element of order 19 in $\mathbb{F}_7[x]/\langle x^3-2\rangle$. There seems to be no simple algorithm for choosing such a thing, but there is a reasonable probabilistic approach: since $\mathbb{F}_{7^3}^\times$ is cyclic of order $7^3 - 1 = 19 \cdot 18$, if we pick an element $g$ at random the probability is $(19-1)/19$ that its order will be *divisible* by 19. Then, whatever its order is, $g^{18}$ will have order either 19 or 1. That is, if $g^{18}$ is not 1, then it is the desired thing. (Generally, in a cyclic group of order $p \cdot m$ with prime $p$ and $p$ not dividing $m$, a random element $g$ has probability $(p-1)/p$ of having order divisible by $p$, and in any case $g^m$ will be either 1 or will have order $p$.)

Since elements of the ground field $\mathbb{F}_7^\times$ are all of order 6, these would be bad guesses for the random $g$. Also, the image of $x$ has cube which is 2, which has order 6, so $x$ itself has order 18, which is not what we want. What to guess next? Uh, maybe $g = x + 1$? We can only try. Compute

$$(x+1)^{18} = (((x+1)^3)^2)^3 \bmod x^3 - 2$$

reducing modulo $x^3 - 2$ at intermediate stages to simplify things. So

$$g^3 = x^3 + 3x^2 + 3x + 1 = 3x^2 + 3x + 3 \bmod x^3 - 2 = 3 \cdot (x^2 + x + 1)$$

A minor piece of luck, as far as computational simplicity goes. Then, in $\mathbb{F}_7[x]$,

$$g^6 = 3^2 \cdot (x^2 + x + 1)^2 = 2 \cdot (x^4 + 2x^3 + 3x^2 + 2x + 1) = 2 \cdot (2x + 2 \cdot 2 + 3x^2 + 2x + 1)$$

$$= 2 \cdot (3x^2 + 4x + 5) = 6x^2 + x + 3 \bmod x^3 - 2$$

Finally,

$$g^{18} = (g^6)^3 = (6x^2 + x + 3)^3 \bmod x^3 - 2$$

$$= 6^3 \cdot x^6 + (3 \cdot 6^2 \cdot 1)x^5 + (3 \cdot 6^2 \cdot 3 + 3 \cdot 6 \cdot 1^2)x^4 + (6 \cdot 6 \cdot 1 \cdot 3 + 1^3)x^3 + (3 \cdot 6 \cdot 3^2 + 3 \cdot 1^2 \cdot 3)x^2 + (3 \cdot 1 \cdot 3^2)x + 3^3$$

$$= 6x^6 + 3x^5 + 6x^4 + 4x^3 + 3x^2 + 6x + 6 = 6 \cdot 4 + 3 \cdot 2 \cdot x^2 + 6 \cdot 2x + 4 \cdot 2 + 3x^2 + 6x + 6 = 2x^2 + 4x + 3$$

Thus, if we've not made a computational error, the endomorphism given by multiplication by $2x^2 + 4x + 3$ in $\mathbb{F}_7[x]/\langle x^3 - 2\rangle$ is of order 19.

To get a matrix, use (rational canonical form) basis $e_1 = 1$, $e_2 = x$, $e_3 = x^2$. Then the matrix of the endomorphism is

$$M = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 3 & 4 \\ 2 & 4 & 3 \end{pmatrix}$$

Pretending to be brave, we check by computing the $19^{th}$ power of this matrix, modulo 7. Squaring repeatedly, we have (with determinants computed along the way as a sort of parity-check, which in reality did discover a computational error on each step, which was corrected before proceeding)

$$M^2 = \begin{pmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \quad M^4 = \begin{pmatrix} 6 & 3 & 2 \\ 1 & 6 & 3 \\ 5 & 1 & 6 \end{pmatrix} \quad M^8 = \begin{pmatrix} 0 & 4 & 2 \\ 1 & 0 & 4 \\ 2 & 1 & 0 \end{pmatrix} \quad M^{16} = \begin{pmatrix} 6 & 5 & 5 \\ 6 & 6 & 5 \\ 6 & 6 & 6 \end{pmatrix}$$

Then

$$M^{18} = M^2 \cdot M^{16} = \begin{pmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \cdot M^{16} = \begin{pmatrix} 6 & 5 & 5 \\ 6 & 6 & 5 \\ 6 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 4 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix}$$

$$M^{19} = M \cdot M^{18} = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 3 & 4 \\ 2 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 4 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix} = \text{ the identity}$$

Thus, indeed, we have the order 19 element.

Note that, in reality, without some alternative means to verify that we really found an element of order 19, we could easily be suspicious that the numbers were wrong.

# Exercises

**10.**[6.0.1] Determine all conjugacy classes in $GL_2(\mathbb{F}_5)$.

**10.**[6.0.2] Determine all conjugacy classes in $GL_2(\mathbb{F}_4)$.

**10.**[6.0.3] Determine all conjugacy classes in $GL_5(\mathbb{F}_2)$.

**10.**[6.0.4] Let $k$ be an algebraically closed field. Determine all conjugacy classes in $GL_2(k)$.

**10.**[6.0.5] Let $k$ be an algebraically closed field. Determine all conjugacy classes in $GL_3(k)$.

**10.**[6.0.6] Find a 31-Sylow subgroup of $GL_3(\mathbb{F}_5)$.

**10.**[6.0.7] Find a 2-Sylow subgroup of $GL_2(\mathbb{Q})$.

**10.**[6.0.8] Find a 2-Sylow subgroup of $GL_2(\mathbb{Q}(i))$.

**10.**[6.0.9] Find a 5-Sylow subgroup of $GL_4(\mathbb{Q})$.