Chapter 1

Modules over a principal ideal domain

In every result in this chapter R denotes a commutative principal ideal domain. But notice that we allow R to be any commutative domain in Definition 2.1 and in Lemma 2.3.

1.1 Free modules

Theorem 1.1 *Let F be a free R-module, and E a submodule of F. Then E is also free, and* $\operatorname{rank} E \leq \operatorname{rank} F$.

Proof. If $\operatorname{rank} F = \infty$, the result is true, so suppose that $\operatorname{rank} F < \infty$.

If $\operatorname{rank} F = 1$, then $F \cong R$, and the submodules of F are the ideals of R (up to isomorphism). But an ideal of R is of the form aR for some $a \in R$. If $a = 0$, then I is free of rank zero. If $a \neq 0$, then the map $x \mapsto xa$ is an isomorphism of R-modules, $R \cong I$, so I is free of rank one.

We now argue by induction. Suppose that $\{f_1, \ldots, f_n\}$ is a basis for F. Define $\alpha : F \to Rf_1$ by

$$\alpha(r_1 f_1 + \ldots + r_n f_n) = r_1 f_1.$$

Then α is a surjective R-module homomorphism with kernel $Rf_2 + \ldots + Rf_n$, which is free of rank $n-1$. Let θ denote the restriction of α to E. Since $\ker\theta \subset \ker\alpha$, $\ker\theta$ is free of rank $\leq n-1$ by the induction hypothesis. The image of θ is an ideal of R, so is free of rank at most one. However, by Corollary **??**, $E \cong \ker\theta \oplus \operatorname{im}\theta$ so E is free of rank $\leq n$. □

We cheated in the last result. Rank is defined as the cardinality of a basis, so the first sentence of the proof is inadequate: we need to distinguish between different infinite cardinals. But we will ignore this matter. A proof that covers the case of infinite cardinals can be found in several books, for example in Hungerford.

Remarks. 1. The theorem is false if R is not a PID. Because then R contains an ideal that is not a free module. For example, the ideal (x, y) in $k[x, y]$ is not a free module.

2. It is possible for a free module to have a proper submodule of the same rank. For example, take the ideal $(2) \subset \mathbb{Z}$.

3. If M is a finitely generated module over a principal ideal domian R, then there is a surjective map $\alpha : F \to M$ from a finite rank free module F. If we write $K = \ker \alpha$, there is a short exact sequence

$$0 \to K \to F \to M \to 0$$

with both F and K free of finite rank. This is called a free resolution of R. Such resolutions are important because the map $K \to F$ can be represented by a matrix (compare this to a linea map between two vector spaces), and M is determined by that matrix. This allows us to carry over several ideas from linear algebra, for example, the row operations, and the idea of putting a matric in echelon form.

Corollary 1.2 *If an R module can be generated by n elements, so can every submodule of it.*

Proof. Let $\alpha : F \to M$ be a surjective map with F free of rank n. If N is a submodule of M, then the restriction of α gives a surjective map $\alpha^{-1}(N) \to N$. Since $\alpha^{-1}(N)$ is a submodule of F it is free of rank $\leq n$, so can be generated by $\leq n$ elements. Since the images of those generators provide a set of generators for N, the result follows (if $\alpha^{-1}(N)$ has rank $< n$, take several zeroes to get exactly n generators for it). □

Power series. Let k be a field. The ring of formal power series $k[[x]]$ consists of all power series

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots$$

with coefficients in k. We add and multiply these in the usual way. These are formal expressions and there is no question of convergence. It is easy to see that the units are those power series in which $\alpha_0 \neq 0$. There is a unique maximal ideal (x) and the non-zero ideals are the ideals (x^n), $n \geq 0$. In particular, $k[[x]]$ is a principal ideal domain.

Exercises. 1. A commutative domain R is called a Euclidean domain if there is a function $\phi : R\backslash\{0\} \to \mathbb{N} \cup \{0\}$ such that

1. $\phi(xy) \geq \max\{\phi(x), \phi(y)\}$;

2. if $a, b \in R$ and $b \neq 0$, then there exits $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$.

Show that a Euclidean domain is a principal ideal domain.

2. Use the previous exercise to show that $\mathbb{Z}[i]$, the ring of Gaussian integers, is a principal ideal domain.

1.2 Torsion and torsion-free modules

Definition 2.1 Let R be a commutative domain and M an R-module. An element $m \in M$ is torsion if $rm = 0$ for some non-zero $r \in R$. The torsion submodule of M, which we denote by τM, consists of all the torsion elements in M. If $\tau M = 0$ we say that M is torsion-free. If $\tau M = M$ we say that M is a torsion module. $\Diamond$

It is easy to check the following:

1. the set of torsion elements do form a submodule;
2. every submodule of a torsion-free module is torsion-free;
3. every submodule and every quotient of a torsion module is a torsion module;
4. a sum of torsion modules is a torsion module;
5. a sum of torsion-free modules is torsion-free.

Example 2.2 1. Over the ring $\mathbb{Z}$, the modules $\mathbb{Z}$ and $\mathbb{Q}$ are both torsion-free. Both $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Z}_2 = \mathbb{Z}/(2)$ are torsion modules. The module $\mathbb{Q} \oplus \mathbb{Z}_2$ is neither torsion nor torsion-free. Every finite abelian group G is a torsion $\mathbb{Z}$-module because if $g \in G$, then $n.g = 0$ for some $n > 0$.

2. Let (V, θ) consist of a k-vector space and a k-linear endomorphism of it. Make V into a $k[x]$-module by making x act as θ. Then V is a torsion R-module. To see this, observe that if $\dim V = n$, and $v \in V$, then $\{v, xv, x^2v, \ldots, x^nv\}$ is linearly depenedent, so there are non-zero scalars $\lambda_0, \ldots, \lambda_n$ such that

$$(\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n)v = 0.$$

3. Let $M = k[x, y]/(x)$. Then M can be viewed as both a $k[x, y]$-module and as a module over $k[y] = k[x, y]/(x)$. As a $k[x, y]$-module M is torsion, but as a $k[y]$-module it is torsion-free. $\Diamond$

Lemma 2.3 *Let R be a commutative domain and M an R-module. Then τM is a submodule of M, and $M/\tau M$ is torsion-free.*

Proof. If m and n are torsion elements of M, then $xm = ym = 0$ for some non-zero elements $x, y \in R$. Hence $xy(m \pm n) = 0$; since $xy \neq 0$, $m \pm n$ is torsion. If $r \in R$, then rm is torsion because $x(rm) = rxm = 0$. Hence τM is a submodule of M.

Let $0 \neq x \in R$, and suppose that $x.[m + \tau M] = 0$. Then $xm \in \tau M$, so there is a non-zero element $y \in R$ such that $y(xm) = 0$. Since $(xy)m = 0$ and $xy \neq 0$, $m \in \tau M$. Therefore $[m + \tau M] = 0$. We have shown that the only torsion element in $M/\tau M$ is zero, so $M/\tau M$ is torsion-free. $\square$

Remark. Let R be a PID. If I is a non-zero ideal of R, then R/I has finite length. A finitely generated R-module is torsion if and only if it has finite length. (Prove this.)

If $p_1, \ldots, p_t$ are primes in R and $f = p_1^{n_1} \cdots p_t^{n_t}$ then the composition factors of $R/(f)$ are the $R/(p_i)$s occurring with multiplicities n_i.

Theorem 2.4 *Let R be a PID. A finitely generated torsion-free R-module is free.*

Proof. Let $m_1, \ldots, m_n$ be a set of generators for a torsion-free R-module M. We can suppose that all the m_i are non-zero. The map $R \to Rm_1$ defined by $r \mapsto rm_1$ is an R-module isomorphism because m_1 is not torsion. In particular, Rm_1 is free.

Renumber the m_i so that $\{m_1, \ldots, m_s\}$ is a maximal linearly independent subset of $\{m_1, \ldots, m_n\}$. Thus $s \geq 1$ and $F := Rm_1 + \cdots + Rm_s$ is free. If $s = n$, we are done, so suppose that $s < n$. Hence if $i > s$, $x_i m_i \in F$ for some $0 \neq x_i \in R$. Define $x = x_{s+1} x_{s+2} \ldots x_n$. Then x is non-zero and $xM \subset F$. The map $\theta : M \to F$ defined by $\theta(m) = xm$ is an R-module homomorphism and is injective because M is torsion-free. Thus $M \cong \theta(M)$. By Theorem 1.1, $\theta(M)$ is free. Hence M is free. □

A torsion-free module need not be free if it is not finitely generated. For example, $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Theorem 2.5 *If M is a finitely generated R-module, then $M = F \oplus \tau M$ with F free.*

Proof. The module $M/\tau M$ is torsion-free and finitely generated, so is free. Corollary **??** now implies that $M = \tau M \oplus F$ with F free. □

Remarks. 1. In writing $M = \tau M \oplus F$ with F free, there are usually many choices for F. For example, over $\mathbb{Z}$, the module $M = \mathbb{Z} \oplus \mathbb{Z}/(2) = F \oplus \tau M$ may also be written as $M = E \oplus \tau M$ with $E = \{(a, \bar{a}) \mid a \in \mathbb{Z}\}$, and E is free with basis $(1, \overline{1})$.

2. Theorem 2.5 shows that to understand finitely generated modules over a PID we must understand the structure of the torsion modules. The rest of this chapter is devoted to that task. The first step is to introduce a finer notion of torsion, namely p-torsion for each prime $p \in R$. Then, in analogy with the way in which the torsion submodule of a finitely generated module "splits off", meaning $M \cong M/\tau M \oplus$ (somthing), a torsion module splits up as a direct sum of its p-torsion submodules. we are then left with understanding the structure of a p-torsion module.

1.3 Structure of modules

In a PID R, a non-zero element p is prime if and only if it is irreducible, if and only if pR is maximal.

Definition 3.1 Let p be a prime in R. An R-module M is p-torsion, or p-primary, if for each $m \in M$, $p^n m = 0$ for $n \gg 0$. For each R-module M we write

$$M(p) = \{m \in M \mid p^n M = 0 \text{ for } n \gg 0\}.$$

Just as for the torsion module, it is easy to check that $M(p)$ is a submodule of M, and it is the largest p-torsion submodule of M.

Theorem 3.2 *Let M be a finitely generated torsion R-module. Then*

$$M = \bigoplus_{primes\ p \in R} M(p),$$

and $M(p) = 0$ for all except a finite number of p.

Proof. Let $m \in M$ and suppose that $\mathrm{Ann}(m) = Rs$ where $s = p_1^{n_1} \ldots p_t^{n_t}$; here we have used the fact that R is a UFD (= unique factorization domain) to write s as a product of primes in a unique way. For each i write $s_i = s/p_i^{n_i}$. Then $gcd(s_1, \ldots, s_t) = 1$, so $1 = \sum_{i=1}^t r_i s_i$ for some elements $r_i \in R$. Now

$$p_i^{n_i}(r_i s_i m) = r_i s m = 0,$$

so $r_i s_i m \in M(p_i)$. But $m = \sum r_i s_i m$, so $m \in \sum M(p_i)$ and

$$M = \sum_{\text{primes } p \in R} M(p).$$

We now claim that this sum is finite. By hypothesis M is finitely generated, say $M = Rm_1 + \ldots + Rm_n$. The argument in the previous paragraph shows that each m_i is in a *finite* sum of the $M(p)$s. Hence there is a finite sum of the $M(p)$s such that each m_i is contained in that finite sum. Since those m_i generate all of M, M itself is contained in a finite sum of the $M(p)$s. We can therefore write

$$M = M(p_1) + \cdots + M(p_t)$$

for some finite set of distinct primes $p_1, \ldots, p_t$.

We now prove by induction on t that this is a direct sum. If $t = 1$ that is clear, so suppose that $t > 1$. Suppose to the contrary that $m_1 + \ldots + m_t = 0$ with each $m_i \in M(p_i)$ and that some m_i is non-zero. (Warning: these m_is are NOT the generating m_is that appear in the previous paragraph!) Without loss of generality we may suppose that $m_1 \neq 0$ and that $m_2 \neq 0$. Choose a and b such that $p_1^a m_1 = p_2^b m_2 = 0$. Since $gcd(p_1, p_2) = 1$ there are elements $x, y \in R$ such that $xp_1^a + yp_2^b = 1$. Then

$$0 \neq m_2 = (xp_1^a + yp_2^b)m_2 = xp_1^a m_2.$$

In particular, $p_1^a m_2 \neq 0$. Therefore

$$0 = p_1^a(m_1 + \cdots + m_t) = p_1^a m_2 + \cdots + p_1^a m_t$$

is a sum of non-zero terms in $M(p_2) + \cdots + M(p_t)$, contradicting the induction hypothesis. We conclude that $\sum_{i=1}^{t} M(p_i)$ is a direct sum. □

Exercise. Show that if $\psi : M \to N$ is an isomorphism of R-modules, then ψ maps each $M(p)$ isomorphically onto each $N(p)$.

We now examine the finitely generated p-torsion modules. When M is finitely generated and p-torsion there is an n such that $p^n M = 0$; if $M = Rm_1 + \cdots + Rm_t$, and $p^{n_i} m_i = 0$, then $n = \max\{n_1, \ldots, n_t\}$ works.

Lemma 3.3 *Let p be prime. The only ideals of R that contain (p^n) are (p^i) with $0 \leq i \leq n$.*

Proof. Certainly these ideals contain $p^n R$. Conversely, if $xR \supset p^n R$, then x divides p^n and, since R is a unique factorization domain, $x = up^i$ for some unit u and i with $0 \leq i \leq n$, whence $xR = p^i uR = p^i R$. □

It follows that the submodules of $R/p^n R$ are exactly

$$\frac{R}{(p^n)} \supset \frac{(p)}{(p^n)} \supset \frac{(p^2)}{(p^n)} \supset \cdots \supset \frac{(p^{n-1})}{(p^n)} \supset \frac{(p^n)}{(p^n)} = 0.$$

Also notice that $(p^i)/(p^n) \cong R/(p^{n-i})$.

Lemma 3.4 *In any domain R, if $0 \neq a = bc$, then $bR/aR \cong R/cR$.*

Proof. Because bR/aR is cyclic with generator $\bar{b} = [b + aR]$, $bR/aR \cong R/\operatorname{Ann}(\bar{b})$ by Lemma **??**. Now $x \in \operatorname{Ann}(\bar{b})$ if and only if $xb \in aR$, or if and only if there is $y \in R$ such that $xb = ay = bcy$, and this is equivalent to the condition that $x \in cR$; in other words $\operatorname{Ann}(\bar{b}) = cR$. □

Lemma 3.5 *Let p be a prime. If $m \in M$ and $p^n m = 0$ and $p^{n-1} m \neq 0$, then $\operatorname{Ann}(m) = Rp^n$.*

Proof. The annihilator of m is an ideal of R containing Rp^n, so must be of the form Rp^i for some $0 \leq i \leq n$. However, if $i \neq n$, then $p^{n-1} \in p^i R$, and this contradicts the hypothesis that $p^{n-1} m \neq 0$. □

Proposition 3.6 *Let M be a finitely generated p-torsion module such that $p^n M = 0$ but $p^{n-1} M \neq 0$. Let $m \in M$ be an element such that $p^{n-1} m \neq 0$. Then there is a submodule N of M such that*

$$M = Rm \oplus N \cong R/p^n R \oplus N.$$

Proof. Consider the set of pairs (Q, θ) where $Q \supset Rm$ is a submodule of M and $\theta : Q \to Rm$ is an R-module homomorphism such that $\theta|_{Rm} = \mathrm{id}_{Rm}$. It follows from Lemma **??.??** that Rm is a direct summand of Q. We define a partial order on these pairs by declaring $(Q_1, \theta_1) \geq (Q_2, \theta_2)$ if $Q_1 \supset Q_2$ and $\theta_1|_{Q_2} = \theta_2$. By Zorn's Lemma this set has a maximal member, say (Q, θ).

We will now show that $Q = M$, which will prove the Proposition. Suppose to the contrary that $Q \neq M$. Then M/Q is a non-zero p-torsion module, so we can choose $m' \in M \backslash Q$ such that $pm' \in Q$. By Lemma 3.5, $\mathrm{Ann}([m'+Q]) = pR$.

For some $y \in R$, $\theta(pm') = ym$. Therefore $p^{n-1}ym = p^{n-1}\theta(pm') = \theta(p^n m') = 0$, so we conclude that $y \in pR$. Let's write $y = pz$. Thus $\theta(pm') = pzm$.

Notice that $\theta(m')$ is not defined because $m' \notin Q$. However, we can define $\psi : Q + Rm' \to Rm$ by $\psi(q + rm') = \theta(q) + rzm$. This map is well-defined because if $q + rm' = q' + r'm'$, then $(r - r')m' = q' - q \in Q$ so $r - r' = ps$ for some $s \in R$ because $\mathrm{Ann}([m' + Q]) = pR$. Therefore

$$\begin{aligned}
\psi(q + rm') - \psi(q' + r'm') &= \theta(q - q') + rzm - r'zm \\
&= \theta(q - q') + spzm \\
&= \theta(q - q') + s\theta(pm') \\
&= \theta(q - q' + spm') \\
&= \theta(q - q' + (r - r')m) \\
&= 0.
\end{aligned}$$

The map ψ is an R-module homomorphism and $\psi|_{Rm} = \mathrm{id}_{Rm}$, so $(Q+Rm', \psi) > (Q, \theta)$, contradicting the choice of Q. Hence $Q = M$. □

Theorem 3.7 *If M is a finitely generated p-torsion R-module, then*

$$M \cong R/(p^{n_1}) \oplus \cdots \oplus R/(p^{n_t}) \tag{3-1}$$

for some integers $n_1 \geq n_2 \geq \ldots \geq n_t \geq 1$ that are uniquely determined by M.

Proof. Choose n_1 such that $p^{n_1}M = 0$ but $p^{n_1-1}M \neq 0$. By Proposition 3.6, there is an $m \in M$ such that $M = Rm \oplus N \cong R/(p^{n_1}) \oplus N$. If $N = 0$ we can stop, and if $N \neq 0$ we can continue this process with N in place of M. That is, we choose n_2 such that $p^{n_2}N = 0$ but $p^{n_2-1}N \neq 0$, et cetera.

To see that this process eventually stops, consider the finitely generated module M/pM. It is a module over the field $k = R/(p)$. However,

$$M/pM = R/(p) \oplus N/pN,$$

so $\dim_k N/pN = \dim_k M/pM - 1$. Because the dimension drops by ne each time we split off a summand of the form $R/(p^{n_i})$, the process stops.

We now show that the n_is are uniquely determined. Consider the chain $M \supset pM \supset \cdots \supset P^{n_1}M = 0$ and set $L_n = p^n M/p^{n+1}M$. Since pR annihilates L_n, L_n is a k-vector space. The numbers $d_n := \dim_k L_n$ are invariants of M; they depend only on the isomorphism class of M. Since $p^n(R/Rp^{n_i}) = 0$ if and only if $n \geq n_i$,

$$\begin{aligned}
p^n M &\cong p^n R/p^{n_1}R \oplus \cdots \oplus p^n R/Rp^{n_t} \\
&\cong R/p^{n_1-n}R \oplus \cdots \oplus R/Rp^{n_s-n}
\end{aligned}$$

where the second sum is only over those $n_i > n$. Therefore d_n is the number of summands in (3-1) with $n_i \geq n+1$. In other words, the number of summands in (3-1) of the form $R/(p^{n+1})$ is $d_n - d_{n+1}$; but this depends only on M. $\square$

Theorem 3.8 *Let M be a finitely generated module over a PID R. Then $M \cong R^d \oplus \tau M$ for a unique $d \geq 0$. Furthermore, τM is isomorphic to a direct sum of modules of the form $R/(p^n)$ for various primes $p \in R$ and positive integers n; for a particular p and n, the number of summands of the form $R/(p^n)$ depends only on M.*

The p^ns that occur in the decomposition of M are called the elementary divisors of M and they are counted with multiplicity. The module M is completely determined up to isomorphism by its elementary divisors and the rank of $M/\tau M$.

Example 3.9 Take $R = \mathbb{Z}$. If G is a finitely generated abelian group, then $G \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus$ (finite group) and the finite group is a direct sum of cyclic p-groups $\mathbb{Z}/p^n\mathbb{Z}$ for various p and n. For example, because $120 = 2^3.3.5$,

$$\mathbb{Z}/(120) \cong \mathbb{Z}/(2^3) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(5).$$

We may identify each summand with a submodule of $\mathbb{Z}/(120)$. The decomposition becomes

$$\mathbb{Z}/(120) = (15)/(120) \oplus (40)/(120) \oplus (24)/(120).$$

$\Diamond$

Example 3.10 If $R = k[x]$, the primes are the irreducible polynomials and the cyclic p-torsion modules are $k[x]/(f^n)$ with f irreducible. If $g \in k[x]$ is not a constant, we may write $g = f_1^{n_1} \ldots f_t^{n_t}$ as a product of irreducibles, and then

$$k[x]/(f) \cong k[x]/(f_1^{n_1}) \oplus \ldots \oplus k[x]/(f_t^{n_t}).$$

$\Diamond$

There is another way to decompose torsion modules over a PID. To see this, consider the finite abelian group

$$G = \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(q^3) \oplus \mathbb{Z}/(q^2) \oplus \mathbb{Z}/(q)$$

where p and q are distinct primes. Then

$$G \cong \mathbb{Z}/(pq) \oplus \mathbb{Z}/(pq^2) \oplus \mathbb{Z}/(p^2q^3),$$

so we have written G as a direct sum of cyclic modules $\mathbb{Z}/(f_1) \oplus \mathbb{Z}/(f_2) \oplus \mathbb{Z}/(f_3)$ with $f_1 | f_2$ and $f_2 | f_3$. Theorem 3.13 gives the general result, but first we need a preliminary result which is important in its own right.

Lemma 3.11 *Let R be a commutative domain. If $R = Rx + Ry$, then*

$$R/(xy) \cong R/(x) \oplus R/(y).$$

Proof. By hypothesis we can write $1 = ux + vy$. And $Rx \cap Ry = Rxy$ because if $rx = sy$, then $r = r(ux + vy) = urx + rvy \in Ry$ so $rx \in Rxy$; the reverse inclusion is obvious. It follows that

$$R/(xy) = Rx/(xy) \oplus Ry/(xy) \cong R/(y) \oplus R/(x),$$

where the last isomorphism follows from the remark before Lemma 3.5. □

Applying this lemma inductively gives the following result.

Lemma 3.12 *If $p_1, \ldots, p_t$ are distinct primes in a PID R, then*

$$R/(p_1^{n_1} \ldots p_t^{n_t}) \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_t^{n_t}).$$

The previous two results are versions of the *Chinese Remainder Theorem.* In one form this says the following. If $a_1, \ldots, a_n \in \mathbb{Z}$ satisfy $(a_i, a_j) = 1$ for all $i \neq j$, and if $b_1, \ldots, b_n \in \mathbb{Z}$ are arbitrary, then there exists $x \in \mathbb{Z}$ such that $x \equiv b_j \pmod{a_j}$ for all j. To see this, prove that $\mathbb{Z}/(a_1 \cdots a_n) \cong \mathbb{Z}/(a_1) \bigoplus \cdots \bigoplus \mathbb{Z}/(a_n)$, where the map from $\mathbb{Z}$ is given by $x \mapsto (x \pmod{a_1}), \ldots, x \pmod{a_n})$. The fact that this map is surjective solves the problem.

Theorem 3.13 *Let M be a finitely generated torsion module. There exist $e_1, \ldots, e_t \in R$ such that $M \cong R/Re_1 \bigoplus \cdots \bigoplus R/Re_t$, and $e_1 \mid e_2, e_2 \mid e_3, \ldots, e_{t-1} \mid e_t$. The $e_1, \ldots, e_t$ are uniquely determined (up to unit multiples) by M.*

Proof. There are primes p_j (not necessarily distinct) and integers $n_j \geq 1$ such that

$$M \cong \bigoplus_{j=1}^{k} R/Rp_j^{n_j}.$$

Let $\{q_1, \ldots, q_s\}$ be the distinct primes amongst $p_1, \ldots, p_k$. For each i set $m_i = \max\{n_j \mid p_j = q_i\}$ i.e., m_i is maximal such that $q_i^{m_i} = p_j^{n_j}$ for some i.

Collecting the terms $R/Rp_j^{n_j}$, it follows that $\bigoplus_{i=1}^{s} R/Rq_i^{m_i}$, is a direct summand of M, and a complement is N say. Write $b_1 = q^{m_1} \cdots q_s^{m_s}$. By Lemma 3.12, $R/(b_1) \cong \bigoplus_{i=1}^{s} R/Rq_i^{m_i}$. Hence $R/(b_1)$ is a direct summand of M, and the complement N is the direct sum of various $R/Rp_j^{n_j}$. The important point is that if $R/Rp_j^{n_j}$ appears in the expression for N, then $p_j^{n_j}$ divides b_1.

Repeating the argument, we see that N has a direct summand of the form R/Rb_2, with b_2 chosen in the same fashion as was b_1. Because b_1 involved the largest powers of the primes q_1, it follows that b_2 divides b_1. We continue in this way until, eventually, $M = R/Rb_1 \bigoplus R/Rb_2 \bigoplus \cdots$ with $b_2 \mid b_1$, $b_3 \mid b_2$ etc. Relabel the b's as e's, and the theorem is proved. □

The elements $e_1, \ldots, e_t$ are called the invariant factors of M.

The difference between the elementary divisors and the invariant factors can be seen in the next two examples. The abelian groups of order 24 are:

Group	*Invariant factors*	*Elementary divisors*
$\mathbb{Z}_{24} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_3$	24	$8, 3$
$\mathbb{Z}_{12} \oplus \mathbb{Z}_2 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	$12, 2$	$4, 3, 2$
$\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$6, 2, 2$	$3, 2, 2, 2$

And consider the following modules over $R = k[x]$ for which the product of the invariant factors is $p^3q^2 = (x-1)^3(x+1)^2$:

Module	*Invariant factors*	*Elementary divisors*
$R/(p) \oplus R/(pq) \oplus R/(pq)$	pq, pq, p	p, p, p, q, q
$R/(pq) \oplus R/(p^2q)$	pq, p^2q	p, p^2, q, q
$R/(p^3) \oplus R/(q) \oplus R/(q)$	q, p^3q	p^3, q, q
$R/(p) \oplus R/(p) \oplus R/(pq^2)$	pq^2, p, p	p, p, p, q^2
$R/(p) \oplus R/(p^2q^2)$	p, p^2q^2	p, p^2, q^2
$R/(p^2q^3)$	p^2q^3p	p^3, q^2

A close examination of the previous proof yields the following result.

Proposition 3.14 *If M is a finitely generated torsion module, then the product of the elementary divisors of M equals the product of the invariant factors of M.*

Application to finite abelian groups. Remember that an abelian group is the same thing as a $\mathbb{Z}$-module. A finitely generated abelian group is torsion if and only if it is finite. Hence the structure theorem for $\mathbb{Z}$-modules implies that

every finite abelian group is a direct sum of cyclic abelian groups.

Chapter 2

Linear algebra

Throughout this chapter k denotes a field, and T denotes a k-linear transformation of a finite dimensional k-vector space V.

We will apply the structure theorem for finite dimensional modules over the polynomial ring $k[x]$ to obtain various canonical forms for a matrix representing a linear transformation of a finite dimensional vector space.

2.1 Linear transformations and matrices

For computational purposes it is helpful to represent vectors and linear transformations by matrices. To do this one must first choose bases for the vector spaces involved. We will write vectors as column matrices and the action of a linear transformation on a vector is given by left multiplication by a matrix.

Matrix representations. Let $T : U \to V$ be a linear map between two finite dimensional k-vector spaces. Let $\mathcal{B} = \{u_1, \ldots, u_n\}$ and $\mathcal{C} = \{v_1, \ldots, v_m\}$ be bases for U and V respectively. Define scalars $\{\alpha_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ by the requirement that

$$T(u_j) = \sum_{i=1}^{m} \alpha_{ij} v_i \qquad \text{for all } i \text{ and } j. \tag{1-1}$$

We assemble these scalars into a single $m \times n$ matrix

$$M_{\mathcal{C}}^{\mathcal{B}}(T) := (\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix},$$

that depends on the bases $\mathcal{B}$ and $\mathcal{C}$.

Vectors $u \in U$ can be represented as column vectors with respect to the basis $\mathcal{B}$,

$$[u]_{\mathcal{B}} := \lambda_1 u_1 + \cdots + \lambda_n u_n \longleftrightarrow \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

We write $[Tu]_{\mathcal{C}}$ for the matrix representation of Tu with respect to the basis $\mathcal{C}$. Matrix multiplication is defined so that

$$[Tu]_{\mathcal{C}} = M_{\mathcal{C}}^{\mathcal{B}}(T)[u]_{\mathcal{B}}.$$

The notation is cumbersome but it allows us to be precise.

Let $S : V \to W$ be another linear ransformation and $\mathcal{D}$ a basis for W. Then

$$M_{\mathcal{D}}^{\mathcal{B}}(ST)[u]_{\mathcal{B}} = [STU]_{\mathcal{D}} = M_{\mathcal{D}}^{\mathcal{C}}(S)[Tu]_{\mathcal{C}} = M_{\mathcal{D}}^{\mathcal{C}}(S)M_{\mathcal{C}}^{\mathcal{B}}(T)[u]_{\mathcal{B}}$$

for all $u \in U$, so

$$M_{\mathcal{D}}^{\mathcal{C}}(S)M_{\mathcal{C}}^{\mathcal{B}}(T) = M_{\mathcal{D}}^{\mathcal{B}}(ST).$$

Change of basis. If the bases for U and V change, so do the matrices representing u and T. If $\mathcal{B}'$ and $\mathcal{C}'$ are bases for U and V there are invertible matrices $P \in \mathrm{GL}_n(k)$ and $Q \in \mathrm{GL}_m(k)$ such that

$$[u]_{\mathcal{B}'} = P[u]_{\mathcal{B}} \text{ and } [v]'_{\mathcal{C}} = Q[v]_{\mathcal{C}}.$$

Thus, $P = M_{\mathcal{B}'}^{\mathcal{B}}(\mathrm{id}_U)$ and $Q = M_{\mathcal{C}'}^{\mathcal{C}}(\mathrm{id}_V)$. It follows that

$$M_{\mathcal{C}'}^{\mathcal{B}'}(T) = M_{\mathcal{C}'}^{\mathcal{B}'}(\mathrm{id}_V\, T\, \mathrm{id}_U) = M_{\mathcal{C}'}^{\mathcal{C}}(\mathrm{id}_V)M_{\mathcal{C}}^{\mathcal{B}}(T)M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_U) = QM_{\mathcal{C}}^{\mathcal{B}}(T)P^{-1}.$$

In other words, if A is the matrix representing T with respect to the bases $\mathcal{B}$ and $\mathcal{C}$, and B is the matrix representing T with respect to the bases $\mathcal{B}'$ and $\mathcal{C}'$, then

$$B = QAP^{-1}.$$

The matrices A and B *have the same intrinsic properties* because they both represent the linear transformation T.

Matrices $A, B \in M_{m\times n}(k)$ are similar if there exist $P \in GL_n(k)$ and $Q \in GL_m(k)$ such that $B = QAP^{-1}$. You should check that similarity is an equivalence relation.

We define an action of the group $\mathrm{GL}_n(k)\times\mathrm{GL}_m(k)$ on $M_{m\times n}(k)$ by declaring $(P, Q).A = QAP^{-1}$. The similarity classes are the orbits for this action.

It is a basic problem to describe the similarity classes of matrices. This problem has many aspects, algebraic, geometric, combinatorial, topological, etc. and has been the inspiration for huge amounts of mathematics.

2.2 Linear operators and modules

We now specialize to the case where $U = V$. A linear transformation $T : V \to V$ is called a linear operator.

Because only one vector space is involved, we have one basis rather than two.

Notation. If $\mathcal{B}$ is a basis for V we write $M(T)_{\mathcal{B}}$ for the matrix representing T with respect to $\mathcal{B}$. That is, $M(T)_{\mathcal{B}} = M(T)_{\mathcal{B}}^{\mathcal{B}}$.

If we change the basis for V as in section 2.1, then the matrix A is changed to the matrix $P^{-1}AP$.

Definition 2.1 Two $n \times n$ matrices $A, B \in M_n(k)$ are conjugate if there exists $P \in GL_n(k)$ such that $B = P^{-1}AP$. $\Diamond$

The problem now is to describe the conjugacy classes of $n \times n$ matrices. These are the orbits of $GL_n(k)$ on $M_n(k)$ under the conjugation action. **Problem:** find a canonical form for A under conjugacy. The problem may be rephrased: Find a "nice" element in each orbit.

The connection with $k[x]$-modules. Our strategy for understanding T is to associate to it a $k[x]$-module, and then apply the results about finite-dimensional $k[x]$-modules. We make V a $k[x]$-module by defining

$$x.v = Tv$$

for all $v \in V$, and extending linearly so that $(\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n).v = \lambda_0 v + \lambda_1 T(v) + \cdots + \lambda_n T^n(v)$. The point we wish to make is that

> *the theory of finite dimensional modules over $k[x]$ is equivalent to the theory of a single linear operator on a finite dimensional vector space.*

The next result formalizes this important point.

Proposition 2.2 *Let A and B be two $n \times n$ matrices. Make k^n into a $k[x]$-module in two different ways:*

1. *let $M = k^n$ with the $k[x]$-action defined by $x.v = Av$;*
2. *let $N = k^n$ with the $k[x]$-action defined by $x * v = Bv$.*

These two $k[x]$-modules are isomorphic if and only if A and B are conjugate to one another.

Proof. The modules M and N are isomorphic if and only if there is a k-linear isomorphism $\theta : k^n \to k^n$ such that $\theta(x.v) = x * \theta(v)$ for all $v \in k^n$. Such a θ is given by $\theta(v) = Pv$ for some $P \in GL_n(k)$, and the condition $\theta(x.v) = x * \theta(v)$ is equivalent to the condition $PAv = BPv$. Hence the $k[x]$-modules are isomorphic if and only if $PAv = BPv$ for all $v \in k^n$. That is, if and only if $PA = BP$. $\square$

To further emphasize the utility of this point of view, notice that

1. a subspace $W \subset V$ is stable under the action of T (i.e., $T(W) \subset W$) if and only if W is a $k[x]$-submodule of V, and
2. a decomposition $V = W_1 \oplus \cdots \oplus W_t$ into T-stable subspaces is equivalent to a decomposition of V into a direct sum of $k[x]$-submodules.

The structure theorem for modules over a PID may be applied to this situation: it gives a canonical form for each finite dimensional $k[x]$-module and hence gives a way of decomposing V into T-stable subspaces. The next result shows that writing V as a direct sum of T-stable subspaces corresponds to representing T by a "block matrix".

Lemma 2.3 *Suppose that $V = U \bigoplus W$, with $TU \subset U$, and $TW \subset W$. Let $\mathcal{U} = \{u_1, \ldots, u_n\}$, and $\mathcal{W} = \{w_1, \ldots, w_k\}$ be bases for U and W respectively. Then $\mathcal{V} = \mathcal{U} \cup \mathcal{W}$ is a basis for V, and*

$$M(T)_{\mathcal{V}} = \begin{bmatrix} M(T)_{\mathcal{U}} & 0 \\ 0 & M(T)_{\mathcal{W}} \end{bmatrix}$$

More generally, if $V = \bigoplus_k V_k$ is a decomposition into T-stable subspaces and $\mathcal{B}$ is a union of bases from each individual V_k, then $M(T)_{\mathcal{B}}$ decomposes into a block diagonal matrix.

Proof. Obvious. □

The structure theorems for modules over PIDs yield two decompositions of V as a direct sum of cyclic $k[x]$-modules, namely

$$V \cong \bigoplus_{i=1}^{s} \bigoplus_{j} k[x]/(f_i)^{n_{ij}} \tag{2-2}$$

where the f_i are distinct irreducible monics and the $f_i^{n_{ij}}$ are the *elementary divisors* of V, and

$$V \cong \bigoplus_{i=1}^{t} k[x]/(g_i) \tag{2-3}$$

where the g_i are the monic *invariant factors* of V, and $g_1 \mid g_2, g_2 \mid g_3, \ldots, g_{t-1} \mid g_t$.

We observed in Proposition 1.3.14 that

$$g_1 g_2 \cdots g_t = \prod_{i=1}^{s} \prod_{j} f_i^{n_{ij}},$$

i.e., the product of the elementary divisors equals the product of the invariant factors.

Definition 2.4 The minimal polynomial of a linear transformation $T : V \to V$ is the monic polynomial $f \in k[x]$ of least degree such that $f(T) = 0$. ◊

Lemma 2.5 *The minimal polynomial of $T : V \to V$ is the monic generator of the ideal* $\mathrm{Ann}V$ *where V is made into a $k[x]$-module via $x.v = T(v)$. If we decompose V as in (2-2) and (2-3), then that minimal polynomial is*

$$g_t = \prod_{i=1}^{s} f_i^{m_i}$$

where $m_i = \max\{n_{ij} \mid i, j\}$.

Proof. Obvious. □

Notice that $\deg g_t \leq \dim V$ by (2-3), so the degree of the minimal polynomial of T is at most $\dim V$. That is not obvious without the theory of modules over PIDs. Because $M_n(k)$ is a vector space of dimension n^2, all we can say at first is that $\{T^i \mid 0 \leq i \leq n^2\}$ is linearly dependent, so the minimal polynomial of T has degree $\leq n^2$.

Eigenvalues and eigenspaces. Let $T : V \to V$ be a linear operator. Then $\lambda \in k$ is called an eigenvalue for T if there exists $0 \neq v \in V$ such that $Tv = \lambda v$; such a v is called an eigenvector for T. For $\lambda \in k$, define

$$V_\lambda := \{v \in V \mid Tv = \lambda v\};$$

notice that $T(V_\lambda) \subset V_\lambda$. This is a subspace of V, and is called the λ-eigenspace.

If $\lambda_1, \ldots, \lambda_n$ are distinct eigenvalues then the sum $V_{\lambda_1} + \cdots + V_{\lambda_n}$ is a direct sum.

A linear operator $T : V \to V$ is diagonalizable if the matrix representing T is diagonal withe respect to some basis for V.

Lemma 2.6 *The following are equivalent:*

1. *T is diagonalizable;*
2. *there is a basis for V consisting of eigenvectors;*
3. *as a $k[x]$-module V is a direct sum of 1-dimensional submodules.*

Proof. (1) $\Rightarrow$ (2) If T is diagonalizable, say $M(T)_\mathcal{B} = diag(\lambda_1\ \lambda_2\ \cdots\ \lambda_n)$, then each column matrix $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ is an eigenvector with eigenvalue λ_j.

(2) $\Rightarrow$ (3) If $\{v_1, \ldots, v_n\}$ is a basis for V and each v_i is an eigenvector, then $V = kv_1 \oplus \cdots \oplus kv_n$ and each kv_i is a $k[x]$-submodule.

(3) $\Rightarrow$ (1) If $V = kv_1 \oplus \cdots \oplus kv_n$ and each kv_i is a $k[x]$-submodule, then there are scalars $\lambda_i \in k$ such that $Tv_i = xv_i = \lambda_i v_i$. Hence, with respect to the basis $\mathcal{B} = \{v_1, \ldots, v_n\}$, $M(T)_\mathcal{B} = diag(\lambda_1\ \lambda_2\ \cdots\ \lambda_n)$. □

Example 2.7 Suppose that $A \in M_n(\mathbb{C})$ is such that $A^m = 1$. Pick the least such m. The minimal polynomial is $x^m - 1$, so viewing $\mathbb{C}^n$ as a $\mathbb{C}[x]$-module, its biggest invariant factor is $g_t = x^m - 1$. Over $\mathbb{C}$, $x^m - 1$ factors as a product of distinct linear factors

$$x^m - 1 = \prod_{i=0}^{m-1} (x - \varepsilon^i) \qquad \text{where } \varepsilon = e^{2\pi i/m}.$$

Hence each invariant factor g_i is a product of distinct linear factors. The Chinese Remainder theorem therefore implies that $\mathbb{C}[x]/(g_i)$ is a direct sum of 1-dimensional $\mathbb{C}[x]$-submodules. Thus $\mathbb{C}^n$ as a $\mathbb{C}[x]$-module is a direct sum of 1-dimensional submodules. It follows that A is a diagonalizable matrix. ◊

You might find it helpful to think about the previous example without invoking modules. Just factor $0 = A^m - 1 = \prod_{i=0}^{m-1}(A - \varepsilon^i I)$ and look at the individual eigenspaces $\{v \in \mathbb{C}^n \mid Av = \varepsilon^i v\}$.

2.3 The rational canonical form

Consider the $k[x]$-module $V = k[x]/(g)$ where

$$g = \alpha_0 + \alpha_1 x + \cdots + \alpha_{r-1}x^{r-1} + x^r.$$

Write $T : V \to V$ for the linear map $T(v) = xv$. The set

$$\mathcal{B} = \{\overline{1}, \overline{x}, \ldots, \overline{x^{r-1}}\}$$

is a basis for V, where $\overline{a}$ denotes the image of a in V. Because

$$\begin{aligned}
T\overline{1} &= \overline{x},\\
T\overline{x} &= \overline{x^2},\\
&\vdots \qquad \vdots\\
T\overline{x^{r-2}} &= \overline{x^{r-1}},\\
T\overline{x^{r-1}} &= -(\alpha_0\overline{1} + \alpha_1\overline{x} + \cdots + \alpha_{r-1}\overline{x^{r-1}})
\end{aligned}$$

the matrix of T with respect to $\mathcal{B}$ is

$$M(T)_{\mathcal{B}} = \begin{pmatrix}
0 & 0 & \cdots & 0 & 0 & -\alpha_0\\
1 & 0 & \cdots & 0 & 0 & -\alpha_1\\
0 & 1 & \cdots & 0 & 0 & -\alpha_2\\
\vdots & & & & & \vdots\\
0 & 0 & \cdots & 1 & 0 & -\alpha_{r-2}\\
0 & 0 & \cdots & 0 & 1 & -\alpha_{r-1}
\end{pmatrix} \tag{3-4}$$

This is called the companion matrix to g. The minimal polynomial of T is g.

Proposition 3.1 *Let $T : V \to V$ be a linear transformation of a finite dimensional k-vector space. Then there is a decomposition $V = \bigoplus V_t$ such that $T(V_t) \subset V_t$ for all t, and bases for each V_t such that $M(T|_{V_t})$ is the companion matrix for the minimal polynomial of $T|_{V_t}$.*

Proof. Consider V as a $k[x]$-module with x acting as T, and decompose V into a direct sum of cyclic $k[x]$-modules. Then use (2-3). □

Corollary 3.2 *Let $T : V \to V$ be a linear transformation of a finite dimensional k-vector space. Then there is a basis $\mathcal{B}$ for V such that*

$$M(T)_{\mathcal{B}} = \begin{pmatrix}
M_1 & 0 & 0 & \cdots & 0 & 0\\
0 & M_2 & 0 & \cdots & 0 & 0\\
\vdots & & & & & \vdots\\
0 & 0 & 0 & \cdots & 0 & M_t
\end{pmatrix} \tag{3-5}$$

where the M_i are the companion matrices for the invariant factors g_i of T.

Proof. Use (2-3). □

This is the rational canonical form for T and can be achieved over any field.

Lemma 3.3 *Let $A, B \in M_n(k)$. Let $P, Q \in GL_n(k)$ be such that $P^{-1}AP$, and $Q^{-1}BQ$ are in rational canonical form. Then A and B are conjugate if and only if $P^{-1}AP = Q^{-1}BQ$ (up to ordering of blocks).*

Proof. By Proposition 2.2, A and B are conjugate if and only if the $k[x]$-modules they determine are isomorphic. But isomorphic modules have the same invariant factors and, conversely, two modules are isomorphic if they have the same invariant factors. □

Changing the field. When we speak of a linear operator $T : V \to V$, the underlying field k needs to be specified because we must say that V is a vector space over k. However, when we explicitly write out a matrix we usually just write out the matrix without saying what field the entries belong to. For example, a matrix with integer entries might be viewed as a matrix over $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or any other field containing $\mathbb{Q}$. The question then arises, *does the rational canonical form of a given matrix change as the field changes?* The answer is NO because the rational canonical form is determined by the invariant factors, and these are entirely characterized by the fact that $g_1 | g_2$, ...

An improvement. I think we can all agree that the more zeroes there are in a matrix the happier we are. Certainly this is one reason we like the rational canonical form. But sometimes it is not helpful to use the rational canonical form. For example, suppose that $T : \mathbb{R}^6 \to \mathbb{R}^6$ is a linear transformation with minimal polynomial

$$(x^2 - 4)(x^2 + 1)(x^2 + x + 1).$$

Then, as an $\mathbb{R}[x]$-module with x acting as T,

$$\mathbb{R}^6 \cong \frac{\mathbb{R}[x]}{(x^2-4)(x^2+1)(x^2+x+1)} \cong \frac{\mathbb{R}[x]}{(x-2)} \oplus \frac{\mathbb{R}[x]}{(x+2)} \oplus \frac{\mathbb{R}[x]}{(x^2+1)} \oplus \frac{\mathbb{R}[x]}{(x^2+x+1)}$$

In some ways the second expression is nicer. For example, it makes it clear that T has two eigenspaces of dimension one with eigenvalues ± 2, and two other 2-dimensional T-stable subspaces, and that $\mathbb{R}^6$ is the direct sum of these. It therefore seems sensible to pick a basis reflecting this, so that the matrix for T becomes

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & -1 & 0 & 0 & \\ 0 & 0 & 1 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0 & -1 & \\ 0 & 0 & 0 & 0 & 1 & -1 & \end{pmatrix}$$

Here we have used two 2×2 blocks that are the companion matrices for the elementary divisors x^2+1 and x^2+x+1.

However, there is only one invariant factor, namely the minimal polynomial, so if we write T in rational canonical form we must mutiply out this minimal polynomial to get

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

and the rational canonical form does not reflect the structure of $\mathbb{R}^6$ under the action of T in a good way.

2.4 Jordan Normal Form

Throughout this section we suppose that k is algebraically closed.

Since the irreducible polynomials in $k[x]$ are those of degree one, it follows from (2-2) that

$$V \cong k[x]/(x-\lambda_1)^{n_1} \bigoplus \cdots \bigoplus k[x]/(x-\lambda_t)^{n_t} \tag{4-6}$$

for various $\lambda_1, \ldots, \lambda_t \in k$.

Consider $V = k[x]/(x-\lambda)^n$. Write $T : V \to V$ for the linear map $T(v) = xv$. A basis for V is given by

$$\mathcal{B} = \{v_1 = \overline{1}, v_2 = \overline{x-\lambda}, v_3 = \overline{(x-\lambda)^2}, \ldots, v_n = \overline{(x-\lambda)^{n-1}}\}$$

where for $a \in k[x]$, $\overline{a}$ denotes the image of a in V. Because

$$\begin{aligned} Tv_1 &= \lambda v_1 + v_2, \\ Tv_2 &= \lambda v_2 + v_3, \\ &\vdots \qquad\quad \vdots \\ Tv_{n-1} &= \lambda v_{n-1} + v_n, \\ Tv_n &= \lambda v_n, \end{aligned}$$

the matrix of T with respect to $\mathcal{B}$ is

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & \cdots & 1 & \lambda & 0 \\ 0 & 0 & \cdots & 0 & 1 & \lambda \end{pmatrix} \tag{4-7}$$

This is called the Jordan normal form for T. The minimal polynomial of T is $(x-\lambda)^n$.

Note that kv_n is a submodule (this is equivalent to v_n being an eigenvector for T), that $(kv_{n-1}+kv_n)/kv_e$ is a submodule of V/kv_n, that $(kv_{n-2}+kv_{n-1}+kv_n)/kv_n$ is a submodule of $V/(kv_{n-1}+kv_n)$, etc.

Theorem 4.1 (k algebraically closed) *Let $T : V \to V$ be a linear transformation of a finite dimensional vector space. Consider V as a $k[x]$-module with x acting as T. Then V decomposes as into a direct sum of $k[x]$-submodules*

$$\begin{aligned} V &= V_1 \bigoplus V_2 \bigoplus \cdots \bigoplus V_t \\ &\cong k[x]/(x-\lambda_1)^{n_1} \bigoplus \cdots \bigoplus k[x]/(x-\lambda_t)^{n_t} \end{aligned}$$

where $T(V_i) \subset V_i$ for all i, the $x - \lambda_i$ are the elementary divisors of T. There is a basis $\mathcal{B}$ for V such that

$$M(T)_{\mathcal{B}} = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & M_2 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & M_t \end{pmatrix} \tag{4-8}$$

where M_i is the $n_i \times n_i$ matrix

$$\begin{pmatrix} \lambda_i & 0 & \cdots & 0 & 0 & 0 \\ 1 & \lambda_i & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & \cdots & 1 & \lambda_i & 0 \\ 0 & 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix} \tag{4-9}$$

This is called the Jordan Normal Form for T, and the M_i are called the Jordan blocks of M.

Corollary 4.2 (k algebraically closed) *Two matrices are conjugate if and only if they have the same Jordan normal form (up to ordering of the Jordan blocks).*

Nilpotent Matrices. A linear transformation T is nilpotent if $T^m = 0$ for some m. The only eigenvalue for a nilpotent linear transformation is 0. The number of conjugacy classes of nilpotent linear transformations of an n-dimensional vector space is therefore equal to the number of possible Jordan blocks (with zeroes on the diagonal). If the Jordan blocks of a nilpotent $n \times n$ matrix are of size $e_1, \ldots, e_d$ then $n = e_1 + \cdots + e_d$; conversely if $n = e_1 + \cdots + e_d$, then there is a Jordan normal form (for a nilpotent T) with blocks of size $e_1, \ldots, e_d$. Hence the number of conjugacy classes of nilpotent linear transformations of an n-dimensional vector space equals the number of ways of writing $n = e_1 + \cdots + e_d$. If $n \in \mathbb{N}$ and $e_1, \ldots, e_d$ are positive integers such that $n = e_1 + \cdots + e_d$, then we call $(e_1, \ldots, e_d)$ a partition of n. Hence the number of conjugacy classes of nilpotent linear transformations of a n-dimensional vector space equals the number of partitions of n.

The partitions of n are also in bijection with the conjugacy classes in the symmetric group S_n. There are deep relations between the representation theory of the group S_n and the nilpotent $n \times n$ matrices.

Eigenvalues. The λ_i that occur in the Jordan blocks for T are the eigenvalues of T, and each Jordan block with diagonal entry λ_i provides one eigenvector (more precisely, one 1-dimensional subspace of eigenvectors) of eigenvalue λ_i. Since λ is an eigenvalue for T if and only if $\ker(T-\lambda) \neq 0$, $\dim(\ker(T-\lambda_i)) = \#$ Jordan blocks with λ_i on the diagonal.

Jordan decomposition. A linear transformation S is semi-simple if V can be written $V = V_1 \bigoplus \cdots \bigoplus V_n$ where each V_j is 1-dimensional, and $S(V_j) \subset V_j$. Thus, S is semisimple $\iff$ V has a basis consisting of eigenvectors for $S \iff S$ is diagonalisable. When k is algebraically closed, an arbitrary linear transformation T can be written as $T = S + N$ where S is semisimple, N is nilpotent and $SN = NS$; to see this write T in Jordan normal form, take S to be the "diagonal part," and N to be the "off-diagonal part." This is called the Jordan decomposition of T.

2.5 The Characteristic Polynomial.

Let k be any field. If $A \in M_n(k)$, then $xI - A$ is an $n \times n$ matrix over $k[x]$, so its determinant, $\det(xI - A)$, is in $k[x]$. The characteristic polynomial of A is

$$p_A(x) := \det(xI - A).$$

If $B = P^{-1}AP$ for $P \in GL_n(k)$, then $xI - B = P^{-1}(xI - A)P$, so $p_B(x) = \det(xI - B) = \det(P^{-1})\det(xI - A)\det(P) = \det(xI - A) = p_A(x)$. So the characteristic polynomial is invariant under conjugation. Hence if T is a linear transformation, $P_T(x)$ is well-defined: just take $p_A(x)$ for any matrix A that represents T with respect to any basis. We call $p_T(x)$ the characteristic polynomial of T.

Proposition 5.1 *The eigenvalues of T are the zeroes of p_T.*

Proof. λ is an eigenvalue for $T \iff \ker(T-\lambda) \neq 0 \iff \det(T-\lambda) = 0 \iff p_T(\lambda) = 0$. □

An important property of determinants is that

$$\det \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = (\det A)(\det B). \tag{5-10}$$

More generally, if

$$A = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & M_2 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & M_t \end{pmatrix} \tag{5-11}$$

then $p_A = p_{M_1} p_{M_2} \cdots p_{M_t}$.

Theorem 5.2 (Cayley-Hamilton Theorem) *For any linear transformation T, $p_T(T) = 0$.*

Proof. By Lemma 2.5, it suffices to show that the minimal polynomial of T divides p_T. Let A be the rational canonical form for T, and suppose that A is written as in Corollary 3.2 with the M_i being the companion matrices for the invariant factors $g_1, \ldots, g_t$ of T, with $g_1 | \cdots | g_t$. A computation shows that the characteristic polynomial for the companion matrix of the polynomial g is g itself. Hence, $p_T = p_A = g_1 \cdots g_t$. Since the minimal polynomial for T is g_t, the result follows. □

Proposition 5.3 *The characteristic polynomial of T is the product of the invariant factors of T, and this equals the product of the elementary divisors of T.*

Proof. Combine the observations in the proof of Theorem 5.2 with Proposition 1.3.14 □

Trace. The trace of a matrix $A = (\alpha_{ij}) \in M_n(k)$ is the sum of its diagonal entries, namely

$$\mathrm{Tr}(A) = \alpha_{11} + \alpha_{22} + \cdots + \alpha_{nn}.$$

Its basic properties are:

(a) $tr(A + B) = tr(A) + tr(B)$.

(b) $tr(AB) = tr(BA)$.

(c) If the characteristic polynomial of A is $x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, then $tr(A) = -c_{n-1}$; this follows at once by looking at the coefficient of x^{n-1} in $\det(xI - A)$.

(d) If $P \in GL_n(k)$, then $tr(P^{-1}AP) = tr(A)$ because $P^{-1}AP$ and A have the same characteristic polynomials;

(e) The trace of a linear transformation T may be unambiguously defined as the trace of the matrix representing T with respect to any basis.

(f) If k is algebraically closed, and $A \subset GL_n(k)$ satisfies $A^m = 1$, then A is diagonalisable; if $P^{-1}AP = \mathrm{diag}(\lambda_1, \ldots, \lambda_k)$ then $tr(A) = tr(P^{-1}AP) = \lambda_1 + \cdots + \lambda_k$ where $\lambda_1, \ldots, \lambda_k$ are the eigenvalues for A (counted with multiplicities).

2.6 Computation

Let R be a PID and M an R-module of finite length. How do we find the invariant factors for a module M?

Let M be a finitely generated R-module, and choose generators $m_1, \ldots, m_n$. Let R^n be the free R-module with basis $e_1, \ldots, e_n$ and define $\varphi : R^n \to M$ by

$\varphi(e_j) = m_j$, $j = 1, \ldots, n$. Then $\ker\varphi \subset R^n$ is also finitely generated (and free), so let $v_1, \ldots, v_m$ be a set of generators for $\ker\varphi$. Let R^m be the free R-module with basis $f_1, \ldots, f_m$ and define $\psi : R^m \to R^n$ by $\psi(f_i) = v_i$. Thus we have an exact sequence

$$R^m \xrightarrow{\psi} R^n \xrightarrow{\varphi} M \longrightarrow 0.$$

There are elements $a_{ij} \in R$ such that

$$v_i = \sum_{j=1}^{n} a_{ij} e_j, \qquad (i = 1, \ldots, m).$$

We call the $m \times n$ matrix $A := (a_{ij})$ the relations matrix; the terminology is because the rows of the matrix give "relations" between the generators $m_1, \ldots, m_n$ for M; i.e.,

$$a_{i1}m_1 + a_{i2}m_2 + \cdots + a_{in}m_n = 0, \qquad (1 \le i \le m).$$

If we write elements of R^m and R^n as row vectors with respect to the chosen bases, the map $\psi : R^m \to R^n$ is given by right multiplication by A.

Of course, there are many choices for generating sets for M, which then changes φ and $\ker\varphi$; likewise, $\ker\varphi$ has many different generating sets, so the relations matrix is not uniquely determined.

However, changing the generators for M corresponds to performing elementary row operations on A, and changing the generators for $\ker\varphi$ corresponds to performing elementary column operations on A. For example, switching the p^{th} and q^{th} rows of A corresponds to switching m_p and m_q in the generating set for M; replacing m_p by $m_p + am_q$ corresponds to replacing row p by the sum of row p and a times row q, et cetera.

If all the entries of A are zero, then M is free with basis $m_1, \ldots, m_n$. So, suppose that not all entries of A are zero.

Claim: Let $d_1 = \gcd(a_{ij})$. We can perform elementary row and column operations on A to obtain a matrix in which the 11-entry is d, and all other entries in the first row and column of A are zero. Proof: First perform elementary row operations on A so that all the zeroes in the first row occur at the right hand end of the row, and all the zeroes in the first column occur at the bottom. If there is only one non-zero entry in the first row, and in the first columnn we are done, so suppose this is not the case. Suppose that a_{11} and a_{12} are non-zero (the argument for a_{11} and a_{21} is similar).

Let's assume we have a Euclidean algorithm so there are elements $q, r \in R$ such that $a_{11} = qa_{12} + r$, with r "smaller" than a_{12}. Then $r = a_{11} - qa_{12}$ so replacing C_1 $C_1 - qC_2$ replaces a_{11} by r. Now we can repeat this, performing elementary column operations on C_1 and C_2 so that eventually the 11-entry is d_1. $\Diamond$

Our matrix A is now of the form

$$A = \begin{pmatrix} d_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

where d_1 divides every entry in the $(m-1)\times(n-1)$ matrix A_1. We can repeat the process for A_1, thus obtaining a matrix of the form

$$A = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & A_3 \end{pmatrix}$$

where d_2 is the gcd of the entries in A_2, and so on. Eevntually, we obtain a diagonal matrix, with diagonal entries $d_1, d_2, \ldots, d_r$ where $r = \min\{m, n\}$ and zeroes elsewhere. It might happen that some of d_is are zero.

If $m < n$, then M has a free summand of rank $\geq n - m$. The d_is that are not units or zero are the invariant factors of τM, the torsion submodule of M.