MATH 542 MODULES

Suggested Review: Basic facts about vector spaces, basis, linear transformations, matrices, 11.1 and 11.2 in Dummit and Foote and well as basic group theory and ring theory.

Groups, subgroups, normal subgroups, quotient groups. Rings, Ideals, left and right ideals, quotient rings, Integral domain, principal ideals, principal ideal domains (PIDs), Euclidean domains.

Assumption: R is a ring with identity 1.

1. Basic Theory of Modules

Definition 1.1. *Suppose M is a set with operation $+$. Suppose that there is a map $R \times M \to M$. Denote the image of (r, m) by rm (or $r \cdot m$) where $r \in R$ and $m \in M$.*
M is called an R-module (or module over R) if

(1) *M is an abelian group under $+$*
(2) $(a+b)x = ax + bx \qquad a, b \in R, \quad x \in M$
(3) $a(x+y) = ax + ay \qquad a \in R, \quad x, y \in M$
(4) $(ab)x = a(bx) \qquad a, b \in R, \quad x \in M$
(5) $1x = x \qquad x \in M$

Notes:

a) The map $R \times M \to M$ is called the action of R on M.
b) In (1) we are assuming that $+$ is commutative and associative, has identity 0 and each $x \in M$ has an additive inverse $-x$, and that $-x$ is unique.
c) If $R = F$ where F is a field then modules over F are called vector spaces over F.

Example 1.2. *Let M be an abelian group with operation $+$. Let $R = \mathbb{Z}$. We define an action of $\mathbb{Z}$ on M by:*

$$nx = \begin{cases} \underbrace{x + x + \cdots + x}_{n \text{ times}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

for $n \in \mathbb{Z}$, $x \in M$. Then M is a $\mathbb{Z}$ module. We call this action the natural action. Note that any abelian group is a $\mathbb{Z}$-module under the natural action.

Example 1.3. *Suppose R is a ring with 1 . Let $M = R$. Define an action of R on M by $ax =$ product of a and x in R. So $M = R$ is a module over R. In this example M is called a regular module over R.*

Example 1.4. *Suppose R is a ring with 1. Let $M = R^n = \{(r_1, \ldots, r_n) \mid r_1, \ldots r_n \in \mathbb{R}\}$. Define $(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$ and $a(r_1, \ldots, r_n) = (ar_1, \ldots, ar_n)$. Then R^n is an R module.*

1.1. **Basic Properties.** Suppose M is an R-module. Then

a) $0x = 0$ for $x \in M$
b) $a0 = 0$ for $a \in R$
c) $(-a)x = a(-x) = -(ax)$
d) $(-1)x = -x$ for $x \in M$

Proof. a)

$$\begin{aligned} 0x + 0x &= (0+0)x \text{ - axiom of } M \\ &= 0x \text{ - axiom of } R \\ &= 0x + 0 \text{ - axiom of } M \end{aligned}$$

So $0x = 0$ by cancellation. b) is proved similarly. c) $(-a)x + ax = ((-a) + a)x = 0x = 0$, d) $(-1)x = -(1x) = -x$. □

Definition 1.5 (Subtraction)**.** *Suppose M is an R-module. Define*

$$x - y = x + (-y) \text{ for } x, y \in M$$

Then $a(x - y) = ax - ay$ for $a \in R,\ x, y \in M$.

1.2. **Submodules.**

Definition 1.6. *Suppose M is an R-module. A submodule of M is a subgroup N of M which is closed under the action of R. In other words, N is a subset of M such that*

(1) $0 \in N$
(2) $x, y \in N \Rightarrow x + y \in N$
(3) $x \in N \Rightarrow -x \in N$
(4) $x \in N, r \in R \Rightarrow rx \in N$

Note:

a) (3) follows from (4)
b) $\{0\}$ and M are submodules of M
c) We write $N \leq M$ and say N is a submodule of M.

Example 1.7. *Let M be an abelian group. We saw that M is a $\mathbb{Z}$ module under the natural action. Any submodule of M is a subgroup of M (by definition). Conversely, any subgroup of M is a submodule of M.*

Example 1.8. *Let $M = \mathbb{Z}^2$, then M is a $\mathbb{Z}$ module. Let $N = \{(a_1, a_2) \in \mathbb{Z}^2 \mid 2a_1 + 3a_2 = 0\}$. Then $N \leq M$ (exercise).*

Question 1.1. *Is any submodule of $\mathbb{Z}^2$ obtained this way? (other than $\{0\}$, $\mathbb{Z}^2$) ? Answer no: consider submodule of all even coefficients. Describe all submodules of $\mathbb{Z}^2$.*

Example 1.9. *Let R be arbitrary. Regard R as an R-module (via the regular action). Then the submodules of R are left ideals of R. If R is commutative then the submodules of R are the ideals of R.*

1.3. **Quotient Modules.**

Definition 1.10 (Quotient groups)**.** *Suppose H is a normal subgroup of a group G. Then $G/H = \{gH \mid g \in G\}$ is a group under the operation $(g_1H)(g_2H) = g_1g_2H$. Note also that $g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H$.*

Definition 1.11 (Quotient Module)**.** *Suppose $N \leq M$. Then N is a subgroup of M but M is abelian and hence any subgroup of M is normal. Thus we can form the quotient group*

$$M/N = \{x + N \mid x \in M\}$$

and we have

$$\begin{aligned} x + N = y + N &\Leftrightarrow (-y) + x \in N \\ &\Leftrightarrow x + (-y) \in N \\ &\Leftrightarrow x - y \in N \end{aligned}$$

The operation on M/N is

$$(x + N) + (y + N) = (x + y) + N.$$

Since M is abelian, M/N is also an abelian group. We define the action of R on M/N by

$$a(x + N) = ax + N.$$

Is this operation well defined? Suppose that $x + N = y + N$ (1) where $x, y \in M$. If $a \in R$, we must show that $ax + N = ay + N$ (2). By (1) we have $x - y \in N$ since N is a subgroup of M. Thus $ax - ay \in N$ since N is a submodule and so $ax + N = ay + N$. So the action is well defined. It is easy to check that M/N satisfies axioms $(2) - (5)$ in the definition of a module . Therefore M/N is a module.

Conclusion. Suppose $N \leq M$. Then M/N is a module called the quotient module of M by N. The zero element is $0 + N$. Also $-(x + N) = (-x) + N$.

Notation. Suppose $N \leq M$. We write $\bar{M} = M/N$. Also write $\bar{x} = x + N$. Then

$$\begin{aligned} \bar{x} = \bar{y} &\Leftrightarrow x - y \in N \\ \bar{x} + \bar{y} &= \overline{x + y} \\ a\bar{x} &= \overline{ax} \\ -\bar{x} &= \overline{-x} \end{aligned}$$

Example 1.12. *Suppose R is an arbitrary ring. Regard R as an R-module. Suppose L is a left ideal of R (i.e. a submodule of R). Then $L \leq R$ so we can form the quotient module R/L.*

1.4. **Module homomorphisms.**

Definition 1.13. *Let M, M' be R-modules. A homomorphism from M into M' is a map $\phi : M \to M'$ so that*

a) $\phi(x + y) = \phi(x) + \phi(y) \qquad x, y \in M$
b) $\phi(rx) = r\phi(x) \qquad r \in R,\ x \in M$

Note. If $R = F$ a field then homomorphisms are called linear transformations.

Example 1.14. *Define $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ by $\phi(a_1, a_2) = 2a_1 + 3a_2$. Then ϕ is a $\mathbb{Z}$-module homomorphism.*

Definition 1.15. *Suppose $\phi : M \to M'$ is an R-module homomorphism. Define the kernel to be*

$$ker(\phi) = \{x \in M \mid \phi(x) = 0\}$$

and the image of ϕ to be

$$im(\phi) = \{\phi(x) \mid x \in M\}$$

Then $ker(\phi) \leq M$ and $im(\phi) \leq M'$.

Example 1.16. *Let $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ be as above. Then $ker(\phi) = \{(a_1, a_2) \in \mathbb{Z}^2 \mid 2a_1 + 3a_2 = 0\}$ and $im(\phi) = \mathbb{Z}$ since $gcd(2, 3) = 1$.*

Definition 1.17. *Suppose M, M' are R-modules. An* isomorphism *from M to M' is a bijective homomorphism $\phi : M \to M'$. We say M, M' aare* isomorphic *(written $M \simeq M'$) if there is an isomorphism from M to M'.*

Exercise 1.18. *Suppose $\phi : M \to M'$ is an isomorphism. Show that $\phi^{-1} : M' \to M$ is also an isomorphism. Show that $\simeq$ is an equivalence relation.*

Note. Suppose $\phi : M \to M'$ is a homomorphsim. Then

- ϕ injective $\Leftrightarrow \ker(\phi) = \{0\}$
- ϕ surjective $\Leftrightarrow im(\phi) = M'$

The Natural Homomorphsim. Suppose $N \leq M$. Then

$$M/N = \{x + N \mid x \in M\}$$

is an R-module. Define $\pi : M \to M/N$ by $\pi(x) = \bar{x} = x + N$. One checks that π is a homomorphism. Call π the natural (canonical) homomorphism. Note that $\ker(\pi) = N$ and $im(\pi) = M/N$. so that π is a surjective homomorphism with kernel N.

Theorem 1.19 (1st Isomorphism Theorem for Modules)**.** *Suppose $\phi : M \to M'$ is a surjective homomorphsim of R-modules with kernel N. Then*

$$M' \simeq M/N$$

Proof. Define $\psi : M/N \to M'$ by

$$\psi(x + N) = \phi(x).$$

We must check that

- ψ is well-defined
- ψ preserves addition
- ψ preserves the action of R
- ψ is injective
- ψ is surjective

By the first isomorphism theorem for groups everthing holds except perhaps that ψ preserves the action. To check that note that

$$\begin{aligned}\psi(r(x+n)) &= \psi(rx+N) \quad \text{by definition of action on} M/N \\ &= \phi(rx) \quad \text{by definition of } \psi \\ &= r\phi(x) \quad \phi \text{ is } R\text{-module homomorphism} \\ &= r\psi(x+N) \quad \text{by definition of } \psi\end{aligned}$$

□

Problem 1.1. *Let $M = \mathbb{Z}^2$ and $N = \{(a_1, a_2) \mid 2a_1 + 3a_2 = 0\}$. Show that $M/N \simeq \mathbb{Z}$ (as Z-modules)*

Proof. Define $\phi : M \to \mathbb{Z}$ by $\phi(a_1, a_2) = 2a_1 + 3a_2$. Then $\ker(\phi) = N$ and ϕ is surjective. Therefore by the first isomorphism theorem $M/N \simeq \mathbb{Z}$. □

Theorem 1.20 (Lattice Isomorphism theorem (4th))**.** *Suppose $N \leq M$.*

a) *If K is a submodule of M which contains N then K/N is a submodule of M/N.*
b) *Any submodule of M/N is equal to K/N for some unique submodule K of M containing N.*

Proof. Exercise. □

Definition 1.21. *Suppose $M_1, M_2, \ldots, M_k$ are R-modules. Define*

$$M_1 \oplus M_2 \oplus \cdots \oplus M_k = \{(x_1, x_2, \ldots, x_k) \mid x_1 \in M_1, x_2 \in M_2, \ldots, x_k \in M_k\}$$

Define

$$(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) = (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k)$$

and

$$a((x_1, x_2, \ldots, x_k) = (ax_1, ax_2, \ldots, ax_k).$$

Then $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ is an R-module called the external direct sum *of $M_1, M_2, \ldots, M_k$.*

Example 1.22. $\underbrace{R \oplus R \oplus \cdots \oplus R}_{n \text{ times}} = R^n$

1.5. **The building blocks for modules.** Suppose R is a commutative ring with 1. Suppose $a \in R$. Let

$$(a) = Ra = \{ra \mid r \in R\}.$$

Then (a) is an ideal of R. Hence (a) is a submodule of R (regarded as an R-module). Thus we can form the quotient module $R/(a)$. If $a = 0$ we get $R/(0) \simeq R$. If R is a PID we'll prove that any finitely generated module is isomorphic to a direct sum of modules of the form $R/(a)$.

Example 1.23. *Let $R = \mathbb{Z}$. Then*

$$\mathbb{Z}/(2) = \{0 + (2), 1 + (2)\} = \{\bar{0}, \bar{1}\}$$

is a $\mathbb{Z}$-module and so is

$$\mathbb{Z}/(3) = \{\bar{0}, \bar{1}, \bar{2}\}.$$

Let

$$M = \mathbb{Z}/(2) \oplus \mathbb{Z}/(3) = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$$

Example 1.24. *Consider the $\mathbb{Z}$-module*

$$M = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}}_{\text{free part}} \oplus \underbrace{\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(12)}_{\text{torsion part}}$$

Definition 1.25. *Suppose M is an R-module. Suppose $M_1, M_2, \ldots, M_k$ are submodules of M. We define*

$$M_1 + M_2 + \cdots M_k = \{m_1 + m_2 + \cdots + m_k \mid m_1 \in M_1, m_2 \in M_2, \ldots, m_k \in M_k\}.$$

Then $M_1 + M_2 + \cdots + M_k \leq M$.

Note.

$$M = M_1 + M_2 + \cdots M_k \Leftrightarrow \forall x \in M, \quad x \text{ can be expressed in the above form.}$$

Definition 1.26. *Suppose $M_1, M_2, \ldots, M_k \leq M$. We say that M is the* internal direct sum *if every $x \in M$ can be expressed uniquely in the form*

$$x = x_1 + x_2 + \cdots + x_k \text{ where } x_1 \in M_1, x_2 \in M_2, \ldots x_k \in M_k.$$

Proposition 1.27. *Suppose that $M_1, M_2, \ldots, M_k \leq M$. Then M is the internal direct sum of $M_1, M_2, \cdots, M_k$ if and only if*

a) $M = M_1 + M_2 + \cdots + M_k$
b) $x_1 + x_2 + \cdots + x_k = 0 \Rightarrow x_1 = x_2 = \cdots = x_k = 0$

Also b) can be replaced by the equivalent condition:

b') $(M_1 + \cdots + M_i) \cap M_{i+1} = \{0\}$ *for* $i = 1, \ldots, k-1$

Proof. Exercise. □

Example 1.28. *Suppsoe $M_1, M_2 \leq M$. Then M is the internal direct sum of M_1 and M_2 if and only if*

a) $M = M_1 + M_2$
b') $M_1 \cap M_2 = \{0\}$

Exercise 1.29. *Let $M = \mathbb{Z}^2$. Let $M_1 = \{(a_1, a_2) \mid 2a_1 + 3a_2 = 0\}$ and $M_2 = \{(a_1, a_2) \mid a_1 + a_2 = 0\}$. Show that M is the internal direct sum of M_1 and M_2.*

The connection between internal and external direct sums.

a) Suppose $M_1, M_2, \ldots, M_k \leq M$ and M is the internal direct sum of $M_1, M_2, \ldots, M_k$. Define

$$\phi : M_1 \oplus M_2 \oplus \cdots \oplus M_k \to M$$

by $\phi(x_1, \ldots, x_k) = x_1 + x_2 \cdots + x_k$. Then ϕ is an R-module homomorphism (check this) and since M is the internal direct sum of $M_1, \ldots, M_k$ then ϕ is an isomorphism. Thus

$$M \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_k$$

b) Suppose $M_1, M_2, \ldots, M_k$ are modules. Let $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ and let

$$M_1' = \{(x_1, 0, \ldots, 0) \mid x_1 \in M_1\}$$

$$\vdots$$

$$M_k' = \{(0, \ldots, 0, x_k) \mid x_k \in M_k\}$$

Then $M_1' \simeq M_1, \ldots, M_k' \simeq M_k$. Moreover, M is the internal direct sum of $M_1', \ldots, M_k'$.

Notation. Suppose $M_1, \ldots, M_k \leq M$. We often write $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ to mean that M is the internal direct sum of $M_1, \ldots, M_k$. This abuse of notation will not cause any confusion.

Problem 1.2. *Let $M = \mathbb{Z}/(6) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ as a $\mathbb{Z}$ module. Let $M_1 = \{\bar{0}, \bar{3}\}$ and $M_2 = \{\bar{0}, \bar{2}, \bar{4}\}$. Show that $M = M_1 \oplus M_2$ (internal).*

Proof. We must show that $M = M_1 + M_2$ and $M_1 \cap M_2 = \{\bar{0}\}$. Note that $\bar{1} = \bar{3} + \bar{4}$. Where $\bar{3} \in M_1$ and $\bar{4} \in M_2$. Therefore $\bar{1} \in M_1 + M_2$, hence $n\bar{1} \in M_1 + M_2$ for all $n \in \mathbb{Z}$. Therefore $M = M_1 + M_2$. Also clearly $M_1 \cap M_2 = \{0\}$. □

Note. In the above problem, if follows that $M \simeq M_1 \oplus M_2$ but clearly $M_1 \simeq \mathbb{Z}/(2)$ and $M_2 \simeq \mathbb{Z}/(3)$. Therefore $M \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$. Therefore $\mathbb{Z}/(6) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$ as $\mathbb{Z}$ modules.

Exercise 1.30. *Suppse that $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ (internal). Suppose that $N_1 \leq M_1, \ldots, N_k \leq M_k$. Let $N = N_1 + N_2 + \cdots + N_k$. Show that*

$$M/N \simeq (M_1/N_1) \oplus \cdots \oplus (M_k/N_k)\,.$$

(Hint: use the first isomorphism theorem)

The submodule Rx. Suppose M is a module and $x \in M$. Let

$$Rx = \{rx \mid r \in R\}$$

Then Rx is a submodule of M containing x. In fact Rx is the smallest submodule of M containing x. (i.e. Rx is contained in all modules that contain x). Rx is called the *submodule of M generated by x* or the *cyclic* submodule of M generated by x. The element x is called a generator of Rx.

Example 1.31. *Suppose M is an abelian group regarded as a $\mathbb{Z}$-module. Let $x \in M$. Then $\mathbb{Z}x = \{nx \mid n \in \mathbb{Z}\}$ which is the cyclic subgroup generated by x.*

Definition 1.32. *Suppose M is a module and $x_1, x_2, \ldots, x_k \in M$. The submodule*

$$Rx_1 + Rx_2 + \cdots + Rx_k = \{r_1x_1 + r_2x_2 + \cdots r_kx_k \mid r_1, r_2, \ldots, r_k \in R\}$$

is called the submodule of M generated by $x_1, x_2, \ldots, x_k$. It is the smallest submodule of M containing $x_1, x_2, \ldots, x_k$.

Definition 1.33. *Let M be a module. M is said to be* finitely generated *if there exists $x_1, x_2, \ldots, x_k \in M$ such that $M = Rx_1 + Rx_2 + \cdots + Rx_k$. In that case $\{x_1, \ldots, x_k\}$ is called a* generating set *for M or a* spanning set*.*

Recall. A left ideal of R is a subgroup L of R under $+$ which is closed under left multiplication by elements of R (i.e. $r \in R, \ell \in L \Rightarrow r\ell \in L$). If R is commutative, left ideals are simply ideals.

Definition 1.34. *Suppose M is a module. We define*

$$Ann(M) = \{r \in R \mid rx = 0 \ \ \forall x \in M\}$$

Then $Ann(M)$ is an ideal of R (Exercise). $Ann(M)$ is called the annihilator of M.

Definition 1.35. *Suppose M is a module and $x \in M$. Let*

$$Ann(x) = \{r \in R \mid rx = 0\}$$

Then $Ann(x)$ is a left ideal of R (Exercise). $Ann(x)$ is called the annihilator of x.

Proposition 1.36. *Suppose R is commutative. Suppose $M = Rx$ is a cyclic module with generator x. Then $Ann(M) = Ann(x)$.*

Proof. " $\subseteq$" Let $r \in Ann(M)$. Then $ry = 0$ for all $y \in M$. Therefore $rx = 0$ and so $r \in Ann(x)$.
"*supseteq*" Suppose $r \in Ann(x)$ then $rx = 0$. We want to show that $ry = 0$ for all $y \in M$. Let $y \in M$. Then $y = sx$ for some $s \in R$. So

$$\begin{aligned} ry &= rsx \\ &= srx \text{ since } R \text{ commutative.} \\ &= s0 \\ &= 0 \end{aligned}$$

So $ry = 0$ for all r and so $r \in Ann(M)$. □

Exercise 1.37. *Suppose $M_1, \ldots, M_k \leq M$. Show that*

$$Ann(M_1 + \cdots + M_k) = Ann(M_1) \cap Ann(M_2) \cap \cdots \cap Ann(M_n)$$

Corollary 1.38. *Suppose R is commutative and $M = Rx_1 + \cdots Rx_k$ is a finitely generated module over R. Then*

$$Ann(M) = Ann(x_1) \cap Ann(x_2) \cap \cdots \cap Ann(x_k)$$

Theorem 1.39 (Structure of cyclic modules)**.**
a) *Suppose $M = Rx$ is a cyclic module with generator x. Then $M \simeq R/L$ where $L = Ann(x)$.*
b) *Suppose that L is a left ideal of R. Then R/L is a cyclic module with generator $x = 1 + L$. Moreover $L = Ann(x)$ in that case.*
c) *Suppose R is a commutative ring and L_1 and L_2 are left ideals of R. Then*

$$R/L_1 \simeq R/L_2 \Leftrightarrow L_1 = L_2$$

Proof. **a)** Suppose $M = Rx$ and let $L = Ann(x)$. We define $\phi : R \to M$ by $\phi(r) = rx$ for $r \in R$. Then for $r_1, r_2 \in R$ we have

$$\phi(r_1 + r_2) = (r_1 + r_2)x = rx_1 + rx_2 = \phi(r_1) + \phi(r_2).$$

Also for $r_1, r_2 \in R$ we have $\phi(r_1 r_2) = r_1 r_2 x = r_1 \phi(r_2)$. Therefore ϕ is an R-module homomorphism. Since $M = Rx$, ϕ is surjective. Also

$$\begin{aligned} \ker(\phi) &= \{r \in R \mid \phi(r) = 0\} \\ &= \{r \in R \mid rx = 0\} \\ &= Ann(x) \\ &= L \end{aligned}$$

By the first isomorphism theorem $M \simeq R/L$.

b) Suppose L is a left ideal of R. Let $M = R/L$. Let $x = 1 + L \in M$. Then

$$\begin{aligned} Rx &= \{rx \mid r \in R\} \\ &= \{r(1+L) \mid r \in R\} \\ &= \{r + L \mid r \in R\} \\ &= R/L \\ &= M \end{aligned}$$

Therefore $M = Rx$ and so M is cyclic with generator x. Finally,

$$\begin{aligned} Ann(x) &= \{r \in R \mid rx = 0\} \\ &= \{r \in R \mid r(1+L) = 0 + L\} \\ &= \{r \in R \mid r \in L\} = L \end{aligned}$$

c) Exercise. □

1.6. **Structure of cyclic modules over a PID.** Suppose R is an *integral domain*. This means that R is commutative with 1, $1 \neq 0$ and for $a, b \in R$, $ab = 0 \Rightarrow$ $a = 0$ or $b = 0$. If $a, b \in R$ then we say a is an *associate* of b if $a = ub$ for some unit $u \in R$. We write this as $a \sim b$. Then $\sim$ is an equivalence relation on R. Recall that if $a, b \in R$ then

$$\begin{aligned} (a) = (b) &\Leftrightarrow a \mid b \text{ and } b \mid a \\ &\Leftrightarrow a \sim b \end{aligned}$$

Example 1.40. *Let $R = \mathbb{Z}$. The units of $\mathbb{Z}$ are ± 1. So if $a, b \in \mathbb{Z}$, $(a) = (b) \Leftrightarrow a \sim b \Leftrightarrow a = \pm b$.*

Theorem 1.41 (Structure of cyclic modules over a PID)**.** *Suppose R is a PID. If M a cyclic module over R then $M \simeq R/(a)$ for some $a \in R$ and conversely $R/(a)$ is cyclic for any $a \in R$. Additionally two such modules $R/(a)$ and $R/(b)$ are isomorphic iff $a \sim b$.*

Proof. Suppose R is a PID. If M is a cyclic module over R then $M \simeq R/L$ for some submodule (i.e. ideal) L of R by the previous theorem. Since R is a PID $L = (a)$ for some $a \in R$. Therefore $M \simeq R/(a)$ for some $a \in R$. Conversely if $a \in R$ then $R/(a)$ is cyclic (by previous theorem). Finally if $a, b \in R$ then $R/(a) \simeq R/(b) \Leftrightarrow (a) = (b)$ by part c) of the previous theorem. Therefore by the above discussion $a \sim b$. □

Example 1.42. *Let $R = \mathbb{Z}$. Then any integer is an associate of a unique integer ≥ 0. So the cyclic $\mathbb{Z}$- modules (i.e. cyclic groups) are the $\mathbb{Z}$ modules $\mathbb{Z}/(0), \mathbb{Z}/(1), \mathbb{Z}/(2), \ldots$. Note that $\mathbb{Z}/(0) \simeq \mathbb{Z}$ and $\mathbb{Z}/(1) = \{0\}$.*

1.7. **Free modules.**

Definition 1.43. *Suppose M is an R-module and $\beta = \{x_1, x_2, \ldots, x_k\}$ is a subset of M.*

a) *β is called a generating set (or spanning set) for M if every $x \in M$ can be written as*

$$x = \sum_{i=1}^{k} r_i x_i$$

where $r_i \in R$.

(1) *β is said to be* independent *if*

$$\left(\sum_{i=1}^{k} r_i x_i = 0\right) \Rightarrow r_i = 0 \ \forall i$$

c) *β is said to be dependent if β is not independent.*
d) *β is called a* basis *for M if β is an independent spanning set for M.*

Exercise 1.44. *Show that β is a basis for M if every $x \in M$ can be expressed uniquely in the form $\sum_{i=1}^{k} r_i x_i$ where $r_i \in R$.*

Definition 1.45. *A module M is said to be* free *if it has a basis $\beta = \{x_1, \ldots, x_k\}$.*

Property 1.1 (Universal Property of Free Modules)**.** *Suppose M is a free R-module with basis $\beta = \{x_1, x_2, \ldots, x_k\}$. Suppose M' is another R-module and $\gamma = \{y_1, y_2, \ldots, y_k\}$ is a subset of M'. Then there exists a unique homomorphism $\phi : M \to M'$ so that $\phi(x_i) = y_i$ for $i = 1, \ldots, k$.*

Proof. Define $\phi : M \to M'$ by

$$\phi(\sum_{i=1}^{k} r_i x_i) = \sum_{i=1}^{k} r_i y_i$$

for $r_i \in R$. ϕ is well-defined since β is a basis. ϕ is a homomorphism and $\phi(x_i) = y_i$ for $i = 1, \ldots, k$. Suppose ψ is any homomorphism from M to M' so that $\psi(x_i) = y_i$. Then

$$\psi(\sum_{i=1}^{k} r_i x_i) = \sum_{i=1}^{k} \psi(r_i x_i) = \sum_{i=1}^{k} r_i \psi(x_i) = \sum_{i=1}^{k} r_i y_i$$

hence $\phi = \psi$. □

Example 1.46. *Let $M = \mathbb{R}^k$. Let $e_1 = (1, 0, \ldots, 0), \ldots, e_k = (0, \ldots, 0, 1)$. Let $\beta = \{e_1, \ldots, e_k\}$ then β is a basis for M called the* standard basis.

Proposition 1.47. *Suppose M is a free module with basis $\beta = \{x_1, \ldots, x_k\}$. Define $\phi : R^n \to M$ by*

$$\phi(r_1, \ldots, r_n) = \sum_{i=1}^{k} r_i x_i \text{ for } r_i \in R$$

Thus ϕ is an isomorphism and so

$$M \simeq R^n$$

Proof. ϕ is a homomorphism. It is surjective since β is a generating set for M. ϕ is injective since β is independent. □

Key Question. Let M be a free module over R. Is it true that any two bases contain the same number of elements?

Notes

a) This is equivalent to $R^n \simeq R^m \Rightarrow n = m$.
b) We will prove this when R is an integral domain. It is in fact true when R is commutative. In general it is false.

Lemma 1.48. *Suppose R is an integral domain. suppose M is a free module with basis $\beta = \{x_1, \ldots, x_m\}$. Suppose $\gamma = \{y_1, \ldots, y_n\} \subset M$ and $n > m$. Then γ is dependent.*

Proof. First, each $y_j = \sum_{i=1}^{n} q_{ij}x_i$ for $j = 1, \ldots, n$ where $q_{ij} \in R$ and (q_{ij}) is an $m \times n$ matrix over R. Consider the equation

$$\sum_{j=1}^{n} r_j y_j = 0 \tag{1}$$

We want to find $r_1, \ldots, r_n$ not all 0 satisfying 1. Now

$$\begin{aligned} LHS &= \sum_{j=1}^{n} r_j \left(\sum_{i=1}^{m} q_{ij}x_j \right) = \sum_{j=1}^{n}\sum_{i=1}^{m} r_j q_{ij} x_i \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} r_j q_{ij} x_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} r_j q_{ij} \right) x_i \end{aligned}$$

Thus (1) holds iff

$$\sum_{j=1}^{n} q_{ij} r_j = 0 \quad i = 1, \ldots, m \tag{2}$$

this is a homogeneous system of m equations in n unknowns where $n > m$. If R were a field then from linear algebra we would know that (2) has a nontrivial solution.

Definition 1.49. *The* quotient field *or field of fractions of an integral domain R is the field*

$$F = \{[a, b] \mid a, b \in R,\ b \neq 0, [a, b] = [c, d] \text{ if } a = ec, b = ed, \text{ for some } e \in R\}$$

with addition $[a, b] + [c, d] = [ad + cb, bd]$ and multiplication given by $[a, b][c, d] = [ac, bd]$.

Exercise 1.50. *Check that the quotient field is actually a field when R is an integral domain.*

Let F = quotient field of R. F exists since R is an integral domain. Now (2) can be regarded as a system of equations with coefficients from F. Then from linear algebra we have a nontrivial solution for (2) in F. We can write our solution as $r_1 = a_1/b, \ldots, r_n = a_n/b$ where $r_1, \ldots, r_n \in R,\ b \in R \setminus \{0\}$. Thus $r_1 = a_1, \ldots, r_n = a_n$ is a non-trivial solution of (2) over R. Therefore (1) also has a non-trivial solution over R and γ is dependent. □

Theorem 1.51. *Suppose M is a free module over an integral domain R. Then the* rank *of M denoted $rk(M)$ is the number of elements in a basis. By the previous theorem this is well defined.*

Exercise 1.52. *Suppose R is an integral domain*

a) *If M is a free module of rank n and $M \simeq M'$. Show that M' is a free module of rank n.*
b) *Show that $R^m \simeq R^n$ implies $m = n$.*

Matrice.

(1) $M_{m\times n}(R)$ is the set of all $m \times n$ matrices over R.Then $M_{m\times n}(R)$ is an R-module with component addition and component action.
(2) $R^n = M_{n\times 1}(R)$ if we view R^n as the set of column matrices whose ijth entry is a_{ij}

(3) If $A \in M_{m\times n}(R)$ and $B \in M_{n\times p}(R)$ then $AB \in M_{m\times p}(R)$ is defined as usual.
(4) $M_{n\times n}(R)$ is a ring using matrix addition and multiplication.
(5) If $A \in M_{n\times n}$ we say that A is invertible if there exists $B \in M_{n\times n}(R)$ so that

$$AB = BA = I$$

In that case B is unique and denoted by A^{-1}.
(6) If R is commutative and $A \in M_{n\times n}(R)$ we define $\det A \in R$ as usual. Then A is invertible iff $\det A$ is a unit.

Example 1.53. *Let* $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_{2\times 2}(\mathbb{Z})$. *Then* $\det A = -2 \neq \pm 1$ *so* A *is not invertible in* $inM_{2\times 2}(\mathbb{Z})$.

Assumption. R is an integral domain so the rank of a free module over R is well defined.

Coordinates. Suppose M is a free module of rank n. Let

$$\beta = \{x_1, x_2, \ldots, x_n\}$$

be a basis for M. If $x \in M$ then x can be uniquely expressed in teh form

$$x = \sum_{i=1}^{n} r_i x_i \text{ where } r_1, \ldots, r_n \in R$$

We define

$$[x]_\beta = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \in R^n$$

$[x]_\beta$ is called teh coordinate vector of x relative to β.

Definition 1.54. *An* endomorphism *of* M *is an* R *module homomorphism from* M *to* M. *(If* $R = F$ *is a field then an endomorphism is called a linear operator.) If* ϕ *is an endomorphism of* M *then*

$$\phi(x_j) = \sum_{i=1}^{n} a_{ij} x_i \text{ for } j = 1, \ldots, n$$

where $A = (a_{ij}) \in M_{n\times n}(R)$. *In that case we define*

$$[\phi]_\beta = A = (a_{ij})$$

$[\phi]_\beta$ *is called the matrix of* ϕ *relative to* β.

Proposition 1.55. *Let* B *be a basis for a free module* M *of rank* n. *Then*

a) $x \to [x]_\beta$ *is an* R*-module isomorphism of* M *onto* R^n.
b) *If* ϕ *is an endomorphism of* M *then*

$$[\phi(x)]_\beta = [\phi]_\beta [x]_\beta \ \forall\ x \in M$$

Moreover $[\phi]_\beta$ *is the unique matrix in* $M_{n\times n}(R)$ *with this property.*

c) *If ϕ, ψ are endomorphisms of M and $r \in R$ then*

$$[\phi + \psi]_\beta = [\phi]_\beta + [\psi]_\beta$$

$$[r\phi]_\beta = r[\phi]_\beta$$

$$[\phi\psi]_\beta = [\phi]_\beta + [\psi]_\beta$$

Where $\phi + \psi$, $r\phi$, $\phi\psi$ are defined as usual.

Proof. Same proof as in linear algebra. □

Change of Basis. Suppose M is a free module of rank n with bases $\beta = \{x_1, \ldots, x_n\}$ and $\gamma = \{y_1, \ldots, y_n\}$. Then

$$y_j = \sum_{i=1}^{n} q_{ij} x_i, \ j = 1, \ldots, n$$

where $Q = (q_{ij}) \in M_{n\times n}(R)$. Q is called the change of basis matrix from γ to β. We denote Q by $change(\gamma, \beta)$.

Proposition 1.56. *Suppose β, γ are bases for a free module M of rank n. Let $Q = change(\gamma, \beta)$. Then*

a) *$[x]_\beta = Q[x]_\gamma$ for all $x \in M$. Moreover Q is the unique matrix in $M_{n\times n}(R)$ with this property.*
b) *Q is invertible. $Q^{-1} = change(\beta, \gamma)$.*
c) *If ϕ is an endomorphism of M then*

$$[\phi]_\gamma = Q^{-1}[\phi]_\beta Q$$

Proof. a), b) Exercises. To prove c):

$$\begin{aligned} [\phi(x)]_\gamma &= Q^{-1}[\phi(x)]_\beta \\ &= Q^{-1}[\phi]_\beta[x]_\beta \\ &= Q^{-1}[\phi]_\beta Q[x]_\gamma \end{aligned}$$

Therefore $Q^{-1}[\phi]_\beta Q = [\phi]_\gamma$. □

Exercise 1.57.
Suppose that M is a free module of rank n with basis $\beta = \{x_1, \ldots, x_n\}$. Suppose Q is an invertible matrix in $M_{n\times n}(R)$. Define

$$y_j = \sum_{i=1}^{n} q_{ij} x_i \quad j = 1, \ldots, n$$

where $Q = (q_{ij})$. Let $\gamma = \{y_1, \ldots, y_n\}$. Then γ is a basis for M and $Q = change(\gamma, \beta)$.

Suppose R is a PID. If $M = \{0\}$ we regard the empty set as a basis for M. Hence M is free of rank 0.

Theorem 1.58. *Suppose R is a PID. Suppose M is a free module of rank n where $n \geq 0$. Suppose $N \leq M$. Then N is a free module of rank $m \leq n$.*

Proof. We prove this by induction on n. Suppose $n = 0$. Therefore $M = \{0\}$ and so $N = \{0\}$. Therefore N is free of rank 0. Suppose $n \geq 1$. Assume that the theorem is true for free modules of rank $n-1$. If M has a basis $\beta = \{x_1, \ldots, , x_n\}$ let $M_2 = Rx_2 + Rx_3 + \cdots + Rx_n$. Then $\{x_2, \ldots, x_n\}$ is a basis for M_2 (why?). Therefore M_2 is free of rank $n-1$. By the induction hypothesis any submodule of M_2 is free of rank $\leq n-1$. If N is contained in M_2 then N is free of rank $\leq n-1$ and hence of rank $\leq n$. Assume N is not contained in M_2. Now $N \cap M_2 \leq M_2$. Thus $N \cap M_2$ is free of rank $\leq n-1$. Thus $N \cap M_2$ has a basis $\{y_2, \ldots, y_m\}$ where $m - 1 \leq n - 1$. Our strategy is to find a vector $y_1 \in N$ so that $\{y_1, y_2, \ldots, y_m\}$ is a basis for N. Now every element of N is also an element of M and hence expressible in the form

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n$$

where $r_1, r_2, \ldots, r_n \in R$. Let I be the set of all elements $r \in R$ which occur as the coefficients of x_1 in an expression for some element of N. Then I is an ideal of R. Since R is a PID then $I = (a)$ for some $a \in R$. Since N is not contained in M_2 then $I \neq \{0\}$. Therefore $a \neq 0$. Now $a \in I$. Thus there exists $y_1 \in N$ of the form

$$y_1 = ax_1 + \sum_{i=2}^{n} a_i x_i \qquad (\#)$$

where $a_2, \ldots, a_n \in R$. We will show that $\{y_1, \ldots, y_m\}$ is a basis for N. To show $\{y_1, \ldots, y_n\}$ generates N let $x \in N$. Since $x \in M$ we have

$$x = r_1x_1 + \sum_{i=2}^{n} r_i x_i$$

where $r_1, r_2, \ldots, r_n \in R$. Since $x \in N$ then $r_1 \in I$ so $r_1 = s_1 a$ for some $s_1 \in R$. Therefore

$$x = s_1ax_1 + \sum_{i=2}^{n} r_i x_i$$

and so

$$\begin{aligned} x &= s_1(y_1 - + \sum_{i=2}^{n} a_i x_i) + + \sum_{i=2}^{n} r_i x_i \\ &= s_1 y_1 + \underbrace{\sum_{i=2}^{n} (r_i - s_1 a_i) x_i}_{(*)} \end{aligned}$$

From the form of $(*)$ we can see that $(*)$ is in M_2. Also $(*) = x - s_1y_1$ and so $(*) \in N$. Therefore $(*) \in N \cap M_2$. Therefore $(*)$ is a linear combination of $\{y_2, \ldots, y_m\}$. To show $\{y_1, \ldots, y_m\}$ is independent consider an equation

$$\sum_{i=1}^{m} r_i y_i = 0 \qquad (\#)$$

where $r_1, \ldots, r_m \in R$. We must show that $r_1 = r_2 = \cdots = r_m = 0$. By substituting in for y_1 in (#) we have

$$r_1(ax_1 + \sum_{i=2}^{n} a_i x_i) + \sum_{i=2}^{m} r_i y_i = 0$$

so that

$$r_1 a x_1 + \sum_{i=2}^{n} r_1 a_i x_i + \underbrace{\sum_{i=2}^{m} r_i y_i = 0}_{(**)}$$

Now $(**)$ is in $N \cap M_2$ and hence in M_2 and hence is a linear combination of $x_2, \ldots, x_n$. But $\{x_1, \ldots, x_n\}$ is independent so $r_1 a = 0$. But $a \neq 0$ which means $r_1 = 0$. By (#) we have

$$\sum_{i=2}^{m} r_i y_i = 0$$

but $\{y_2, \ldots, y_m\}$ is independent. Therefore $r_2 = 0, \ldots, r_m = 0$. Therefore $\{y_1, \ldots, y_m\}$ is independent and therefore is a basis for N. Therefore N is free of rank m and $m \leq n$.

□

Definition 1.59. *Suppose A is an $m \times n$ matrix over R. An elementary row operation on A is one of the following:*

a) *Add a times row i to row j where $a \in R$ and $i \neq j$. ($AR_{ij}(a)$)*
b) *Interchange rows i and j where $i \neq j$. (IR_{ij})*
c) *Multiply row i by u where u is a unit in R. ($MR_{ij}(u)$)*

Similarly we define elementary column operations $AC_{ij}(a)$, IC_{ij}, $MC_i(u)$.

Definition 1.60. *A $n \times n$ matrix E is called* elementary *if it can be obtained from I by a single elementary row or column operation.*

Example 1.61. *Let $R = \mathbb{Z}$. Then*

$$E = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$$

is elementary by $AR_{12}(3)$ or by $AC_{21}(3)$.

Proposition 1.62. *Suppose A is an $m \times n$ matrix over R*

a) *Suppose E is an elementary matrix obtained from I by the elementary row operation O. Then EA can be obtained from A by O.*
b) *Suppose E is an elementary matrix obtained from I by the elementary column operation O. Then AE can be obtained from A by O.*

Corollary 1.63. *If E is an elementary matrix then E is invertible and E^{-1} is also elementary.*

Corollary 1.64. *If A is the product of elementary matrices then A is invertible.*

Definition 1.65. *Suppose $A, B \in M_{m\times n}(R)$. We say that A is equivalent to B written $A \sim B$ if there exists an invertible matrix $J \in M_{m\times m}(R)$ and an invertible $K \in M_{m\times m}(R)$ so that*

$$B = JAK.$$

(Check that $\sim$ is an equivalence relation.)

Corollary 1.66. *Suppose that $A, B \in M_{m\times n}(R)$ and B can be obtained from A by a sequence of elementary row and column operations. Then $A \sim B$.*

Definition 1.67. *A Smith normal form (SNF) is an $m \times n$ matrix over R of the form*

$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

where $d_1, d_2, \ldots, d_r$ are non zero elements of R and $d_1 \mid d_2 \mid \cdots \mid d_r$

Recall Suppose R is a Euclidean domain with norm N. Then $N(a)$ is a non-negative integer for any $a \in R$ with $a \neq 0$. If $a, b \in R$ and $b \neq 0$ then there exists $a, r \in R$ with $a = qb + r$ and either $r = 0$ or $r \neq 0$ and $N(r) < N(b)$

Lemma 1.68 (The basic step)**.** *Suppose $A = (a_{ij})$ is an $m \times n$ matrix over R with $a_{11} \neq 0$. Suppose R is a Euclidean domain. Then A is equivalent to a matrix $B = (b_{ij})$ so that $b_{11} \neq 0$ and either*

a) $N(b_{11}) < N(a_{11})$

b) $B = \begin{pmatrix} b_{11} & 0 & 0 & \cdots \\ 0 & b_{22} & b_{23} & \cdots \\ 0 & b_{32} & \ddots & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ *and b_{11} divides b_{ij} for $i, j > 2$.*

Proof. (Algorithm)

Case 1) Suppose a_{11} does not divide some entry directly below. Suppose for simplicity a_{11} does not divide a_{21}. Then

$$a_{21} = qa_{11} + r$$

where $r \neq 0$ and $N(r) < N(a_{11})$. So

$$A = \begin{pmatrix} a_1 1 & \cdots \\ qa_{11} + r & \cdots \\ \vdots & \ddots \end{pmatrix} \quad AR_{12}(-q) \quad \rightarrow$$

$$\begin{pmatrix} a_{11} & \cdots \\ r & \cdots \\ \vdots & \ddots \end{pmatrix} \quad IR_{12} \quad \rightarrow$$

$$\begin{pmatrix} r & \cdots \\ a_{11} & \cdots \\ \vdots & \ddots \end{pmatrix} = B$$

Case 2) Suppose a_{11} does not divide some entry directly to the right. Do as in Case 1) with elementary column operations.

Case 3) Suppose a_{11} divides all entries directly below and to the right. Add multiples of row 1 to the rows and column 1 to the other columns to get a matrix

$$\begin{pmatrix} a_{11} & 0 & 0 & \cdots \\ 0 & a'_{22} & a'_{23} & \cdots \\ 0 & a'_{32} & \ddots & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

If a_{11} divides a'_{ij} call this matrix B and we are done. Suppose a_{11} does not divide a'_{ij} for some $i, j \geq 2$. Perform $AC_{j1}(1)$ to get

$$\begin{pmatrix} a_{11} & 0 & 0 & \cdots \\ a'_{2j} & a'_{22} & a'_{23} & \cdots \\ a'_{3j} & a'_{32} & \ddots & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

and proceed as in Case 1).

□

Theorem 1.69. *Suppose R is a PID. Suppose $A \in M_{n\times n}(R)$. Then A is equivalent to a Smith normal form S.*

Proof. (Where R is a Euclidean Domain). If $A = 0$ we can take $S = 0$. Suppose $A \neq 0$. By performing row and column interchanges we can obtain a matrix whose $(1, 1)$ entry is $\neq 0$. (In practice, move the non-zero entry o fsmallest norm to $(1, 1)$ positon using interchanges). Repeat the Basic Step until option b) in the Basic Step Lemma occurs. We get a new matrix of the form

$$\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & \ddots & \cdots & \cdots \\ \vdots & \vdots & X & \cdots \\ 0 & \vdots & \vdots & \ddots \end{pmatrix}$$

where b_{11} divides all entries of X. Notice that any matrix which is equivalent to X will have all entries divisible by b_{11}. Repeat until a Smith Normal Form is obtained. □

Notes.

a) Suppose R is a PID (not necessarily a Euclidean domain). In the proof of the Theorem one needs a replacement for the Basic Step Lemma using the length function. (See assignment)

b) The nonzero entries $d_1, d_2 \ldots d_r$ appearing in a Smith Normal Form equivalent to A are uniquely determined up to association.

Problem 1.3. *Let* $A = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & 0 \\ 3 & 0 & 4 \end{pmatrix} \in M_{3\times 3}(\mathbb{Z})$. *Find the Smith Normal Form equivalent to* A.

Solution.

$$A \to^{IC_{13}} \begin{pmatrix} 2 & 2 & 3 \\ 0 & 3 & 2 \\ 4 & 0 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 2 & 1 \\ 0 & 3 & 2 \\ 4 & 0 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 2 \\ 2 & 3 & 0 \\ -1 & 0 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 2 \\ 0 & -1 & -4 \\ 0 & 2 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -4 \\ 0 & 2 & 6 \end{pmatrix}$$

$$X = \begin{pmatrix} -1 & -4 \\ 2 & 6 \end{pmatrix} \to \begin{pmatrix} -1 & -4 \\ 0 & -2 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -2 & 0 \end{pmatrix} \text{ So}$$

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

■

Definition 1.70. *Suppose $(a_{ij}) = A \in M_{m\times n}(R)$. Let L be a free module of rank m with basis $\{x_1, \ldots, x_m\}$. Let $y_j = \sum_{i=1}^{m} a_{ij}x_i$ for $j = 1, \ldots, n$ and let $K = Ry_1 + Ry_2 + \cdots + Ry_n$. Let*

$$M = L/K = \{x + K \mid x \in L\} = \{\bar{x} \mid x \in L\}$$

Notice that $\{x_1, \ldots, x_m\}$ generates L. Therefore $\{\bar{x}_1, \ldots, \bar{x}_m\}$ generates M. Notice that $y_j \in K$ for $j = 1, \ldots, n$. Therefore $\bar{y}_j = 0$ for all j. So

$$\sum_{i=1}^{m} a_{ij}\bar{x}_i = 0$$

for $j = 1, \ldots, n$.

In summary. $\{\bar{x}_1, \ldots, \bar{x}_m\}$isa generating set for M and these generators satisfy the relations

$$\sum_{i=1}^{m} a_{ij}\bar{x}_i = 0 \quad j = 1, \ldots, n$$

A is called the *relations matrix* for M. M is also called teh module determined by generators and relations with relations matrix A.

Note. We could have used a different free module L' with different basis $\{x'_1, \ldots, x'_m\}$. The resulting M' is isomorphic to M.

Example 1.71. *Let $R = \mathbb{Z}$ Let M be the module determined by the generators $\{\bar{x}_1, \bar{x}_2, \bar{x}_3\}$ and the relations*

$$3\bar{x}_1 + \bar{x}_2 + 4\bar{x}_3 = 0$$
$$4\bar{x}_1 + 4\bar{x}_2 + 4\bar{x}_3 = 0$$

Formally $M = L/K$ where L is free with basis $\{x_1, x_2, x_3\}$ and K is the submodule of L generated by $3x_1 + x_2 + 4x_3$ and $4x_1 + 4x_2 + 4x_3$. The relations matrix of M is

$$\begin{pmatrix} 3 & 4 \\ 1 & 4 \\ 4 & 4 \end{pmatrix}$$

Proposition 1.72. *Suppose $A, A' \in M_{m\times n}(R)$ and $A \sim A'$. Let M and M' be the modules determined by generators and relations with relations matrices A and A' respectively. Then $M \simeq M'$.*

Proof. We have

$$A = QAP \qquad (1)$$

where Q, P are invertible. ($Q$is $m \times m$ and P is $n \times n$.) Recall that $M = L/K$ where L is a free module of rank M with basis $\{x_1, \ldots, x_m\}$ and K is the submodule of L generated by $\{y_1, \ldots, y_n\}$ where

$$\sum_{i=1}^{m} a_{ij} x_i, \quad j = 1, \ldots, n \qquad (2)$$

Let $A = (a_{ij}), A' = (a'_{ij}), Q = (q_{ij}), Q^{-1} = (\hat{q}_{ij}), P = (p_{ij})$ and let

$$x'_j = \sum_{i=1}^{m} \hat{q}_{ij} x_i, \quad i - 1, \ldots, m \qquad (3)$$

Since Q^{-1} is invertible $\{x'_1, \ldots, x'_m\}$ is a bsis for L. Let

$$y'_j = \sum_{i=1}^{n} p_{ij} y_i \quad j = 1, \ldots, n \qquad (4)$$

Since P is invertibel $\{y'_1, \ldots, y'_n\}$ is a generating set for K (See homework). Then one can show that

$$y_j = \sum_{i=1}^{m} a'_{ij} x'_i, \quad j = 1, \ldots, n$$

Therefore M is the module determined by generators and relations with relations matrix A' and so is M'. Therefore $M \simeq M'$ □

Exercise 1.73. *Suppose M is a module and $x \in M$ where $Ann(x) = \{0\}$. Let $a \in R$. Show that*

$$Rx/Rax \simeq R/(a)$$

Convention $R^0 = \{0\}$ by convention. Therefore R^n is a free module of rank n for all $n \geq 0$.

Theorem 1.74. *Suppose M is a finitely generated module over a PID R which is generated by a set of m elements. Then*

(1) *M is isomorphic to the module determined by generators and relations with relations matrix of the form*

$$S = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & c_1 & & & & \\ & & & & \ddots & & & \\ & & & & & c_\tau & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \end{pmatrix} \qquad (*)$$

where $c_1, \ldots, c_\tau$ are non zero, non unitrs and $c_1 \mid c_2 \mid \cdots \mid c_\tau$.

b) *In that case*

$$M \simeq R/(c_1) \oplus \cdots R/(c_\tau) \oplus R^\rho$$

where $\rho = m -$ *# non zero entries of Smith Normal Form.*

Proof. a) Suppose M is generated by $\{z_1, \ldots, z_m\}$. Let L be a free module with basis $\{x_1, \ldots, x_m\}$. By the universal property of free modules there exists a homomorphism $\phi : L \to M$ so that $\phi(x_i) = z_i$ for $i = 1, \ldots, m$. Since $\{z_1, \ldots, z_m\}$ generates M, ϕ is surjective. Let $K = \ker \phi$. Then by the first isomorphism theorem $M \simeq L/K$. From now on assume that $M = L/K$ where L is free with basis $\{x_1, \ldots, x_m\}$, K is a submodule of a free module L and hence K is free. In particular K is finitely generated. Let $\{y_1, \ldots, y_n\}$ be a generating set for K. Then since $\{x_1, \ldots, x_m\}$ is a basis for L we can write

$$y_j = \sum_{i=1}^{m} a_{ij} x_i \quad j = 1, \ldots, n$$

where $A = (a_{ij}) \in M_{m \times n}(R)$. Therefore M is the module determine dby generators and relations with relations matrix A. Next we know that $A \sim S$ where S is a Smith normal form. We can assume S has the form $(*)$. Hence as we just proved M is isomorphic to the module determined by generators and relations with relations matrix S.

b) Suppose M satisfies the conclusion of a). We can assume that M equals the module determined by S. So $M = L/K$ where L has basis $\{x_1, \ldots, x_m\}$, K has generating set $\{y_1, \ldots, y_n\}$ and the reations matrix is S. We write

$$S = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & c_1 & & & & \\ & & & & \ddots & & & \\ & & & & & c_\tau & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \end{pmatrix} = \begin{pmatrix} d_1 & & & & & & & \\ & \ddots & & & & & & \\ & & \ddots & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & & d_s & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \end{pmatrix}$$

where $d_i = 1$ for $i = 1, \ldots, k$ and $d_{k+i} = c_i$ for $i = 1, \ldots, \tau$. Then

$$\begin{aligned} y_1 &= d_1 x_1 \\ y_2 &= d_2 x_2 \\ &\vdots \\ y_s &= d_s x_s \\ y_j &= 0, \quad j > s \end{aligned}$$

Hence

$$L = Rx_1 \oplus \cdots \oplus Rx_m$$

since $\{x_1, \ldots, x_m\}$ is a basis for L. Also

$$\begin{aligned} K &= Ry_1 + \cdots + Ry_n \\ &= Ry_1 + \cdots + Ry_s \\ &= Rd_1x_1 + \cdots + Rd_sx_s \\ &= Rd_1x_1 + \cdots + Rd_sx_s + R0x_{s+1} + \cdots + R0x_m \end{aligned}$$

From homework we know

$$K = Rd_1x_1 \oplus \cdots \oplus Rd_sx_s \oplus R0x_{s+1} \oplus \cdots \oplus R0x_m$$

Therefore $M = L/K$ (from homework) so

$$\begin{aligned} M &\simeq \left(Rx_1/Rd_1x_1\right) \oplus \cdots \oplus \left(Rx_s/Rd_sx_s\right) \oplus \left(Rx_{s+1}/R0x_{s+1}\right) \oplus \cdots \\ &\simeq R/(d_1) \oplus \cdots \oplus R/(d_s) \oplus \underbrace{R/(0) \oplus \cdots \oplus R/(0)}_{m-s} \\ &\simeq R/(1) \oplus \cdots \oplus R/(1) \oplus R/(c_1) \oplus \cdots \oplus R/(c_\tau) \oplus R^{m-s} \\ &\simeq R/(c_1) \oplus \cdots \oplus R/(c_\tau) \oplus R^{m-s} \end{aligned}$$

□

Example 1.75. *Let M be the module over $\mathbb{Z}$ determined by generators and relations with relations matrix*

$$A = \begin{pmatrix} 3 & 4 \\ 1 & 4 \\ 4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix} = S$$

Then by the theorem part b) we have $M \sim \mathbb{Z}/(4) \oplus \mathbb{Z}^{3-2} = \mathbb{Z}/(4) \oplus \mathbb{Z}$.

Note. Taking a closer look at the example and the proof of the theorem we can assume that $M = L/K$ where M has basis $\{x_1, x_2, x_3\}$ and K has generating set $\{y_1, y_2\}$ where $R = \mathbb{Z}$ and $y_1 = x_1$ and $y_2 = 4x_2$. Thus $L = Rx_1 \oplus Rx_2 \oplus Rx_3$ and $K = Rx_1 \oplus R4x_2 \oplus R0x_3$. From homework we know that

$$M = L/K \simeq \left(Rx_1/Rx_1\right) \oplus \left(Rx_2/R4x_2\right) \oplus \left(Rx_3/R0x_3\right) \simeq \mathbb{Z}/(4) \oplus \mathbb{Z}$$

The uniqueness question. Given finitely generated M are the elements $c_1, \ldots, c_\tau$ and the integer ρ in the theorem uniquely determined (up to associates)?

Exercise 1.76. *Suppose that $M = M_1 \oplus M_2$. Show that $M/M_1 \simeq M_2$.*

Definition 1.77. *Suppose M is a module. Let*

$$Tor(M) = \{x \in M \mid ax = 0 \text{ for some } a \neq 0 \in R\}$$

Then $Tor(M) \leq M$ (exercise). $Tor(M)$ is called the torsion submodule of M.

Exercise 1.78.
a) *If $M = M_1 \oplus \cdots \oplus M_n$ then $Tor(M) = Tor(M_1) \oplus \cdots \oplus Tor(M_n)$*
b) *If M is free then $Tor(M) = \{0\}$.*
c) *If $Ann(M) \neq \{0\}$ then $Tor(M) = M$.*

Exercise 1.79. *Compare and contrast* $Ann(M), Tor(M), aM, Ma$.

Proposition 1.80. *Suppose that*

$$M \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)} \oplus R^\rho$$

where $0 \neq c_1, \ldots, c_\tau \in R$ *and* $\rho \geq 0$. *Then*

$$Tor(M) \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)}$$

and

$${}^{M}\!/_{Tor(M)} \simeq R^\rho.$$

Proof. We know that

$$M = M_1 \oplus \cdots \oplus M_\tau \oplus L$$

where $M_1, \ldots, M_\tau, L \leq M$, $M_i \simeq R/(c_i)$ and $L \simeq R^\rho$. Then

$$Tor(M) = Tor(M_1) \oplus \cdots \oplus Tor(M_\tau) \oplus Tor(L)$$

But $M_i \simeq R/(c_i)$ and so $Ann(M_i) = (c_i) \neq \{0\}$. Therefore $Tor(M_i) = M_i$ for all i. Also L is free so $Tor(L) = \{0\}$. Therefore

$$Tor(M) = M_1 \oplus \cdots \oplus M_\tau$$

So

$${}^{M}\!/_{Tor(M)} \simeq L \simeq R^\rho$$

and

$$Tor(M) \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)}$$

□

Corollary 1.81. *Suppose that*

$$M \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)} \oplus R^\rho$$

and

$$M \simeq {}^{R}\!/_{(d_1)} \oplus \cdots \oplus {}^{R}\!/_{(d_j)} \oplus R^\sigma$$

where $c_1, \ldots, c_\tau, d_1, \ldots, d_j$ *are nonzero elements of* R *and* $\rho, \sigma \geq 0$. *Then*

$${}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)} \simeq {}^{R}\!/_{(d_1)} \oplus \cdots \oplus {}^{R}\!/_{(d_j)}$$

and $\rho = \sigma$.

Proof. We know that

$$Tor(M) \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)}$$

and

$$Tor(M) \simeq {}^{R}\!/_{(d_1)} \oplus \cdots \oplus {}^{R}\!/_{(d_j)}$$

Therefore

$${}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)} \simeq {}^{R}\!/_{(d_1)} \oplus \cdots \oplus {}^{R}\!/_{(d_j)}$$

Also

$${}^{M}\!/_{Tor(M)} \simeq R^\rho$$

and

$$M/Tor(M) \simeq R^\sigma$$

Therefore $R^\rho \simeq R^\sigma$. By a previous theorem $\rho = \sigma$. □

Progress on the uniqueness question: We can assume $\rho = 0$.

Definition 1.82. *Suppose M is a module and $a \in R$. We define*

$$M_a = \{x \in M \mid ax = 0\}$$

and

$$aM = \{ax \mid x \in M\}$$

Then $Ma \leq M$ and $aM \leq M$.

Lemma 1.83. *Suppose M is a module and $a \in R$. If $M \simeq M_1 \oplus \cdots \oplus M_n$ then*

$$M_a \simeq (M_1)_a \oplus \cdots \oplus (M_n)_a$$

and

$$aM \simeq (aM_1) \oplus \cdots \oplus (aM_n)$$

Proof. Exercise. (First for internal then for external direct sum) □

Lemma 1.84. *Suppose that $M \simeq R/(a)$ where a is a nonzero element of R. Then suppose that p is an irreducible element of R (i.e. a non unit such that if $p = ab$ then either a or b is a unit.) Then*

a) *If $p \nmid a$ then $M_p = \{0\}$ and $pM = M = R/(a)$*
b) *If $p \mid a$ then $M_p \simeq R/(p)$ and $pM \simeq R/(a/p)$*

Proof. a) Suppose $p \nmid a$. Then since p is irreducible, p and a are relatively prime. Also $aM = \{0\}$. Hence $paM = \{0\}$. Thus by the homework we have

$$aM = M_p \text{ and } pM = M_a$$

and

$$M = M_a \oplus M_p$$

So

$$M_p = aM = \{0\}$$

Also $M = M_a \oplus M_p = M_a \oplus \{0\} = M_a$ and so

$$pM = M_a = M.$$

b) Suppose $p \mid a$. Then $a = pb$ for some $b \in F$. We can assume $M = R/(a)$. So

$$M = \{r + (a) \mid r \in R\} = \{\bar{r} \mid r \in R\}$$

Then for $r \in R$

$$\begin{aligned} \bar{r} \in M_p &\Leftrightarrow p\bar{r} = 0 \\ &\Leftrightarrow \overline{pr} = 0 \\ &\Leftrightarrow pr \in (a) \\ &\Leftrightarrow a \mid pr \\ &\Leftrightarrow pb \mid pr \\ &\Leftrightarrow r \in (b) \end{aligned}$$

Therefore

$$M_p = {}^{(b)}\!/_{(a)} = {}^{(b)}\!/_{(pb)} \simeq {}^{(1)}\!/_{(p)} \text{ (from homework)}$$
$$\simeq R/_{(p)}$$

Next

$$\begin{aligned} pM &= \{p\bar{r} \mid r \in R\} \\ &= \{\overline{pr} \mid r \in R\} \\ &= (p)/(a) \\ &= (p)/(bp) \\ &= (1)/(b) \\ &= R/(b) = R/(a/p) \end{aligned}$$

□

Lemma 1.85. *Suppose that p is an irreducible element of R. If*

$$\underbrace{R/_{(p)} \oplus \cdots \oplus R/_{(p)}}_{m} \simeq \underbrace{R/_{(p)} \oplus \cdots \oplus R/_{(p)}}_{n}$$

then $m = n$.

Proof. Exercise. □

Shorthand. The shorthand for $M_1 \oplus \cdots \oplus M_n$ is $\bigoplus_{i=1}^{n} M_i$.

Theorem 1.86. *Suppose $c_1, \ldots, c_\tau$ and $c'_1, \ldots, c'_{\tau'}$ are nonzero non units in R so that*

$$c_1 \mid c_2 \mid \cdots \mid c_\tau$$

and

$$c'_1 \mid c'_2 \mid \cdots \mid c'_{\tau'}.$$

Suppose

$$\bigoplus_{i=1}^{\tau} R/_{(c_i)} \simeq \bigoplus_{i=1}^{\tau'} R/_{(c'_i)}$$

Then $\tau = \tau'$ and $c_i \sim c'_i$ for $i = 1, \ldots, \tau$

Proof. (We allow the empty sum on either side which is by definition $\{0\}$). let

$$N = \sum_{i=1}^{\tau} L(c_i)$$

where $L(c_i)$ is the length of c_i. We prove the theorem by induction on N. Suppose $N = 0$. Then $\tau = 0$ (no c_i's). Therefore the left hand side is $\{0\}$ and so the right hand side is $\{0\}$. Therefore $\tau' = 0$ and therefore $\tau = \tau'$. Therefore vacuously $c_i \sim c_i'$ for $i = 1, \ldots, \tau$. Assume $N > 0$ and assume that the theorem holds for all smaller N. Let

$$M = \bigoplus_{i=1}^{\tau} R/(c_i) \simeq \bigoplus_{i=1}^{\tau'} R/(c_i')$$

Let p be any irreducible element of R. Let $k \geq 0$ be chosen so that $c_1, \ldots, c_k$ are not divisible by p adn $c_{k+1}, \ldots, c_\tau$ are divisible by p. Similarly introduce $k' \geq 0$ for the elements $c_1', \ldots, c_{\tau'}'$. Then by the two previous lemmas

$$M_p \simeq \bigoplus_{i=1}^{\tau} \left(R/(c_i)\right)_p = \bigoplus_{i=k+1}^{\tau} R/(p).$$

Similarly

$$M_p \simeq \bigoplus_{i=k'+1}^{\tau'} R/(p).$$

Therefore

$$\bigoplus_{i=k+1}^{\tau} R/(p) = \bigoplus_{i=k'+1}^{\tau'} R/(p).$$

By a previous lemma we have $\tau - k = \tau' - k$. This holds for any choice of p. Suppose p is chosen so that $p \mid c_1$. Therefore $p \mid c_i$ for all i. Then $k = 0$. Thus $\tau = \tau' - k$. Therefore $\tau \leq \tau'$. Finally, once and for all chose p such that $p \mid c_1$. Exactly as above we get $k = 0$ and so $\tau - 0 = \tau - k'$ and so $k' = 0$ and we have $p \mid c_i$ and $p \mid c_i'$ for all $i = 1, \ldots, \tau$. Recall that

$$M \simeq \bigoplus_{i=1}^{\tau} R/(c_i) \text{ and } \bigoplus_{i=1}^{\tau} R/(c_i')$$

Thus

$$pM \simeq \bigoplus_{i=1}^{\tau} p\left(R/(c_i)\right) \simeq \bigoplus_{i=1}^{\tau} R/(c_i/p)$$

But $c_i/p \sim 1$ for $i = 1, \cdots, \ell$. Therefore

$$pM \simeq \bigoplus_{i=\ell+1}^{\tau} R/(c_i/p)$$

Similarly

$$pM \simeq \bigoplus_{i=\ell'+1}^{\tau} R/(c_i'/p)$$

Thus

$$\bigoplus_{i=\ell+1}^{\tau} R/(c_i/p) \simeq \bigoplus_{i=\ell'+1}^{\tau} R/(c_i'/p)$$

By the induction hypothesis $\tau - \ell = \tau - \ell'$ and so $\ell = \ell'$ and $c_i/p \sim c_i'/p$ for $i = \ell+1, \ldots, \tau$ and therefore $c_i \sim c_i'$ for $i = \ell+1, \ldots, \tau$. Also $c_i \sim p \sim c_i'$ for $i = 1, \ldots, \ell$. Thus $c_i \sim c_i'$ for $i = 1, \ldots, \tau$ □

Theorem 1.87 (Fundamental Theorem for finitely generated modules over a PID)**.** *Suppose M is a finitely generated module over a PID R. Then there exists nonzero nonunit elements $c_1, \ldots, c_\tau$ such that $c_1 \mid c_2 \mid \cdots \mid c_\tau$ and an integer $\rho \geq 0$ such that*

$$M \simeq R/(c_1) \oplus \cdots \oplus R/(c_\tau) \oplus R^\rho$$

Moreover the elements $c_1, \ldots, c_\tau$ are uniquely determined in order up to association and ρ is unique.

Proof. We have proved the first statement. For uniqueness suppose

$$M = \bigoplus_{i=1}^{\tau} R/(c_i) \oplus R^\rho \simeq \bigoplus_{i=1}^{\tau'} R/(c_i') \oplus R^{\rho'}$$

where c_i, ρ, c_i', ρ' are as above. We proved

$$\bigoplus_{i=1}^{\tau} R/(c_i) \simeq \bigoplus_{i=1}^{\tau'} R/(c_i')$$

and $\rho = \rho'$. By the uniqueness theorem $\tau = \tau'$ and $c_i \sim c_i'$ for $i = 1, \ldots, \tau$ □

Definition 1.88. *Let $M, c_1, \ldots, c_\tau, \rho$ be as in the fundamental theorem. The elements $c_1, \ldots, c_\tau$ in order are called the invariant factors of M. The integer ρ is called the free rank of M.*

Note. If M is a finitely generated $\mathbb{Z}$ module (i.e. a finitely generated abelian group) then the invariant factors $c_1, \ldots, c_\tau$ are always chosen positive, in which case they are unique.

Problem 1.4. *Let M be the $\mathbb{Z}$ module determined by generators and relations with relations matrix*

$$A = \begin{pmatrix} 2 & 4 & 6 \\ 6 & 24 & 24 \\ 12 & 18 & 30 \end{pmatrix}$$

Find the invariant factors and the free rank of M.

Solution.
$A \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}$ hence $M \simeq Z/(2) \oplus Z/(6) \oplus Z/(6) \oplus \mathbb{Z}^{3-3} \simeq Z/(2) \oplus Z/(6) \oplus Z/(6)$. Thus the invariant factors are $2, 2, 6$ and the free rank is 0. ■

Definition 1.89. *Suppose M is a module. We say that M is a* torsion module *is $Tor(M) = M$.*

Proposition 1.90. *Suppose M is a finitely generated R module. Then the following are equivalent:*

a) *M is a torsion module.*
b) *Free rank of M is 0.*
c) *$Ann(M) \neq \{0\}$*

Moreover if M is a torsion module then

$$M \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)}$$

where $c_1, \ldots, c_\tau$ are the invariant factors of M and $Ann(M) = (c_\tau)$.

Proof. By the fundamental theorem we have

$$M \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)} \oplus R^\rho$$

where $c_1, \ldots, c_\tau$ are the invariant factors of M and ρ is the free rank of M.

"a) $\Rightarrow$ b)" Suppose $Tor(M) = M$. We saw that $M/Tor(M) \simeq R^\rho$ so $R^\rho = \{0\}$ and so $\rho = 0$.

"b) $\Rightarrow$ c)" Suppose M has free rank 0, i.e. $\rho = 0$. Then $M \simeq {}^{R}\!/_{(c_1)} \oplus \cdots \oplus {}^{R}\!/_{(c_\tau)}$ thus

$$Ann(M) = \bigcap_{i=1}^{\tau} Ann(R/(c_i)) = \bigcap_{i=1}^{\tau} (c_i) = (c_\tau)$$

since $c_1 \mid c_2 \mid \cdots \mid c_\tau$.

" c) $\Rightarrow$ a)" Suppose $Ann(M) \neq \{0\}$. Then we may chose $a \in Ann(M) \setminus \{0\}$. Then $ax = 0$ for all $x \in M$. Hence $Tor(M) = M$.

□

Example 1.91. *For $R = \mathbb{Z}$, finitely generated torsion $\mathbb{Z}$-modules are precisely the finite abelian groups. Any such group is isomorphic to ${}^{\mathbb{Z}}\!/_{(c_1)} \oplus \cdots \oplus {}^{\mathbb{Z}}\!/_{(c_\tau)}$ where $c_i \geq 2$ and $c_1 \mid c_2 \mid \cdots \mid c_\tau$.*

Proposition 1.92. *Suppose a, b are nonzero relatively prime elements of R (i.e. $gcd(a, b) = 1$). Then*

$${}^{R}\!/_{(ab)} \simeq {}^{R}\!/_{(a)} \oplus {}^{R}\!/_{(b)}.$$

Proof. Define

$$\phi : R \to {}^{R}\!/_{(a)} \oplus {}^{R}\!/_{(b)}$$

by $r \mapsto (\bar{r}, \bar{r})$. Check that ϕ is a homomorphism and is surjective (using $gcd(a, b) = 1$) and $\ker \phi = (ab)$. □

Corollary 1.93. *Suppose $b_1, \ldots, b_k \neq 0$ are pairwise coprime elements of R. Then*

$${}^{R}\!/_{(b_1 b_2 \cdots b_k)} \simeq {}^{R}\!/_{(b_1)} \oplus \cdots \oplus {}^{R}\!/_{(b_k)}.$$

Example 1.94. *Let $R = \mathbb{Z}$.*

$${}^{R}\!/_{(60)} = {}^{\mathbb{Z}}\!/_{(60)} \simeq {}^{\mathbb{Z}}\!/_{(2^2)} \oplus {}^{R}\!/_{(3)} \oplus {}^{\mathbb{Z}}\!/_{(5)}.$$

Theorem 1.95 (Primary Decomposition Theorem)**.** *Suppose M is a finitely generated torsion module over a PID R. Then there exists irreducible elements $p_1, \ldots, p_k \in R$ (not necessarily distinct) and positive integers $e_1, \ldots, e_k$ such that*

$$M \simeq {}^{R}\!/_{(p_1^{e_1})} \oplus \cdots \oplus {}^{R}\!/_{(p_k^{e_k})} \qquad (\#)$$

Moreover the irreducible elements and the positive integers are uniquely determined up to order of summands.

Proof. Standard. □

Terminology. $(\#)$ is called the primary decomposition of M. The sequence $p_1^{e_1}, \ldots, p_k^{e_k}$ is called the sequence of elementary divisors of M.

Example 1.96. *Consider the finite abelian group with invariant factors $10, 60, 300$. So $M \simeq \mathbb{Z}/(10) \oplus \mathbb{Z}/(60) \oplus \mathbb{Z}/(300)$. Now $10 = 2 \cdot 5,\ 60 = 2^2 \cdot 3 \cdot 5,\ 300 = 2^2 \cdot 3 \cdot 5^2$ so*

$$\mathbb{Z}/_{(10)} \simeq \mathbb{Z}/_{(2)} \oplus \mathbb{Z}/_{(5)},$$
$$\mathbb{Z}/_{(60)} \simeq \mathbb{Z}/_{(2^2)} \oplus \mathbb{Z}/_{(3)} \oplus \mathbb{Z}/_{(5)},$$
$$\mathbb{Z}/_{(300)} \simeq \mathbb{Z}/_{(2^2)} \oplus \mathbb{Z}/_{(3)} \oplus \mathbb{Z}/_{(5^2)}$$

Hence

$$M \simeq \mathbb{Z}/_{(2)} \oplus \mathbb{Z}/_{(2^2)} \oplus \mathbb{Z}/_{(2^2)} \oplus \mathbb{Z}/_{(3)} \oplus \mathbb{Z}/_{(3)} \oplus \mathbb{Z}/_{(5)} \oplus \mathbb{Z}/_{(5)} \oplus \mathbb{Z}/_{(5^2)}$$

The elementary divisors of M are

$$2, 2^2, 2^2, 3, 3, 5, 5, 5^2$$

Note. The invariant factors of a finitely generated torsion module can be recovered from the elementary divisors (and vice-versa). If M is a finite abelian group the order of M equals the product of the invariant factors which equals the product of elementary divisors.

Example 1.97. *Suppose M is the finite abelian group with elementary divisors*

$$3, 3, 3^2, 5^2, 5^3, 7, 7^2, 7^3$$

The invariant factors are (in reverse order)

$$3^2 \cdot 5^3 \cdot 7^3, 3 \cdot 5^2 \cdot 7^2, 3 \cdot 7$$

Recall. The order of a finite abelian group is the product of its elementary divisors.

Problem 1.5. *Classify all abelian groups of order 400 up to isomorphism.*

Solution. $400 = 2^4 \cdot 5^2$. 5^2 decomposes as 5^2 or $5, 5$. The sequence of powers of 2 whose product is 2^4 is given in the following list

2^4	4	
$2^3, 2$	3 1	
$2^2, 2^2$	2 2	partitions of 4
$2^2, 2, 2$	2 1 1	
$2, 2, 2, 2$	1 1 1 1	

■

Thus the abelian groups of over 400 up to isomorphism are given by $P \oplus Q$ where

$$\begin{aligned} P \ &\simeq \ {}^{\mathbb{Z}}\!/_{(16)} \text{ or } {}^{\mathbb{Z}}\!/_{(8)} \oplus {}^{\mathbb{Z}}\!/_{(2)} \text{ or } {}^{\mathbb{Z}}\!/_{(4)} \oplus {}^{\mathbb{Z}}\!/_{(4)} \text{ or } {}^{\mathbb{Z}}\!/_{(4)} \oplus {}^{\mathbb{Z}}\!/_{(2)} \oplus {}^{\mathbb{Z}}\!/_{(2)}, \\ &\quad \text{or } {}^{\mathbb{Z}}\!/_{(2)} \oplus {}^{\mathbb{Z}}\!/_{(2)} \oplus {}^{\mathbb{Z}}\!/_{(2)} \oplus {}^{\mathbb{Z}}\!/_{(2)} \end{aligned}$$

and

$$Q \simeq {}^{\mathbb{Z}}\!/_{(25)} \text{ or } {}^{\mathbb{Z}}\!/_{(5)} \oplus {}^{\mathbb{Z}}\!/_{(5)}.$$

Therefore there are 10 abelian groups of order 400 up to isomorphism.

Example 1.98. *By considering the partitions of* 5 *we see there are* 7 *abelian groups of order* p^5 *up to isomorphism for any prime* p*. There are* 51 *groups of order* 32*,* 11 *abelian groups of order* 64*.*

Assume.

a) F is a field and $R = F[\lambda]$ the ring of polynomials over R in the indeterminant λ. R is a Euclidean domain with norm N defined by $N(a(\lambda)) = deg(a(\lambda))$ for $0 \neq a(\lambda) \in R$ hence R is a PID.

b) Assume T is a linear operator on V a finite dimensional vector space over R. This means $T : V \to V$ is a homomorphism of vector spaces over F. We use T to give V the structure of an R module by defining

$$f(\lambda)v = f(T)v$$

for $f(\lambda) \in R$ and $v \in V$. The R module V is called the R module associated to T.

Proposition 1.99. *V is a finitely generated torsion R-module.*

Proof. Any finite generating set for V over F is also a finite generating set for V over R. Hence V is finitely generated over R. To show that V is a torsion R module we must show that $Tor(V) = V$. Let $x \in V$. Let $dim_F(V) = n$. Consider

$$\{x, \lambda x, \lambda^2 x, \ldots, \lambda^n x\}$$

This set has $n+1$ elements and therefore is dependent over F. Hence there exist $a_0, a_1, \ldots, a_n \in F$ not all 0 such that

$$a_0 x + a_1 \lambda x + \cdots + a_n \lambda^n x = 0$$

Therefore

$$(a_0 + a_1 \lambda + \cdots + a_n \lambda^n)x = 0$$

But $a_0 + a_1\lambda + \cdots + a_n\lambda^n$ is a nonzero element of R. Therefore $x \in Tor(V)$ and so $Tor(V) = V$ and so V is a torsion R module. □

Theorem 1.100. *Suppose V is the module associated with a linear operator T. Thus*

$$V \simeq {}^{R}\!/_{(f_1(\lambda))} \oplus \cdots \oplus {}^{R}\!/_{(f_\tau(\lambda))}$$

where $f_1(\lambda), \ldots, f_\tau(\lambda)$ are monic polynomials over F of degree ≥ 1 so that $f_1(\lambda) \mid f_2(\lambda) \mid \cdots \mid f_\tau(\lambda)$ Moreover the polynomials $f_1(\lambda), \ldots, f_\tau(\lambda)$ are uniquely determined. Hence

$$V = V_1 \oplus \cdots \oplus V_\tau$$

where $V_1, \ldots, V_\tau$ are R submodules of V so that V_i is cyclic with annihilator $(f_i(\lambda))$ for $i = 1, \ldots, \tau$.

Notes.

a) The polynomials $f_1(\lambda), \ldots, f_\tau(\lambda)$ are called the invariant factors of T.
b) V_i is a submodule of V. We saw on a homework assignment that this means that the V_i is a T-invariant subspace of V. Hence we may restrict T to a linear operator T_i on V_i defined by $T_i x = Tx$. for $x \in V_i$. Then the R module V_i is the R module associated to T_i.

Conclusion. We are reduced to analyzing the case when the R module associated to T is cyclic with nonzero annihilator.

Note. The theorem follows from the proposition and the fundamental theorem.

Definition 1.101. *Suppose $f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$ is a monic polynomial over F of degree $n \geq 1$. We define the companion matrix of $f(\lambda)$ to be the $n \times n$ matrix*

$$C_{f(\lambda)} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-1} \\ 0 & 0 & \cdots & 0 & 1 & -a_n \end{pmatrix}$$

Recall. If $A \in M_{n\times n}(F)$, the characteristic polynomial of A is $\chi_A(\lambda) = \det(\lambda I - A)$. If $T : V \to V$ is a linear operator and T has matrix A relative to some basis β for V, we define the characteristic polynomial of T to be

$$\chi_T(\lambda) = \chi_A(\lambda)$$

Exercise 1.102. *Let $C = C_{f(\lambda)}$. Show that $\chi_C(\lambda) = f(\lambda)$.*

Proposition 1.103. *Suppose that T is a linear operator on V so that the associated R module V is cyclic with annihilator $(f(\lambda))$ where $f(\lambda)$ is a monic polynomial of degree ≥ 1. then V has a basis β so that*

$$[T]_\beta = C_{f(\lambda)}$$

Proof. By assumption there exists $x \in V$ so that $V = Rx$ and $Ann(x) = Ann(V) = (f(\lambda))$. Let $n = deg(f(\lambda))$ so

$$f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$$

Since $Ann(x) = (f(\lambda))$ it follows that $f(\lambda)$ is the monic polynomial of smallest degree so that $f(\lambda)x = 0$. Hence

$$(\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0)x = 0 \qquad (1)$$

and no polynomial of smaller degree does this. Thus the set

$$\beta = \{x, \lambda x, \ldots, \lambda^{n-1}x\}$$

is independent over F. We next see that β spans V over F since $V = Rx$, every vector in V is a linear combination of vectors of the form $\lambda^n x$ where $m \geq 0$. But

$$\lambda^m x = F - \text{linear combination of } \beta$$

for $m \geq n$ (**Exercise:** use (1) and induction on m). Therefore every x in V is an F-linear combination of β. So β is a basis for V. Let $x_1 = x, x_2 = \lambda x, \ldots$. We must calculate $[T]_\beta$. Now

$$\begin{aligned} T(x_1) &= \lambda x_1 = \lambda x = x_2 \\ T(x_2) &= x_3 \\ &\vdots \\ T(x_{n-1}) &= x_n \\ T(x_n) &= \lambda x_n = \lambda^n x = -a_0 x_1 - a_1 x_2 \cdots - a_{n-1} x_n \end{aligned}$$

So

$$[T]_\beta = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-1} \\ 0 & 0 & \cdots & 0 & 1 & -a_n \end{pmatrix} = C_{f(\lambda)}$$

□

Definition 1.104. *Suppose $f_1(\lambda), \ldots, f_\tau(\lambda)$ are monic polynomials of degree ≥ 1 over F so that*

$$f_1(\lambda) \mid f_2(\lambda) \mid \cdots \mid f_\tau(\lambda)$$

The matrix

$$C = \begin{pmatrix} C_{f_1(\lambda)} & 0 & \cdots & 0 \\ 0 & C_{f_2(\lambda)} & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & C_{f_\tau(\lambda)} \end{pmatrix}$$

is the rational canonical form (RCF) *determined by $f_1(\lambda), f_2(\lambda), \ldots, f_\tau(\lambda)$.*

Note. If C is as above then $\chi_C(\lambda) = f_1(\lambda), \ldots, f_\tau(\lambda)$

Theorem 1.105 (RCF theorem)**.** *If T isa linear operator on V with invariant factors $f_1(\lambda), \cdots, f_\tau(\lambda)$ then there exists a basis β for V so that $[T]_\beta$ is the RCF determined by $f_1(\lambda), \ldots, f_\tau(\lambda)$. Conversely if V has a basis β so that $[T]_\beta$ is the RCF determined by $f_1(\lambda), \ldots, f_\tau(\lambda)$ then T has invariant factors $f_1(\lambda), \ldots, f_\tau(\lambda)$.*

Proof. The first statement follows from the last theorem and the last proposition. The converse is an exercise. □

Corollary 1.106. *Let T be as in the theorem. Then*

$$\chi_T(\lambda) = f_1(\lambda) \cdots f_\tau(\lambda)$$

where $f_1(\lambda), \ldots, f_\tau(\lambda)$ are the invariant factors of T.

Corollary 1.107. *If $A \in M_{n \times n}(F)$ then A is similar to a unique RCF.*

Example 1.108. *Suppose $F = \mathbb{Q}$. Suppose that T has invariant factors*

$$f_1(\lambda) = (\lambda - 1)(\lambda^2 + 1),\ f_2(\lambda) = (\lambda - 1)^2(\lambda + 1)(\lambda^2 + 1)$$

Note that $f_1(\lambda) = \lambda^3 - \lambda^2 + \lambda - 1$ and $f_2(\lambda) = \lambda^5 - \lambda^4 - \lambda + 1$. Then

$$[T]_\beta = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

where

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

and

$$\chi_T(\lambda) = (\lambda - 1)^3(\lambda^2 + 1)^2(\lambda + 1)$$

Definition 1.109. *Suppose T is a linear operator on V. Let $f_1(\lambda), \ldots, f_k(\lambda)$ be the invariant factors of T. Define the minimal polynomial of T to be $f_k(\lambda)$. It is denoted by $\mu_T(\lambda)$.*

Proposition 1.110 (About the minimal polynomial)**.** *Suppose T is a a linear operator on V.*

a) *If $f(\lambda) \in F[\lambda]$ then $f(T) = 0 \Leftrightarrow \mu_T(\lambda) \mid f(\lambda)$. So $\mu_T(\lambda)$ is the monic polynomial over F of smallest degree ≥ 1 so that $\mu_T(T) = 0$.*
b) *$\mu_T(\lambda) \mid \chi_T(\lambda)$. Moreover $\mu_T(\lambda)$ and $\chi_T(\lambda)$ have the same irreducible factors over F.*
c) *(Cayley-Hamilton Theorem) $\chi_T(T) = 0$*

Proof. Let $f_1(\lambda), \ldots, f_k(\lambda)$ be the invariant factors of T. Then

$$\mu_T(\lambda) = f_k(\lambda) \quad (1)$$

and

$$\chi_T(\lambda) = f_1(\lambda) \cdots f_k(\lambda) \quad (2)$$

a) We know that $(f_k(\lambda))$ is the annihilator of the R module V. Therefore $\mu_T(\lambda)$ is the annihilator of the R module V. Hence if $f(\lambda) \in F[\lambda]$ we have

$$\begin{aligned} \mu_T(\lambda) \mid f(\lambda) &\Leftrightarrow f(\lambda) \in (\mu_T(\lambda)) \\ &\Leftrightarrow f(\lambda) \in Ann(V) \\ &\Leftrightarrow f(\lambda)v = 0\ \forall\ v \in V \\ &\Leftrightarrow f(T)v = 0\ \forall\ v \in V \\ &\Leftrightarrow f(T) = 0 \end{aligned}$$

b) By (1) and (2) we have $\mu_T(\lambda) \mid \chi_T(\lambda)$ Therefore any irreducible factor of $\mu_T(\lambda)$ is an irreducible factor of $\chi_T(\lambda)$. Conversely, suppose that $p(\lambda)$ is an irreducible factor of $\chi_T(\lambda)$. Therefore by (2) we have $p(\lambda) \mid f_i(\lambda)$ for some i but $f_i(\lambda) \mid f_k(\lambda)$ so $p(\lambda) \mid f_k(\lambda)$ so $p(\lambda) \mid \mu_T(\lambda)$.
c) By (b) $\mu_T(\lambda) \mid \chi_T(\lambda)$. By (a) $\chi_T(T) = 0$

□

Definition 1.111. *Suppose $A \in M_{n\times n}(F)$. Choose any linear operator T so that A represents T relative to some basis. The* invariant factors *of A are defined to be the invariant factors of T. (***Exercise.** *This notion is well defined.) We define the minimal polynomial of A to be the minimal polynomial of T. We denote it $\mu_A(\lambda)$ so by definition $\mu_A(\lambda) = \mu_T(\lambda)$. Also by definition of $\chi_T(\lambda)$ we have $\chi_T(\lambda) = \chi_A(\lambda)$*

Note. Suppose that $A \in M_{n\times n}(F)$ with invariant factors $f_1(\lambda), \ldots, f_k(\lambda)$ then $\mu_A(\lambda) = f_k(\lambda)$ and $\chi_A(\lambda) = f_1(\lambda)\cdots f_k(\lambda)$. Also A is similar to the RCF determined by $f_1(\lambda), \ldots, f_k(\lambda)$.

$$\begin{pmatrix} C_{f_1(\lambda)} & 0 & \cdots & 0 \\ 0 & C_{f_2(\lambda)} & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & C_{f_\tau(\lambda)} \end{pmatrix}$$

Conversely if A is similar to this RCF then $f_1(\lambda), \ldots, f_k(\lambda)$ are the invariant factors of A. Finally the proposition about the minimal polynomial holds for A.

Problem 1.6. *Let* $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ -1 & 0 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{Q})$.

a) *Find the invariant factors, the minimal polynomial and the characteristic polynomial of A*

b) *Find the rational canonical form RCF which is similar to A*

Solution.

$$\chi_A(\lambda) = \det(\lambda I - A) = \det \begin{pmatrix} \lambda - 1 & 0 & 0 \\ 0 & \lambda - 2 & -1 \\ 1 & 0 & \lambda - 2 \end{pmatrix} = (\lambda - 1)(\lambda - 2)^2$$

So the irreducible factors of $\chi_A(\lambda)$ are $(\lambda - 1), (\lambda - 2)$. So the irreducible factors of $\mu_A(\lambda)$ are $(\lambda - 1), (\lambda - 2)$. Also $\mu_A(\lambda) \mid \chi_A(\lambda)$. So the possibilities for $\mu_A(\lambda)$ are $(\lambda - 1)(\lambda - 2)$ or $(\lambda - 1)(\lambda - 2)^2$ (i.e $\lambda^2 - 3\lambda + 2$ or $\lambda^3 - 5\lambda^2 + 8\lambda - 4$. Now $A^2 - 3A + 2I = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 8 \\ -6 & 0 & 8 \end{pmatrix} \neq 0$ which means $\mu_A(\lambda) = \lambda^3 - 5\lambda^2 + 8\lambda - 4$ and there is only one invariant factor, namely $(\lambda - 1)(\lambda - 2)^2$. Therefore A is similar to

$$C_{\lambda^3 - 5\lambda^2 + 8\lambda - 4} = \begin{pmatrix} 0 & 0 & 4 \\ 1 & 0 & -8 \\ 0 & 1 & 5 \end{pmatrix}$$

■

Note. Suppose in this problem we had found $A^2 - 3A + 2I = 0$. Then we would have $\mu_A(\lambda) = (\lambda - 1)(\lambda - 2)$ and so the invariant factors would have been $(\lambda - 2), (\lambda - 1)(\lambda - 2)$ and A would have been similar to

$$\begin{pmatrix} c_{\lambda - 2} & 0 \\ 0 & c_{(\lambda - 1)(\lambda - 2)} \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$$

Proposition 1.112. *Suppose T is a linear operator. Suppose that $A = [T]_\beta$ for some basis β of V over F. Then $V \simeq R$-module determined by generators and relations with relations matrix $(\lambda I - A)$*

Proof. Exercise. (Handout) □

Finding the invariant factors. Suppose T is a linear operator with $A = [T]_\beta$ for some β. We can do the following

$$(\lambda I - A) \to \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1(\lambda) & & \\ & & & & \ddots & \\ & & & & & f_k(\lambda) \end{pmatrix}$$

where $f_1(\lambda), \ldots, f_k(\lambda)$ are monic polynomials of degree ≥ 1 so that $f_1(\lambda) \mid \cdots \mid f_k(\lambda)$. (There are no zeros on the diagonal since V is a torsion R-module. i.e. free rank of V is 0). Therefore

$$V \simeq {}^{R}\!/_{(f_1(\lambda))} \oplus \cdots \oplus {}^{R}\!/_{(f_k(\lambda))}$$

Hence $f_1(\lambda), \ldots, f_k(\lambda)$ are the invariant factors of T (or A).

Example 1.113. *Let* $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ -1 & 0 & 2 \end{pmatrix}$ *then*

$$\lambda I - A = \begin{pmatrix} \lambda - 1 & 0 & 0 \\ 0 & \lambda - 2 & -1 \\ 1 & 0 & \lambda - 2 \end{pmatrix} \text{ sim } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (\lambda - 1)(\lambda - 2)^2 \end{pmatrix}$$

A has invariant factors $(\lambda - 1)(\lambda - 2)^2$

Definition 1.114. *Suppose $\alpha \in F$. The $n \times n$* Jordan block*with eigenvalue α is the matrix*

$$J = J_n(\alpha) = \begin{pmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 1 & \alpha & 0 & \cdots & 0 \\ & \ddots & \ddots & \cdots & \vdots \\ & & 1 & \alpha & 0 \\ & & & 1 & \alpha \end{pmatrix}$$

Note that $\chi_J(\lambda) = (\lambda - \alpha)^n$

Example 1.115. *Let $F = \mathbb{C}$, $\alpha = 7$, $n = 3$. Then* $J_3(7) = \begin{pmatrix} 7 & 0 & 0 \\ 1 & 7 & 0 \\ 0 & 1 & 7 \end{pmatrix}$.

Proposition 1.116. *Suppose T is a linear operator on V so that the corresponding R module V is cyclic with annihilator $((\lambda - \alpha)^n)$. Then there exists a basis β for V such that $[T]_\beta = J_n(\alpha)$.*

Proof. We are given that $V = Rx$ for some $x \in V$ and $Ann(x) = ((\lambda - \alpha)^n)$. We saw when proving RCF that then $x, \lambda x, \lambda^2 x, \ldots, \lambda^{n-1}x$ is a basis for V over F. It follows that

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

is also a basis for V over F. (**Exercise.** Show that it is independent over F). Let $x_1 = x, x_2 = (\lambda - \alpha)x, \ldots$. Let $\beta = \{x_1, \ldots, x_n\}$ a basis for V over F. Notice that

$$\begin{aligned} (\lambda - \alpha)x_1 &= x_2 \\ (\lambda - \alpha)x_2 &= x_3 \\ &\vdots \\ (\lambda - \alpha)x_n &= 0 \text{ since } Ann(x) = ((\lambda - \alpha)^n) \end{aligned}$$

Hence

$$\begin{aligned} \lambda x_1 &= \alpha x_1 + x_2 \\ \lambda x_2 &= \alpha x_2 + x_3 \\ &\vdots \\ \lambda x_n &= \alpha x_n \end{aligned}$$

Therefore

$$\begin{aligned} Tx_1 &= \alpha x_1 + x_2 \\ Tx_2 &= \alpha x_2 + x_3 \\ &\vdots \\ Tx_n &= \alpha x_n \end{aligned}$$

So

$$[T]_\beta = \begin{pmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 1 & \alpha & 0 & \cdots & 0 \\ & \ddots & \ddots & \cdots & \vdots \\ & & 1 & \alpha & 0 \\ & & & 1 & \alpha \end{pmatrix} = J_n(\alpha)$$

□

Assume. $F = \mathbb{C}$. Any monic irreducible polynomial over $\mathbb{C}$ has the form $(\lambda - \alpha)$ where $\alpha \in \mathbb{C}$ by the Fundamental Theorem of Algebra.

Definition 1.117. *Suppose T is a linear operator on V over $F = \mathbb{C}$. Regard V as an R module. The elementary divisors of this R module have the form $(\lambda - \alpha_1)^{n_1}, \ldots, (\lambda - \alpha_\ell)^{n_\ell}$ where $\alpha_1, \ldots, \alpha_\ell \in F$, $n_1, \ldots, n_\ell \geq 1$. These polynomials are called the elementary divisors of T. If $A = [T]_\beta$ for some β these polynomials are called the elementary divisors of A. Note that the product of these polynomials is $\chi_T(\lambda)$ or $\chi_A(\lambda)$.*

Theorem 1.118 (Jordan Canonical Form Theorem)**.** *Suppose T is a linear operator on a vector space V over $F = \mathbb{C}$. If*

$$(\lambda - \alpha_1)^{n_1}, \ldots, (\lambda - \alpha_\ell)^{n_\ell} \qquad (1)$$

are the elementary divisors of T then there exists a basis β for V such that

$$[T]_\beta = \begin{pmatrix} J_{n_1}(\alpha_1) & & \\ & \ddots & \\ & & J_{n_\ell}(\alpha_\ell) \end{pmatrix} \qquad (2)$$

Conversely if there is a basis β so that (2) holds then the elementary divisors of T are given by (1).

Proof. The first statement follows from the primary decomposition theorem and the previous proposition. The second proposition is an exercise. □

Definition 1.119. *A matrix of the form (2) is called the Jordan canonical form (JCF).*

Corollary 1.120. *Suppose $A \in M_{n\times n}(\mathbb{C})$. Then A is similar to a JCF matrix which is unique up to the order of the Jordan blocks. In fact if the elementary divisors of A are given by (1) then A is similar to the JCF in (2).*

Problem 1.7. *Let*

$$A = \begin{pmatrix} 26 & 23 & 17 & -10 & -26 & -6 & 9 & 15 & -2 \\ -51 & -39 & -33 & 14 & 47 & 9 & -21 & -24 & 2 \\ 84 & 67 & 57 & -25 & -79 & -16 & 37 & 41 & -4 \\ 37 & 29 & 25 & -10 & -34 & -7 & 17 & 17 & -2 \\ 9 & 11 & 7 & -6 & -10 & -3 & 3 & 7 & -2 \\ -126 & -103 & -85 & 40 & 120 & 26 & -53 & -63 & 6 \\ -34 & -29 & -23 & 12 & 34 & 8 & -13 & -19 & 2 \\ -67 & -53 & -45 & 20 & 64 & 13 & -29 & -33 & 2 \\ -71 & -56 & -48 & 21 & 66 & 13 & -30 & -35 & 44 \end{pmatrix}$$

a) *Find the invariant factors of A.*
b) *Find the elementary divisors of A*
c) *Find the JCF which is similar to A*

Solution. Use a computer program to do this. The invariant factors are $\lambda - 2, \lambda^3 - 2\lambda^2, \lambda^5 - 4\lambda^4 + 4\lambda^3$. The elementary divisors are $(\lambda-2), (\lambda-2), (\lambda-2)^2, \lambda^2, \lambda^3$. The JCF is

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

■

Exercise 1.121. *Suppose A is an $n \times n$ matrix. Show that A is diagonalizable (i.e. similar to a diagonal matrix) $\Leftrightarrow \mu_A(\lambda) = (\lambda - \alpha_1) \cdots (\lambda - \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are distinct complex numbers.*