IV.C. Modules over a PID

Let R be a principal ideal domain, and M an R-module. (Since R is commutative, left vs. right is immaterial.) We begin with a simple statement about generators and relations (which indeed has nothing to do with R being a PID).

IV.C.1. PROPOSITION. *M is finitely generated $\iff$ $M \cong R^n/K$ (with K an R-submodule of R^n).*

PROOF. ($\Longleftarrow$): $M = R\langle \bar{e}_1, \ldots, \bar{e}_n \rangle$.
($\Longrightarrow$): If $M = R\langle x_1, \ldots, x_n \rangle$ (i.e. M is f.g.), then define $\eta \colon R^n \twoheadrightarrow M$ by $\sum_i r_i \mathbf{e}_i \mapsto \sum_i r_i x_i$; by the Fundamental Thm., $M \cong R^n / \ker(\eta)$. $\square$

The following generalizes II.K.4 ($\mathbb{Z}$-module case) and a standard linear algebra result ($\mathbb{F}$-module case).

IV.C.2. THEOREM. *Any submodule K of R^n is isomorphic to R^{n_0}, for some $n_0 \leq n$.*

PROOF. The result holds trivially for $n = 0$.

Assume it "for $n-1$" and consider the projection $\pi \colon R^n \twoheadrightarrow R$ sending $\sum_i r_i \mathbf{e}_i \mapsto r_1$, with $\ker(\pi) \cong R^{n-1}$.

If $\pi(K) = \{0\}$ then we're done by induction. (Why?)

Otherwise, as an R-submodule of R, $\pi(K)$ is an ideal — in a PID. So we have $\pi(K) = (\mathfrak{r})$ for some $\mathfrak{r} \in R \backslash \{0\}$, and moreover this $\mathfrak{r} = \pi(\kappa)$ for some $\kappa \in K$. Observe that $\text{ann}(\kappa) = \{0\}$ since $\kappa \in R^n$ and R is a domain.

Now any $k \in K$ can be written in the form

$$k = (k - \tfrac{\pi(k)}{\mathfrak{r}}\kappa) + \tfrac{\pi(k)}{\mathfrak{r}}\kappa \in (\ker(\pi) \cap K) + R\kappa,$$

since $\pi(k - \frac{\pi(k)}{\mathfrak{r}}\kappa) = \pi(k) - \frac{\pi(k)}{\mathfrak{r}}\mathfrak{r} = 0$. Moreover, we have that $(\ker(\pi) \cap K) \cap R\kappa = \{0\}$, as $r\kappa \in \ker(\pi) \implies 0 = \pi(r\kappa) = r\pi(\kappa) = r\mathfrak{r} \implies r = 0 \implies r\kappa = 0$. By the direct-sum theorem IV.B.25, it now follows that

$$K = (\ker(\pi) \cap K) \oplus R\kappa.$$

Applying the inductive assumption to the submodule $(\ker(\pi)\cap K)\subset R^{n-1}$, it takes the form R^{m_0} for some $m_0 \leq n-1$. Finally, since $\mathrm{ann}(\kappa)=\{0\}$, $R\kappa \cong R$; and $K\cong R^{m_0+1}$. □

We want to get from "ugly" presentations $M\cong R^n/K$ to "nice" ones like $Rx_1\oplus\cdots\oplus Rx_k\oplus R^r$. The starting point is to write K with respect to a base. More precisely, *given* a submodule $K\subset R^n$, we may compose the isomorphism $R^{n_0}\overset{\cong}{\to} K$ guaranteed by IV.C.2 — or, more generally, *any surjective homomorphism* $R^m \twoheadrightarrow K$ — with the inclusion $K\hookrightarrow R^n$ to get an R-module homomorphism

(IV.C.3)
$$\begin{aligned} R^m &\overset{\theta}{\to} R^n \\ \mathbf{e}'_j &\mapsto \theta(\mathbf{e}'_j) =: \underline{a}^j \quad (j=1,\ldots,m) \end{aligned}$$

whose image is K.

IV.C.4. DEFINITION. The $n\times m$ matrix of θ with respect to the standard bases ($\{\mathbf{e}'_j\}$ of R^m, $\{\mathbf{e}_i\}$ of R^n) is

$$_{\mathbf{e}}[\theta]_{\mathbf{e}'} := A := \begin{pmatrix} \uparrow & & \uparrow \\ \underline{a}^1 & \cdots & \underline{a}^m \\ \downarrow & & \downarrow \end{pmatrix}.$$

A is called a **relations matrix** for $M:=R^n/K$, and we can write[11]

$$M\cong R^n/\theta(R^m) \underset{\text{bases}}{\overset{\text{in}}{=}} R^n/A\cdot R^m = \frac{R\langle \mathbf{e}_1,\ldots,\mathbf{e}_n\rangle}{R\langle \sum_i a_i^1\mathbf{e}_i,\ldots,\sum_i a_i^m \mathbf{e}_i\rangle}.$$

Our hopes are pinned on transforming A into something nice, for which we have to revisit the elementary matrices from §III.C. Recall that

$$\begin{aligned} \mathrm{GL}_n(R) :=& \text{ invertible } n\times n \text{ matrices with entries in } R \\ =& \; n\times n \text{ matrices with entries in } R \text{ and } \det\in R^*, \end{aligned}$$

e.g. for $R=\mathbb{Z}$ we need $\det = \pm 1$.

IV.C.5. EXAMPLE. The *elementary matrices* of (III.C.4) belong to $\mathrm{GL}_n(R)$. We will need some notation for these:

[11] The notation $R\langle\cdots\rangle$ simply means all R-linear combinations of the elements inside the angle brackets; a_i^j means the i^{th} entry of $\underline{a}^j$.

- $T_{ij}^{(n)}(a) := \mathbb{1}_n + a\mathbf{e}_{ij}$, where $a \in R$, has inverse $T_{ij}(-a)$:
- $P_{ij}^{(n)} := \mathbb{1}_n + \mathbf{e}_{ij} + \mathbf{e}_{ji} - \mathbf{e}_{ii} - \mathbf{e}_{jj} = P_{ji}^{(n)}$ is its own inverse.
- $D_i^{(n)}(u) := \mathbb{1}_n + (u-1)\mathbf{e}_{ii}$, where $u \in R^*$, has inverse $D_i^{(n)}(u^{-1})$.

IV.C.6. PROPOSITION. *Let A be an $n \times m$ relations matrix for (a f.g. R-module) M. Let $P \in \mathrm{GL}_n(R)$, $Q \in \mathrm{GL}_m(R)$. Then PAQ is a relations matrix for M.*

PROOF. P corresponds to a change of basis $\{\mathbf{e}_i\} \mapsto \{\tilde{\mathbf{e}}_i\}$ for R^n, and Q to a change of basis $\{\mathbf{e}'_j\} \mapsto \{\tilde{\mathbf{e}}'_j\}$ for R^m: that is, $P = {}_{\tilde{\mathbf{e}}}[\mathrm{id}_{R^n}]_{\mathbf{e}}$ (i.e. $\mathbf{e}_k = \sum_i p_{ik}\tilde{\mathbf{e}}_i$), while $Q = {}_{\mathbf{e}'}[\mathrm{id}_{R^m}]_{\tilde{\mathbf{e}}'}$ (i.e. $\tilde{\mathbf{e}}'_\ell = \sum_j q_{j\ell}\mathbf{e}'_j$). So

$$PAQ = {}_{\tilde{\mathbf{e}}}[\mathrm{id}_{R^n}]_{\mathbf{e}} \cdot {}_{\mathbf{e}}[\theta]_{\mathbf{e}'} \cdot {}_{\mathbf{e}'}[\mathrm{id}_{R^m}]_{\tilde{\mathbf{e}}'} = {}_{\tilde{\mathbf{e}}}[\theta]_{\tilde{\mathbf{e}}'}$$

is just a matrix of θ with respect to different bases of R^m and R^n. $\square$

In practice, you may not need to keep track of how the bases change, but just to find some PAQ which is in a nice form (the *normal form* below). At the risk of beating elementary matrices into the ground:

IV.C.7. EXAMPLE. Let's see how to compute various "PAQ's". Here A is any $n \times n$ matrix over R.

To get this matrix from A	do the following (to A)
$T_{ij}^{(n)}(a) \cdot A$	add $a\times$(row j) to (row i)
$A \cdot T_{ij}^{(m)}(a)$	add $a\times$(column i) to (column j)
$P_{ij}^{(n)} \cdot A$	swap rows i and j
$A \cdot P_{ij}^{(m)}$	swap columns i and j
$D_i^{(n)}(u) \cdot A$	multiply row i by u
$A \cdot D_i^{(m)}(u)$	multiply column i by u

The operations on the RHS of the table will be called **elementary operations (EOs)**.

The structure theorem for $\mathbb{Z}$-modules. We are now going to state and prove the main results for abelian groups ($R = \mathbb{Z}$). Later we will generalize the proof, first to the case where R a Euclidean domain, and then to the general PID case.

IV.C.8. LEMMA-DEFINITION. *Every $A \in M_{n\times m}(\mathbb{Z})$ can be transformed by EOs into a matrix in **normal form**:*

$$\left.\left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right),\ (D \mid 0),\ \left(\begin{array}{c} D \\ \hline 0 \end{array}\right),\ D,\ \text{or } 0\ \right\} \begin{array}{l}\textit{henceforth summarized} \\ \textit{by } ``\left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right)",\end{array}$$

with $D = \operatorname{diag}(d_1, d_2, \ldots, d_k)$ a diagonal matrix and $d_1 \mid d_2 \mid \cdots \mid d_k$.

IV.C.9. THE FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS/$\mathbb{Z}$-MODULES (FTFGAG). *Any finitely generated abelian group G may be expressed* uniquely *in the form*

(IV.C.10) $$\underbrace{\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}}_{G_{tor}} \times \underbrace{\mathbb{Z}^r}_{G/G_{tor}}$$

where $d_i \geq 2$ and $d_1 \mid d_2 \mid \cdots \mid d_k$.

EASY PART OF PROOF (ASSUMING LEMMA IV.C.8). Putting everything together:

- G finitely generated $\implies G \cong \mathbb{Z}^n/K$ with relations matrix A.
- Lemma IV.C.8 $\implies$ EOs convert A to normal form.
- Example IV.C.7 $\implies$ the resulting matrix is of the form PAQ with $P \in \mathrm{GL}_n(\mathbb{Z})$ and $Q \in \mathrm{GL}_m(\mathbb{Z})$.
- Prop. IV.C.6 $\implies$ PAQ is a relations matrix for G.

Conclude that

$$\begin{aligned} G \ &\cong\ \mathbb{Z}^n/(PAQ)(\mathbb{Z}^m)\ =\ \mathbb{Z}^n/\left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right)\mathbb{Z}^m \\ &=\ \frac{\mathbb{Z}\langle X_1, \ldots, X_n\rangle}{\langle d_1X_1, \ldots, d_kX_k\rangle} = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^{n-k}, \end{aligned}$$

where $r = n - k$ is the number of complete rows of zeroes in the normal form.[12] □

IV.C.11. DEFINITION. In IV.C.9, r is the **rank** (of the free part) of G, and $d_1, \ldots, d_k$ the **torsion exponents** (or **invariant factors**) of G. (G is finite $\iff r = 0$.)

IV.C.12. EXAMPLE. Consider

$$G := \frac{\mathbb{Z}\langle X, Y, Z\rangle}{\langle 11X - 21Y - 10Z,\ X - 6Y - 5Z\rangle} = \frac{\mathbb{Z}^3}{K}.$$

Clearly $K \cong \mathbb{Z}^2$, and in the "standard" bases (cf. IV.C.4) we have

$$A = \begin{pmatrix} 11 & 1 \\ -21 & -6 \\ -10 & -5 \end{pmatrix}.$$

Applying EOs, we reduce to normal form:

$$\xrightarrow[\text{to (col. 1)}]{\text{add } (-11)\times\text{(col. 2)}} \begin{pmatrix} 0 & 1 \\ 45 & -6 \\ 45 & -5 \end{pmatrix} \xrightarrow[\text{from (row 3)}]{\text{subtract (row 2)}} \begin{pmatrix} 0 & 1 \\ 45 & -6 \\ 0 & 1 \end{pmatrix} \xrightarrow[\text{from (row 3)}]{\text{subtract (row 1)}} \begin{pmatrix} 0 & 1 \\ 45 & -6 \\ 0 & 0 \end{pmatrix}$$

$$\xrightarrow[\text{to (row 2)}]{\text{add } 6\times\text{(row 1)}} \begin{pmatrix} 0 & 1 \\ 45 & 0 \\ 0 & 0 \end{pmatrix} \xrightarrow[\text{cols. 1 and 2}]{\text{swap}} \left(\begin{array}{cc} 1 & 0 \\ 0 & 45 \\ \hline 0 & 0 \end{array}\right),$$

concluding that $d_1 = 1$, $d_2 = 45$, $r = 1$, and

$$G \ \cong\ \frac{\mathbb{Z}\langle \tilde{X}, \tilde{Y}, \tilde{Z}\rangle}{\langle \tilde{X}, 45\tilde{Y}\rangle} \ =\ \mathbb{Z}_{45} \times \mathbb{Z}.$$

We now return to the proofs.

[12] Here I am writing $\{X_i\}$ for the base of $\mathbb{Z}^n$ corresponding to the $\{\mathbf{e}_i\}$ in the first line.

PROOF OF IV.C.8. Let $A \in M_{n\times m}(\mathbb{Z})$, and write

$$a_{ij} := (i,j)^{\text{th}} \text{ entry of } A, \qquad R_s := s^{\text{th}} \text{ row of } A,$$
$$\text{and } \; C_t := t^{\text{th}} \text{ column of } A.$$

A row or column will be said to be *cleared* if it has only one nonzero entry. As we change A by EOs, it will (at intermediate steps) have the form

$$\left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & \mathbf{0} \\ 0 & & d_k & \\ \hline & \mathbf{0} & & A' \end{array}\right),$$

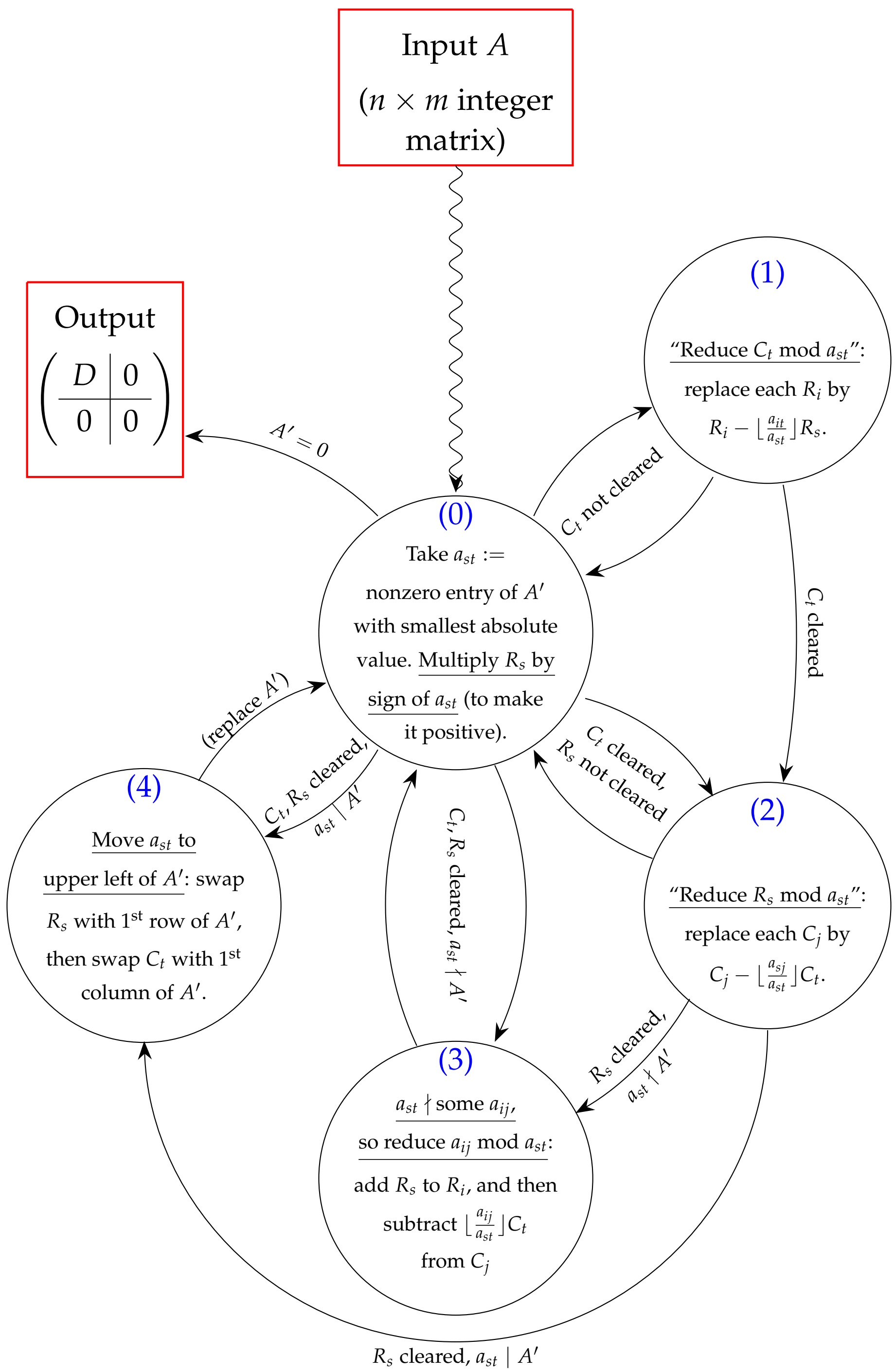
with $d_1 \mid d_2 \mid \cdots \mid d_k$, and A' *not* of the form

$$\left(\begin{array}{c|c} d & \leftarrow 0 \rightarrow \\ \hline \uparrow & \\ 0 & * \\ \downarrow & \end{array}\right).$$

We will write $a_{st} \mid A'$ if a_{st} divides all entries of A'. Recall that for $q \in \mathbb{Q}$, the *floor function* $\lfloor q \rfloor$ is defined to be the greatest integer less than or equal to q.

On the next page, we present an algorithm for reducing A to normal form. The goal is to reach (4) and reduce the size of A' (i.e. increase k by 1). Since one either progresses all the way around the outer semicircle ($(1) \to (2) \to (4)$) or reduces $|a_{st}|$ upon returning to (0) (which cannot reduce indefinitely!), the algorithm terminates. $\square$

EO Normalization Algorithm ($R = \mathbb{Z}$):



PROOF OF UNIQUENESS IN IV.C.9. Suppose that

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r \overset{(\dagger)}{\cong} \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_\ell} \times \mathbb{Z}^s,$$

where $d_1 \mid \cdots \mid d_k$ and $e_1 \mid \cdots \mid e_\ell$ (with $d_i, e_j \geq 2$). We must show that $r = s$, $k = \ell$, and $d_j = e_j$ ($\forall j = 1, \ldots k$).

First, because the LHS and RHS of $(\dagger)$ are isomorphic groups. they have isomorphic torsion and free parts:

$$\text{(a) } \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_\ell}, \quad \text{(b) } \mathbb{Z}^r \cong \mathbb{Z}^s.$$

Now (b) $\Longrightarrow$ the "cokernels" of multiplication by 2 are the same:

$$\frac{\mathbb{Z}^r}{2 \cdot \mathbb{Z}^r} \cong \frac{\mathbb{Z}^s}{2 \cdot \mathbb{Z}^s} \implies (\mathbb{Z}/2\mathbb{Z})^r \cong (\mathbb{Z}/2\mathbb{Z})^s \implies 2^r = 2^s$$

whence $r = s$.[13]

Next, let $\mathcal{A}_m(G)$ denote the number of elements of order dividing m; then (a) $\Longrightarrow$ $\mathcal{A}_{e_1}(\mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_\ell}) = \mathcal{A}_{e_1}(\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k})$. By an easy calculation, this yields

$$\gcd(e_1, e_1) \cdot \gcd(e_1, e_2) \cdots \gcd(e_1, e_\ell) = \gcd(e_1, d_1) \cdots \gcd(e_1, d_k)$$

hence

$$e_1^\ell = \prod_{j=1}^{k} \gcd(e_1, d_j) \leq e_1^k,$$

from which we conclude that $\ell \leq k$. A symmetric argument shows $\ell \geq k$, so $\ell = k$; in particular, the above inequality is an equality so that $\gcd(e_1, d_j) = e_1\,(\forall j) \implies e_1 \mid d_j\,(\forall j)$. Again, a symmetric argument (taking $\mathcal{A}_{d_1}$ on both sides of (a)) shows $d_1 \mid e_j\,(\forall j)$. But then $d_1 \mid e_1$ and $e_1 \mid d_1 \implies e_1 = d_1$.

Repeating the argument starting with

$$\mathcal{A}_{e_2}(\mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_k}) = \mathcal{A}_{e_2}(\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k})$$

gives

$$\gcd(e_2, e_1) \cdot \prod_{j=2}^{k} \gcd(e_2, e_j) = \underset{(=e_1)}{\gcd(e_2, d_1)} \cdot \prod_{j=2}^{k} \gcd(e_2, d_j)$$

[13]If you prefer, you can argue using II.K.4 that $r \leq s$ and $s \leq r$.

$$\implies e_2^{k-1} = \prod_{j=2}^{k} \gcd(e_2, e_j) = \prod_{j=2}^{k} \gcd(e_2, d_j) \le e_2^{k-1}.$$

Clearly the inequality is an equality, and so $\gcd(e_2, d_j) = e_2$ hence $e_2 \mid d_j$ for each j. On the other hand, taking $\mathcal{A}_{d_2}$ of both sides gives $d_2 \mid e_j$. So $d_2 \mid e_2$ and $e_2 \mid d_2 \implies d_2 = e_2$.

Continue in this manner until you get all $d_j = e_j$. □

Using the Chinese Remainder Theorem to decompose the $\mathbb{Z}_{d_j}$ factors in (IV.C.10) yields the

IV.C.13. COROLLARY (p-primary version of FTFGAG). *Any finitely generated abelian group G may be expressed* (*uniquely up to rearrangement of factors*) *in the form*

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z}^r,$$

where the $\{p_i\}$ are not-necessarily-distinct primes.

IV.C.14. REMARK. The abelian groups of order p^n (p prime) are in 1-to-1 correspondence with the **partitions** of n:

$$n = n_1 + \cdots + n_k \ (n_1 \le \cdots \le n_k) \quad \longleftrightarrow \quad \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}}.$$

Together with IV.C.13, this allows you to find all abelian groups of a given order: e.g., for order $360 = 2^3 3^2 5$, we have

$$G \cong \{\mathbb{Z}_{2^3} \text{ or } (\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^2}) \text{ or } (\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1})\} \\ \times \{\mathbb{Z}_{3^2} \text{ or } (\mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1})\} \times \mathbb{Z}_5.$$

IV.C.15. EXAMPLE. Let's see how to transform a more complicated matrix than the one in IV.C.12 into normal form, by applying the EO Normalization Algorithm. (You won't need to follow the algorithm this precisely in working problems. The point of going through this example is to know what to do *if* you get stuck!)

$$A = \begin{pmatrix} 4 & -10 & -2 & 20 & 30 \\ 0 & 28 & -2 & -60 & 90 \\ 3 & -3 & -2 & 6 & -9 \\ 7 & -7 & -4 & 14 & -21 \end{pmatrix}.$$

(0) $A' = A$, $a_{st} = a_{33} = -2$. Changing the sign of R_3 yields

$$\begin{pmatrix} 4 & -10 & -2 & 20 & 30 \\ 0 & 28 & -2 & -60 & 90 \\ -3 & 3 & 2 & -6 & 9 \\ 7 & -7 & -4 & 14 & -21 \end{pmatrix}.$$

(1) Reduce C_3 mod 2 (replace R_1, R_2, R_4 by $R_1 + R_3$, $R_2 + R_3$, $R_4 + 2R_3$):

$$\begin{pmatrix} 1 & -7 & 0 & 14 & 39 \\ -3 & 31 & 0 & -66 & 99 \\ -3 & 3 & 2 & -6 & 9 \\ 1 & -1 & 0 & 2 & 3 \end{pmatrix}.$$

(2) Reduce R_3 mod 2:

$$\begin{pmatrix} 1 & -7 & 0 & 14 & 39 \\ -3 & 31 & 0 & -66 & 99 \\ 1 & 1 & 2 & 0 & 1 \\ 1 & -1 & 0 & 2 & -3 \end{pmatrix}.$$

Since R_3 is not cleared, we must return to (0):

(0) $a_{st} = a_{11} = 1$.

(1) Reduce C_1 mod 1:

$$\begin{pmatrix} 1 & -7 & 0 & 14 & 39 \\ 0 & 10 & 0 & -24 & 216 \\ 0 & 8 & 2 & -14 & -38 \\ 0 & 6 & 0 & -12 & -42 \end{pmatrix}.$$

(2) Reduce R_1 mod 1:

$$\left(\begin{array}{c|cccc} 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 10 & 0 & -24 & 216 \\ 0 & 8 & 2 & -14 & -38 \\ 0 & 6 & 0 & -12 & -42 \end{array}\right).$$

which displays our new 3×4 A'. Step (4) does nothing.

(0) $a_{st} = a_{33} = 2$.

(1) done.

(2) Reduce R_3 mod 2:

$$\left(\begin{array}{c|cccc} 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 10 & 0 & -24 & 216 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 0 & -12 & -42 \end{array}\right).$$

(4) Swap m_{33} to top left position in A':

$$\left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 10 & -24 & 216 \\ 0 & 0 & 6 & -12 & -42 \end{array}\right)$$

and reset A' to be the smaller 2×3 matrix.

(0) $a_{st} = a_{43} = 6$.

(1) Reduce C_3 mod 6 (subtract R_4 from R_3):

$$\left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 4 & -12 & 258 \\ 0 & 0 & 6 & -12 & -42 \end{array}\right).$$

Since C_3 is not cleared, we return to

(0) $a_{st} = a_{33} = 4$.

(1) Reduce C_3 mod 4 (subtract R_3 from R_4):

$$\left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 4 & -12 & 258 \\ 0 & 0 & 2 & 0 & -300 \end{array}\right).$$

Good grief! C_3 is *still* not cleared!

(0) $a_{st} = a_{43} = 2$.

(1) Reduce C_3 mod 2:

$$\left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -12 & 858 \\ 0 & 0 & 2 & 0 & -300 \end{array}\right).$$

(2) Reduce R_4 mod 2:

$$\left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -12 & 858 \\ 0 & 0 & 2 & 0 & 0 \end{array}\right).$$

(4) Swap a_{43} to the top left position in A':

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & -12 & 858 \end{array}\right)$$

and reset A' to be the smaller 1×2 matrix.

(0) $a_{st} = a_{44} = -12$. Change the sign, bypass (1), and

(2) Reduce R_4 mod 12:

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 12 & 6 \end{array}\right).$$

Since R_4 is not cleared, we return to

(0) $a_{st} = a_{45} = 6$.

(2) Reduce R_4 mod 6:

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

(4) Swap the last two columns and replace A':

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 \end{array}\right) = (D \mid 0).$$

At last, we arrive at the normal form!

The structure theorem in the general case. Again let R be a PID.

IV.C.16. LEMMA-DEFINITION. *Every $A \in M_{n\times m}(R)$ can be transformed by invertible row and column operations*[14] *into a matrix in* ***normal form***

$$\left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_k & \\ \hline & 0 & & 0 \end{array}\right) =: \mathrm{nf}(A)$$

where the ***invariant factors*** $d_1 \mid \cdots \mid d_k$ *are unique up to units.* (*The matrix* $\mathrm{nf}(A)$ *itself is thus well-defined up to units.*)

PROOF. We break this into two parts: existence and uniqueness.

Step 1A : Reduction to normal form for R a Euclidean domain.

Let $\delta\colon R\backslash\{0\} \to \mathbb{Z}_{>0}$ be a Euclidean function. We describe how to modify the EO Normalization Algorithm above:

(0′) Take a_{st} to the nonzero entry of A' with smallest δ.

$$\begin{array}{c} \\ R_i \\ \\ R_s \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} & C_t & & C_j & \end{array} \\ \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & a_{it} & \cdot & a_{ij} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & a_{st} & \cdot & a_{sj} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \end{array}$$

(1′) Subtract (for each i) qR_s from R_i, where $a_{it} = qa_{st} + r$ (replaces a_{it} by r, with $\delta(r) < \delta(a_{st})$).

(2′) Subtract (for each j) $\tilde{q}C_t$ from C_j, where $a_{sj} = \tilde{q}a_{st} + \tilde{r}$ (replaces a_{sj} by $\tilde{r}$, with $\delta(\tilde{r}) < \delta(a_{st})$).

(3′) (a) Add R_s (cleared) to R_i; then (b) subtract $q'C_t$ from C_j where $a_{ij} = q'a_{st} + r'$ (replaces a_{ij} by r', with $\delta(r') < \delta(a_{st})$).

(4′) Swap a_{st} to the upper left of A'.

[14] i.e. $A \mapsto PAQ$, P and Q invertible over R. EOs will not in general be enough, but suffice for Euclidean domains.

Again one either proceeds all the way around the outer semicircle $((1') \to (2') \to (4'))$, or reduces $\delta(a_{st})$, so the process must terminate.

Step 1B: Reduction to normal form in general.

Let $\ell\colon R\backslash\{0\} \to \mathbb{N}$ be the length function. (Since R is a PID, R is a UFD, and this is well-defined.) For (0″), we take a_{st} to be the nonzero entry of A' with smallest ℓ (e.g. a unit, if there is one). (4″) is the same as (4′). We need replacements for (1′), (2′), and (3′)(b) when $a_{st} \nmid a_{it}$ (resp. a_{sj}, a_{ij}), since the Euclidean algorithm isn't available.

In fact, EOs won't suffice. Though (1″) [resp. (2″) and (3″)(b)] will still be given by row [resp. column] operations, or (equivalently) left- [resp. right-]multiplication by invertible matrices, the operations/matrices involved are of a slightly more general nature.

For (2″), here is what we can do.[15] Set $a := a_{st}$, $b := a_{sj}$, and let $x, y \in R$ be such that

$$xa + yb = d := \gcd(a, b),$$

$z := \frac{b}{d}$, $w := -\frac{a}{d}$. Right-multiplication by

$$\begin{array}{c} \\ R_t \\ \\ R_j \\ \\ \end{array}\overset{\begin{array}{ccccccccc} & & & C_t & & & C_j & & \end{array}}{\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & x & & & z & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & y & & & w & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}}$$

replaces ...	C_t	C_j	a_{st}	a_{sj}
by ...	$xC_t + yC_j$	$zC_t + wC_j$	$xa_{st} + ya_{sj} = d$	$za_{st} + wa_{sj} = 0$

[15] The analogues for (1″) and (3″)(b) are essentially the same and left to you.

which may "undo" our clearing of C_j.[16] But this is not a problem, as it creates a new entry ("d" in the (s,t) place) with length $\ell(d) < \ell(a_{st})$ (where $\ell(a_{st})$ was the previous shortest length). So as before, the minimal length is reduced each time we return to (0″) without passing through (4″) and reducing the size of A'.

Step 2: Uniqueness of the invariant factors.

Define $\Delta_i(A) := \gcd\{i \times i \text{ minors of } A\}$ and

$$\mathfrak{r}(A) := \max\{i \mid \Delta_i(A) \neq 0\} \qquad \text{("determinantal rank").}$$

By multilinearity of determinants, any $i \times i$ minor of PAQ (where $P \in M_{n\times n}(R)$, $Q \in M_{m\times m}(R)$) is an R-linear combination of $i \times i$ minors of A. Hence $\Delta_i(A) \mid \Delta_i(PAQ)$ in R. But if P, Q are invertible, this applies in reverse and

$$\Delta_i(A) \sim \Delta_i(PAQ).$$

Now suppose

$$PAQ = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & \mathbf{0} \\ & & d_k & \\ \hline & \mathbf{0} & & 0 \end{array}\right), \quad P'AQ' = \left(\begin{array}{ccc|c} d_1' & & & \\ & \ddots & & \mathbf{0} \\ & & d_k' & \\ \hline & \mathbf{0} & & 0 \end{array}\right).$$

On the one hand, direct computation implies

$$\begin{cases} \Delta_i(PAQ) = d_1 \cdots d_i \\ \Delta_i(P'AQ') = d_1' \cdots d_i' \end{cases} \quad (\forall i).$$

On the other, $\Delta_i(PAQ) \sim \Delta_i(A) \sim \Delta_i(P'AQ')$ $(\forall i)$. We conclude that $d_i \sim d_i'$ $(\forall i)$ and $k = \mathfrak{r}(A) = \ell$. □

IV.C.17. EXAMPLE. For an $n \times n$ matrix A over $\mathbb{F}[\lambda]$ ($\mathbb{F}$ a field), we can take

$$\Delta_{n-1}(A) \;=\; \text{monic gcd of entries of } \operatorname{adj}(A)$$

[16]This was already a feature of the original Step (3), though not of Step (2).

and

$$\Delta_n(A) \;=\; \det(A)/(\text{coefficient of highest power of } \lambda)$$

since we are free to multiply the Δ_i by units.

Suppose B is an $n \times n$ matrix over $\mathbb{F}$, and $A = \lambda \mathbb{1}_n - B$. The characteristic polynomial of B is

$$p_B(\lambda) = \Delta_n(A) = \prod_{i=1}^{n} d_i(A).$$

We will show (later) that

$$d_n(A) = \frac{\Delta_n(A)}{\Delta_{n-1}(A)}$$

is the minimal polynomial $m_B(\lambda)$ of B. For instance, consider

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

We reduce A to normal form with row and column operations:

$$A = \lambda \mathbb{1}_3 - B = \begin{pmatrix} \lambda-1 & -1 & -1 \\ -1 & \lambda-1 & -1 \\ -1 & -1 & \lambda-1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & \lambda-1 & -1 \\ \lambda-1 & -1 & -1 \\ -1 & -1 & \lambda-1 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda^2-2\lambda & -\lambda \\ 0 & -\lambda & \lambda \end{pmatrix} \mapsto \begin{pmatrix} 1 & & \\ & -\lambda & \lambda^2-2\lambda \\ & 0 & \lambda^2-3\lambda \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 1 & & \\ & \lambda & \\ & & \lambda^2-3\lambda \end{pmatrix}}_{=\mathrm{nf}(A)}.$$

Conclude that the invariant factors of A are $d_1(A) = 1$, $d_2(A) = \lambda$, and $d_3(A) = \lambda^2 - 3\lambda$; the last of these is indeed the minimal polynomial of B:

$$B^2 - 3B = \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} - 3 \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 0.$$

We are finally ready to state and prove our main result:

IV.C.18. THE STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER A PID. *Any f.g. module M over R may be expressed* (*up to isomorphism*) *uniquely in the form*

$$R/(\delta_1) \oplus \cdots \oplus R/(\delta_\ell) \, \oplus \, R^t \, , \tag{IV.C.19}$$

where the $\delta_i \notin R^*$ and $\delta_1 | \cdots | \delta_\ell$.

More precisely, M is an internal direct sum of cyclic modules:

$$\begin{cases} M = Rz_1 \oplus \cdots \oplus Rz_s \quad (z_i \in M) \\ \textit{where } \ \text{ann}(z_1) \supset \cdots \supset \text{ann}(z_s) \, ; \end{cases} \tag{IV.C.20}$$

and the annihlator ideals (*hence also the number s*) *are uniquely determined.*

As we saw in the $\mathbb{Z}$-module case, the uniqueness part does not follow from the uniqueness of the d_i in the normal form for A. (There are obviously many presentations R^n/K of M, with *different n*.) What we can do immediately is the existence part:

PROOF OF (IV.C.19)-(IV.C.20) (EXISTENCE OF DECOMPOSITION). We have

$$M \cong R^n/K \cong R^n/\theta(R^m) \cong R^n/A{\cdot}R^m \cong R^n/PAQ{\cdot}R^m,$$

with the last step given by change of bases for R^n, R^m. By IV.C.16 we may arrange to have $PAQ = \text{nf}(A) = \left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right)$ (with $D = \text{diag}(d_1, \ldots, d_k)$) hence

$$M \cong R^n / \left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right) {\cdot} R^m.$$

That is, there is an R-module homomorphism

$$\begin{aligned} \rho \colon R^n &\twoheadrightarrow M \\ \mathbf{e}_i &\mapsto \rho(\mathbf{e}_i) =: x_i \end{aligned}$$

with kernel $K = R\langle d_1\mathbf{e}_1, \ldots, d_k\mathbf{e}_k \rangle \subseteq R^n$, where $d_1 | \cdots | d_k$ ($\implies (d_1) \supset \cdots \supset (d_k)$).

Since ρ is surjective, $M = \sum_{i=1}^{n} Rx_i$. We describe these summands: for any i, we have $0 = rx_i \; (= r\rho(\mathbf{e}_i) = \rho(r\mathbf{e}_i)) \iff r\mathbf{e}_i \in K$.

- If $i > k$, $r\mathbf{e}_i \in K \iff r = 0$ hence $\mathrm{ann}(x_i) = \{0\}$ and $Rx_i \cong R$.
- If $i < k$, $r\mathbf{e}_i \in K \iff d_i | r$. So $\mathrm{ann}(x_i) = (d_i)$ and $Rx_i \cong R/(d_i)$.

Finally, $0 = \sum_i r_i x_i = \rho(\sum_i r_i \mathbf{e}_i) \implies \sum_i r_i \mathbf{e}_i \in K \; (\forall i) \implies d_i | r_i \; (\forall i)$ $\implies$ each $r_i x_i = 0$. So the homomorphism $\oplus_i Rx_i \twoheadrightarrow M$ is injective, and $M = \oplus_{i=1}^{n} Rx_i \cong R/(d_1) \oplus \cdots \oplus R/(d_k) \oplus R^{n-k}$.

Now it may be that none, some, or all of the $\{d_i\}$ are units; assume that the units are $d_1, \ldots, d_{k_0}$ (here $0 \leq k_0 \leq k$). Then $Rx_i = \{0\}$ for $i = 1, \ldots, k_0$. Writing $\ell := k - k_0$, $\delta_i := d_{k_0+i}$, $t := n - k$, $s := n - k_0$, and $z_i := x_{k_0+i}$ yields the specific forms of the decompositon shown in IV.C.19 and (IV.C.20). □

Uniqueness considerations. Finishing the proof of the structure theorem requires some preliminary results about decomposing torsion modules.

IV.C.21. DEFINITION. The **torsion submodule** of an R-module M is

$$\mathrm{tor}(M) := \{x \in M \mid rx = 0 \text{ for some } r \in R \backslash \{0\}\}.$$

M is a **torsion** module if $M = \mathrm{tor}(M)$.

IV.C.22. PROPOSITION. *A f.g. module M over a PID R is an internal direct sum of the form* $\mathrm{tor}(M) \oplus R^t$.

PROOF. By the existence part of the structure theorem (that we have now proved),

$$M = Rz_1 \oplus \cdots \oplus Rz_s \cong R/(d_1) \oplus \cdots \oplus R/(d_\ell) \oplus \underbrace{R \oplus \cdots \oplus R}_{t \text{ copies}}.$$

Given $m = \sum_{i=1}^{\ell} r_i z_i + \sum_{i=\ell+1}^{s} r_i z_i \in \mathrm{tor}(M)$, there exists $r \in R \backslash \{0\}$ such that $0 = rm = \sum_{i=1}^{\ell} rr_i z_i + \sum_{i=\ell+1}^{s} rr_i z_i$. Since M is a direct sum, $0 = (rr_i) z_i$ for $i = 1, \ldots, s$. But for $i > \ell$, $\mathrm{ann}(z_i) = \{0\} \implies rr_i = 0$ $\implies r_i = 0$ (as R is a domain). So $\mathrm{tor}(M) \subset R/(d_1) \oplus \cdots \oplus R/(d_\ell)$. The reverse inclusion is clear. □

IV.C.23. DEFINITION. Let $p \in R$ be a prime. The ***p*-primary component** of M is

$$\mathcal{A}_p(M) := \{x \in M \mid p^k x = 0 \text{ for some } k \in \mathbb{N}\}.$$

IV.C.24. LEMMA. *Let $p_1, \ldots, p_\ell$ be a list of* distinct[17] *primes in R. Then $\sum_{i=1}^{\ell} \mathcal{A}_{p_i}(M) = \oplus_{i=1}^{\ell} \mathcal{A}_{p_i}(M)$ ($\subset \text{tor}(M)$).*

PROOF. By induction, it suffices to show that

$$\mathcal{A}_{p_1} \cap \textstyle\sum_{i=2}^{\ell} \mathcal{A}_{p_i}(M) = \{0\}.$$

Given x in the LHS, we have $p_1^{k_1} x = 0 = p_2^{k_2} \cdots p_\ell^{k_\ell} x$ for some $k_i \in \mathbb{N}$. But as the primes are distinct, $\gcd(p_1^{k_1}, p_2^{k_2} \cdots p_\ell^{k_\ell}) = 1$. So there exist $m, n \in R$ such that $x = 1x = (mp_1^{k_1} + np_2^{k_2} \cdots p_\ell^{k_\ell})x = 0$. □

IV.C.25. THEOREM. *Assume M is a f.g. torsion module over a PID R. Then $M = \oplus_{p \in R \text{ prime}} \mathcal{A}_p(M) \cong \oplus_i R/(p_i^{e_i})$, where p_i are* not necessarily distinct *primes in R and $e_i \in \mathbb{Z}_{>0}$. Both direct sums are finite, which is to say that $\mathcal{A}_p(M)$ is nonzero for only finitely many*[18] *primes.*

PROOF. We know $M = \oplus_{j=1}^{k} R/(d_j)$, $d_j \in R \backslash \{0\}$ and $d_1 | \cdots | d_k$. Moreover, $d_j = \prod_{\ell=1}^{m} p_\ell^{e_{j\ell}}$ ($\forall j$) for some list of *distinct* primes $\{p_\ell\}$ (and $\{e_{j\ell} \in \mathbb{N}\}$). So we will *almost* be through if we can check that

$$R/(d_j) = \oplus_{\ell=1}^{m} R/(p_\ell^{e_{j\ell}}).$$

(Note that $d_1 | \cdots | d_k \implies e_{1\ell} \leq e_{2\ell} \leq \cdots \leq e_{k\ell}$ for each ℓ.) By induction, this reduces to the following module-theoretic version of the Chinese Remainder Theorem:

$$R/(fg) \cong R/(f) \oplus R/(g) \quad \text{if } (f,g) = R. \tag{IV.C.26}$$

To see this, let x be a generator of the LHS and rx an arbitrary element. Then $(f,g) = R \implies \exists\, r_i \in R$ with $r_1 f + r_2 g = r \implies rx = r_1 f x + r_2 g x \implies$

$$R/(fg) = Rx = Rfx + Rgx.$$

[17]This means non-associate: they don't generate the same ideal.

[18]Again, we are thinking of primes "up to units"; or equivalently, in terms of the corresponding prime ideals.

Next, $g(fx) = (fg)x = 0 \implies (g) \subset \mathrm{ann}(fx)$; while $0 = r(fx) \implies rf \in (fg) \implies rf = r'fg \implies r = r'g \implies r \in (g)$. So $Rfx \cong R/(g)$, and similarly $Rgx \cong R/(f)$. Finally, $y \in Rfx \cap Rgx \implies gy = 0 = fy \implies y = 1y = (r_1'f + r_2'g)y = 0$, finishing off (IV.C.26).

So we have proved

$$M \cong \bigoplus_i^{\text{finite}} R/(p_i^{e_i}),$$

and moreover the proofs of (IV.C.26) and (IV.C.19) show that the direct sum is internal. Therefore, we are reduced to

(IV.C.27)

If $M = \oplus_{j,\ell} Rx_{j\ell} = \oplus_{j,\ell} R/(p_\ell^{e_{j\ell}})$, then $\mathcal{A}_{p_\ell}(M) = \oplus_j R/(p_\ell^{e_{j\ell}})$ $(\forall \ell)$.

Clearly one has "$\supseteq$" on the right. To see the reverse inclusion "$\subseteq$", we need $\mathcal{A}_{p_{\ell_0}}(M) \cap \oplus_{j,\ell \neq \ell_0} R/(p_\ell^{e_{j\ell}}) = \{0\}$. But the "$\oplus_{j,\ell \neq \ell_0}$" here belongs to $\sum_{\ell \neq \ell_0} \mathcal{A}_{p_\ell}(M)$, so we are done by the proof of Lemma IV.C.24. □

IV.C.28. REMARK. We can view the isomorphism in the last theorem as an internal direct sum. The summands $R/(p_i^{e_i})$ are called **primary cyclic submodules** of M, and the $p_i^{e_i}$ are the **elementary divisors** of M.

We are at last ready for the

PROOF OF UNIQUENESS IN IV.C.18. Assume

$$M = Rz_1 \oplus \cdots \oplus Rz_s = Rw_1 \oplus \cdots \oplus Rw_r,$$

with annihilators (invariant factors) $d_1 | \cdots | d_s$ resp. $d_1' | \cdots | d_r'$. The last few annihilators in each list may be zero. The number of these trivial annihilators is the same on each side, as $M/\mathrm{tor}(M)$ has well-defined rank (R is commutative). So *we may assume that* $M = \mathrm{tor}(M)$ and all the d_i, d_j' are nonzero.

Next, decompose all the Rz_i resp. Rw_j into sums of primary cyclic submodules, viz.

$$M = \oplus_\ell \oplus_{j=1}^s R/(p_\ell^{e_{j\ell}}) = \oplus_\ell \oplus_{k=1}^r R/(p_\ell^{e'_{k\ell}}).$$

If these factors are the same, there is only one way to put them back together to get $d_1|\cdots|d_s$ and $d'_1|\cdots|d'_r$, and this will prove they are the same set of divisors. Since

$$\mathcal{A}_{p_\ell}(M) = \oplus_{j=1}^s R/(p_\ell^{e_{j\ell}}) = \oplus_{k=1}^r R/(p_\ell^{e'_{k\ell}}),$$

we may assume that $M = \mathcal{A}_p(M)$ for a single prime $p \in R$.

Considering the filtration[19] by R-submodules

$$M \supset pM \supset p^2M \supset \cdots ,$$

each $\frac{p^nM}{p^{n+1}M} =: M^{(n)}$ is an $R/(p)$-module (since $pM^{(n)} = 0$). Since (p) is prime and R is a PID, (p) is in fact maximal, and $R/(p)$ a field, making $M^{(n)}$ a vector space. Writing

$$M = \mathcal{A}_p(M) = \oplus_{j=1}^s R/(p^{e_j}) = \oplus_{k=1}^r R/(p^{e'_k}),$$

we have

$$M^{(n)} = \bigoplus_{j=1}^s \frac{(p^n)/(p^{e_j})}{(p^{n+1})/(p^{e_j})} = \bigoplus_{j=1}^s \begin{cases} 0, & \text{if } e_j \leq n \\ \frac{(p^n)}{(p^{n+1})}, & \text{otherwise} \end{cases}$$

(and also the same with s resp. e_j replaced by r resp. e'_k).

Let D_n resp. D'_n be the number of e_j resp. e'_k greater than n. Since

$$R/(p) \to (p^n)/(p^{n+1})$$
$$\bar{r} \longmapsto \bar{r}p^n$$

is an isomorphism of $R/(p)$-modules, we find that

$$M^{(n)} \cong (R/(p))^{D_n} \cong (R/(p))^{D'_n}$$

as a vector space over the field $R/(p)$. Hence $D_n = D'_n$. Since n was arbitrary, we conclude that (up to reordering) the e_j and e'_k are the same. □

[19]a nested sequence of submodules, usually indexed by a set of integers.