Chapters 10 & 12 Modules

DEF'N: R a (not nec. comm) ring with 1

M a (left-) R-module is an abelian group M^+ and an R-action i.e. a map
$$R \times M \longrightarrow M$$
$$(r, m) \longmapsto rm$$
satisfying
$$1 \cdot m = m$$
$$r(s(m)) = (rs)m$$
$$(r+s)m = rm + sm$$
$$r(m+m') = rm + rm'$$

An R-submodule $M' \subseteq M$ is a subgroup $(M')^+ \leq M^+$ with $R \cdot M' \subseteq M'$

EXAMPLES:

⓪ $R = \mathbb{F}$ a field, $\left\{\begin{matrix} R\text{-modules} \\ M \end{matrix}\right\} = \left\{\begin{matrix} \mathbb{F}\text{-vector spaces} \\ V \end{matrix}\right\}$

R-submodules = $\mathbb{F}$-linear subspaces

① $R = \mathbb{Z}$

$\{R\text{-modules } M\} = \{\text{abelian groups } A\}$

since for $n \in \mathbb{Z}$, $n \cdot a = \begin{cases} a + a + \dots + a \\ (-a) + \dots + (-a) \end{cases}$

$\mathbb{Z}$-submodules = subgroups

② $R = \mathbb{F}[x]$, $\mathbb{F}$ a field

$$\left\{ \begin{array}{c} R\text{-modules} \\ \mathbb{F}[x]\text{-modules} \\ M \end{array} \right\} = \left\{ \begin{array}{l} \mathbb{F}\text{-vector spaces } \overset{M}{\overset{\shortparallel}{V}} \\ \text{plus } V \xrightarrow{T} V \text{ an } \mathbb{F}\text{-linear transformation} \\ \quad v \longmapsto x \cdot v \end{array} \right\}$$

$$\Rightarrow \quad v \longmapsto f(x) \cdot v = f(T) \cdot v$$

for $f(x) \in \mathbb{F}[x]$

$\mathbb{F}[x]$-submodules of V

= T-stable subspaces $U \subseteq V$

③ $M = R$ is a module over R itself (via left multiplication)

and $\{R\text{-submodules of } R\}$

$= \{\text{ideals } I \subset R\}$

④ $M = R^A =$ <u>free</u> R-module with <u>basis</u> $\{e_a\}_{a \in A} = \{ r_{a_1} e_{a_1} + \ldots + r_{a_m} e_{a_m} : r_i \in R, a_j \in A \}$

= column vectors with entries in R with positions indexed by A and usual + and scaling

all but finitely many zero

An R-module M is <u>free</u> $\Leftrightarrow$ it has a basis

e.g. $M = R^n = \left\{ \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} : r_i \in R \right\}$

Having an R-basis $\{e_a\}_{a\in A}$ for an R-module M means

- $\{e_a\}_{a\in A}$ $\underline{R\text{-span}}$ M

  i.e. every $m\in M$ can be written as $r_{a_1}e_{a_1}+\ldots+r_{a_m}a_m$

AND

- $\{e_a\}_{a\in A}$ are $\underline{R\text{-linearly independent}}$

  $r_{a_1}e_{a_1}+\ldots+r_{a_m}e_{a_m}=0$ in M

  $\Rightarrow r_{a_i}=0 \;\forall i$

EXERCISE: An R-module M is $\underline{\text{free}}$ $\Leftrightarrow$ it has a basis $\{m_j\}_{j\in J}$ $\Leftrightarrow$ every $m\in M$ has a unique expression $m = r_{j_1}m_{j_1}+\ldots+r_{j_t}m_{j_t}$

---

e.g. if $R=\mathbb{Z}$

$M=\mathbb{Z}^n$ is a free ~~R~~ $\mathbb{Z}$-module with ~~R-basis~~ $\mathbb{Z}$-basis $e_1,\ldots,e_n$

but $M=\mathbb{Z}/n\mathbb{Z}$ is a non-free $\mathbb{Z}$-module.

It's $\underline{\mathbb{Z}\text{-spanned}}$ by $\{\bar{1}\}$, but not $\mathbb{Z}$-lin. indep. since $\underset{\substack{\uparrow\\ \mathbb{Z}}}{n}\cdot\bar{1}=\bar{0}$

e.g. $M = \mathbb{Z}$ as a $\mathbb{Z}$-module

has $\{2,3\}$ as a minimal $\mathbb{Z}$-spanning set under $\subseteq$

not $\mathbb{Z}$-lin. indep:

$(3)\cdot 2 + (-2)\cdot 3 = 0$

not both zero!

but not a $\mathbb{Z}$-basis

only $\{+1\}$, $\{-1\}$ are bases for $\mathbb{Z}$

DEF'N: $M \xrightarrow{\varphi} N$ is an R-module homomorphism

means $M^+ \xrightarrow{\varphi} N^+$ is a group homom.

and $\varphi(rm) = r\varphi(m)$ $\forall r \in R$.

epimorphism / surjection
monomorphism / injection
isomorphism
automorphism

} as usual

Given $M \subseteq N$ an R-submodule,

$\leadsto$ N/M = the quotient R-module

$N/M = N^+/M^+ = \{n+M : n \in N\}$

with $N \overset{\pi}{\twoheadrightarrow} N/M$, $n \longmapsto n+M$

+ all 4 Noether Thm's.

e.g.
$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \cup & & \cup \\ \ker\varphi & & \operatorname{im}\varphi \end{array}$$

and $M/\ker\varphi \cong \operatorname{im}\varphi$

The R-submodule of M gen'd by $\{m_j\}_{j\in J}$

$$:= \Big\{ \overset{\text{finite sum}}{\sum_j} r_j m_j : r_j \in R \Big\} = \sum_{j\in J} R m_j$$

$$= Rm_1 + \cdots + Rm_t \quad \text{if} \quad J = \{1,2,\ldots,t\}$$

DEF'N – PROP:

The following are equivalent for an R-module M, and define M being a Noetherian R-module:

(i) $\nexists\ M_1 \subsetneqq M_2 \subsetneqq \cdots$ an ∞ ascending chain of R-submodules

(the ACC = ascending chain condition)

(ii) every R-submodule of M is finitely gen'd, and can cut down any generating set to a finite one.

DEF'N – PROP:

The following are equivalent for an R-module M, and define M being a Noetherian R-module:

(i) $\nexists\ M_1 \subsetneqq M_2 \subsetneqq \cdots$ an ∞ ascending chain of R-submodules

(the ACC = ascending chain condition)

(ii) every R-submodule of M is finitely gen'd, and can cut down any generating set to a finite one.

proof: (i) $\Rightarrow$ (ii):

Assuming ACC for M, given N an R-submodule of M, then maybe $N=\{0\}$ and $\emptyset$ generates it.

Otherwise pick $n_1 \in N-\{0\}$ and maybe $N = Rn_1$, so done.

Otherwise pick $n_2 \in N - Rn_1$ and maybe $N = Rn_1 + Rn_2$, so done.

This process stops, else we have

$$Rn_1 \subsetneqq Rn_1 + Rn_2 \subsetneqq Rn_1 + Rn_2 + Rn_3 \subsetneqq$$

violating ACC.

$\underline{(ii) \Rightarrow (i)}$: Assuming all R-submodules of M are fin. gen'd, given $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ a chain of R-submodules, since $M_\infty := \bigcup_{i=1}^{\infty} M_i$ is an R-submodule

$$= Rm_1 + \cdots + Rm_N$$

for some $m_1, \ldots, m_N \in M_t$ and then $M_t = M_{t+1} = \cdots = M_\infty$ and the chain terminates. $\blacksquare$

REMARK: (ii) shows Noetherian rings R $=$ rings R that are Noetherian as R-modules

---

Very important ...

COROLLARY: If $M \subset N$ is an R-submodule, then

N is a Noetherian R-module $\iff$ both M and N/M are Noeth. R-modules

COROLLARY: If $M \subset N$ is an R-submodule, then

N is a Noetherian R-module $\iff$ both M and N/M are Noeth. R-module

proof: ($\Rightarrow$): If N is Noeth.

then $M \subseteq N$ has ACC since N does.

and N/M has ACC because

$$\left\{ \begin{array}{c} R\text{-submodules } \bar{N}' \\ \text{of } N/M \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} R\text{-submodules } N' \\ \text{of } N \text{ containing } M \end{array} \right\}$$

$$\bar{N}_1' \subset \bar{N}_2' \subset \cdots \qquad\qquad [M \subset]\, N_1 \subset N_2 \subset \cdots$$

($\Leftarrow$): Suppose both M and N/M have ACC

and we're given

$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq N$

($\Leftarrow$): Suppose both M and N/M have ACC

and we're given

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq N$$

$(-)\cap M$

$$N_i \hookrightarrow N \to N/M$$

image $\bar{N}_i$

$N_1 \cap M \subseteq N_2 \cap M \subseteq \cdots$

R-submodules of M

$\Rightarrow \exists\, t_1$ with

$N_{t_1} \cap M = N_{t_1+1} \cap M = \cdots$

$\bar{N}_1 \subseteq \bar{N}_2 \subseteq \cdots$ in N/M

R-submods of N/M

$\Rightarrow \exists\, t_2$ with

$\bar{N}_{t_2} = \bar{N}_{t_2+1} = \cdots$

so let $t = \max(t_1, t_2)$

and we claim $N_t \underset{\subseteq}{=} N_{t+1} = N_{t+2} = \cdots$

since given $n \in N_{t+1}$

since $\bar{n} \in \bar{N}_{t+1} = \bar{N}_t$ $\exists\, n' \in N_t$

with $\bar{n}' = \bar{n}$ in N_{t+1}/M

$n' - n \in M$

so $n' - n \in N_{t+1} \cap M = N_t \cap M$

$\Rightarrow n \in N_t$ $\blacksquare$

Noetherian R-modules so far...

DEF'N - PROP:

The following are equivalent for an R-module M, and define M being a <u>Noetherian</u> R-module:

(i) $\nexists\ M_1 \subsetneq M_2 \subsetneq \cdots$ an ∞ ascending chain of R-submodules

(the ACC = ascending chain condition)

(ii) every R-submodule of M is finitely gen'd, and can cut down any generating set to a finite one.

COROLLARY: If $M \subset N$ is an R-submodule, then

N is a Noetherian R-module $\iff$ both M and N/M are Noeth. R-module

COROLLARY:

Let R be a Noeth. ring (e.g. R a P.I.D. or $\mathbb{Z}[x_1,\dots,x_n]$, $\mathbb{F}[x_1,\dots,x_n]$, or their quotients)

Then

(i) every free R-module R^n with a finite basis is a Noeth. R-module,

(ii) more generally, every finitely generated R-module M is a Noeth. R-module,

(iii) and even better, every finitely generated R-module M has a presentation as the cokernel $R^n/\mathrm{im}(A)$ of a finite matrix

$$A=(a_{ij})_{\substack{i=1,\dots,n\\ j=1,\dots,\ell}} \in R^{n\times \ell}, \text{ i.e.}$$

$$M \cong \operatorname{coker}\left(R^\ell \xrightarrow{A} R^n\right) = R^n/\mathrm{im}(A)$$

$$x=\begin{bmatrix} x_1 \\ \vdots \\ x_\ell \end{bmatrix} \longmapsto Ax \qquad = R^n \Big/ R\begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \dots + R\begin{bmatrix} a_{1\ell} \\ \vdots \\ a_{n\ell} \end{bmatrix}$$

proof: (i) every free R-module R^n with a finite basis is a Noeth. R-module.

This follows via induction on n.

BASE CASE $n=1$: $R^1 = R$ as R-module, and we assumed R is a Noeth. ring, so R is a Noeth. R-module.

INDUCTIVE STEP:

Note that the projection homomorphism

$$R^n \xrightarrow{\pi} R \qquad \begin{bmatrix} r_1 \\ \vdots \\ r_{n-1} \\ r_n \end{bmatrix} \mapsto r_n$$

has $\ker(\pi) = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_{n-1} \\ 0 \end{bmatrix} \in R^n \right\} \cong R^{n-1}$

and $\mathrm{im}(\pi) = R$

so $R^n / \ker(\pi) \cong \mathrm{im}(\pi)$

$$\boxed{R^n / R^{n-1} \cong R}$$

and R^{n-1}, R Noeth. by induction

$\Rightarrow R^n$ Noeth.

For (ii): every finitely generated R-module M is a Noeth. R-module,

note that M is gen'd by $m_1, m_2, \dots, m_n$

$\iff M = Rm_1 + \dots + Rm_n$

$\iff$ this R-mod homomorphism is surjective:

$$\begin{aligned} R^n &\xrightarrow{\ f\ } M \\ e_i &\longmapsto m_i \\ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} &\longmapsto r_1 m_1 + \dots + r_n m_n \end{aligned}$$

and hence $M = \mathrm{im}(f) \cong \underbrace{\underset{\text{Noeth.}}{R^n} / \ker(f)}_{\Rightarrow \text{ Noeth.}}$

For (iii): every finitely generated R-module M has a presentation via a matrix $A \in R^{\ell \times n}$

$$M \cong \operatorname{coker}\left(R^\ell \xrightarrow{A} R^n\right) = R^n / \operatorname{im}(A)$$

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_\ell \end{bmatrix} \longmapsto Ax \qquad = R^n \Big/ R\begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \dots + R\begin{bmatrix} a_{1\ell} \\ \vdots \\ a_{n\ell} \end{bmatrix}$$

we just continue the proof of part (ii):

If $M = Rm_1 + \dots + Rm_n$, then

$M = \operatorname{im}(f) \cong R^n / \ker(f)$ where $R^n \xrightarrow{f} M$, $e_i \longmapsto m_i$.

But $\ker(f)$ is a R-submodule of $\underbrace{R^n}_{\text{Noeth.!}}$,

so $\ker(f)$ is finitely gen'd as an R-module,

say by vectors $\begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix}, \begin{bmatrix} a_{12} \\ \vdots \\ a_{n2} \end{bmatrix}, \dots, \begin{bmatrix} a_{1\ell} \\ \vdots \\ a_{n\ell} \end{bmatrix} \in R^n$

Thus $\ker(f) = R\begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \dots + R\begin{bmatrix} a_{1\ell} \\ \vdots \\ a_{n\ell} \end{bmatrix} = \operatorname{im} A$ if $A = \begin{bmatrix} a_{11} & \cdots & a_{1\ell} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{n\ell} \end{bmatrix}$.

so $M \cong R^n / \ker(f) = R^n / \operatorname{im}(A)$

$= \operatorname{coker}\left(R^\ell \xrightarrow{A} R^n\right)$. ∎

When R is not just a Noeth. ring, but a PID, we can do much better.

<u>THEOREM</u>: For R a P.I.D., every matrix $A \in R^{n \times \ell}$ can be brought to Smith Normal Form

$$S = \underbrace{\left[\begin{array}{c|c} \begin{matrix} d_1 & & 0 \\ & d_2 & \\ 0 & & \ddots \; d_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right]}_{\ell} \Bigg\} n \quad \text{with } d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r \text{ in } R$$

via invertible row and column operations over R, that is, $\exists\, P \in GL_n(R) = \{P \in R^{n\times n} : \det P \in R^\times\}$
$Q \in GL_\ell(R)$

such that $PAQ = S$.

As a consequence, if M is a fin. gen'd. R-module presented as $M = \operatorname{coker}(A)$, then

$$M \cong R^n / \operatorname{im}(A) \cong R^n / \operatorname{im}(S)$$

$$\cong R^n \Big/ R\begin{bmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \dots + R\begin{bmatrix} 0 \\ \vdots \\ d_r \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\cong R/(d_1) \oplus \dots \oplus R/(d_r) \oplus R^{n-r}$$

a direct sum of <u>cyclic modules</u> $= \begin{cases} R \\ \text{or} \\ R/(d) \end{cases}$

$\boxed{\begin{array}{l}\text{COR: Fin. gen'd abelian groups are}\\ \text{direct sums of cyclic groups}\\ \qquad A \cong \mathbb{Z}^{n-r} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\end{array}}$

<u>REMARK</u>: Smith normal form over a PID R generalizes the situation over a field $\mathbb{F}$, where $A \in \mathbb{F}^{n \times l}$ can be brought by row operations to row-echelon form

$$A \mapsto PA = \begin{bmatrix} 0 & \cdots & 0 & 1 & * & * & 0 & * & * & 0 & * & \cdots & * \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & * & 0 & * & \cdots & * \\ \vdots & & & & & & & & & & & & \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ & & & & & & \vdots & & & & & & \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}$$

and then using column operations to this form:

$$PA \mapsto PAQ = \begin{array}{c} r\left\{ \vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}} \right. \\ \end{array} \underbrace{\left[\begin{array}{ccc|c} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ \hline & 0 & & 0 \end{array}\right]}_{l} \Bigg\}\, n = S \quad \text{where } r = \operatorname{rank} A.$$

We can think of P, Q as a change-of-bases in both $\mathbb{F}^l$ and $\mathbb{F}^n$:

$$\begin{tikzcd} \mathbb{F}^l \arrow[r, "A"] & \mathbb{F}^n \arrow[d, "P", "\wr"'] \\ \mathbb{F}^l \arrow[u, "Q", "\wr"'] \arrow[r, "S = PAQ"] & \mathbb{F}^n \end{tikzcd}$$

<u>proof of THM:</u> Here is one Smith normal form algorithm for $A = \begin{bmatrix} a_{11} & \cdots & a_{1\ell} \\ \vdots & & \vdots \\ a_{n1} & & a_{n\ell} \end{bmatrix} \in R^{n \times \ell}$ with R a PID

that performs invertible row and col operations in stages that either make the ideal $(a_{11}) \subset R$ strictly larger, or the quantity $n+\ell$ strictly smaller.

<u>CASE 0:</u> If $A \neq 0$, $\exists\, a_{ij} \neq 0$, so WLOG $a_{11} \neq 0$ by permuting rows and columns (and (a_{11}) got bigger; end stage)

<u>CASE 1:</u> $a_{11} \mid a_{ij}\ \forall i,j$

Use a_{11} to clear out 1st row and column, and induct on $n+\ell$:
$$\left[\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & a_{22} & & \\ \vdots & & * & \\ 0 & & & \end{array}\right]$$
(end stage).

<u>CASE 2:</u> $\exists\, a_{ij}$ not divisible by a_{11}

... on next page ...

CASE 2: $\exists\, a_{ij}$ not divisible by a_{11}

CASE 2a: $\exists$ such an a_{ij} in 1^{st} row or column.
WLOG by symmetry it's in 1^{st} column, and by row permutations, it is a_{21}

So $A = \begin{bmatrix} a_{11} & \cdots \\ a_{21} & \cdots \\ \cdots & \end{bmatrix}$ If $a_{21} \mid a_{11}$, swap rows 1 & 2, so (a_{11}) gets bigger; end stage.

If $a_{21} \nmid a_{11}$, then $g = \gcd(a_{11}, a_{21})$ properly divides both, so $(g) \supsetneq (a_{11})$

and $g = ra_{11} + sa_{21}$

$\Big\downarrow$ divide by g

$1 = r\hat{a}_{11} + s\hat{a}_{21}$ where $\hat{a}_{11} = \frac{a_{11}}{g}$, $\hat{a}_{21} = \frac{a_{21}}{g}$

Then $P = \left[\begin{array}{cc|ccc} r & s & & 0 & \\ -\hat{a}_{21} & +\hat{a}_{11} & & & \\ \hline & & 1 & & 0 \\ & 0 & & 1 & \\ & & 0 & & 1 \end{array}\right]$ has $\det P = r\hat{a}_{11} + s\hat{a}_{21} = 1$

and $PA = \begin{bmatrix} g & \cdots \\ * & \ddots \\ \vdots & \end{bmatrix}$

so (a_{11}) got bigger; end stage.

CASE 2b: a_{11} divides all of 1^{st} row and column, but $a_{11} \nmid a_{ij}$ for some $i, j \geq 2$.
Then use a_{11} to zero out 1^{st} row and column, and then add column j to column 1, putting us back in CASE 2a.

Then why is $M = R^n/\mathrm{im}(A) \cong R^n/\mathrm{im}(\underset{\substack{\| \\ PAQ}}{S})$?

Roughly speaking, we have again done a change-of-basis in R^n and R^l with P, Q:

$$\begin{tikzcd} R^l \arrow[r, "A"] & R^n \arrow[d, "P", "\wr"'] \\ R^l \arrow[u, "Q", "\wr"'] \arrow[r, "PAQ=S"] & R^n \end{tikzcd}$$

More formally, $\mathrm{im}(A) = \mathrm{im}(AQ)$

since $x \in \mathrm{im}A \iff x = Ay$ for some y

$\iff x = AQy'$ where $y' = Q^{-1}y$

$\iff x \in \mathrm{im}AQ$

And then to show $R^n/\mathrm{im}(AQ) \cong R^n/\mathrm{im}(\underbrace{PAQ}_{=S})$,

note the composite map $R^n \xrightarrow[\sim]{P} R^n \twoheadrightarrow R^n/\mathrm{im}(PAQ)$

$$\begin{tikzcd} R^n \arrow[r, "P", "\sim"'] \arrow[rr, bend right, "f"'] & R^n \arrow[r, two heads] & R^n/\mathrm{im}(PAQ) \end{tikzcd}$$

is surjective, with

$x \in \ker(f) \iff Px \in \mathrm{im}(PAQ)$ i.e. $\ker(f) = \mathrm{im}AQ$

$\iff x \in \mathrm{im}AQ$

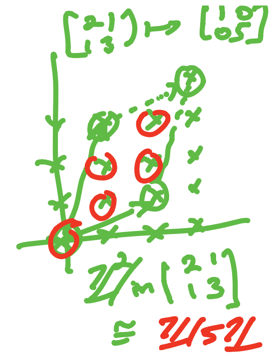
So f induces an isomorphism $R^n/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$

$$R^n/\mathrm{im}A = \underset{\substack{\| \\ R^n/\mathrm{im}AQ}}{} \qquad \underset{\substack{\| \\ R^n/\mathrm{im}(PAQ)}}{}$$

$\blacksquare$

EXAMPLE: $R = \mathbb{Z}$

$$A = \begin{bmatrix} 10 & 8 & 18 \\ 6 & 4 & 10 \\ 14 & 12 & 26 \\ 20 & 16 & 36 \end{bmatrix} \in \mathbb{Z}^{4\times 3}$$



$$\xmapsto{\text{subtract col2 from col1}} \begin{bmatrix} 2 & 8 & 18 \\ 2 & 4 & 10 \\ 2 & 12 & 26 \\ 4 & 16 & 36 \end{bmatrix} \xmapsto{\text{use } 2 \text{ to zero 1st col}} \begin{bmatrix} 2 & 8 & 18 \\ 0 & -4 & -8 \\ 0 & 4 & 8 \\ 0 & 0 & 0 \end{bmatrix} \xmapsto{\text{use } 2 \text{ to zero 1st row}} \begin{bmatrix} 2 & 0 & 0 \\ 0 & -4 & -8 \\ 0 & 4 & 8 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\xmapsto{\text{add row 2 to row 3}} \begin{bmatrix} 2 & 0 & 0 \\ 0 & -4 & -8 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \xmapsto{\text{subtract } 2\cdot\text{col 2 from col 3}} \begin{bmatrix} 2 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \xmapsto{\text{scale row 2 by } -1} S$$

OK, since $-1 \in \mathbb{Z}^\times$

$$S = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = PAQ = \text{Smith normal form}$$

$$\underset{d_1}{2} \mid \underset{d_2}{4}$$

Hence the $\mathbb{Z}$-module (abel. group)

$$\mathrm{coker}(A) = \mathbb{Z}^4/\mathrm{im}(A) \cong \mathbb{Z}^4/\mathrm{im}(S)$$

$$= \mathbb{Z}^4/\mathrm{im}\begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^2$$

Writing $\boxed{M = R^\beta \oplus \bigoplus_{i=1}^{t} R/(d_i)}$

one calls β the <u>rank</u> of M as an R-module

or $\beta := \mathrm{rank}_R(M)$, and β is <u>unique</u>

(see HW 6 EXER. 12.1.1,2,3,4)

One calls the R^β summand the <u>free</u> <u>part</u> of M

and $\bigoplus_{i=1}^{t} R/(d_i)$ the <u>torsion</u> <u>part</u> or $\mathrm{Tor}(M)$.

There are two useful ways to write $\mathrm{Tor}(M)$ <u>uniquely</u>:

(see D&F §12.1 for proof)

INVARIANT FACTOR FORM

$$\mathrm{Tor}(M) \cong \bigoplus_{i=1}^{t} R/(d_i)$$

with $(d_1) \supseteq (d_2) \supseteq \cdots\cdots$ (comes from Smith normal form)

ELEMENTARY DIVISOR FORM

$$\mathrm{Tor}(M) \cong \bigoplus_{\substack{\text{primes } p \in R \\ \text{irreducibles}}} \bigoplus_{i=1}^{l_p} R/(p^{\lambda_i^{(p)}})$$

with $\lambda_1^{(p)} \geq \lambda_2^{(p)} \geq \cdots \geq \lambda_{l_p}^{(p)}$ (≥ 1)

(comes from INV. FACTOR FORM using Sun Ze's Thm.)

EXAMPLE: $R = \mathbb{Z}$

in neither of the unique forms

$$M = \mathbb{Z}^4 \oplus \mathbb{Z}/\underbrace{100}_{2^2\cdot 5^2}\mathbb{Z} \oplus \mathbb{Z}/\underbrace{3000}_{2^3\cdot 3^1\cdot 5^3}\mathbb{Z} \oplus \mathbb{Z}/\underbrace{280}_{2^3\cdot 5^1\cdot 7^1}\mathbb{Z}$$

Sun Ze's Theorem

$$\cong \mathbb{Z}^4 \oplus \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z}$$
$$\oplus \mathbb{Z}/3^1\mathbb{Z}$$
$$\oplus \mathbb{Z}/5^3\mathbb{Z} \oplus \mathbb{Z}/5^2\mathbb{Z} \quad \mathbb{Z}/5^1\mathbb{Z}$$
$$\oplus \mathbb{Z}/7^1\mathbb{Z}$$

ELEM. DIVISOR FORM

Sun Ze's Theorem

(reassembling each column)

$$\cong \mathbb{Z}^4 \oplus \mathbb{Z}/2^3\cdot 3^1\cdot 5^3\cdot 7^1\mathbb{Z} \oplus \mathbb{Z}/2^3\cdot 5^2\mathbb{Z} \oplus \mathbb{Z}/2^2\cdot 5^1\mathbb{Z}$$
$$= \mathbb{Z}^4 \oplus \mathbb{Z}/\underbrace{21000}_{d_3}\mathbb{Z} \oplus \mathbb{Z}/\underbrace{200}_{d_2}\mathbb{Z} \oplus \mathbb{Z}/\underbrace{20}_{d_1}\mathbb{Z}$$

INV. FACTOR FORM

§12.2 Rational Canonical Form

Now we can return to the example of $R=\mathbb{F}[x]$, to deduce some consequences for a finite dim'l $\mathbb{F}$-vector space V with a linear operator $V \xrightarrow{T} V$.

Since this V becomes an $\mathbb{F}[x]$-module, which is finitely gen'd by any $\mathbb{F}$-basis of V, one has a unique invariant factor form

$$\underbrace{V \cong}_{\text{as } \mathbb{F}[x]\text{-module}} \mathbb{F}[x]^{\beta} \oplus \bigoplus_{i=1}^{m} \mathbb{F}[x]/(a_i(x))$$

with $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$ in $\mathbb{F}[x]$, $a_i(x)$ all monic polynomials

But $\beta=0$ else $\dim_{\mathbb{F}} V \geq \dim_{\mathbb{F}} \mathbb{F}[x] = \infty$,

so $$\boxed{\underbrace{V \cong}_{\text{as } \mathbb{F}[x]\text{-module}} \bigoplus_{i=1}^{m} \underbrace{\mathbb{F}[x]/(a_i(x))}_{\substack{\text{each of these is a}\\ \text{an } \mathbb{F}\text{-linear}\\ T\text{-stable subspace}}}}.$$

Given a monic polynomial $a(x) = x^d + b_{d-1}x^{d-1} + \dots + b_1 x + b_0$ in $\mathbb{F}[x]$, then $\mathbb{F}[x]/(a(x))$ has an $\mathbb{F}$-basis $\{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{d-1}\}$ and mult. by x acts in this basis via the <u>companion matrix</u> $C_{a(x)}$:

$$C_{a(x)} = \begin{array}{c|c} & \begin{array}{cccccc} \bar{1} & \bar{x} & \bar{x}^2 & \cdots & \bar{x}^{d-2} & \bar{x}^{d-1} \end{array} \\ \begin{array}{c} \bar{1} \\ \bar{x} \\ \bar{x}^2 \\ \vdots \\ \bar{x}^{d-2} \\ \bar{x}^{d-1} \end{array} & \begin{bmatrix} 0 & & & & & -b_0 \\ 1 & 0 & & 0 & & -b_1 \\ & 1 & 0 & & & -b_2 \\ & & 1 & \ddots & & \vdots \\ & 0 & & \ddots & 0 & \\ & & & & 1 & -b_{d-1} \end{bmatrix} \end{array}$$

since
$x \cdot \bar{1} = \bar{x}$
$x \cdot \bar{x} = \bar{x}^2$
$\vdots$
$x \cdot \bar{x}^{d-2} = \bar{x}^{d-1}$
$x \cdot \bar{x}^{d-1} = \bar{x}^d$
$= -\sum_{i=0}^{d-1} b_i \bar{x}^i$

<u>COROLLARY</u>: Every $\mathbb{F}$-linear operator $V \xrightarrow{T} V$ has a unique <u>rational canonical form</u> via a change of basis:

$$T = \begin{bmatrix} \boxed{C_{a_1(x)}} & & & \\ & \boxed{C_{a_2(x)}} & & \\ & & \ddots & \\ & & & \boxed{C_{a_m(x)}} \end{bmatrix}$$

with $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$ and each $a_i(x)$ monic in $\mathbb{F}[x]$.

Furthermore, $\det(xI - T) = a_1(x) a_2(x) \cdots a_m(x)$ and $a_m(x)$ is the <u>minimal polynomial</u> for T, meaning

$$\ker\left(\begin{array}{ccc} \mathbb{F}[x] & \longrightarrow & \mathbb{F}^{n \times n} \\ x & \longmapsto & T \end{array} \right) = (a_m(x)).$$

COROLLARY: Every $\mathbb{F}$-linear operator $V \xrightarrow{T} V$ has a unique rational canonical form via a change of basis:

$$T = \begin{bmatrix} \boxed{C_{a_1(x)}} & & & \\ & \boxed{C_{a_2(x)}} & & \\ & & \ddots & \\ & & & \boxed{C_{a_m(x)}} \end{bmatrix}$$

with $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$ and each $a_i(x)$ monic in $\mathbb{F}[x]$.
Furthermore, $\det(xI - T) = a_1(x) a_2(x) \cdots a_m(x)$ and $a_m(x)$ is the minimal polynomial for T, meaning
$\ker\left(\begin{array}{ccc} \mathbb{F}[x] & \longrightarrow & \mathbb{F}^{n \times n} \\ x & \longmapsto & T \end{array} \right) = (a_m(x))$.

proof: The uniqueness comes from the uniqueness of invariant factor form for

$$V = \bigoplus_{i=1}^{m} \mathbb{F}[x]/(a_i(x))$$

The assertion about $\det(xI - T)$ comes from checking that $\det C_{a(x)} = a(x)$, which is an easy exercise in column expansion.

To see that $\ker\left(\begin{array}{ccc} \mathbb{F}[x] & \longrightarrow & \mathbb{F}^{n \times n} \\ x & \longmapsto & T \end{array} \right) = (f(x))$ forces $(f(x)) = (a_m(x))$, note that $a_m(\bar{x})$ annihilates $V = \bigoplus_{i=1}^{m} \mathbb{F}[x]/(a_i(x))$, so $a_m(T) = 0$ in $\mathbb{F}^{n \times n}$, and hence $f(x)$ divides $a_m(x)$. But no lower degree polynomial in $\bar{x}$ annihilates $\mathbb{F}[x]/(a_m(x))$, so it can't annihilate V, i.e. $\deg f = \deg a_m$ so $(f(x)) = (a(x))$. ∎

EXAMPLE: Who are the similarity classes
$A \approx PAP^{-1}$
of matrices $A \in \mathbb{F}_3^{2\times 2}$?
Which ones are in $GL_2(\mathbb{F}_3)$?

Either $V = \mathbb{F}_3^2 \xrightarrow{A} \mathbb{F}_3^2$ has

$$V \cong \mathbb{F}_3[x]/(a_1(x)) \oplus \mathbb{F}_3[x]/(a_1(x)) \text{ with } a_1(x) = x + b_0$$

monic, linear
so $b_0 \in \mathbb{F}_3$

and A is similar to $\begin{bmatrix} b_0 & 0 \\ 0 & -b_0 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$ or $\begin{bmatrix} -1 & \\ & -1 \end{bmatrix}$ or $\begin{bmatrix} 0 & \\ & 0 \end{bmatrix}$

OR

$$V \cong \mathbb{F}_3[x]/(a_1(x)) \text{ with } a_1(x) = x^2 + b_1 x + b_0$$

and A is similar to $\begin{bmatrix} 0 & -b_0 \\ 1 & -b_1 \end{bmatrix}$ with $b_0, b_1 \in \mathbb{F}_3$ (9 choices total)

Among these, the cases with $b_0 \neq 0$ lie in $GL_2(\mathbb{F}_3)$

so $\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$, $\begin{bmatrix} -1 & \\ & -1 \end{bmatrix}$, and $\underbrace{\begin{bmatrix} 0 & -b_0 \\ 1 & -b_1 \end{bmatrix} \text{ with } b_0 \in \{\pm 1\},\ b_1 \in \mathbb{F}_3}_{\text{6 choices total}}$

$$\boxed{\begin{array}{l} \det(xI - T) \\ \quad \} \; x=0 \\ b_0 = \det(-T) = (-1)^n \det T \\ \quad \neq 0 \iff T \text{ invertible} \end{array}}$$

§12.3 Jordan Canonical Form

When $\mathbb{F}$ is algebraically closed, e.g. $\mathbb{F}=\mathbb{C}$ or $\mathbb{F}=\overline{\mathbb{F}_p}$, the monic irreducible polynomials $p(x)$ in $\mathbb{F}[x]$ are all linear of the form $p(x)=x-c$ with $c\in\mathbb{F}$.

Hence the elementary divisor form for an operator $V \xrightarrow{T} V$ as an $\mathbb{F}[x]$-module is

$$V \cong \bigoplus_{c\in\mathbb{F}} \bigoplus_{i=1}^{\ell_c} \mathbb{F}[x]/\left((x-c)^{\lambda_i^{(c)}}\right)$$

with $\lambda_1^{(c)} \geq \lambda_2^{(c)} \geq \cdots \geq \lambda_{\ell(c)}^{(c)}$ (≥ 1)

The $\lambda\times\lambda$ matrix J_c^λ for mult. by $\bar{x}$ acting in the basis $\{\bar{1}, \overline{x-c}, \overline{(x-c)}^2, \ldots, \overline{(x-c)}^{\lambda-1}\}$ for $\mathbb{F}[x]/((x-c)^\lambda)$ is called a Jordan block of size λ with eigenvalue c:

$$J_\lambda = \begin{array}{c} \\ \bar{1} \\ \overline{x-c} \\ \overline{(x-c)}^2 \\ \vdots \\ \overline{(x-c)}^{\lambda-1} \end{array} \begin{array}{c} \begin{array}{ccccc} \bar{1} & \overline{x-c} & \overline{(x-c)}^2 & \cdots & \overline{(x-c)}^{\lambda-1} \end{array} \\ \begin{bmatrix} c & & & & \\ 1 & c & & & \\ & 1 & c & & \\ & & 1 & \ddots & \\ & & & \ddots & \ddots \\ & & & 1 & c \end{bmatrix} \end{array}$$

since

$\bar{x}\cdot\bar{1} = \bar{x} = c\cdot\bar{1} + \overline{x-c}$

$\bar{x}\cdot(\overline{x-c}) = c\cdot(\overline{x-c}) + \overline{(x-c)}^2$

$\vdots$

$\bar{x}\cdot(\overline{x-c})^k = c(\overline{x-c})^k + (\overline{x-c})^{k+1}$

__COROLLARY:__ For algebraically closed fields $\mathbb{F}$, every linear operator $V \xrightarrow{T} V$ with $\dim_{\mathbb{F}} V$ finite has a change-of-basis to a unique <u>Jordan canonical form</u> with Jordan blocks of size $\lambda_1^{(c)} \geq \lambda_2^{(c)} \geq \cdots \geq \lambda_{\ell_c}^{(c)}$ for various scalars $c \in \mathbb{F}$

$$\begin{bmatrix} \ddots & & & \\ & \left.\boxed{\begin{matrix} c & & 0 \\ 1 & c & \\ & \ddots & \ddots & \\ 0 & & 1 & c \end{matrix}}\right\}\lambda_1^{(c)} & & \\ & & \left.\boxed{\begin{matrix} c & & 0 \\ 1 & c & \\ & \ddots & \ddots & \\ 0 & & 1 & c \end{matrix}}\right\}\lambda_2^{(c)} & \\ & & & \ddots \end{bmatrix}$$

a bit painful to draw the general form!

Furthermore,

$$\det(xI - T) = \prod_{c \in \mathbb{F}} (x-c)^{|\lambda^{(c)}|} \quad \text{where } |\lambda^{(c)}| = \lambda_1^{(c)} + \lambda_2^{(c)} + \cdots$$

and the <u>minimal polynomial</u> for T is $m_T(x) = \prod_{c \in \mathbb{F}} (x-c)^{\lambda_1^{(c)}}$.

In particular, T is diagonalizable $\Leftrightarrow$ each $\lambda_1^{(c)} \leq 1$ $\Leftrightarrow$ $m_T(x)$ has distinct roots.

<u>COROLLARY</u>: For algebraically closed fields $\mathbb{F}$, every linear operator $V \xrightarrow{T} V$ with $\dim_{\mathbb{F}} V$ finite has a change-of-basis to a unique <u>Jordan canonical form</u> with Jordan blocks of size $\lambda_1^{(c)} \geq \lambda_2^{(c)} \geq \cdots \geq \lambda_{\ell_c}^{(c)}$ for various scalars $c \in \mathbb{F}$

$$\begin{bmatrix} \ddots & & & \\ & \left.\boxed{\begin{matrix} c & & 0 \\ 1 & c & \\ & \ddots & \ddots \\ 0 & & 1 \; c \end{matrix}}\right\}\lambda_1^{(c)} & & \\ & & \left.\boxed{\begin{matrix} c & & 0 \\ 1 & c & \\ & \ddots & \ddots \\ 0 & & 1 \; c \end{matrix}}\right\}\lambda_2^{(c)} & \\ & & & \ddots \end{bmatrix}$$

a bit painful to draw the general form!

Furthermore,

$$\det(xI - T) = \prod_{c \in \mathbb{F}} (x-c)^{|\lambda^{(c)}|} \quad \text{where } |\lambda^{(c)}| = \lambda_1^{(c)} + \lambda_2^{(c)} + \cdots$$

and the <u>minimal polynomial</u> for T is $m_T(x) = \prod_{c \in \mathbb{F}} (x-c)^{\lambda_1^{(c)}}$.

In particular, T is diagonalizable $\Leftrightarrow$ each $\lambda_1^{(c)} \leq 1$ $\Leftrightarrow$ $m_T(x)$ has distinct roots

<u>proof</u>: Uniqueness comes from uniqueness of elementary divisor form over $\mathbb{F}[x]$.

The assertion about $\det(xI-T)$ comes from

$$\det(xI - J_c^{(\lambda)}) = (x-c)^{\lambda}.$$

The rest of the assertions are easy to check. ∎

<u>EXAMPLE</u>: How many conjugacy classes of A in $GL_5(\mathbb{C})$ are there with $\det(xI - A) = (x+i)^2(x-4)^3$?

A has Jordan form $\left[\begin{array}{c|c} B & 0 \\ \hline 0 & C \end{array}\right]$ where $B = \begin{bmatrix} \boxed{-i} & \\ & \boxed{-i} \end{bmatrix}$ or $\begin{bmatrix} -i & 0 \\ 1 & -i \end{bmatrix}$

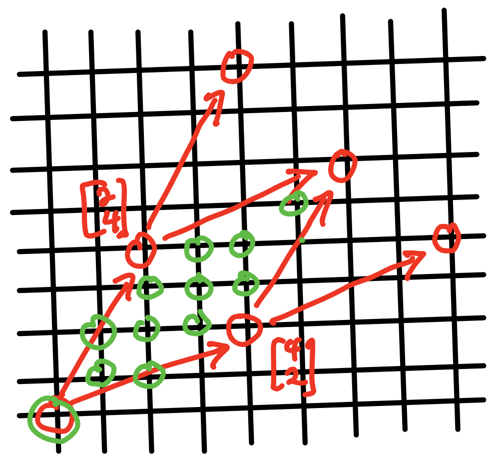
and $C = \begin{bmatrix} \boxed{4} & & \\ & \boxed{4} & \\ & & \boxed{4} \end{bmatrix}$ or $\begin{bmatrix} \boxed{\begin{matrix} 4 & 0 \\ 1 & 4 \end{matrix}} & \\ & \boxed{4} \end{bmatrix}$ or $\begin{bmatrix} 4 & 0 & 0 \\ 1 & 4 & 0 \\ 0 & 1 & 4 \end{bmatrix}$, so $2 \cdot 3 = 6$ choices

REMARKS on lattices

A <u>lattice</u> L of rank r is a free abelian group $L \cong \mathbb{Z}^r$.

e.g. $L = \mathrm{im}\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix} \subset \mathbb{Z}^2$

$$= \mathbb{Z}\begin{bmatrix} 4 \\ 2 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 2 \\ 4 \end{bmatrix}$$



12 coset reps for $\mathbb{Z}^2/\mathrm{im}A$

$12 = |\det A|$

$= \left|\det\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}\right|$

$= 16 - 4 = 12$ ✓

The green circled points give us 12 coset representatives for the <u>quotient group</u>

$\mathbb{Z}^2/L = \mathbb{Z}^2/\mathrm{im}A$, but what is its abelian group structure?

<u>PROP:</u> If $A \in \mathbb{Z}^{n \times n}$ has <u>full</u> <u>rank</u>

i.e. $\mathrm{rank}_{\mathbb{Q}}(A) = n$, and Smith normal form $S = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix}$, then $L = \mathrm{im} A$

has $\mathbb{Z}^n / L = \mathrm{coker} A$ of <u>cardinality</u>

$$|\det A| = |\det S| = |\mathrm{coker} A| = d_1 d_2 \cdots d_n$$

and $\mathbb{Z}^n / L = \mathrm{coker} A \cong \mathrm{coker} S \cong \bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z}$

<u>proof:</u> We've seen all the cokernel isomorphism assertions,

and $\det S = d_1 \cdots d_n = \left| \bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} \right|$.

Also note, since $S = PAQ$ with $P, Q \in GL_n(\mathbb{Z})$

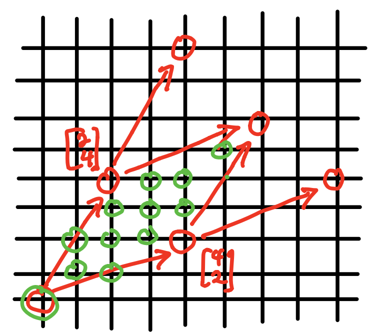
one has $\det S = \det PAQ$

$$= \underbrace{\det P}_{=\pm 1} \det A \cdot \underbrace{\det Q}_{=\pm 1}$$

$$= \pm \det A \qquad \blacksquare$$

e.g. $L = \mathrm{im}\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix} \subset \mathbb{Z}^2$

$= \mathbb{Z}\begin{bmatrix} 4 \\ 2 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 2 \\ 4 \end{bmatrix}$

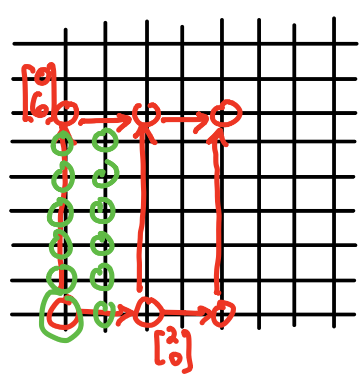


$L = \mathrm{im} A = \mathrm{im}\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}$ has Smith form $\begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix} = S$

$\mapsto \begin{bmatrix} 4 & -6 \\ 2 & 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 & -6 \\ 2 & 0 \end{bmatrix} \mapsto$

so $S = PAQ$ for some $P, Q \in GL_2(\mathbb{Z})$.

Changing $A \mapsto AQ$ alters the choice of lattice generators for $\mathrm{im} A = \mathrm{im} AQ$, while P performs a <u>lattice change of basis</u> on $\mathbb{Z}^2$:



$$\begin{aligned} \mathbb{Z}^2/L &= \mathrm{coker}\, A \\ &\cong \mathrm{coker}\, S \\ &= \mathbb{Z}^2 / \mathbb{Z}\begin{bmatrix} 2 \\ 0 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 0 \\ 6 \end{bmatrix} \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \end{aligned}$$