20250519 MATH4302 NOTE 3[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Basics of R-module

Definition 1.1. (**R-module**)
Let R be a ring, and M be a set. If:
(1) There is an operation $+ : M \times M \to M$, such that:

$$\begin{aligned}
\forall m, n, k \in M, & (m+n)+k = m+(n+k) \\
\forall m, n \in M, \quad & m+n = n+m \\
\exists 0 \in M, \forall m \in M, \quad & 0+m = m \\
\forall m \in M, \exists -m \in M, \quad & (-m)+m = 0
\end{aligned}$$

(2) There is an operation $* : R \times M \to M$, such that:

$$\begin{aligned}
\forall r, s \in R, \forall m \in M, \quad & (rs)*m = r*(s*m) \\
\forall m \in M, \quad & 1*m = m \\
\forall r, s \in R, \forall m \in M, & (r+s)*m = r*m+s*m \\
\forall r \in R, \forall m, n \in M, & r*(m+n) = r*m+r*n
\end{aligned}$$

Then M is a R-module.

Example 1.2. Let G be a set.
G is an Abelian group iff G is a $\mathbb{Z}$-module.

Example 1.3. Let R be a set.
If R is a ring, then R is a R-module.

Definition 1.4. (**R-linear Map**)
Let $M, \overline{M}$ be R-modules, and $f : M \to \overline{M}$ be a map. If:

$$\begin{aligned}
\forall m, n \in M, & f(m+n) = f(m)+f(n) \\
\forall r \in R, \forall m \in M, \ & f(r*m) = r*f(m)
\end{aligned}$$

Then $f \in \mathcal{L}(M, \overline{M})$ is R-linear.

Example 1.5. Let $f : M \to M$ be R-linear. $M_f = M$ is a $R[x]$-module:

$$\begin{aligned}
+_f : M_f \times M_f \to M_f, \quad & m +_f n = m+n \\
*_f : R[x] \times M_f \to M_f, & a_i x^i *_f m = a_i * f^i(m)
\end{aligned}$$

Example 1.6. Let G, H be Abelian groups, and $f : G \to H$ be a map.
f is a group homomorphism iff f is $\mathbb{Z}$-linear.

Definition 1.7. (**Submodule**)
Let M, N be R-modules.
If for some R-linear map $\iota : N \to M$,
for all map $f : K \to N$,
f is R-linear iff $\iota \circ f$ is R-linear,
then N is a R-submodule of M.

Proposition 1.8. Let M be a R-module, and N be a subset of M. If:

$$\begin{aligned} \forall m, n \in N, m + n &\in N \\ 0 &\in N \\ \forall r \in R, \forall m \in N,\ r * m &\in N \end{aligned}$$

Then $N \subseteq M$ is a R-submodule of M.

Proof. For some R-linear map $\iota : N \to M, m \mapsto m$,
for all map $f : K \to N$,
f is R-linear iff $\iota \circ f$ is R-linear.
Quod. Erat. Demonstrandum. □

Definition 1.9. (**Invariant Submodule**)
Let M be a R-module with a R-submodule N, and $f : M \to M$ be R-linear.
If N is a $R[x]$-submodule of M_f, then N is invariant under f.

Example 1.10. Let G be an Abelian group with subset H.
H is a subgroup of G iff H is a $\mathbb{Z}$-submodule of G.

Example 1.11. Let R be a ring with subset I.
I is an ideal of R iff I is a R-submodule of R.

Definition 1.12. (**Product Module**)
Let $(M_\mu)_{\mu \in J}, N$ be R-modules.
If for some R-linear maps $(\pi_\mu : N \to M_\mu)_{\mu \in J}$,
for all R-linear maps $(f_\mu : K \to M_\mu)_{\mu \in J}$,
for some unique R-linear map $g : K \to N$, $(\pi_\mu \circ g = f_\mu)_{\mu \in J}$,
then $N = \prod_{\mu \in J} M_\mu$ is a R-product module of $M_1, \cdots, M_k$.

Proposition 1.13. Let $(M_\mu)_{\mu\in J}$ be R-modules, and N be the collection of all map $m : J \to \bigcup_{\mu\in J} M_\mu$ with each $m(\mu) \in M_\mu$. If:

$$\forall m, n \in N, (m + n)(\mu) = m(\mu) + n(\mu)$$
$$\forall r \in R, \forall m \in N,\ (r * m)(\mu) = r * m(\mu)$$

Then $N = \prod_{\mu\in J} M_\mu$ is a R-product module of $(M_\mu)_{\mu\in J}$.

Proof. For some R-linear maps $(\pi_\mu : N \to M_\mu, m \mapsto m(\mu))_{\mu\in J}$,
for all R-linear maps $(f_\mu : K \to M_\mu)_{\mu\in J}$,
for some unique R-linear map $g : K \to N, g(k)(\mu) = f_\mu(k)$, $(\pi_\mu \circ g = f_\mu)_{\mu\in J}$.
Quod. Erat. Demonstrandum. □

Proposition 1.14. Let $(M_\mu)_{\mu\in J}$ be R-modules.
If $N, \overline{N}$ are R-product modules of $(M_\mu)_{\mu\in J}$,
then $N, \overline{N}$ are isomorphic.

Proof. We may divide our proof into four steps.
Step 1: Define the unique lift of $(\pi_\mu)_{\mu\in J}$ to $\overline{N}$ as τ.
Step 2: Define the unique lift of $(\overline{\pi}_\mu)_{\mu\in J}$ to N as $\overline{\tau}$.
Step 3: $\overline{\tau} \circ \tau$ is the unique lift id_N of $(\pi_\mu)_{\mu\in J}$ to N
Step 4: $\tau \circ \overline{\tau}$ is the unique lift $id_{\overline{N}}$ of $(\overline{\pi}_\mu)_{\mu\in J}$ to $\overline{N}$.
Quod. Erat. Demonstrandum. □

Proposition 1.15. Let M_1, M_2 be R-modules.
If $N_{12} = M_1 \times M_2, N_{21} = M_2 \times M_1$,
then N_{12}, N_{21} are isomorphic.

Proof. We may divide our proof into four steps.
Step 1: Define the unique lift of $\pi_{12,2}, \pi_{12,1}$ to N_{21} as $\tau_{12,21}$.
Step 2: Define the unique lift of $\pi_{21,1}, \pi_{21,2}$ to N_{12} as $\tau_{21,12}$.
Step 3: $\tau_{21,12} \circ \tau_{12,21}$ is the unique lift $id_{N_{12}}$ of $\pi_{12,1}, \pi_{12,2}$ to N_{12}.
Step 4: $\tau_{12,21} \circ \tau_{21,12}$ is the unique lift $id_{N_{21}}$ of $\pi_{21,2}, \pi_{21,1}$ to N_{21}.
Quod. Erat. Demonstrandum. □

Proposition 1.16. Let M_1, M_2, M_3 be R-modules.
If $N_{12} = M_1 \times M_2, N_{(12)3} = N_{12} \times M_3, N_{123} = M_1 \times M_2 \times M_3$,
then $N_{(12)3}, N_{123}$ are isomorphic.

Proof. We may divide our proof into six steps.
Step 1: Define $\tau_{(12)3,1} = \pi_{12,1} \circ \pi_{(12)3,12}, \tau_{(12)3,2} = \pi_{12,2} \circ \pi_{(12)3,12}$.
Step 2: Define the unique lift of $\tau_{(12)3,1}, \tau_{(12)3,2}, \pi_{(12)3,3}$ to N_{123} as $\tau_{(12)3,123}$.

Step 3: Define the unique lift of $\pi_{123,1}, \pi_{123,2}$ to N_{12} as $\tau_{123,12}$.
Step 4: Define the unique lift of $\tau_{123,12}, \pi_{123,3}$ to $N_{(12)3}$ as $\tau_{123,(12)3}$.
Step 5: $\tau_{123,(12)3} \circ \tau_{(12)3,123}$ is the unique lift $id_{N_{(12)3}}$ of $\pi_{(12)3,12}, \pi_{(12)3,3}$ to $N_{(12)3}$.
Step 6: $\tau_{(12)3,123} \circ \tau_{123,(12)3}$ is the unique lift $id_{N_{123}}$ of $\pi_{123,1}, \pi_{123,2}, \pi_{123,3}$ to N_{123}.
Quod. Erat. Demonstrandum. □

Example 1.17. Let $(G_\mu)_{\mu\in J}, H$ be Abelian groups.
H is the product group of $(G_\mu)_{\mu\in J}$ iff H is the $\mathbb{Z}$-product module of $(G_\mu)_{\mu\in J}$.

Definition 1.18. (**Direct Sum Module**)
Let $(M_\mu)_{\mu\in J}, N$ be R-modules.
If for some R-linear maps $(\iota_\mu : M_\mu \to N)_{\mu\in J}$,
for all R-linear maps $(f_\mu : M_\mu \to K)_{\mu\in J}$,
for some unique R-linear map $g : N \to K$, $(g \circ \iota_\mu = f_\mu)_{\mu\in J}$,
then $N = \bigoplus_{\mu\in J} M_\mu$ is a direct sum module of $M_1, \cdots, M_k$.

Proposition 1.19. Let $(M_\mu)_{\mu\in J}$ be R-modules, and N be the collection of all map $m : J \to \bigcup_{\mu\in J} M_\mu$ with each $m(\mu) \in M_\mu$ and finitely many $m(\mu) \neq 0$. If:

$$\forall m, n \in N, (m+n)(\mu) = m(\mu) + n(\mu)$$
$$\forall r \in R, \forall m \in N,\ (r * m)(\mu) = r * m(\mu)$$

Then $N = \bigoplus_{\mu\in J} M_\mu$ is a direct sum module of $(M_\mu)_{\mu\in J}$.

Proof. For some R-linear maps $\left(\iota_\mu : M_\mu \to N, m \mapsto n(\nu) = \begin{Bmatrix} m & \text{if} & \nu = \mu; \\ 0 & \text{if} & \nu \neq \mu; \end{Bmatrix}\right)_{\mu\in J}$,
for all R-linear maps $(f_\mu : M_\mu \to K)_{\mu\in J}$,
for some unique R-linear map $g : N \to K, g(m) = \sum_{\mu\in J} f_\mu(m(\mu))$, $(g \circ \iota_\mu = f_\mu)_{\mu\in J}$.
Quod. Erat. Demonstrandum. □

Proposition 1.20. Let $(M_\mu)_{\mu\in J}$ be R-modules.
If $N, \overline{N}$ are coproduct modules of $(M_\mu)_{\mu\in J}$,
then $N, \overline{N}$ are isomorphic.

Proof. We may divide our proof into four steps.
Step 1: Define the unique gluing of $(\iota_\mu)_{\mu\in J}$ to $\overline{N}$ as $\jmath$.
Step 2: Define the unique gluing of $(\bar\iota_\mu)_{\mu\in J}$ to N as $\bar\jmath$.
Step 3: $\jmath \circ \bar\jmath$ is the unique gluing id_N of $(\iota_\mu)_{\mu\in J}$ to N.
Step 4: $\bar\jmath \circ \jmath$ is the unique gluing $id_{\overline{N}}$ of $(\bar\iota_\mu)_{\mu\in J}$ to $\overline{N}$.
Quod. Erat. Demonstrandum. □

Proposition 1.21. Let M_1, M_2 be R-modules.
If $N_{12} = M_1 \oplus M_2, N_{21} = M_2 \oplus M_1$,
then N_{12}, N_{21} are isomorphic.

Proof. We may divide our proof into four steps.
Step 1: Define the unique gluing of $\iota_{2,12}, \iota_{1,12}$ to N_{21} as $\jmath_{21,12}$.
Step 2: Define the unique gluing of $\iota_{1,21}, \iota_{2,21}$ to N_{12} as $\jmath_{12,21}$.
Step 3: $\jmath_{21,12} \circ \jmath_{12,21}$ is the unique gluing $id_{N_{12}}$ of $\iota_{1,12}, \iota_{2,12}$ to N_{12}.
Step 4: $\jmath_{12,21} \circ \jmath_{21,12}$ is the unique gluing $id_{N_{21}}$ of $\iota_{2,21}, \iota_{1,21}$ to N_{21}.
Quod. Erat. Demonstrandum. □

Proposition 1.22. Let M_1, M_2, M_3 be R-modules.
If $N_{12} = M_1 \oplus M_2, N_{(12)3} = N_{12} \oplus M_3, N_{123} = M_1 \oplus M_2 \oplus M_3$,
then $N_{(12)3}, N_{123}$ are isomorphic.

Proof. We may divide our proof into six steps.
Step 1: Define the unique gluing of $\iota_{1,123}, \iota_{2,123}$ to N_{12} as $\jmath_{12,123}$.
Step 2: Define the unique gluing of $\jmath_{12,123}, \iota_{3,123}$ to $N_{(12)3}$ as $\jmath_{(12)3,123}$.
Step 3: Define $\jmath_{1,(12)3} = \iota_{12,(12)3} \circ \iota_{1,12}, \jmath_{2,(12)3} = \iota_{12,(12)3} \circ \iota_{2,12}$.
Step 4: Define the unique gluing of $\jmath_{1,(12)3}, \jmath_{2,(12)3}, \iota_{3,(12)3}$ to N_{123} as $\jmath_{123,(12)3}$.
Step 5: $\jmath_{123,(12)3} \circ \jmath_{(12)3,123}$ is the unique gluing $id_{N_{(12)3}}$ of $\iota_{12,(12)3}, \iota_{3,(12)3}$ to $N_{(12)3}$.
Step 6: $\jmath_{(12)3,123} \circ \jmath_{123,(12)3}$ is the unique gluing $id_{N_{123}}$ of $\iota_{1,123}, \iota_{2,123}, \iota_{3,123}$ to N_{123}.
Quod. Erat. Demonstrandum. □

Example 1.23. Let $(G_\mu)_{\mu \in J}, H$ be Abelian groups.
H is the coproduct group of $(G_\mu)_{\mu \in J}$ iff H is the $\mathbb{Z}$-coproduct module of $(G_\mu)_{\mu \in J}$.

Definition 1.24. (**Quotient Module**)
Let M be a R-module with a R-submodule I.
Define the collection M/I of all I-cosets as the R-quotient module of M over I.

Example 1.25. Let M be a R-module with a R-submodule I.
M/I is a R-module:

$$\begin{aligned} \forall m+I, n+I \in M/I, m+I+n+I &= m+n+I \\ \forall m+I \in M/I, \forall r \in R, \quad r*(m+I) &= r*m+I \end{aligned}$$

Example 1.26. Let M be a R-module with a R-submodule I.
For some R-linear map $\pi : M \to M/I, m \mapsto m + I$,
for all R-linear map $f : M \to N$ with $f|_I = 0$,
for some unique R-linear map $g : M/I \to N, m + I \mapsto f(m)$, $g \circ \pi = f$.

Example 1.27. Let $f : M \to N$ be R-linear.
$g : M/\mathbf{Ker}(f) \to N, m + \mathbf{Ker}(f) \mapsto f(m)$ is an embedding.

Example 1.28. Let M be a R-module with R-submodules N, I.
$(N + I)/I, N/(N \cap I)$ are isomorphic.

Example 1.29. Let M be a R-module with R-submodules I, J.
$(M/J)/(I/J), M/I$ are isomorphic.

Example 1.30. Let M be a R-module with a R-submodule I.
The map that sends every R-submodule N of M containing I to the R-submodule N/I of M/I is bijective.

Definition 1.31. (**Annihilator**)
Let M be a R-module with subset S.
Define the R-annihilator of S as $\mathbf{Ann}_R(S) = \{r \in R : r * S = \{0\}\}$.

Example 1.32. Let G be an Abelian group with subset S.
$\mathbf{Ann}_{\mathbb{Z}}(S) = \mathbf{Ord}_G(S)\mathbb{Z}$.

Example 1.33. Let R be a ring with subset S.
If $1 \in S$, then $\mathbf{Ann}_R(S) = \{0\}$.

Definition 1.34. (**Minimal Polynomial**)
Let M be a R-module with subset S, and $f : M \to M$ be R-linear.
If for some $g(x) \in R[x]$, $\mathbf{Ann}_{R[x]}(S_f) = g(x)R[x]$,
then define the minimal polynomial of f on S as $g(x)$.

Definition 1.35. (**Torsion**)
Let M be a R-module.
(1) If a subset S of M satisfies $\mathbf{Ann}_R(S) \neq \{0\}$, then S is R-torsioned.
(2) If M has no nonzero torsioned subset, then M is R-torsion-free.

Example 1.36. Let R be a ring.
(1) A nonzero subset S of R is R-torsioned iff S is a zero divisor in R.
(2) R is R-torsion-free iff R is an integral domain.

2 Generating R-module

Definition 2.1. (**Spanning Set**)
Let M be a R-module.
(1) If S is a subset of M with $R * S = M$, then M is R-spanned by S.
(2) If M is R-spanned by some finite subset, then M is finitely R-spanned.
(3) If every R-submodule of M is finitely R-spanned, then M is R-Noetherian.

Example 2.2. Let R be a ring.
R is R-spanned by $\{1\}$.

Example 2.3. Let $R = \mathbb{C}[x_1, x_2, x_3, \cdots], I = x_1R + x_2R + x_3R + \cdots$.
For any finite subset S of I, for some $k \geq 1$, $SR \subseteq x_1R + \cdots + x_kR \subsetneq I$.

Proposition 2.4. Let M be a R-module with a R-submodule N.
If M is R-Noetherian, then N is R-Noetherian.

Proof. It suffices to notice that every R-submodule K of N is a R-submodule of M. Quod. Erat. Demonstrandum. □

Example 2.5. Let M be a R-module with a R submodule I.
If M is R-spanned by S, then M/I is R-spanned by S/I.

Proposition 2.6. Let M be a R-module with a R-submodule I.
If M is R-Noetherian, then M/I is R-Noetherian.

Proof. It suffices to notice that every submodule N/I of M/I pullbacks to a submodule N of M. Quod. Erat. Demonstrandum. □

Example 2.7. Let M be a R-module with subsets S, T and a R-submodule I.
If $I, M/I$ are R-spanned by $S, T/I$, then M is R-spanned by $S \cup T$.

Proposition 2.8. Let M be a R-module with subsets S, T and a R-submodule I. If $I, M/I$ are R-Noetherian, then M is R-Noetherian.

Proof. It suffices to notice that every submodule N of M corresponds to submodules $N \cap I, N/(N \cap I) \cong (N+I)/I$ of $I, M/I$. Quod. Erat. Demonstrandum. $\square$

Example 2.9. Let M_μ be R-modules with product module N. If each M_μ is R-spanned by m_{μ,s_μ}, then N is R-spanned by $n_{\mu,s_\mu}(\nu) = \begin{Bmatrix} m_{\mu,s_\mu} & \text{if} & \nu = \mu; \\ 0 & \text{if} & \nu \neq \mu; \end{Bmatrix}$ iff there is finitely many nonzero M_μ.

Example 2.10. Let M_μ be R-modules with direct sum module N. If each M_μ is R-spanned by m_{μ,s_μ}, then N is R-spanned by $n_{\mu,s_\mu}(\nu) = \begin{Bmatrix} m_{\mu,s_\mu} & \text{if} & \nu = \mu; \\ 0 & \text{if} & \nu \neq \mu; \end{Bmatrix}$.

Proposition 2.11. Let M_1, M_2 be R-modules.
If M_1, M_2 are R-Noetherian, then $M_1 \oplus M_2$ is R-Noetherian.

Proof. It suffices to notice that $(M_1 \oplus M_2)/M_1 \cong M_2$.
Quod. Erat. Demonstrandum. $\square$

Proposition 2.12. If R is R-Noetherian, then $R[x]$ is $R[x]$-Noetherian.

Proof. For all ideal $I[x]$ of $R[x]$, consider the following set:

$$I = \{a_m \in R : a_m x^m \cdots \in I[x]\}$$

Since $(a_m + b_n)x^{m+n} \cdots = x^n(a_m x^m \cdots) + x^m(b_n x^n \cdots)$, I is closed under addition.
Since $I[x]$ contains 0, I contains 0.
Since $\lambda a_m x^m \cdots = \lambda(a_m x^m \cdots)$, I is closed under scalar multiplication.
Since R is Noetherian, I is finitely generated. WLOG, assume that $I = a_m R + b_n R + c_k R, m \leq n \leq k$. By construction, every $f(x) \in I[x]$ can be reduced to $p(x)a(x) + q(x)b(x) + r(x)c(x) + s(x)$, where $\deg s(x) < k$, so $a(x), b(x), c(x), 1, \cdots, x^{k-1}$ generates $I[x]$. Quod. Erat. Demonstrandum. $\square$

Proposition 2.13. Let R be a ring, $I_1, \cdots, I_k$ be pairwise coprime ideals of R, and $I = I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$. The map below is a ring isomorphism:

$$\widetilde{\pi} : \frac{R}{I} \to \frac{R}{I_1} \oplus \cdots \oplus \frac{R}{I_k}, r + I \mapsto (r + I_1, \cdots, r + I_k)$$

Proof. Define the maps below:

$$\pi_1 : R \to \frac{R}{I_1}, r \mapsto r + I_1, \cdots, \pi_k : R \to \frac{R}{I_k}, r \mapsto r + I_k, \pi = \pi_1 \oplus \cdots \oplus \pi_k$$

Step 1: Since $\pi_1, \cdots, \pi_k$ are ring homomorphisms, π is a ring homomorphism.
Step 2: Since $\mathbf{Ker}(\pi_1) = I_1, \cdots, \mathbf{Ker}(\pi_k) = I_k$, $\mathbf{Ker}(\pi) = I$.
Step 3: Define $J_1 = I_2 \cdots I_{k-1} I_k, \cdots, J_k = I_1 I_2 \cdots I_{k-1}$.
Since $I_1 + J_1 = \cdots = I_k + J_k = R$, some $i_1 + j_1 = \cdots = i_k + j_k = 1$,
so every $(r_1 + I_1, \cdots, r_k + I_k)$ has a preimage $r_1 j_1 + \cdots + r_k j_k$.
Quod. Erat. Demonstrandum. $\square$

Definition 2.14. (**Linearly Independent Set**)
Let M be a R-module.
(1) If S is a subset of M with $R * S \cong R^S$, then S is R-linearly independent.
(2) If a linearly independent subset S R-spans M, then S is a R-basis of M.
(3) If M has a R-basis, then M is R-free.

Example 2.15. Let M be a R-module.
M has a maximal R-linearly independent set S.

Example 2.16. $\{2\}$ is a maximal $\mathbb{Z}$-linearly independent set in $\mathbb{Z}$,
but $\mathbb{Z}$ is not $\mathbb{Z}$-spanned by $\{2\}$.

Example 2.17. Let R be a ring with ideal I.
I is R-free iff I is principal.

Proposition 2.18. Let R be a field, and M be a R-module with maximal R-linearly independent set S. M is R-spanned by S.

Proof. For all $m \in M$, if $m \in S$, then $m = 1 * m$ is R-spanned by S.
If $m \notin S$, then S is linearly independent while $S \cup \{m\}$ is linearly dependent.
For some $r_1, \cdots, r_k, r \in R$ with $r \neq 0$, for some distinct $m_1, \cdots, m_k \in S$,
$r_1 * m_1 + \cdots + r_k * m_k + r * m = 0$, so $m = -\frac{r_1}{r} * m_1 - \cdots - \frac{r_k}{r} * m_k \in R * S$.
Quod. Erat. Demonstrandum. $\square$

Proposition 2.19. Let R be a ring, $I_1, \cdots, I_k$ be ideals of R contained in a common maximal ideal I of R. The R-spanning set below is minimal:

$$\{(1 + I_1, I_2, \cdots, I_{k-1}, I_k), \cdots, (I_1, I_2, \cdots, I_{k-1}, 1 + I_k)\} \subseteq \frac{R}{I_1} \oplus \cdots \oplus \frac{R}{I_k}$$

Proof. It suffices to notice that the $\frac{R}{I}$-spanning set below is minimal:

$$\{(1 + I, I, \cdots, I, I), \cdots, (I, I, \cdots, I, 1 + I)\} \subseteq \left(\frac{R}{I}\right)^k$$

Quod. Erat. Demonstrandum. □

3 Classifying R-module

Definition 3.1. (**Invariant Ideal**)
Let R be a ring, and $A \in \mathbf{M}_{\mu,\nu}(R)$.
Define the σ^{th} invariant ideal $I_\sigma(A)$ of A
as the ideal generated by all $\sigma * \sigma$ minor a of A.

Definition 3.2. (**Invariant Factor**)
Let R be a principal ideal domain, and $A \in \mathbf{M}_{\mu,\nu}(R)$.
If $I_\sigma(A) = i_\sigma(A)R, I_{\sigma-1}(A) = i_{\sigma-1}(A)R$ are nonzero,
then define the σ^{th} invariant factor $d_\sigma(A)$ of A as $\frac{i_\sigma(A)}{i_{\sigma-1}(A)}$.

Proposition 3.3. Let R be a principal ideal domain, and $A \in \mathbf{M}_{\mu,\nu}(R)$.
For some $P \in \mathbf{GL}_\mu(R), Q \in \mathbf{GL}_\nu(R)$:

$$PAQ = \begin{pmatrix} d_1(A) & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & d_\sigma(A) & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Proof. It suffices to find P, Q, such that the $(1,1)^{\text{th}}$ entry of PAQ divides the others.
Step 1: By performing the following type of row operation, we may refine the $(1,1)^{\text{th}}$ entry of A, such that it divides the 1^{st} column of A:

$$\begin{pmatrix} x_{11} & x_{21} \\ -\frac{a_{21}}{g_{11,21}} & \frac{a_{11}}{g_{11,21}} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} g_{11,21} & * \\ 0 & * \end{pmatrix}, \text{ where } g_{11,21} = \mathbf{GCD}_R(a_{11}, a_{21})$$

Step 2: By performing the following type of column operation, we may refine the $(1,1)^{\text{th}}$ entry of A, such that it divides the 1^{st} row of A:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_{11} & -\frac{a_{12}}{g_{11,12}} \\ x_{12} & \frac{a_{11}}{g_{11,12}} \end{pmatrix} = \begin{pmatrix} g_{11,12} & 0 \\ * & * \end{pmatrix}, \text{ where } g_{11,12} = \mathbf{GCD}_R(a_{11}, a_{12})$$

Step 3: Consider the following ascending chain of principal ideals:

$$a_{11}^{(1)}R \overset{\text{step 1}}{\subseteq} a_{11}^{(2)}R \overset{\text{step 2}}{\subseteq} a_{11}^{(3)}R \overset{\text{step 1}}{\subseteq} a_{11}^{(4)}R \overset{\text{step 2}}{\subseteq} \cdots$$

As R is a principal ideal domain, this chain stablizes, so we obtain another representa-

tive PAQ of A, such that its $(1,1)^{\text{th}}$ entry divides both the 1^{st} column and the 1^{st} row.
Step 4: By performing the following type of row operation, we may clear the 1^{st} column while fixing 1^{st} row:

$$\begin{pmatrix} 1 & 0 \\ -\frac{a_{21}}{a_{11}} & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ 0 & * \end{pmatrix}, \text{ where } a_{11}|a_{21}$$

Step 5: By performing the following type of column operation, we may clear the 1^{st} row while fixing the 1^{st} column:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & -\frac{a_{12}}{a_{11}} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ a_{21} & * \end{pmatrix}, \text{ where } a_{11}|a_{12}$$

Step 6: By performing the following types of mixed operations and then repeat step 1-4, we may refine the $(1,1)^{\text{th}}$ entry of A, such that it divides a particular entry:

$$\begin{pmatrix} 1 & x_{22} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} x_{11} & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} g_{11,22} & -a_{11} \\ a_{22} & 0 \end{pmatrix}, \text{ where } g_{11,22} = \mathbf{GCD}_R(a_{11}, a_{22})$$
$$\begin{pmatrix} x_{11} & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x_{22} & 1 \end{pmatrix} = \begin{pmatrix} g_{11,22} & a_{22} \\ -a_{11} & 0 \end{pmatrix}, \text{ where } g_{11,22} = \mathbf{GCD}_R(a_{11}, a_{22})$$

Step 7: Consider the following ascending chain of principal ideals:

$$a_{11}^{(1)}R \overset{\text{step } 6}{\subseteq} a_{11}^{(2)}R \overset{\text{step } 6}{\subseteq} a_{11}^{(3)}R \overset{\text{step } 6}{\subseteq} a_{11}^{(4)}R \overset{\text{step } 6}{\subseteq} \cdots$$

As R is a principal ideal domain, this chain stabilizes, so we obtain another representative PAQ of A, such that its $(1,1)^{\text{th}}$ entry divides every entry, so it is $d_1(A)$. We proceed with the remaining $(\sigma-1)*(\sigma-1)$ block. Quod. Erat. Demonstrandum. □

Proposition 3.4. Let R be a principal ideal domain,
and M be a μ-dimensional R-module with R-submodule N.
(1) For some R-basis $\{m_1, \cdots, m_\mu\}$ of M,
for some nonzero ascending chain $\{d_1, \cdots, d_\nu\}$ in R,
$\{d_1 * m_1, \cdots, d_\nu * m_\nu\}$ is a R-basis of N.
(2) For all R-bases $\{m_1, \cdots, m_\mu\}, \{m'_1, \cdots, m'_\mu\}$ of M,
for all nonzero ascending chains $\{d_1, \cdots, d_\nu\}, \{d'_1, \cdots, d'_{\nu'}\}$ in R,
if $\{d_1 * m_1, \cdots, d_\nu * m_\nu\}, \{d'_1 * m_1, \cdots, d'_{\nu'} * m_{\nu'}\}$ are R-bases of N,
then $\nu = \nu', d_1 \sim d'_1, d_2 \sim d'_2, \cdots$.

Proof. We may divide our proof into two steps.
Step 1: As R is a principal ideal domain, R is R-Noetherian, so M is R-Noetherian,

and N is the image of a R-linear map from some σ-dimensional R-module K to M:

$$B = P \circ \begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & d_\nu & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \circ Q$$

Assume that the columns of P are $\{m_1, \cdots, m_\mu\}$.
As $P \in \mathbf{GL}(M)$, $\{m_1, \cdots, m_\mu\}$ is a R-basis of M.
As $Q \in \mathbf{GL}(K)$ and $d_1, \cdots, d_\nu$ are nonzero, $\{d_1 * m_1, \cdots, d_\nu * m_\nu\}$ is a R-basis of N.
Step 2: As $\{m_1, \cdots, m_\mu\}, \{m'_1, \cdots, m'_\mu\}$ are R-bases of M,
for some $S \in \mathbf{GL}(M)$, $m'_1 = Sm_1, m'_2 = Sm_2, \cdots$.
As $\{d_1 * m_1, \cdots, d_\nu * m_\nu\}, \{d'_1 * m'_1, \cdots, d'_{\nu'} * m'_{\nu'}\}$ are R-bases of N,
$\nu = \nu'$, and for some $T \in \mathbf{GL}(N)$, $d'_1 * m'_1 = Td_1 * m_1, d'_2 * m'_2 = Td_2 * m_2, \cdots$.
As $d'_1 * Sm_1 = Td_1 * m_1, d'_2 * Sm_2 = Td_2 * m_2, \cdots$, $d_1 \sim d'_1, d_2 \sim d'_2, \cdots$.
Quod. Erat. Demonstrandum. □

Definition 3.5. (**Invariant Ideal**)
Let R be a ring, and M be a R-module minimally generated by μ elements.
Define the σ^{th} invariant ideal $I_\sigma(M)$ of M as the ideal generated by all element a such that $a * M$ is generated by at most $\mu - \sigma$ elements.

Definition 3.6. (**Invariant Factor**)
Let R be a principal ideal domain, and M be a R-module minimally generated by μ elements. If $I_\sigma(M) = d_\sigma(M)R$ is nonzero, then define the σ^{th} invariant factor of M as $d_\sigma(M)$.

Proposition 3.7. Let R be a principal ideal domain with an irreducible element p, and $A \in \mathbf{M}_{\sigma,\mu}(R)$ be a multiple of p.

$$d_\tau(A) = d_\tau\left(\frac{R^\mu}{\mathbf{Im}(A)}\right)$$

Proof. As $d_1(A)R, \cdots, d_\nu(A)R, \{0\}, \cdots, \{0\}$ are contained in the same maximal ideal pR of R, $\frac{R^\mu}{\mathbf{Im}(A)} \cong \frac{R}{d_1(A)R} \oplus \cdots \oplus \frac{R}{d_k(A)R} \oplus \frac{R}{\{0\}} \oplus \cdots \oplus \frac{R}{\{0\}}$ is minimally generated by μ elements. As a consequence, $a * \frac{R^\mu}{\mathbf{Im}(A)} \cong \frac{aR}{d_1(A)R} \oplus \cdots \oplus \frac{aR}{d_k(A)R} \oplus \frac{aR}{\{0\}} \oplus \cdots \oplus \frac{aR}{\{0\}}$ is generated by at most $\mu - \tau$ elements iff $d_\tau(A)$ divides a. Quod. Erat. Demonstrandum. □

Example 3.8. Let R be a principal ideal domain,
and M be a R-module minimally generated by μ elements.
(1) For some nonzero, nonunit ascending chain $\{d_1, \cdots, d_\nu\}$ in R,
for some $\mu \geq \nu$, $M \cong \frac{R}{d_1 R} \oplus \cdots \oplus \frac{R}{d_\nu R} \oplus R^{\mu-\nu}$.
(2) For all nonzero, nonunit ascending chains $\{d_1, \cdots, d_\nu\}, \{d'_1, \cdots, d'_{\nu'}\}$ in R,
for all $\mu \geq \nu, \mu' \geq \nu'$, if $M \cong \frac{R}{d_1 R} \oplus \cdots \oplus \frac{R}{d_\nu R} \oplus R^{\mu-\nu} \cong \frac{R}{d'_1 R} \oplus \cdots \oplus \frac{R}{d'_{\nu'} R} \oplus R^{\mu'-\nu'}$,
then $\nu = \nu', d_1 \sim d'_1, d_2 \sim d'_2, \cdots, \mu = \mu'$.

Example 3.9. Let R be a principal ideal domain,
and M be a R-module minimally generated by μ elements.
(1) For some irreducible elements $\{p_1, \cdots, p_k\}$ in R,
for some $\{n_{1,1} \geq \cdots \geq n_{1,\nu_1}, \cdots, n_{k,1} \geq \cdots \geq n_{k,\nu_k}\}$,
for some $\mu \geq \nu = \nu_1 + \cdots + \nu_k$,
$M \cong \left(\frac{R}{p_1^{n_{1,1}} R} \oplus \cdots \oplus \frac{R}{p_1^{n_{1,\nu_1}} R}\right) \oplus \cdots \oplus \left(\frac{R}{p_k^{n_{k,1}} R} \oplus \cdots \oplus \frac{R}{p_k^{n_{k,\nu_k}} R}\right) \oplus R^{\mu-\nu}$.
(2) For all irreducible elements $\{p_1, \cdots, p_k\}, \{p'_1, \cdots, p'_{k'}\}$ in R,
for all $\{n_{1,1} \geq \cdots \geq n_{1,\nu_1}, n_{k,1} \geq \cdots \geq n_{k,\nu_k}\}, \{n'_{1,1} \geq \cdots \geq n'_{1,\nu'_1}, n'_{k',1} \geq \cdots \geq n'_{k',\nu'_{k'}}\}$, for all $\mu \geq \nu = \nu_1 + \cdots + \nu_k, \mu' \geq \nu' = \nu'_1 + \cdots + \nu'_{k'}$,
if $M \cong \left(\frac{R}{p_1^{n_{1,1}} R} \oplus \cdots \oplus \frac{R}{p_1^{n_{1,\nu_1}} R}\right) \oplus \cdots \oplus \left(\frac{R}{p_k^{n_{k,1}} R} \oplus \cdots \oplus \frac{R}{p_k^{n_{k,\nu_k}} R}\right) \oplus R^{\mu-\nu}$
and $M \cong \left(\frac{R}{{p'}_1^{n'_{1,1}} R} \oplus \cdots \oplus \frac{R}{{p'}_1^{n'_{1,\nu'_1}} R}\right) \oplus \cdots \oplus \left(\frac{R}{{p'}_{k'}^{n'_{k',1}} R} \oplus \cdots \oplus \frac{R}{{p'}_{k'}^{n'_{k',\nu'_{k'}}} R}\right) \oplus R^{\mu-\nu}$,
then $k = k'$, and up to permutation, $p_1 \sim p'_1, \nu_1 = \nu'_1, n_{1,1} = n'_{1,1}, n_{1,2} = n'_{1,2}, \cdots, p_2 \sim p'_2, \nu_2 = \nu'_2, n_{2,1} = n'_{2,1}, n_{2,2} = n'_{2,2}, \cdots, \mu = \mu'$.

References

[1] H. Ren, “Template for math notes,” 2021.