Case (2). $\exists\ i, i'$ s.t

$r_1 > r_i, \quad r_1' > r_{i'}'$.

Consider $\dfrac{A}{p^{r_1-1}A}$.

Then $LHS \cong \underbrace{\dfrac{\mathbb{Z}}{p\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{p\mathbb{Z}}}_{i}$, $RHS \cong \underbrace{\dfrac{\mathbb{Z}}{p\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{p\mathbb{Z}}}_{i'}$

$\Rightarrow i = i'$.

Then by induction on the maximal p-order of A. we're done. #

Key Lemma: $A \xrightarrow{\phi} A'$ epimorphism of abelian groups.

If A' is free then $\exists\ B \leq A$, s.t

$\phi|_B : B \simeq A'$

and $A = B \oplus \mathrm{Ker}(\phi)$

pf: Let $\{\bar{x}_i\}_{i\in I}$ be a basis of A'.

Take any $x_i \in A$, s.t $\phi(x_i) = \bar{x}_i$.

Set $B = \langle x_i \rangle_{i \in I} \leq A$

Then (i) $A = B + \ker\phi$ and

(ii) $B \cap \ker\phi = 0$.

pf of (i): $\forall x \in A$, $\exists\, n_i \in \mathbb{Z}$, s.t

$$\phi(x) = \sum n_i \overline{x_i} = \sum n_i \phi(x_i)$$

$$= \phi\left(\sum \phi(n_i x_i)\right)$$

$\Rightarrow x - \sum n_i x_i \in \ker\phi$

$\Rightarrow x \in \ker\phi + B$.

pf of (ii): $x \in \ker\phi \cap B$

$$\phi\left(x = \sum n_i x_i\right) = \sum n_i \underset{\overline{x_i}}{\overset{\shortparallel}{\phi(x_i)}} = 0$$

$\Rightarrow n_i = 0 \;\; \forall i$. i.e $x = 0$.

Therefore, (i) + (ii) $\Rightarrow$ $A = B \oplus \ker(\phi)$

It also follows that $\phi|_B : B \simeq A'$

#

Prop 1: $A = \mathbb{Z}\langle S\rangle$. finitely generated free abelian grp.

Then $\forall\, A' \leq A$, one has

(i) A' is again finitely generated, free abelian.

(ii). $r(A') \leq r(A)$.

Pf: (i) Do induction on $|S|$.

$S = \{x_1, \ldots, x_n\}$.

Consider the projection

$$\begin{array}{ccc} \mathbb{Z}\langle S\rangle = \mathbb{Z}\langle x_1\rangle \oplus \cdots \oplus \mathbb{Z}\langle x_n\rangle & \xrightarrow{p_1} & \mathbb{Z}\langle x_1\rangle \\ \cup & & \cup \\ A' & \xrightarrow{\phi \triangleq p_1|_{A'}} & p_1(A') \end{array}$$

$p_1(A') \leq \langle x_1\rangle = \mathbb{Z}$. $\Rightarrow p_1(A')$ is free

Key Lemma $\Rightarrow$ $A' = B' \oplus \mathrm{Ker}(\phi)$, $B' \simeq p_1(A')$ free.

$\mathrm{Ker}(\phi) \leq \mathrm{Ker}\, p_1 = \mathbb{Z}\langle x_2, \ldots x_n\rangle \xRightarrow{\text{by induction}} \mathrm{Ker}(\phi)$ free

$\Rightarrow A'$ free.

(ii) $\mathbb{Z}^{r(A')} \simeq A' \leq A \simeq \mathbb{Z}^{r(A)}$.

Then we get $\mathbb{Z}^{r(A')} \xhookrightarrow{\phi} \mathbb{Z}^{r(A)}$.

$\forall p$ prime number, ψ induces the injection

$$\begin{array}{ccc} \dfrac{\mathbb{Z}^{r(A')}}{p\mathbb{Z}^{r(A')}} & \overset{\bar{\psi}}{\hookrightarrow} & \dfrac{\mathbb{Z}^{r(A)}}{p\mathbb{Z}^{r(A)}} \\ \| & & \| \\ \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\oplus r(A')} & & \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\oplus r(A)} \end{array}$$

$$\Rightarrow \quad p^{r(A')} \leq p^{r(A)} \quad \Rightarrow r(A') \leq r(A).$$

#

Prop 2: A, finitely generated torsion free group (i.e. $A_{tor} = \{0\}$)

Then A is free.

pf: Take a maximal subset of A with the following property

$$\left.\begin{array}{l} n_1 x_1 + \cdots + n_s x_s = 0 \\ n_i \in \mathbb{Z} \end{array}\right\} \Rightarrow n_1 = \cdots = n_s = 0$$

「Compare with the notion of a maximal linearly independent set of vectors in Linear Algebra !」

Set $B = \langle x_1, \ldots, x_s \rangle \leq A$

Clearly, $B \cong \mathbb{Z}^s$ is free.

If $B = A$, we're done.

Otherwise, we take a set of generators

$\{x_1, \dots, x_s, y_1, \dots, y_t\}$ for A.

note, $\forall y_i$, $\exists m_i \in \mathbb{Z}^+$, s.t

$$m_i y_i \in \langle x_1, \dots, x_s \rangle = B$$

Thus, $\exists m \in \mathbb{Z}^+$, s.t

$$m \cdot x \in B, \quad \forall x \in A.$$

Consider the morphism

$$A \xrightarrow{\phi_m} A$$
$$x \longmapsto mx$$

A torsion free $\Rightarrow \ker(\phi_m) = \{0\} \Rightarrow A \cong \mathrm{Im}(\phi_m)$;

$$\mathrm{Im}(\phi_m) = m \cdot A \subseteq B$$

By ~~Key~~ Prop 1, $m \cdot A$ is free. thus A is also free.

#

Proof of Theorem: A, f.g, abelian grp.

Consider $A \xrightarrow{\phi} A/A_{tor}$

Note A/A_{tor} is f.g, and torsion-free.

Pf: if $\bar{x} \in A/A_{tor}$. $m\bar{x} = 0$,

then for $x \in A$, with $\phi(x) = \bar{x}$

$\phi(mx) = m\bar{x} = 0 \Rightarrow m \cdot x \in \operatorname{Ker} \phi = A_{tor}$

$\Rightarrow \exists n \in \mathbb{Z}^+,\ n(mx) = 0 \Rightarrow (n \cdot m)x = 0$

$\Rightarrow x \in A_{tor} \Rightarrow \bar{x} = 0 \in A/A_{tor}$ ⌋

By Prop 2, $\Rightarrow A/A_{tor}$ free

By Key Lemma, $\exists A_{free} \le A$, s.t

$$A = A_{free} \oplus \operatorname{Ker}\phi = A_{free} \oplus A_{tor}$$

$\phi|_{A_{free}} : A_{free} \simeq A/A_{tor}$ which is free.

Thus $A_{tor} \cong A/A_{free}$ is also f.g.

$\Rightarrow A_{tor}$ is a finite abelian #

<u>Theorem of elementary divisor</u> (Improving prop 1).

$A = \mathbb{Z}\langle S\rangle$ is f.g. free abelian.

Then $\forall A' \leq A$, $\exists$ a basis

$\{x_1, \dots, x_s\}$ of A,

and (uniquely determined) natural numbers

$1 \leq m_1 \mid m_2 \mid m_3 \mid \cdots \mid m_t$, $\quad t \leq s$

Such that

A' is freely generated by

$\{m_1x_1, \dots, m_tx_t\}$.

Pf: Consider the set

$\Sigma = \{ n_1 \mid n_1x_1 + \cdots + n_sx_s \in A'$, where $\{x_1, \cdots x_s\}$ is a basis of A (not fixed) $\}$

Let m_1 be the least positive integer in $\Sigma \cap \mathbb{N}$

and $m_1x_1 + n_2x_2 + \cdots + n_sx_s \in A'$

Then $m_1 / n_i \;, i \geq 2$.

Indeed, $\forall i, n_i \in \mathbb{Z}$. This is because

$\{x_i, x_2, \ldots, x_1, \ldots x_s\}$ is again a basis

$\Rightarrow \quad n_i \geq m_1$

$\Rightarrow \quad n_i = q_i \cdot m_1 + r_i, \qquad 0 \leq r_i \leq m_1 - 1$

Thus $\quad n_1 x_1 + n_2 x_2 + \cdots + n_s x_s$

$= m_1 (x_1 + q_2 x_2 + \cdots + q_s x_s) + \; r_2 x_2 + \cdots + r_s x_s$

But $\{x_1 + q_2 x_2 + \cdots + q_s x_s, x_2, \ldots, x_s\}$ is again a basis of

$A. \;\Rightarrow\; r_i \in \mathbb{Z}, \; \forall i.$

$\Rightarrow \quad r_i = 0. \quad \forall i.$

Thus, Set $y_1 = x_1 + q_2 x_2 + \cdots + q_s x_s$.

then $\{y_1, x_2, \ldots, x_s\}$ is a basis of A.

and $m_1 y_1 \in A'$.

$$\mathbb{Z}^{s-1}$$
$$\text{is}$$

Now Consider $\quad A' \cap \cancel{\mathbb{Z}} \langle x_2, \ldots, x_s \rangle \;\leq\; \langle x_2, \ldots x_s \rangle$

$$\|o$$
$$A''$$

Note : $A' = \langle m_1 y_1 \rangle \oplus A''$.

Indeed: $\langle m_1 y_1 \rangle \cap A'' = \{0\}$.

Moreover, $\forall x \in A'$

$$x = n_1 \cancel{y_1} + n_2 x_2 + \cdots + n_s x_s$$

But n_1 / m_1. ($n_1 = m_1 q + r$.

$$x - q(m_1 y_1) = r y_1 + n_2 x_2 + \cdots + n_s x_s \in A')$$

$$\Rightarrow r = 0$$

Thus $x \in \langle m_1 y_1 \rangle + A''$

Now, we induction on the rank of A.

we get ~~a~~ basis $\{y_2, \ldots y_s\}$ of $\langle x_2, \ldots x_s \rangle = \mathbb{Z}^{s-1}$

and $m_2 / m_3 / \cdots / m_t$, such that

$\{m_2 y_2, \ldots, m_t y_t\}$ is a basis of A''.

Thus $\{m_1 y_1, \ldots, m_t y_t\}$ is a basis of A'.

$\{y_1, y_2 \ldots y_t\}$ is a basis of A, and

Note $m_1 / m_2 / m_3 \cdots / m_t$. hold.

Exercise:

(i) Use theorem of elementary divisor gives another proof of the structure theorem of finite generated abelian groups.

(ii) Let $\{m_1, m_2, \cdots m_t\}$, $\{\tilde{m}_1, \cdots \tilde{m}_{\tilde{t}}\}$ be two set of natural numbers with properties.

$$m_i \mid m_{i+1}, \quad \tilde{m}_j \mid \tilde{m}_{j+1}.$$
$$1 \leq i \leq t-1 \qquad 1 \leq j \leq \tilde{t}-1$$

Suppose
$$\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_t\mathbb{Z}} \cong \frac{\mathbb{Z}}{\tilde{m}_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{\tilde{m}_{\tilde{t}}\mathbb{Z}}$$

show that: $t = \tilde{t}$ and

$$m_i = \tilde{m}_i, \quad \forall\ 1 \leq i \leq t.$$

(iii) For a finite abelian group, Provide the transformation law from the set of invariant divisors to the set of elementary divisors, and vice versa.

Remark: The essence of the theorem of elementary divisors is the Gaussian elimination theory, together with euclidean algorithm for integers.