Abel 群

定义. 设 $(G,\cdot)$ 为一个群. 若 $\forall a,b\in G$, $a\cdot b=b\cdot a$, 则称 G 为一个 Abel 群. 此时, "$\cdot$" 经常记为 "$+$".

直积、直和

Recall: 设 $(G,\cdot)$, $(H,\cdot)$ 为群,

$$G\times H=\{(g,h)\mid g\in G,\ h\in H\}.$$

$$(g_1,h_1)\cdot(g_2,h_2):=(g_1g_2,\ h_1\cdot h_2)$$

定义: 设 $(G_\alpha,+)$, $\alpha\in I$, 为一族 abel 群. 定义它们的直积群 (direct product) $\left(\prod_{\alpha\in I}G_\alpha,+\right)$ 如下:

$$\prod_{\alpha\in I}G_\alpha=\{(g_\alpha)_{\alpha\in I}\mid g_\alpha\in G_\alpha,\ \forall\alpha\in I\}.$$

$\forall (g_\alpha),(h_\alpha)\in\prod_{\alpha\in I}G_\alpha$, $(g_\alpha)+(h_\alpha):=(f_\alpha)$ 其中 $\forall\alpha\in I$, $f_\alpha=g_\alpha+h_\alpha$.

若 $|I|$ 为有限集, i.e. 对于有限个 abel 群 $(G_1,+),\cdots,(G_n,+)$,

$(\prod_{i=1}^{n} G_i, +)$ 又记为 $(G_1 \times \cdots \times G_n, +)$

定义（外直和）设 $\{G_\alpha\}_{\alpha\in I}$ 为一族 Abel 群，定义它们的（外）直和

direct sum

$(\bigoplus_{\alpha\in I} G_\alpha, +)$ 如下：

$$\bigoplus_{\alpha\in I} G_\alpha := \left\{ (g_\alpha)_{\alpha\in I} \;\middle|\; g_\alpha \in G_\alpha,\ \forall \alpha\in I,\ g_\alpha \text{ 中只有有限个非零} \right\}.$$

$$\left(\subset \prod_{\alpha\in I} G_\alpha \right).$$

$\forall (g_\alpha), (h_\alpha) \in \bigoplus_{\alpha\in I} G_\alpha$.

$(g_\alpha) + (h_\alpha) := (f_\alpha)$，其中 $f_\alpha = g_\alpha + h_\alpha$，$\forall \alpha \in I$.

注：$\bigoplus_{\alpha\in I} G_\alpha < \prod_{\alpha\in I} G_\alpha$.

注：对于有限个 Abel 群 $G_1, \cdots, G_n$.

$$G_1 \times \cdots \times G_n = G_1 \oplus \cdots \oplus G_n.$$

定义(内直和). 设 G 为一个 Abel 群, $\{G_\alpha\}_{\alpha\in I}$ 为 G 中的一族子群, 称 G 为 $\{G_\alpha\}_{\alpha\in I}$ 的内直和, 若 $\forall g\in G$, g 可唯一地表示为

$$g=\sum_\alpha g_\alpha,$$

其中 $g_\alpha\in G_\alpha$, g_α 中只有有限个非零. 此时, 记

$$G=\bigoplus_{\alpha\in I}G_\alpha.$$

注: (内外直和之关系) 设 G 为 Abel 群, $G=\bigoplus_{\alpha\in I}G_\alpha$ 为内直和分解. 则 G 显然同构于 $G_\alpha,\alpha\in I$ 的外直和.

$$\forall g\in G,\quad g=\sum_\alpha g_\alpha \longmapsto (g_\alpha)_{\alpha\in I}.$$

反之, 设 $\{G_\alpha\}_{\alpha\in I}$ 为一族 Abel 群, $G=\bigoplus_{\alpha\in I}G_\alpha$ 为外直和.

记 $i_\alpha: G_\alpha\to\bigoplus_{\alpha\in I}G_\alpha$ 为典则嵌入, $g\longmapsto i_\alpha(g)=(h_\alpha)$,

其中 $h_\beta=\begin{cases} g, & \text{if } \beta=\alpha \\ 0, & \text{if } \beta\neq\alpha. \end{cases}$ $\quad \underset{\substack{\shortparallel\\ G_\alpha'}}{i_\alpha(G_\alpha)} < \bigoplus_{\alpha\in I}G_\alpha.$

则显然 G 为 $G'_\alpha, \alpha\in I$ 的内直和.

⌜ $\forall g \in G \left(= \bigoplus_{\alpha\in I} G_\alpha\right)$. $g = (g_\alpha)_{\alpha\in I}$,

$$g = \sum_\alpha i_\alpha(g_\alpha).$$

$$\pi_\alpha : \bigoplus_{\alpha\in I} G_\alpha \longrightarrow G_\alpha. \quad (g_\alpha) \longmapsto g_\alpha.$$

$$\pi_\alpha \circ i_\alpha = Id_{G_\alpha}, \quad \pi_\alpha \circ i_\beta = 0, \quad \forall \beta \neq \alpha.$$

$$\pi_\beta(g) = \pi_\beta\left(\sum_\alpha i_\alpha(g_\alpha)\right) = \sum_\alpha \pi_\beta \circ i_\alpha(g_\alpha)$$

$$= \pi_\beta \circ i_\beta(g_\beta) = g_\beta. \quad \forall \beta \in I.$$

$$g = \sum_\alpha i_\alpha(\pi_\alpha(g)).$$

⌟

注：设 G, H 为两个 Abel 群.

$$Hom(G, H) = \{ f: G \to H \mid f \text{ 为群同态} \}.$$

$$+: Hom(G,H) \times Hom(G,H) \longrightarrow Hom(G,H)$$

$$(\varphi, \psi) \longmapsto \varphi + \psi$$

其中 $(\varphi+\psi)(g) := \varphi(g)+\psi(g)$

设 $(G_\alpha, \alpha\in I)$ 为一族 Abel 群，H 为另一个 Abel 群，

$$\mathrm{Hom}\left(\bigoplus_{\alpha\in I} G_\alpha, H\right) \xrightarrow{\varphi} \prod_{\alpha\in I} \mathrm{Hom}(G_\alpha, H)$$

$$f \longmapsto \varphi(f) := (f_\alpha)_{\alpha\in I}$$

其中 $f_\alpha = f\circ i_\alpha$，（$i_\alpha: G_\alpha \to \bigoplus_{\alpha\in I} G_\alpha$ 为典则嵌入）

「φ 为单射显然

φ 为满射：$\forall (f_\alpha)_{\alpha\in I} \in \prod_{\alpha\in I}\mathrm{Hom}(G_\alpha, H)$

定义 $f: \bigoplus_{\alpha\in I} G_\alpha \longrightarrow H$

$$\sum_{\alpha\in I} g_\alpha \longmapsto \sum_{\alpha\in I} f_\alpha(g_\alpha).$$

显然 $f\in \mathrm{Hom}(\bigoplus_{\alpha\in I} G_\alpha, H)$，且 $\varphi(f) = (f_\alpha)_{\alpha\in I}$. 」

$$\therefore \mathrm{Hom}\left(\bigoplus_{\alpha\in I} G_\alpha, H\right) \cong \prod_{\alpha\in I}\mathrm{Hom}(G_\alpha, H)$$

练习：$\mathrm{Hom}(H, \prod_{\alpha\in I} G_\alpha) \not\cong \prod_{\alpha\in I} \mathrm{Hom}(H, G_\alpha)$

定义. 设 $(G, +)$ 为一个 Abel 群. G 称为一个自由Abel群 (free abelian group). 若存在 G 中的一族元素 $\{g_\alpha\}_{\alpha\in J}$, s.t. $\{g_\alpha\}_{\alpha\in J}$ 为 G 的一组基 (basis), i.e. $\forall g\in G$, $\exists!\, n_\alpha\in\mathbb{Z}$, $\forall \alpha\in J$, s.t.

$$g = \sum_{\alpha\in J} n_\alpha g_\alpha$$

其中 $n_\alpha, \alpha\in J$ 中只有限个 n_α 非零.

注：设 G 为一个 free abel group, $\{g_\alpha\}_{\alpha\in J}$ 为 G 的一组基. $\langle g_\alpha\rangle$ 为一个无限循环群, $\forall \alpha\in J$,

$$n\cdot g_\alpha = 0 = 0\cdot g_\alpha \Rightarrow n = 0.$$

由 free abelian group 之定义. $\Rightarrow G = \bigoplus_{\alpha\in J} \langle g_\alpha\rangle$

反之也对，设 G 中有一族无限循环群 $\langle g_\alpha \rangle$，$\alpha \in I$，使

$$G = \bigoplus_{\alpha \in I} \langle g_\alpha \rangle .$$

$\{g_\alpha\}_{\alpha \in I}$ 显然为 G 的一组基。$\Rightarrow$ G 为 free abelian group.

命题：设 G 为 abel group，则下列叙述等价：

(1) G 为 free abelian group.

(2) G 为若干个无限循环群的内直和。

(3) G 同构于若干个整数群 $\mathbb{Z}$ 的外直和。

Pf. (1) $\Leftrightarrow$ (2) 已证。

只需证 (2) $\Leftrightarrow$ (3)，而这由内外直和之关系显然 #.

设 G 为自由 Abel 群，$G \xrightarrow[\cong]{u} \bigoplus_{\alpha \in I} \mathbb{Z}$，记 $e_\alpha = i_\alpha(1) \in \bigoplus_{\alpha \in I} \mathbb{Z}$.

其中 $i_\alpha : \mathbb{Z} \longrightarrow \bigoplus_{\alpha \in I} \mathbb{Z}$，（换言之，$e_\alpha = (g_\alpha)_{\alpha \in I} \in \bigoplus_{\alpha \in I} \mathbb{Z}$，其中 $g_\beta = \begin{cases} 1, & \text{if } \beta = \alpha \\ 0, & \text{else} \end{cases}$）

记 ε_α 为 e_α 在同构 $G \xrightarrow[\cong]{u} \bigoplus_{\alpha\in I}\mathbb{Z}$ 下的像 $\left(\varepsilon_\alpha = u^{-1}(e_\alpha)\right)$.

则 $\{\varepsilon_\alpha\}_{\alpha\in I}$ 为 G 的一组基.

$\forall$ Abel 群 H.

$$
\begin{tikzcd}
\mathrm{Hom}(G,H) \arrow[dd, "\cong"'] & & \mathrm{Hom}\left(\bigoplus_{\alpha\in I}\mathbb{Z},H\right) \arrow[ll, "\circ u"', "\cong"] \arrow[d, "\varphi", "\cong"'] \\
& & \prod_{\alpha\in I}\mathrm{Hom}(\mathbb{Z},H) \arrow[d, "\cong"] \\
\prod_{\alpha\in I} H \arrow[rr, equal] & & \prod_{\alpha\in I} H
\end{tikzcd}
$$

$$
\begin{tikzcd}
f \arrow[r, mapsto] \arrow[d, mapsto] & f\circ u^{-1} \arrow[d, mapsto] \\
(f(\varepsilon_\alpha))_{\alpha\in I} & (f\circ u^{-1}\circ i_\alpha)_{\alpha\in I} \arrow[d, mapsto] \\
& (f\circ u^{-1}\circ i_\alpha(1))_{\alpha\in I}
\end{tikzcd}
$$

$$f\circ u^{-1}\circ \underline{i_\alpha(1)} = f\circ u^{-1}(e_\alpha) = f(\varepsilon_\alpha).$$

换言之, $\forall$ Abel 群 H, 从集合 $\{\varepsilon_\alpha\}_{\alpha\in I}$ 到 H 的映射可唯一地延拓为从 G 到 H 的群同态.

由一个集合生成的 free abelian group

设 S 为一个集合，将定义由 S 生成的 free abelian group Z，

粗略地，$Z=\left\{\sum_{x\in S} n_x x \,\middle|\, n_x\in\mathbb{Z},\ n_x\text{中只有有限个非零元}\right\}$.

"+" 显然地定义.

严格地：

$$Z:=\{f:S\to\mathbb{Z} \mid \text{只有有限个 } x\in S,\ \text{使 } f(x)\neq 0\}.$$

$$+:\ Z\times Z\longrightarrow Z$$
$$(f,g)\longmapsto f+g.$$

$(Z,+)$ 为一个 Abel 群.

Z 有一组基：$\{\phi_x \mid x\in S\}$. 其中 $\phi_x: S\longrightarrow\mathbb{Z}$，$y\longmapsto\phi_x(y)=\begin{cases}1, & y=x\\ 0, & \text{else}\end{cases}$

为 x 处的特征函数.

$(\forall f \in \mathbb{Z}, \quad f = \sum_{x\in S} f(x)\,\phi_x \,)$.

$\therefore (\mathbb{Z}, +)$ 为一个 free abelian group，称为由 S 生成的自由 Abel 群.

注意 $\{\phi_x \mid x\in S\} \xleftrightarrow{1:1} S$.

$$\phi_x \longleftarrow\!\shortmid\ x$$

常把 $\mathbb{Z}$ 中的元素 $\sum_{x\in S} n_x \phi_x$ 记为 $\sum_{x\in S} n_x\cdot x$.

$\mathbb{Z}$ 的 universal property：

记 $i: S \to \mathbb{Z}$, $x \mapsto \phi_x$ 为典型嵌入. 则 $\forall$ Abel 群 H, 以及 $f: S\to H$, $\exists!$ 群同态 $\hat{f}: \mathbb{Z}\to H$. s.t. $\hat{f}\circ i = f$.

「 $\hat{f}\left(\sum_{x\in S} n_x\cdot x\right) := \sum_{x\in S} n_x f(x)$. 唯一性显然. 」.

设 $\mathbb{Z}'$ 为另一个 Abel 群，$i': S \to \mathbb{Z}'$ 为一个映射，满足：
$\forall$ Abel 群 H，$f: S \to H$，$\exists!$ 群同态 $\hat{f}: \mathbb{Z}' \to H$，s.t.
$\tilde{f} \circ i' = f$.

则 $\mathbb{Z}' \cong \mathbb{Z}$.

注（Free abelian group 的秩）. G 为 free abelian group

设 G 存在一组由有限个元素构成的基 $\{g_1, \cdots, g_n\}$.

设 $\{h_\alpha\}_{\alpha \in I}$ 为另一组基. 则 $\mathrm{card}(I) < +\infty$，且 $\mathrm{card}(I) \leq n$

若 I 为无限集，则可找到 $h_{\alpha_1}, \cdots, h_{\alpha_m}$，$m > n$，$h_{\alpha_i}$ 两两不同.

$$h_{\alpha_i} = \sum_{j=1}^{n} k_i^j g_j, \quad \forall i = 1, \cdots, m.$$

$$\begin{pmatrix} h_{\alpha_1} \\ \vdots \\ h_{\alpha_m} \end{pmatrix} = \underbrace{\begin{pmatrix} k_1^1 & k_1^2 & \cdots & k_1^n \\ \vdots & & \ddots & \vdots \\ k_m^1 & k_m^2 & \cdots & k_m^n \end{pmatrix}}_{=K} \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix},$$

其中 $k_i^j \in \mathbb{Z}$.
$(m > n)$.

$K \in M_{m\times n}(\mathbb{Z}) \subset M_{m\times n}(\mathbb{Q})$.

由线性代数，$\exists (r_1, \cdots, r_m) \in \mathbb{Q}^m \setminus 0$, s.t.

$$(r_1, \cdots, r_m) \cdot K = (0, \cdots, 0).$$

两边乘以 r_i 的分母的一个公倍数，

$\Rightarrow \exists (l_1, \cdots, l_m) \in \mathbb{Z}^m \setminus 0$, s.t.

$$(l_1, \cdots, l_m) \cdot K = (0, \cdots, 0).$$

$$\Rightarrow (l_1, \cdots, l_m) \cdot \begin{pmatrix} h_{\alpha_1} \\ \vdots \\ h_{\alpha_m} \end{pmatrix} = (l_1, \cdots, l_m) \cdot K \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = (0, \cdots, 0)$$

$$\Rightarrow \sum_{i=1}^{m} l_i h_{\alpha_i} = 0 \Rightarrow \mathrm{card}(I) < +\infty.$$

用相同的推理，$\Rightarrow \mathrm{card}(I) \leq n$. ┘

$\Rightarrow \mathrm{card}(I) = n$.

进一步，可以证明：设 G 为 free abelian group，则 G 的任两组基等势。(c.f. GTM 73).

定义：设 G 为 free abelian group，称 G 的任意一组基的势为 G 的秩（rank）.

$\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

定义：设 G 为一个 Abel 群，$g \in G$ 称为是有限阶的，若 $\exists n \in \mathbb{Z}$, s.t. $n \cdot g = 0$，记 $T = \{g \in G \mid g \text{ 为有限阶}\}$. 则 T 为 G 的一个子群，称为 G 的扭子群（torsion subgroup）.

（挠）

若 $T = 0$，则称 G 是无扭的（torsion free）.

注：若 G 为 free abelian group. $\Rightarrow$ G torsion free.

反之 G torsion free $\not\Rightarrow$ G free abelian

「反例：$(\mathbb{Q}, +)$

若 $\mathbb{Q}$ free abelian，则 $\exists$ $\mathbb{Q}$ 的一组基 $\{r_\alpha\}_{\alpha \in I}$，$\Rightarrow |I| > 1$

$\exists \alpha_1, \alpha_2 \in I$，$\alpha_1 \neq \alpha_2$，对于 r_{α_1}，r_{α_2}，

显然 $\exists\, n, m \in \mathbb{Z}$，且 n, m 均不为零，使 $n \cdot r_{\alpha_1} + m \cdot r_{\alpha_2} = 0$.

又由基之定义，必有 $n = m = 0$，矛盾. # 」

下面：分类有限生成的 Abel 群.

设 G 为有限生成的 Abel 群. 不妨设生成元为 $g_1, \cdots, g_n$,

令 $F = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n\text{个}}$，则有自然满同态：

$$\varphi : F \longrightarrow G, \quad \underset{\underset{(0,\cdots,0,\underset{i\text{-th}}{1},0,\cdots,0)}{\|}}{e_i} \longmapsto g_i$$

令 $K = \ker\varphi$. 则： $G \cong F/K$.

Fact: K 也为有限生成的 Abel 群 (Ref. [Atiyah-Macdonald])

「$\mathbb{Z}$ 为 Noetherian, F 为有限生成的 $\mathbb{Z}$-模, $\Rightarrow F$ 为 Noetherian module,

$\Rightarrow K$ 作为 F 的子模也是有限生成 $\mathbb{Z}$-模 $\Rightarrow K$ 有限生成 Abel 群 」

设 K 的一组生成元为：$b_1, \cdots, b_m$.

设 $b_i = (b_{i1}, \cdots, b_{in}) = (b_{i1}, b_{i2}, \cdots, b_{in}) \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$, $i=1,\cdots,m$.

令 $B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} \in M_{m\times n}(\mathbb{Z})$, B 为 $b_1, \cdots, b_m$ 在

F 的基 $e_1, \cdots, e_n$ 下的系数矩阵.

$$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = B \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

$\forall P \in GL(n;\mathbb{Z})$.

$e_1', \cdots, e_n'$ 也为 F 的一组基.

$$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = B \cdot P \cdot \underbrace{P^{-1} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}}_{= \begin{pmatrix} e_1' \\ \vdots \\ e_n' \end{pmatrix}}$$

$$= (B \cdot P) \cdot \begin{pmatrix} e_1' \\ \vdots \\ e_n' \end{pmatrix}$$

故 $B \cdot P$ 为 K 的生成元 $b_1, \cdots, b_m$ 在新基 $e_1', \cdots, e_n'$ 下的系数矩阵.

$\forall Q \in GL(m;\mathbb{Z})$，看 $Q\cdot B$ 之意义：

$$\begin{pmatrix} b_1' \\ \vdots \\ b_m' \end{pmatrix} = Q \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = QB \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

$\because Q$ 可逆，$\therefore$ $b_1', \cdots, b_m'$ 也为 K 的一组生成元。

$Q\cdot B$：K 的新的生成元 $b_1', \cdots, b_m'$ 在基 $e_1, \cdots, e_n$ 下的系数矩阵。

一般地，$\forall P \in GL(n;\mathbb{Z})$，$Q \in GL(m;\mathbb{Z})$

$Q\cdot B\cdot P$：为 K 的某组生成元在 F 的某组基下的矩阵表示。

Claim：存在 $P \in GL(n;\mathbb{Z})$，$Q \in GL(m;\mathbb{Z})$，使

$$Q\cdot B\cdot P = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \end{pmatrix}，$$ 其中 $d_i \in \mathbb{Z}_{>0}$，且 $d_1 | d_2 | \cdots | d_k$.

$\Big(\Rightarrow \exists F$ 的一组基 $e_1', \cdots, e_n'$，s.t. K 有生成元 $d_1 e_1', \cdots, d_k e_k'$.

$\Rightarrow G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-k\text{个}} \Big)$

Claim 之证明: (Ref. 张贤科"高等代数")

事实上, P, Q 可取为如下三种称为初等方阵之乘积:

(i) $$P_{ij}=\begin{bmatrix}1&&&&&&\\&\ddots&&&&&\\&&0&\cdots&1&&\\&&\vdots&\ddots&\vdots&&\\&&1&\cdots&0&&\\&&&&&\ddots&\\&&&&&&1\end{bmatrix}\begin{array}{l} \\ \\ \leftarrow i\\ \\ \leftarrow j\\ \\ \\ \end{array}$$

(ii) $$P_i(c)=\begin{bmatrix}1&&&&\\&\ddots&&&\\&&c&&\\&&&\ddots&\\&&&&1\end{bmatrix}\begin{array}{l} \\ \\ \leftarrow i\\ \\ \\ \end{array}$$, c 为 $\mathbb{Z}$ 中单位, i.e. $c=\pm1$.

(iii) $$P_{ij}(a)=\begin{array}{cc}\begin{bmatrix}1&&a&&\\&\ddots&&&\\&&\ddots&&\\&&&\ddots&\\&&&&1\end{bmatrix}&\begin{array}{l}\leftarrow i\\ \\ \\ \\ \\ \end{array}\\ \begin{array}{ccccc}&&\uparrow j&&\end{array}&\end{array}$$, $a\in\mathbb{Z}$.

「右乘 P_{ij}: 交换第 i、j 列.

右乘 $P_i(c)$: 第 i 列乘以 c

右乘 $P_{ij}(a)$: 把第 i 列乘以 a 后加到第 j 列上去.

$\Bigg\}$ 初等列变换.

左乘 (i), (ii), (iii) $\longrightarrow$ 初等行变换 」

我们将证：$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}$ 通过$\underbrace{\text{初等行、列变换}}_{\text{初等变换}}$可

变为 $\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \end{pmatrix}$，$d_i \in \mathbb{Z}_{>0}$，$d_1 | d_2 | \cdots | d_k$ 的样子。

Step 1. 通过初等变换，使 $b_{11} > 0$。

Step 2. 通过初等变换，使 b_{11} 整除第一行、第一列中其它元素。

「若 $b_{11} \nmid b_{1i}$，$i \neq 1$。 $\underline{b_{1i} = r \cdot b_{11} + s}$，$0 < s < b_{11}$。

把第1列乘 $-r$ 加到第i列，交换第1列与第i列。则

B 变为：$\begin{pmatrix} s & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots \end{pmatrix}$ $0 < s < b_{11}$，

$\because \operatorname{card}\{n \in \mathbb{Z} \mid 0 < n < b_{11}\} < +\infty$，$\therefore$ 重复上面的步骤，总

可把B变为：$\begin{pmatrix} d_1 & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots \end{pmatrix}$，其中 d_1 整除第一列、第一行中

其它元素。」

Step 3. 通过把第1列(行)乘以适当的倍数加到其它列(行)，可进一步把 B 变为：

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B_1 & \\ 0 & & & \end{pmatrix}$$

Step 4. 对 B_1 做 Step 1 — Step 3，如此反复，可将 B 变为：

$$\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \end{pmatrix}.$$ 其中 $d_i \in \mathbb{Z}_{>0}$.

Step 5. 通过交换行列，可设 $d_1 \leq d_2 \leq \cdots \leq d_k$.

Step 6. 通过初等变换，把 B 变成 $\begin{pmatrix} d_1' & & & \\ & \ddots & & \\ & & d_l' & \\ & & & 0 \end{pmatrix}$，$0 < d_1' \leq \cdots \leq d_l'$，$d_1' | d_2' | \cdots | d_l'$.

「若 $d_1 \nmid d_i$，$i \in \{2, \ldots, k\}$，则

$$\underset{(1)}{\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \end{pmatrix}} \rightsquigarrow \begin{pmatrix} d_1 & d_i & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \end{pmatrix} \overset{\text{Step 2}}{\rightsquigarrow} \begin{pmatrix} s & \cdots & \cdots \\ \vdots & * & \\ \vdots & & \end{pmatrix}$$

$0 < s < d_1$，s | 第1行、列其它元.

$$\xrightarrow{\text{Step 3} - \text{Step 5}} \begin{pmatrix} \tilde{d}_1 & & & \\ & \ddots & & \\ & & \tilde{d}_j & \\ & & & 0 \end{pmatrix}, \quad 0 < \tilde{d}_1 \leq \cdots \leq \tilde{d}_j, \ \tilde{d}_1 < d_1.$$

由于小于 d_1 的正整数只有有限个，重复上述流程(1)

总可将 $\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_k & \\ & & & 0 \end{pmatrix}$ 变为 $\begin{pmatrix} d_1' & & & & \\ & d_2' & & & \\ & & \ddots & & \\ & & & d_p' & \\ & & & & 0 \end{pmatrix}$，其中 $d_1' \mid d_i'$ $\forall i \neq 1$，$d_1' \leq d_2' \leq \cdots d_p'$.

继续对 $\begin{pmatrix} d_2' & & & \\ & \ddots & & \\ & & d_p' & \\ & & & 0 \end{pmatrix}$ 做上述流程.

定理（有限生成Abel群结构定理）. 设 G 为有限生成Abel群，则要么 G 为 free abelian group，要么存在唯一的一组大于1的满足 $m_1 \mid m_2 \cdots \mid m_t$ 的正整数 $m_1, \cdots, m_t$，以及唯一的非负整数 s，使：

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{s\text{个}}.$$

证明：存在性已证.

「可找到 F 的一组基 $e_1', \cdots, e_n'$，K 的一组基 $d_1 e_1', \cdots, d_k e_k'$，其中 $\underbrace{d_1 \mid \cdots \mid d_k}$，

设 $(d_1, \cdots, d_k) = (1, \cdots, 1, m_1, \cdots, m_t)$.

$$\Rightarrow G \cong F/K \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

$$= \underline{\mathbb{Z}/1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/1\mathbb{Z}} \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

$$= \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$ ┘

唯一性：

在 $G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{s\text{个}}$ 下，

$\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z}$ 对应到 G 的 torsion subgroup T，

$$\Rightarrow G/T \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{s\text{个}}.$$

$\Rightarrow G/T$ 为 free abelian group，且 $rk(G/T) = s$.

$m_1, \cdots, m_t$ 的唯一性证明：参见 GTM 73. #

注：$m_1, \cdots, m_t$ 称为 G 的不变因子（invarian factor）.

注：上述定理可推广到 PID 上的有限生成模上.

另一种分解：

引理：设 m 为正整数，$m=p_1^{n_1}\cdots p_s^{n_s}$ 为其素数分解（$n_i\in\mathbb{Z}_{>0}$，$\forall i$，

p_i 为互不相同素数），则 $\mathbb{Z}/m\mathbb{Z}\cong\mathbb{Z}/p_1^{n_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_s^{n_s}\mathbb{Z}$.

证明：定义 ϕ：

$$\begin{aligned}\mathbb{Z}/m\mathbb{Z}&\longrightarrow\mathbb{Z}/p_1^{n_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_s^{n_s}\mathbb{Z}\\ \bar{n}&\longmapsto(n+\langle p_1^{n_1}\rangle,\cdots\cdots,n+\langle p_s^{n_s}\rangle)\end{aligned}$$

则 $\bar{n}\in\ker\phi\iff p_i^{n_i}\mid n$，$\forall i\iff m\mid n\iff\bar{n}=\bar{0}$.

$\therefore\ker\phi=0$，$\therefore\phi$ 为单射.

再证 ϕ 为满射：

只需证：$\forall i$，$(0,\cdots,0,1+\langle p_i^{n_i}\rangle,0,\cdots,0)\in\mathbb{Z}/p_1^{n_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_s^{n_s}\mathbb{Z}$

$\exists\bar{n}$，s.t. $\phi(\bar{n})=(0,\cdots,0,1+\langle p_i^{n_i}\rangle,0,\cdots,0)$.

注意：$\forall j\neq i$，$\langle p_i^{n_i}\rangle+\langle p_j^{n_j}\rangle=\mathbb{Z}$.

$\exists\ u_j \in \langle p_i^{n_i} \rangle,\ v_j \in \langle p_j^{n_j} \rangle$, s.t. $u_j + v_j = 1$.

令 $n = \prod_{j \neq i} (1 - u_j)$，则 $n + \langle p_i^{n_i} \rangle = 1 + \langle p_i^{n_i} \rangle$.

$n + \langle p_j^{n_j} \rangle = 0 + \langle p_j^{n_j} \rangle$.

$\Rightarrow \phi(\bar{n}) = (0, \cdots, 0, 1 + \langle p_i^{n_i} \rangle, 0, \cdots, 0)$ #.

对 $G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ 用引理进一步分解，可得：

$$G \cong \mathbb{Z}/p_1^{s_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{s_k}\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

其中 $p_1, \cdots, p_k$ 为素数（可能有重复），$s_i \in \mathbb{Z}_{>0}$, $\forall i$.

定理：$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$ 由 G 唯一决定的（称为 G 的初等因子 elementary divisors）.

Ref. GTM 73.