Per $n \geq 0$, sia $\mathbf{Z}^n$ il prodotto di n copie di $\mathbf{Z}$. Scriviamo $\mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ per il gruppo additivo degli omomorfismo $\mathbf{Z}^n \to \mathbf{Z}$. Chiamiamo gli elementi di $\mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ *forme lineari.* Esempi di forme lineari sono le proiezioni sulle i-esime coordinate $(x_1, \ldots, x_n) \mapsto x_i$ per $i = 1, \ldots, n$. Ogni forma lineare $\psi \in \mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ ha la forma

$$\psi(x_1, \ldots, x_n) = \lambda_1 x_1 + \ldots + \lambda_n x_n, \qquad \text{per certi } \lambda_1, \ldots, \lambda_n \in \mathbf{Z}.$$

Il gruppo $\mathbf{Z}^n$ è un sottogruppo dello spazio vettoriale $\mathbf{Q}^n$. Per un sottogruppo $H \subset \mathbf{Z}^n$ il *rango* $rk(H)$ di H è la dimensione del $\mathbf{Q}$-spazio vettoriale $\mathrm{Span}_{\mathbf{Q}}(H)$ dentro $\mathbf{Q}^n$. Sia ha che $rk(H) \leq n$. È facile vedere che $H = 0$ se e solo se $rk(H) = 0$. Se H_1 e H_2 sono sottogruppi con $H_1 \cap H_2 = \{0\}$, allora anche $\mathrm{Span}_{\mathbf{Q}}(H_1) \cap \mathrm{Span}_{\mathbf{Q}}(H_2) = \{0\}$. Ne segue che

$$rk(H_1 + H_2) \;=\; rk(H_1) + rk(H_2).$$

Sia $n \geq 0$ si dice che i vettori $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{Z}^n$ formano una $\mathbf{Z}$-*base* di $\mathbf{Z}^n$ se sono linearmente indipendenti in $\mathbf{Q}^n$ e si ha che

$$\mathbf{Z}^n = \{\lambda_1 \mathbf{v}_1 + \ldots + \lambda_n \mathbf{v}_n : \lambda_1, \ldots, \lambda_n \in \mathbf{Z}\}.$$

Lemma 1. *Sia H un sottogruppo non nullo di $\mathbf{Z}^n$. Allora*

(1) esiste un vettore $\mathbf{h} \in H$ e una forma lineare $\phi \in \mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ tali che $\phi(\mathbf{h}) = a \in \mathbf{Z}$ è positivo e minimale;

(2) il vettore $\mathbf{h}$ è uguale a $a\mathbf{v}$ per qualche $\mathbf{v} \in \mathbf{Z}^n$;

(3) si ha che

$$\mathbf{Z}^n = \mathbf{v}\mathbf{Z} \oplus \ker \phi,$$
$$H = \mathbf{h}\mathbf{Z} \oplus (\ker \phi \cap H).$$

Dimostrazione. (1) Esempi di elementi ϕ di $\mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ sono le coordinate. Poiché H contiene qualche vettore $h \in H$ non nullo, esiste una forma lineare ϕ con $\phi(\mathbf{h}) \neq 0$. E esiste quindi anche un $\mathbf{h} \in H$ con $\phi(\mathbf{h}) = a > 0$ minimale.

Per (2) osserviamo che per ogni forma lineare $\psi \in \mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ il valore $\psi(\mathbf{h})$ è divisibile per a. Infatti, dividiamo $\psi(\mathbf{h})$ per a con resto r. Si ha quindi che $\psi(\mathbf{h}) = qa + r$ con $q \in \mathbf{Z}$ e $0 \leq r < a$. Allora il valore della forma lineare $\psi - q\phi$ in $\mathbf{h}$ è uguale a $\psi(\mathbf{h}) - q\phi(\mathbf{h}) = \psi(\mathbf{h}) - qa = r$. Per la minimalità di a abbiamo quindi che $r = 0$. In particolare, le coordinate di $\mathbf{h}$ sono divisibili per a. Abbiamo quindi che $\mathbf{h} = a\mathbf{v}$ per qualche vettore $\mathbf{v} \in \mathbf{Z}^n$.

Per (3) osserviamo prima che $\mathbf{v}\mathbf{Z} \cap \ker \phi$ è zero. Infatti, supponiamo che $k \in \mathbf{Z}$ e che $\phi(k\mathbf{v}) = 0$. Il fatto che $\phi(\mathbf{h}) = a$ e $\mathbf{h} = a\mathbf{v}$ implica che $\phi(\mathbf{v}) = 1$e quindi $k = k\phi(\mathbf{v}) = \phi(k\mathbf{v}) = 0$. Ovviamente anche $\mathbf{h}\mathbf{Z} \oplus (\ker \phi \cap H)$ è zero.

È anche vero che $\mathbf{v}\mathbf{Z} + \ker \phi = \mathbf{Z}^n$. Infatti, sia $\mathbf{x} \in \mathbf{Z}^n$ e sia $\phi(\mathbf{x}) = k$. Allora $\phi(\mathbf{x} - k\mathbf{v}) = 0$ e $\mathbf{x}$ è uguale a $k\mathbf{v} + (x - k\mathbf{v})$. Similmente, si ha che $H = \mathbf{h}\mathbf{Z} + (\ker \phi \cap H)$. Infatti, sia $\mathbf{x} \in H$. Per minimalità di a, il valore $\phi(\mathbf{x})$ è divisibile per a. Sia $\phi(\mathbf{x}) = ka$. Allora $\phi(\mathbf{x} - k\mathbf{h}) = 0$ e $\mathbf{x}$ è uguale a $k\mathbf{h} + (\mathbf{x} - k\mathbf{h})$, come richiesto.

Proposizione 2. *Sia $n \geq 0$ e sia H un sottogruppo di $\mathbf{Z}^n$ allora H è isomorfo a $\mathbf{Z}^m$ per un $m \leq n$.*

Dimostrazione. Procediamo per induzione rispetto al rango di H. Se $rk(H) = 0$ anche $H = 0$ e tutto è banale. Supponiamo che $rk(H) = m > 0$. Allora $H \neq \{0\}$ e Lemma 1 è applichiamo il Lemma 1. Nella notazione del lemma abbiamo che

$$H = h\mathbf{Z} \oplus (\ker \phi \cap H).$$

Poichè $\mathbf{hZ} \cap (\ker \phi \cap H)$ è zero, abbiamo che $rk(H) = rk(h\mathbf{Z}) + rk(\ker \phi \cap H)$ e $rk(h\mathbf{Z}) = 1$. Be segue che il rango di $\ker \phi \cap H$ è $m - 1$. Per induzione $\ker \phi \cap H$ è isomorfo a $\mathbf{Z}^{m-1}$ e quindi si ha che $H \cong \mathbf{Z} \oplus \mathbf{Z}^{m-1} = \mathbf{Z}^m$, come richiesto.

Proposizione 3. *Sia H un sottogruppo di $\mathbf{Z}^n$. Esiste una $\mathbf{Z}$-base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ di $\mathbf{Z}^n$, esiste $m \leq n$ e esistono $a_1, \ldots, a_m \in \mathbf{Z}_{>0}$ tali che $a_1\mathbf{e}_1, \ldots, a_m\mathbf{e}_m$ è una $\mathbf{Z}$-base di H e tali che a_i divide a_{i+1} per ogni $1 \leq i < m$.*

Dimostrazione. Osserviamo che ha senso parlare di una $\mathbf{Z}$-base di H, perché il Lemma 1 dice che H è isomorfo a $\mathbf{Z}^m$ per qualche $m \leq n$.

Procediamo con induzione rispetto a n. Se $H = \{0\}$, la base canonica di $\mathbf{Z}^n$ funziona e non c'e' niente da dimostrare. Se $H \neq \{0\}$ si ha che $n \geq 1$. Nel caso $n = 1$, si ha che $H = a\mathbf{Z}$ per qualche $a > 0$. Allora prendiamo $\mathbf{e}_1 = 1$ e $a_1 = a$.

Se $n > 1$, applichiamo Lemma 1 e usando la notazione del lemma 1 scriviamo $\mathbf{Z}^n = \mathbf{vZ} \oplus \ker \phi$ con sottogruppo $H = \mathbf{hZ} \oplus (\ker \phi \cap H)$. Abbiamo che $\mathbf{h} = a\mathbf{v}$. Per la Proposizione 2, $\ker \phi$ è isomorfo a $\mathbf{Z}^m$ per un $m \leq n$. Poichè $rk(\mathbf{vZ}) + rk(\ker \phi) = n$, abbiamo che $m = n - 1$. Per induzione $\ker \phi$) ammette una base $\mathbf{e}_2, \ldots, \mathbf{e}_n$ e ci sono interi $a_2, \ldots, a_m > 0$ tali che a_i divide a_{i+1} per ogni $i \geq 2$ e che $a_2\mathbf{e}_2, \ldots, a_m\mathbf{e}_m$ è un base di H.

Prendiamo $\mathbf{e}_1$ uguale al vettore $\mathbf{v}$ del Lemma 1. Allora $\mathbf{e}_1, \ldots, \mathbf{e}_n$ è una $\mathbf{Z}$-base di $\mathbf{Z}^n$. Questo segue dal fatto che $\mathbf{Z}^n$ è somma diretta di $\mathbf{vZ}$ e $\ker \phi$. Prendiamo a_1 uguale all'intero a del Lemma 1. Allora $a_1\mathbf{e}_1, \ldots, a_n\mathbf{e}_n$ è una $\mathbf{Z}$-base di H. Questo segue dal fatto che $\mathbf{h} = a\mathbf{v} = a_1\mathbf{e}_1$ e il fatto che H è somma diretta di $\mathbf{hZ}$ e $\ker \phi \cap H$.

L'unica cosa rimasta da dimostrare è che a_1 divide a_2. Per questo consideriamo la forma lineare ψ di $\mathrm{Hom}(\mathbf{Z}^n, \mathbf{Z})$ data da

$$\psi(x_1, \ldots, x_n) = x_1 + x_2, \quad \text{per } (x_1, \ldots, x_n) \in \mathbf{Z}^n.$$

si ha che $\psi(\mathbf{h}) = \psi(a_1\mathbf{e}_1) = a$. Per la minimalità di $a_1 = a = \phi(\mathbf{h})$ del Lemma 1, $a_1 = \psi(\mathbf{h})$ genera il sottogruppo $\psi(H) \subset \mathbf{Z}$. In particolare a_1 divide $\psi(a_2\mathbf{e}_2) = a_2$.

Questo conclude la dimostrazione della proposizione.

Teorema 4. *Ogni gruppo abeliano finitamente generato è isomorfo a*

$$\mathbf{Z}^r \times \mathbf{Z}_{a_1} \times \ldots \times \mathbf{Z}_{a_m},$$

per $r \geq 0$ e interi positivi a_i che hanno la proprietà che a_i divide a_{i+1} per $i \geq 1$.

Dimostrazione. Sia G un gruppo abeliano finitamente generato e siano $g_1, \ldots, g_n$ generatori di G. Definiamo l'omomorfismo $f : \mathbf{Z}^n \longrightarrow G$ come segue

$$f(\lambda_1, \ldots, \lambda_n) = g_1^{\lambda_1} \cdot \ldots \cdot g_n^{\lambda_n}, \qquad \text{per } (\lambda_1, \ldots, \lambda_n) \in \mathbf{Z}^n.$$

Allora f è suriettivo. Sia H il nucleo di f. Il gruppo G è quindi isomorfo a $\mathbf{Z}^n/H$. Per la Proposizione 3 esiste una $\mathbf{Z}$-base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ di $\mathbf{Z}^n$, esiste $m \leq n$ e esistono $a_1, \ldots, a_m \in \mathbf{Z}_{>0}$ tali che $a_1\mathbf{e}_1, \ldots, a_m\mathbf{e}_m$ è una $\mathbf{Z}$-base di H e tali che a_i divide a_{i+1} per ogni $1 \leq i < m$. Questo implica che

$$\begin{aligned}\mathbf{Z}^n/H &\cong (\mathbf{Z}\mathbf{e}_1 \times \ldots \times \mathbf{Z}\mathbf{e}_n)/(\mathbf{Z}a_1\mathbf{e}_1 \times \ldots \times \mathbf{Z}a_m\mathbf{e}_m),\\ &\cong (\mathbf{Z}\mathbf{e}_1/\mathbf{Z}a_1\mathbf{e}_1) \times \ldots \times (\mathbf{Z}\mathbf{e}_m/\mathbf{Z}a_m\mathbf{e}_m) \times \mathbf{Z}\mathbf{e}_{m+1} \times \ldots \times \mathbf{Z}\mathbf{e}_n.\end{aligned}$$

Osserviamo che per ogni $i = 1, \ldots, m$ il gruppo $\mathbf{Z}\mathbf{e}_i/\mathbf{Z}a_i\mathbf{e}_i$ è ciclico di ordine a_i ed è quindi isomorfo a $\mathbf{Z}_{a_i}$. Sia $r = n - m$. Allora abbiamo che

$$G \cong \mathbf{Z}^n/H \cong \mathbf{Z}^r \times \mathbf{Z}_{a_1} \times \ldots \times \mathbf{Z}_{a_m}.$$

come richiesto.

Teorema 5. *Ogni gruppo abeliano finito è isomorfo a*

$$\mathbf{Z}_{a_1} \times \ldots \times \mathbf{Z}_{a_m},$$

per interi positivi a_i che hanno la proprietà che a_i divide a_{i+1} per $i \geq 1$.

Dimostrazione. Questo è ovvio. Se G è un gruppo abeliano finito è anche finitamente generato e possiamo applicare il teorema precedente. In questo caso si ha che $r = 0$.