Basi adattate

Ricordiamo che un gruppo abeliano libero di rango n è un gruppo isomorfo a $\mathbb{Z}^n$. Ogni sottogruppo non banale di $\mathbb{Z}^n$ è ancora libero di rango al più n. Inoltre, se $G \simeq \mathbb{Z}^n$ e $G \simeq \mathbb{Z}^m$, allora $n = m$.

Teorema *Siano G un gruppo libero di rango n ed H un suo sottogruppo. Esistono $\{g_1, \ldots, g_n\}$ base di G, $\{h_1, \ldots, h_n\}$ sistema di generatori di H ed interi $a_1, \ldots, a_n$ tali che $h_i = a_i g_i$ per ogni $i = 1, \ldots, n$.*

Dim. La dimostrazione è per induzione su n. Se $n = 1$ il teorema è certamente vero, perché ogni sottogruppo di $\mathbb{Z}$ è della forma $a\mathbb{Z}$, per qualche $a \in \mathbb{Z}$. Possiamo allora supporre vero il teorema per gruppi di rango $n-1$. Sia $G = \mathbb{Z}^n$. Se $H = 0$ allora il teorema è banalmente vero. Possiamo quindi assumere $H \neq 0$. Per ogni $\psi \in \mathrm{Hom}(G, \mathbb{Z})$, $\psi(H)$ è sottogruppo di $\mathbb{Z}$, quindi esiste a_ψ tale che $\psi(H) = a_\psi \mathbb{Z}$. Essendo $H \neq 0$, per almeno uno ψ avremo $\psi(H) \neq 0$ (esercizio). Dato che in $\mathbb{Z}$ non esistono catene ascendenti infinite di sottogruppi, l'insieme $\{\psi(H) \mid \psi \in \mathrm{Hom}(G, \mathbb{Z})\}$ ha elementi massimali. Sia $\phi(H) = a\mathbb{Z}$ uno di questi. Per quanto osservato prima $a \neq 0$. Fissiamo $h \in H$ tale che $\phi(h) = a$ Preso un qualsiasi $\psi \in \mathrm{Hom}(G, \mathbb{Z})$ sia $d = (\psi(h), a)$il massimo comun divisore tra a e $\psi(h)$, e scriviamo $d = x\psi(h) + ya$ con $x, y \in \mathbb{Z}$. Consideriamo quindi $\eta = x\psi + y\phi \in \mathrm{Hom}(G, \mathbb{Z})$. Abbiamo $\eta(h) = x\psi(h) + y\phi(h) = x\psi(h) + ya = d$. Allora $d\mathbb{Z} \subseteq \eta(H)$. Inoltre $\phi(H) = a\mathbb{Z} \subseteq d\mathbb{Z}$ perchè d divide a. Per la massimalità di $\phi(H)$ deve essere $d\mathbb{Z} = a\mathbb{Z}$, ovvero $a = d$ e quindi a divide $\psi(h)$. Se $h = (v_1, \ldots, v_n)$, e π_i è la proiezione di G sulla i-esima componente, abbiamo quindi che $\pi_i(h) = v_i$ è multiplo di a. Di conseguenza $h^* = \frac{1}{a}h$ è un elemento di G. Dato che $a = \phi(ah^*) = a\phi(h^*)$, abbiamo $\phi(h^*) = 1$. Posto $K = \ker(\phi)$, ovviamente $K \cap \langle h^* \rangle = 0$. Se $g \in G$, l'elemento $g - \phi(g)h^*$ è in K. Infatti $\phi(g - \phi(g)h^*) = \phi(g) - \phi(\phi(g)h^*) = \phi(g) - \phi(g)\phi(h^*) = \phi(g) - \phi(\phi(g)) = 0$. Allora ogni $g \in G$ si scrive come $g = (g - \phi(g)h^*) + \phi(g)h^*$ e questo prova, assieme all'osservazione precedente, che $G = K \oplus \langle h^* \rangle$. Il sottogruppo K è libero di rango $m \leq n$ e allora $G \simeq \mathbb{Z}^m \oplus \langle h^* \rangle$. Di conseguenza $G \simeq \mathbb{Z}^{m+1}$ e si ha $m = n-1$. Possiamo applicare l'ipotesi induttiva al gruppo K ed al suo sottogruppo $K \cap H$. Esistono $\{g_1, \ldots, g_{n-1}\}$ base di K, $\{h_1, \ldots, h_{n-1}\}$ sistema di generatori di $K \cap H$ ed interi $a_1, \ldots, a_{n-1}$ tali che $h_i = a_i g_i$ per ogni $i = 1, \ldots, n-1$. Poniamo $g_n = h^*$, $h_n = h$ e $a_n = a$. È immediato vedere che $\{g_1, \ldots, g_n\}$ è base di G. Se proviamo che $\{h_1, \ldots, h_n\}$ è un sistema di generatori di H il teorema è dimostrato. Preso $v \in H$ sappiamo che $\phi(v) = ax$ per qualche $x \in \mathbb{Z}$. Se $u = v - xh_n$ abbiamo $\phi(u) = \phi(v) - x\phi(h_n) = xa - xa = 0$ e quindi $u \in K \cap H$. Allora $v = u + xh_n$ appartiene a $(K \cap H) + \langle h_n \rangle$ che risulta quindi essere proprio H. Dato che $\langle h_1, \ldots, h_n \rangle = (K \cap H) + \langle h_n \rangle$ abbiamo provato che $\{h_1, \ldots, h_n\}$ è un sistema di generatori per H, e il teorema è dimostrato. □

La base $\{g_1, \ldots, g_n\}$ descritta nel teorema si dice *una base H-adattata.*

Questo teorema ha una conseguenza molto utile.

Proposizione *Siano G un gruppo libero di rango n ed H un suo sottogruppo di rango n. Date $\mathcal{A} = \{x_1, \dots, x_n\}$ base di G, $\mathcal{B} = \{y_1, \dots, y_n\}$ base di H e detta $A \in M(n, \mathbb{Z})$ la matrice di passaggio da $\mathcal{A}$ a $\mathcal{B}$, si ha $|G/H| = |\det(A)|$.*

Dim. Scegliamo $\mathcal{G} = \{g_1, \dots, g_n\}$ e $\mathcal{H} = \{h_1, \dots, h_n\}$ basi H adattate con $h_i = a_i g_i$ per $i = 1, \dots, n$. Possiamo anche supporre che ciascun a_i sia positivo. Dato che $G \simeq \oplus_{i=1}^n \langle g_i \rangle$ e $H \simeq \oplus_{i=1}^n \langle a_i g_i \rangle$, è facile vedere che

$$G/H \simeq \bigoplus_{i=1}^{n} \langle g_i \rangle / \langle a_i g_i \rangle \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$$

e quindi $|G/H| = \prod_{i=1}^n a_i$. Per semplicità di scrittura poniamo $g = (g_1, \dots, g_n)$, $h = (h_1, \dots, h_n)$, $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n)$. Esistono matrici $U, V, D \in M(n, \mathbb{Z})$ tali che

- $g = Ux$;
- $h = Vy$;
- $h = Dg$.

Osserviamo che D è la matrice diagonale il cui termine di posto (i, i) è a_i. Inoltre U, V sono matrici invertibili, visto che sono matrici di passaggio tra basi rispettivamente di G e H. Allora il loro determinante è ± 1. Abbiamo $h = Vy = VAx = VAU^{-1}g$. Quindi $D = VAU^{-1}$ e, per la formula di Binet, $\det(D) = \det(V)\det(A)\det(U)^{-1}$. Dato che $\det(D) = \prod_{i=1}^n a_i = |G/H|$ si ottiene $|G/H| = \left|\det(V)\det(A)\det(U)^{-1}\right| = |\det(A)|$. $\square$