6.3 Automorfismi del prodotto diretto di due gruppi

Teorema 6.3.1 *Siano H e K due gruppi tali che $|H| = m$ e $|K| = n$ con $(m, n) = 1$. Allora, $Aut(H) \times Aut(K) \cong Aut(H \times K)$.*

Nell dimostrazione del teorema useremo il seguente risultato:

Lemma 6.3.2 *Siano H e K due gruppi tali che $|H| = m$ e $|K| = n$ con $(m, n) = 1$. Allora, ogni omomorfismo $\varphi : H \to K$ è banale, cioè $\varphi(h) = 1_k$, per ogni $h \in H$.*

Dimostrazione: Essendo m e n coprimi, esistono $u, v \in \mathbb{Z}$ tali che $um + vn = 1$, e quindi

$$h = h^{um+vn} = h^{um}h^{vn} = (h^u)^m h^{vn} = h^{vn}.$$

dove nell'ultima uguaglianza stiamo usando la (ii) del Corollario 3.5.8 del Teorema di Lagrange. Pertanto, ancora per la (ii) del Corollario 3.5.8,

$$\varphi(h) = \varphi(h^{vn}) = (\varphi(h^v))^n = 1_K.$$

□

Dimostrazione (del Teorema 6.2.2): Definiamo l'applicazione

$$\Phi : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \to \mathrm{Aut}(H \times K), \quad (\alpha, \beta) \mapsto \Phi(\alpha, \beta),$$

dove

$$\Phi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)), \forall (h, k) \in H \times K.$$

I seguenti fatti si verificano facilmente:

1. $\Phi(\alpha, \beta)$ è un omomorfismo, per ogni $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$.

2. $\Phi(\alpha, \beta) \in \mathrm{Aut}(H \times K)$, per ogni $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$ (ovvero Φ è ben definita): infatti, se $(h, k) \in H \times K$ è tale che

$$\Phi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) = (1_H, 1_K),$$

allora, poiché α e β sono iniettive, segue che $(h, k) = (1_H, 1_K)$, e quindi $\Phi(\alpha, \beta)$ è iniettiva, e di conseguenza anche suriettiva, essendo $H \times K$ un insieme finito.

3. Φ è un omomorfismo di gruppi:

$$\Phi\left((\alpha_1, \beta_1)(\alpha_2, \beta_2)\right) = \Phi(\alpha_1, \beta_1) \circ \Phi(\alpha_2, \beta_2).$$

4. Φ è iniettivo: $\ker(\Phi) = (\mathrm{id}_H, \mathrm{id}_K)$.

Resta da dimostrare la suriettività di Φ, utilizzando l'ipotesi $(m, n) = 1$.

Sia $\omega \in \mathrm{Aut}(H \times K)$ e definiamo gli omomorfismi $\omega_1 : H \to H$ e $\gamma : H \to K$ come

$$\omega_1(h) = p_1(\omega(h, 1_K)), \quad \forall h \in H, \tag{6.3}$$

$$\gamma(h) = p_2(\omega(h, 1_K)), \quad \forall h \in H$$

Osserviamo che, per il Lemma 6.3.2, γ è banale, cioè

$$p_2(\omega(h, 1_K)) = 1_K, \quad \forall h \in H.$$

e che quindi

$$\omega(h, 1_K) = (p_1(\omega(h, 1_K)), p_2(\omega(h, 1_K))) = (\omega_1(h), 1_K), \quad \forall h \in H. \tag{6.4}$$

Inoltre, se $\omega_1(h) = 1_H$, allora dalla (6.4)

$$\omega(h, 1_K) = (1_H, 1_K).$$

Poiché ω è un automorfismo, segue che $h = 1_H$, quindi ω_1 è iniettivo essendo $\ker(\omega_1) = \{1_H\}$. Quindi ω_1 è anche suriettivo perchè H è finito, ossia $\omega_1 \in \mathrm{Aut}(H)$.

In modo analogo definiamo gli omomorfismi $\omega_2 : K \to K$ e $\delta : K \to H$ come

$$\omega_2(k) = p_2(\omega(1_H, k)), \quad \forall k \in K.$$

$$\delta(k) = p_1(\omega(1_H, k)), \quad \forall k \in K$$

Sempre per il Lemma 6.3.2, δ è banale e quindi

$$\omega(1_H, k) = (p_1(\omega(1_H, k)), p_2(\omega(1_H, k))) = (1_H, \omega_2(k)), \quad \forall k \in K. \tag{6.5}$$

Dalla (6.5), in modo simile a quanto fatto per ω_1, si dimostra che $\omega_2 \in \mathrm{Aut}(K)$.

Verifichiamo che $\Phi(\omega_1, \omega_2) = \omega$ e che quindi Φ è suriettiva.

Per ogni $(h, k) \in H \times K$,

$$\Phi(\omega_1, \omega_2)(h, k) = (\omega_1(h), \omega_2(k)),$$

mentre, per le (6.4) e (6.5),

$$\omega(h, k) = \omega(h, 1_K)\omega(1_H, k) = (\omega_1(h), 1_K)(1_H, \omega_2(k)) = (\omega_1(h), \omega_2(k)).$$

Quindi $\Phi(\omega_1, \omega_2) = \omega$. □

Osservazione 6.3.3 Senza l'ipotesi $(m, n) = 1$, il teorema non è vero. Ad esempio, $\mathrm{Aut}(\mathbb{Z}_2) \times \mathrm{Aut}(\mathbb{Z}_2)$ è il gruppo banale $\{1\}$, mentre $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, come si verifica facilmente osservando che è un gruppo non abeliano con 6 elementi, oppure costruendo un isomorfismo esplicito.