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, $Aut(H) \times Aut(K) \cong Aut(H \times K)$.*

Dimostrazione: Definiamo l'applicazione

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

I seguenti fatti si verificano facilmente:

1. $\Phi(\alpha, \beta) \in \mathrm{End}(H \times K)$ 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.

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 $\omega_1 : H \to H$ come
$$\omega_1(h) = p_1(\omega(h, 1_K)), \quad \forall h \in H, \tag{6.3}$$
e $\omega_2 : K \to K$ come
$$\omega_2(k) = p_2(\omega(1_H, k)), \quad \forall k \in K. \tag{6.4}$$

Mostriamo che $\omega_1 \in \mathrm{Aut}(H)$. Poiché ω_1 è composizione di omomorfismi, si ha $\omega_1 \in \mathrm{End}(H)$. Inoltre:
$$\begin{aligned}\ker(\omega_1) &= \{h \in H \mid \omega_1(h) = p_1(\omega(h,1_K)) = 1_H\}\\ &= \{h \in H \mid \omega(h,1_K) = (1_H, 1_K)\} = \{1_H\},\end{aligned}$$
dove l'ultima uguaglianza segue dal fatto che $\omega \in \mathrm{Aut}(H\times K)$. La penultima uguaglianza deriva da:
$$p_2(\omega(h,1_K)) = 1_K. \tag{6.5}$$

L'omomorfismo $\gamma \in \mathrm{Hom}(H,K)$ definito da $\gamma(h) = p_2(\omega(h,1_K))$ è banale, ovvero $\gamma(h) = 1_K$ per ogni $h\in H$, cioè $\ker(\gamma) = H$.

Per dimostrarlo, notiamo che, essendo $(m,n) = 1$, esistono $u, v \in \mathbb{Z}$ tali che $um + vn = 1$, e quindi, usando Lagrange:
$$h^{um+vn} = h^{vn} = h.$$

Pertanto:
$$\gamma(h) = \gamma(h^{vn}) = \gamma(h^v)^n = 1.$$

In modo analogo, si dimostra che $\omega_2 \in \mathrm{Aut}(K)$, in quanto composizione di omomorfismi, utilizzando l'uguaglianza
$$p_1(\omega(1_H,k)) = 1_H. \tag{6.6}$$

Quindi, dalle equazioni (6.3), (6.4), (6.5) e (6.6), otteniamo:
$$\begin{aligned}\Phi(\omega_1,\omega_2)(h,k) &= (\omega_1(h), \omega_2(k)) = (\omega_1(h), 1_K)(1_H, \omega_2(k))\\ &= (p_1(\omega(h,1_K)), p_2(\omega(1_H,k))) = \omega(h,k),\end{aligned}$$
e quindi Φ è suriettiva. $\square$

Osservazione 6.3.2 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.