1. Automorfismi del prodotto diretto di due gruppi

Teorema 1.1. *Siano H e K due gruppi tali che $|H| = m$ e $|K| = n$ con $(m, n) = 1$. Allora* $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(H \times K)$.

Proof. Sia

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

I seguenti fatti sono una semplice verifica.

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

(2) $\Phi(\alpha, \beta) \in \mathrm{Aut}(H \times K), \forall\alpha \in Aut(H), \beta \in \mathrm{Aut}(K)$ (Φ é ben definita): infatti fissati (α, β) se $(h, k) \in H \times K$ sono tali che

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

allora essendo α e β iniettive segue che $(h, k) = (1_H, 1_K)$ e quindi $\Phi(\alpha, \beta)$ é iniettiva (e quindi suriettiva).

(3) Φ un omomorfismo di gruppi: $\Phi\left((\alpha_1, \beta_1)(\alpha_2, \beta_2)\right) = \Phi\left((\alpha_1, \beta_1)\right)\circ\Phi\left((\alpha_2, \beta_2)\right)$.

(4) Φ iniettivo: $Ker\Phi = (id_H, id_K)$.

Resta da dimostrare la suriettivita di Φ (usando l'ipotesi che $(m, n) = 1$). Sia $\omega \in \mathrm{Aut}(H \times K)$ e sia $\omega_1 : H \to H$ definita come

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

e sia $\omega_2 : K \to K$ definita come

$$\omega_2(k) = p_2(\omega(1_H, k)), \forall k \in K. \tag{2}$$

Mostriamo che $\omega_1 \in \mathrm{Aut}(H)$. Infatti $\omega_1 \in \mathrm{End}(H)$ in quanto composizione di omomorfisimi. 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 $\omega \in \mathrm{Aut}(H\times K)$, mentre la penultima uguaglianza segue da

$$p_2(\omega(h, 1_K)) = 1_K. \tag{3}$$

Infatti l'omomorfismo $\gamma \in \mathrm{Hom}(H, K)$ definito da $\gamma(h) = p_2(\omega(h, 1_K))$ é banale, $\gamma(h) = 1_K, \forall h \in H$ ossia $Ker\gamma = H$. Per vedere questo osserviamo che $Ker\gamma = \{h^n \mid h \in H\}$. Infatti l'inclusione $\{h^n \mid h \in H\} \subseteq Ker\gamma$ segue da:

$$\gamma(h^n) = (\gamma(h))^n = 1_K$$

(in quanto sto elevando un elemento di K alla potenza $n = |K|$ e usando Lagrange). D'altra parte $|\{h^n \mid h \in H\}| = m = |H| \geq |Ker\gamma|$: infatti l'applicazione data da:

$f : H \to H, h \mapsto h^n$ è bigettiva (non é un omomorfismo!). Infatti essendo $(m, n) = 1$ esistono $u, v \in \mathbb{Z}$ tali che $um + vn = 1$ e quindi $(h^m = 1)$

$$h^{um+vn} = h^{vn} = h$$

e quindi l'inversa di f é data da $f^{-1}(h) = h^v$.

In modo analogo si dimostra che $\omega_2 \in \mathrm{Aut}(K)$ in quanto composizione di omomorfisimi usando l'uguaglianza

$$p_1(\omega(1_H, k)) = 1_H. \tag{4}$$

Quindi dalle (1), (2), (3) e (4) si ottiene:

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

$$(p_1\omega(h, 1_k), p_2\omega(h, 1_K))(p_1\omega(1_H, k), p_2\omega(1_H, k)) = \omega(h, 1_K)\omega(1_H, k) = \omega(h, k),$$

e quindi Φ suriettiva. $\square$

Osservazione 1.2. Senza l'ipotesi il teorema non vale $(m, n) = 1$. Per esempio $\mathrm{Aut}(\mathbb{Z}_2) \times \mathrm{Aut}(\mathbb{Z}_2)$ é 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 anche un isomorfismo esplicito).