

Il teorema fondamentale sugli omomorfismi di gruppi

Maurizio Cornalba

5/11/2011

Il problema che ci poniamo è il seguente. Dati omomorfismi di gruppi $\alpha : G \rightarrow H$ e $\beta : G \rightarrow K$ ci chiediamo sotto quali condizioni esista un omomorfismo $\gamma : H \rightarrow K$ che renda commutativo il diagramma

$$\begin{array}{ccc} & & H \\ & \alpha \nearrow & \downarrow \gamma \\ G & & \\ & \searrow \beta & K \end{array}$$

e, in caso di esistenza, quali siano le sue proprietà di iniettività o suriettività. La risposta è fornita dal seguente risultato.

Teorema 1. *Siano $\alpha : G \rightarrow H$ e $\beta : G \rightarrow K$ omomorfismi di gruppi. Supponiamo che α sia suriettivo. Allora:*

1. *condizione necessaria e sufficiente perché esista una applicazione $\gamma : H \rightarrow K$ tale che $\beta = \gamma \circ \alpha$ è che $\ker \alpha \subset \ker \beta$;*
2. *esiste al più una applicazione $\gamma : H \rightarrow K$ tale che $\beta = \gamma \circ \alpha$; se esiste, è un omomorfismo.*

Supponiamo che γ esista. Allora:

3. *γ è iniettiva se e solo se $\ker \alpha = \ker \beta$;*
4. *γ è suriettiva se e solo se β è suriettiva.*

Dimostrazione. Dimostriamo il punto 1. Se $\gamma \circ \alpha = \beta$ e $g \in \ker \alpha$, allora $\beta(g) = \gamma(\alpha(g)) = \gamma(1) = \gamma(\alpha(1)) = \beta(1) = 1$, e quindi $g \in \ker \beta$. Viceversa, supponiamo che $\ker \alpha \subset \ker \beta$. Dato $h \in H$, esiste un $g \in G$ tale che $\alpha(g) = h$, dato che α è suriettivo. Poniamo allora $\gamma(h) = \beta(g)$. Bisogna mostrare che questa è una buona definizione. Sia allora g' un altro elemento di G tale che $\alpha(g') = h$. Notiamo che $\alpha(g^{-1}g') = h^{-1}h = 1$. Ma allora, per ipotesi, $\beta(g^{-1}g') = 1$, e quindi $\beta(g') = \beta(g)$. Dunque γ è ben definita. È chiaro dalla sua definizione che $\gamma \circ \alpha = \beta$.

Passiamo al punto 2. Supponiamo che $\beta = \gamma \circ \alpha = \gamma' \circ \alpha$. Se h è un qualsiasi elemento di H , possiamo scrivere $h = \alpha(g)$ per qualche $g \in G$. Allora $\gamma'(h) = \gamma'(\alpha(g)) = \beta(g) = \gamma(\alpha(g)) = \gamma(h)$. Ciò mostra che $\gamma' = \gamma$. Supponiamo ora che γ esista e siano $h = \alpha(g)$ e $h' = \alpha(g')$ elementi di H . Notiamo che $\alpha(gg') = hh'$, e che quindi $\gamma(hh') = \beta(gg') = \beta(g)\beta(g') = \gamma(\alpha(g))\gamma(\alpha(g')) = \gamma(h)\gamma(h')$. Questo mostra che γ è un omomorfismo.

Occupiamoci ora del punto 3. Se $g \in \ker \beta$, allora $1 = \beta(g) = \gamma(\alpha(g))$. Quando γ è iniettiva questo implica che $\alpha(g) = 1$, cioè che $g \in \ker \alpha$. Viceversa, se $\ker \alpha = \ker \beta$ e $h = \alpha(g)$ è un elemento di $\ker \gamma$, $1 = \gamma(h) = \beta(g)$, e quindi per ipotesi $g \in \ker \alpha$, cioè $h = \alpha(g) = 1$. Questo mostra che $\ker \gamma = \{1\}$, e quindi che γ è iniettiva.

Infine dimostriamo 4. Se γ è suriettiva lo è anche β in quanto composizione di applicazioni suriettive. Viceversa, se β è suriettiva e k è un qualsiasi elemento di K , esiste $g \in G$ tale che $k = \beta(g)$, e quindi $k = \gamma(\alpha(g))$. Dunque γ è suriettiva. □