3. Spazi quoziente

Sia $f : V \to U$ un omomorfismo di spazi vettoriali sul campo K. Il nucleo di f è un sottospazio vettoriale di V. Ci si può chiedere se, viceversa, dato un sottospazio W di V, vi sia un omomorfismo da V in un altro spazio vettoriale di cui W sia il nucleo. La risposta è affermativa e la costruzione è la seguente. Diciamo che due elementi u e v di V sono equivalenti, e scriviamo $u \sim v$, se $u - v \in W$. Si tratta, per fortuna, di una relazione di equivalenza. In effetti, $u - u = 0 \in W$, $v - u = -(u - v) \in W$ se $u - v \in W$, e infine, se $u \sim v$ e $v \sim z$, allora $u - z = (u - v) + (v - z) \in W$, e quindi $u \sim z$. Indichiamo con V/W il quoziente di V modulo la relazione di equivalenza $\sim$. La classe di equivalenza di un elemento v di V è l'insieme di tutti gli elementi di V della forma $v + w$, dove $w \in W$, che si indica con $v + W$ e si chiama *classe laterale*, o semplicemente *laterale*, di v modulo W. Sia $\varphi : V \to V/W$ l'applicazione naturale, che associa ad ogni elemento di V la sua classe laterale. Si può definire su V/W una struttura di spazio vettoriale. Se u e v sono elementi di V e a è uno scalare si pone

$$\begin{aligned} \varphi(u) + \varphi(v) &= \varphi(u + v)\,, \\ a\varphi(u) &= \varphi(au)\,. \end{aligned} \tag{3.1}$$

Bisogna notare che queste sono buone definizioni, cioè che, se $\varphi(u') = \varphi(u)$ e $\varphi(v') = \varphi(v)$, allora $\varphi(u' + v') = \varphi(u + v)$ e $\varphi(au') = \varphi(au)$. In effetti $u' - u \in W$ e $v' - v \in W$, quindi $u' + v' - (u + v) = u' - u + v' - v \in W$ e $au' - au = a(u' - u) \in W$. Lasciamo al lettore di verificare che V/W, con le operazioni sopra definite, è uno spazio vettoriale. Notiamo piuttosto che le (3.1) dicono che φ è un omomorfismo di spazi vettoriali. È chiaro che φ è suriettivo. Il suo nucleo è l'insieme dei v tali che $\varphi(v) = \varphi(0)$, cioè W.

L'operazione di passaggio al quoziente gode della seguente proprietà universale.

Proposizione (3.2) (Teorema di omomorfismo). *Sia $\alpha : V \to U$ un omomorfismo di spazi vettoriali tale che $\ker(\alpha) \supset W$. Allora vi è uno e un solo omomorfismo $\beta : V/W \to U$ tale che $\alpha = \beta \circ \varphi$. Il nucleo di β è $\ker(\alpha)/W$; in particolare β è iniettivo se e solo se $\ker(\alpha) = W$. Infine β è suriettivo se e solo se α è suriettivo.*

Notiamo innanzitutto che, se β esiste, $\beta(\varphi(v)) = \alpha(v)$ per ogni $v \in V$. Dato che ogni elemento di V/W è della forma $\varphi(v)$ per qualche $v \in V$, β è univocamente determinato. Per dimostrare l'esistenza di β poniamo $\beta(\varphi(v)) = \alpha(v)$. Questa è una buona definizione. Infatti, se $\varphi(v') = \varphi(v)$, allora $v' - v \in \ker(\varphi) = W \subset \ker(\alpha)$, e quindi $\alpha(v') = \alpha(v)$. Poi

$$\begin{aligned} \beta(\varphi(u) + \varphi(v)) = \beta(\varphi(u + v)) = \alpha(u + v) = \alpha(u) + \alpha(u) = \beta(\varphi(u)) + \beta(\varphi(v))\,, \\ a\beta(\varphi(v)) = a\alpha(v) = \alpha(av) = \beta(\varphi(av)) = \beta(a\varphi(v))\,, \end{aligned}$$

e quindi β è un omomorfismo. È chiaro che β è suriettivo se e solo se lo è α. Se invece $\varphi(v) \in \ker(\beta)$, cioè $\alpha(v) = 0$, allora $\varphi(v) \in \varphi(\ker(\alpha)) = \ker(\alpha)/W$, e viceversa. Questo conclude la dimostrazione.

Siano $v_1, \ldots, v_n$ elementi di V. Diremo che $v_1, \ldots, v_n$ sono *linearmente indipendenti modulo* W se $\varphi(v_1), \ldots, \varphi(v_n)$ sono linearmente indipendenti in V/W, cioè se ogni volta che una combinazione lineare $\sum_i a_i v_i$ appartiene a W si ha che $a_i = 0$ per ogni i. Analogamente diremo che $v_1, \ldots, v_n$ costituiscono una base di V modulo W se $\varphi(v_1), \ldots, \varphi(v_n)$ sono una base di V/W. Osserviamo che, se $v_1, \ldots, v_n$ è una base di V modulo W e $w_1, \ldots, w_m$ è una base di W, allora $v_1, \ldots, v_n, w_1, \ldots, w_m$ è una base di V. Infatti se $\sum a_i v_i + \sum b_j w_j = 0$, allora $\sum a_i v_i \in W$ e quindi $a_i = 0$ per ogni i; ne segue che $\sum b_j w_j = 0$ e dunque che $b_j = 0$ per ogni j. Se poi $v \in V$ vi sono scalari a_i tali che $\varphi(v) = \sum a_i \varphi(v_i)$, cioè tali che $v - \sum a_i v_i$ appartenga a W e sia quindi della forma $\sum b_j w_j$; si conclude che $v = \sum a_i v_i + \sum b_j w_j$. Più in generale, supponiamo date una catena

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_{k-1} \subset V_k = V$$

di sottospazi di V, e una base $v_{i,1}, \ldots, v_{i,n_i}$ di V_i modulo V_{i-1} per ogni i tale che $1 \leq i \leq k$. Allora quanto appena osservato mostra, per induzione su k, che

$$v_{1,1}, \ldots, v_{1,n_1}, v_{2,1}, \ldots, v_{2,n_2}, \ldots, v_{k,1}, \ldots, v_{k,n_k}$$

è una base di V.