Lezione 3

Prerequisiti: Applicazioni tra insiemi. Relazioni di equivalenza. Lezione 2.

Omomorfismi di gruppi

In questa lezione introduciamo uno strumento utile a confrontare le strutture di gruppi distinti.

Definizione 3.1 Siano $(G_1, *_1)$ e $(G_2, *_2)$ gruppi. Un'applicazione $f : G_1 \to G_2$ si dice un *omomorfismo (di gruppi)* se, per ogni $x, y \in G_1$,

$$f(x *_1 y) = f(x) *_2 f(y). \tag{1}$$

Se $(G_1, *_1) = (G_2, *_2)$, f si dice *endomorfismo.* Un omomorfismo bigettivo si dice *isomorfismo*. Un endomorfismo bigettivo si dice *automorfismo*.

Nota Se $(G_1, +_1)$ e $(G_2, +_2)$ sono gruppi additivi, la condizione (1) si scrive nella forma:

$$f(x +_1 y) = f(x) +_2 f(y).$$

Se $(G_1, \cdot_1)$ e $(G_2, \cdot_2)$ sono gruppi moltiplicativi,

$$f(x \cdot_1 y) = f(x) \cdot_2 f(y).$$

Se $(G_1, +_1)$ è un gruppo additivo e $(G_2, \cdot_2)$ è un gruppo moltiplicativo,

$$f(x +_1 y) = f(x) \cdot_2 f(y).$$

Se $(G_1, \cdot_1)$ è un gruppo moltiplicativo e $(G_2, +_2)$ è un gruppo additivo,

$$f(x \cdot_1 y) = f(x) +_2 f(y).$$

Esempio 3.2

(a) Sia $(G, *)$ un gruppo. Se H è un sottogruppo di G, l'applicazione di inclusione insiemistica $i : H \to G$ è un omomorfismo di gruppi. Infatti, per ogni $x, y \in H$, stante la Definizione 2.14 di operazione ristretta,

$$i(x *_H y) = i(x * y) = x * y = i(x) * i(y).$$

In particolare, l'applicazione identica id_G di G è un automorfismo del gruppo G.

(b) Siano $(G_1,*_1)$ e $(G_2,*_2)$ gruppi, e sia e_2 l'elemento neutro di G_2. Allora l'applicazione costante $f: G_1 \to G_2$ definita da $f(x)=e_2$ per ogni $x \in G_1$ è un omomorfismo di gruppi. Infatti, per ogni $x, y \in G_1$,

$$f(x *_1 y) = e_2 = e_2 *_2 e_2 = f(x) *_2 f(y).$$

Questo omomorfismo si dice *omomorfismo banale*.

L'omomorfismo è dunque un'applicazione tra gruppi che rispetta le operazioni, ed, in un certo senso, trasforma l'operazione del gruppo di partenza nell'operazione del gruppo di arrivo. La prossima proposizione mostra che quanto detto per le operazioni dei gruppi si estende agli elementi neutri ed ai simmetrici. Inoltre le applicazioni immagine diretta ed immagine inversa conservano i sottogruppi.

Proposizione 3.3 *(Proprietà di conservazione degli omomorfismi di gruppi)* Siano $(G_1,*_1)$ e $(G_2,*_2)$ gruppi e sia $f: G_1 \to G_2$ un omomorfismo di gruppi. Allora valgono le seguenti proprietà.

(a) Se e_1 è l'elemento neutro di G_1, $f(e_1)$ è l'elemento neutro di G_2.
(b) Per ogni $x \in G_1$, il simmetrico di $f(x)$ è $f(\overline{x})$ (ossia $\overline{f(x)} = f(\overline{x})$).
(c) Se H_1 è un sottogruppo di G_1, allora $f(H_1)$ è un sottogruppo di G_2.
(d) Se H_2 è un sottogruppo di G_2, allora $f^{-1}(H_2)$ è un sottogruppo di G_1.

Dimostrazione:
(a) Si ha $f(e_1) = f(e_1 *_1 e_1) = f(e_1) *_2 f(e_1)$, per cui $f(e_1)$ è un elemento idempotente di G_2. In base all'Esercizio 2.10, segue che $f(e_1)$ è l'elemento neutro di G_2.
(b) Sia $x \in G_1$. Allora, detto e_2 l'elemento neutro di G_2, si ha, in base a quanto già dimostrato:

$$e_2 = f(e_1) = f(x *_1 \overline{x}) = f(x) *_2 f(\overline{x}),$$
$$e_2 = f(e_1) = f(\overline{x} *_1 x) = f(\overline{x}) *_2 f(x).$$

Segue che $f(\overline{x})$ è il simmetrico di $f(x)$.
(c) Sia H_1 un sottogruppo di G_1. Allora, in base alla Proposizione 2.21 (a), $e_1 \in H_1$, e pertanto, alla luce di quanto già dimostrato al punto (a), $e_2 = f(e_1) \in f(H_1)$. In particolare $f(H_1) \neq \emptyset$. Siano ora $x, y \in H_1$. Allora, in virtù della caratterizzazione dei sottogruppi, $x *_1 \overline{y} \in H_1$, quindi

$$f(x) *_2 \overline{f(y)} = f(x) *_2 f(\overline{y}) = f(x *_1 \overline{y}) \in f(H_1),$$

ove la prima uguaglianza segue da quanto già dimostrato al punto (b). Ciò prova che $f(H_1)$ è un sottogruppo di G_2.
(d) Sia H_2 un sottogruppo di G_2. Allora, in base alla Proposizione 2.21 (a), $e_2 \in H_2$, e pertanto, alla luce di quanto già dimostrato al punto (a), $f(e_1) = e_2 \in H_2$, ossia $e_1 \in f^{-1}(H_2)$. In particolare $f^{-1}(H_2) \neq \emptyset$. Siano ora $x, y \in f^{-1}(H_2)$. Allora $f(x), f(y) \in H_2$. In virtù della caratterizzazione dei sottogruppi si ha

$$f(x *_1 \overline{y}) = f(x) *_2 f(\overline{y}) = f(x) *_2 \overline{f(y)} \in H_2,$$

ove la seconda uguaglianza segue da quanto già dimostrato al punto (b). Pertanto $x *_1 \overline{y} \in f^{-1}(H_2)$. Ciò prova che $f^{-1}(H_2)$ è un sottogruppo di G_2. □

Nota Se $(G_1, +_1)$ e $(G_2, +_2)$ sono gruppi additivi, le proprietà (a) e (b) della Proposizione 3.3 si scrivono nella forma:

(a) $f(0_{G_1}) = 0_{G_2}$.
(b) per ogni $x \in G_1$, $-f(x) = f(-x)$.

Se $(G_1, \cdot_1)$ e $(G_2, \cdot_2)$ sono gruppi moltiplicativi,

(a) $f(1_{G_1}) = 1_{G_2}$.
(b) per ogni $x \in G_1$, $f(x)^{-1} = f(x^{-1})$.

Se $(G_1, +_1)$ è un gruppo additivo e $(G_2, \cdot_2)$ è un gruppo moltiplicativo,

(a) $f(0_{G_1}) = 1_{G_2}$.
(b) per ogni $x \in G_1$, $f(x)^{-1} = f(-x)$.

Se $(G_1, \cdot_1)$ è un gruppo moltiplicativo e $(G_2, +_2)$ è un gruppo additivo,

(a) $f(1_{G_1}) = 0_{G_2}$.
(b) per ogni $x \in G_1$, $-f(x) = f(x^{-1})$.

Definizione 3.4 Siano $(G_1, *_1)$ e $(G_2, *_2)$ gruppi e sia $f : G_1 \to G_2$ un omomorfismo di gruppi. Allora si dice *nucleo* di f l'insieme

$$\operatorname{Ker} f = f^{-1}\left(\{e_2\}\right) = \left\{x \in G_1 \middle| f(x) = e_2\right\},$$

ove e_2 è l'elemento neutro di G_2.
Si dice *immagine* di f l'insieme

$$\operatorname{Im} f = f\left(G_1\right) = \left\{f(x) \middle| x \in G_1\right\}.$$

Corollario 3.5 Siano $(G_1, *_1)$ e $(G_2, *_2)$ gruppi e sia $f : G_1 \to G_2$ un omomorfismo di gruppi. Allora $\operatorname{Ker} f$ è un sottogruppo di G_1 ed $\operatorname{Im} f$ è un sottogruppo di G_2.

Dimostrazione: In base all'Esempio 2.17 (a), $\{e_2\}$ è un sottogruppo di G_2. Quindi la prima parte della tesi segue dalla Proposizione 3.3 (d). La seconda parte segue dalla Proposizione 3.3 (c). □

Definizione 3.6 Si dice *monomorfismo* un omomorfismo iniettivo. Si dice *epimorfismo* un omomorfismo suriettivo.

Osservazione 3.7 Dalle Definizioni 3.1 e 3.6 segue che un omomorfismo è un isomorfismo se e solo se è un monomorfismo ed un epimorfismo.

Proposizione 3.8 *(Caratterizzazione di monomorfismi ed epimorfismi di gruppi)* Siano $(G_1,*_1)$ e $(G_2,*_2)$ gruppi e sia $f: G_1 \to G_2$ un omomorfismo di gruppi. Allora

(a) f è un monomorfismo se e solo se il nucleo di f è il sottogruppo banale di G_1;

(b) f è un epimorfismo se e solo se l'immagine di f è il sottogruppo totale di G_2.

Dimostrazione: (a) Sia e_1 l'elemento neutro di G_1. Allora, in base alla Proposizione 3.3 (a), $\{e_1\} \subset \mathrm{Ker}f$. Supponiamo che f sia un monomorfismo. Se $x \in \mathrm{Ker}f$, allora $f(x) = e_2 = f(e_1)$, ove e_2 è l'elemento neutro di G_2. Dall'iniettività di f segue che $x = e_1$. Ciò prova che $\mathrm{Ker}f \subset \{e_1\}$, e quindi vale l'uguaglianza. Viceversa, supponiamo che $\mathrm{Ker}f = \{e_1\}$. Siano $x, y \in G_1$ tali che $f(x) = f(y)$. Allora, in base alla Proposizione 3.3 (b),

$$e_2 = f(x) *_2 \overline{f(y)} = f(x) *_2 f(\overline{y}) = f(x *_1 \overline{y}).$$

Dunque $x *_1 \overline{y} \in \mathrm{Ker}f$. Ciò, per ipotesi, implica che $x *_1 \overline{y} = e_1$, ossia che il simmetrico di $\overline{y}$ è x. Ma, in base alla Proposizione 2.8 (a), $\overline{\overline{y}} = y$. Dunque $x = y$. Ciò prova che f è un monomorfismo.
(b) La tesi segue immediatamente dalle Definizioni 3.4 e 3.6, oltre che dal Corollario 3.5. □

Esempio 3.9 Sia $n \in \mathbb{N}$, e sia $f_n : \mathbb{Z} \to \mathbb{Z}$ l'applicazione definita da $a \mapsto na$ per ogni $a \in \mathbb{Z}$. Allora f_n è un endomorfismo di $(\mathbb{Z}, +)$. Infatti, per ogni $a, b \in \mathbb{Z}$,

$$f_n(a+b) = n(a+b) = na + nb = f_n(a) + f_n(b).$$

Si osservi che f_0 è l'omomorfismo banale, f_1 l'automorfismo identico. Sia ora $n \geq 2$. Allora, per ogni $a \in \mathbb{Z}$, si ha che $a \in \mathrm{Ker}\, f_n \Leftrightarrow 0 = f_n(a) = na \Leftrightarrow a = 0$. Dunque si ha che $\mathrm{Ker}\, f_n = \{0\}$. Inoltre $\mathrm{Im}\, f_n = \{na \mid a \in \mathbb{Z}\} = H_n$, che è il sottogruppo di $\mathbb{Z}$ incontrato nell'Esercizio 2.27 (a). Si ha $H_0 = \{0\}$, $H_1 = \mathbb{Z}$, mentre $H_n \neq \mathbb{Z}$ per ogni $n \geq 2$. Abbiamo così che

- f_0 non è né un monomorfismo, né un epimorfismo;
- f_1 è un isomorfismo;
- per ogni $n \geq 2$, f_n è un monomorfismo, ma non un epimorfismo.

Vediamo ora il comportamento degli omomorfismi di gruppi rispetto alla composizione e all'inversione.

Proposizione 3.10 *(Composizione di omomorfismi di gruppi)* Siano $(G_1,*_1)$, $(G_2,*_2)$ e $(G_3,*_3)$ gruppi, e siano $f: G_1 \to G_2$ e $g: G_2 \to G_3$ omomorfismi di gruppi. Allora $g \circ f: G_1 \to G_3$ è un omomorfismo di gruppi.

Dimostrazione: Siano $x, y \in G_1$. Allora

$$g \circ f(x *_1 y) = g(f(x *_1 y)) = g(f(x) *_2 f(y)) = g(f(x)) *_3 g(f(y)) = g \circ f(x) *_3 g \circ f(y).$$

Ciò prova che $g \circ f$ è un omomorfismo di gruppi. □

Proposizione 3.11 *(Isomorfismi inversi)* L'applicazione inversa di un isomorfismo di gruppi è un isomorfismo di gruppi.

Dimostrazione: Siano $(G_1, *_1)$ e $(G_2, *_2)$ gruppi e sia $f: G_1 \to G_2$ un isomorfismo di gruppi. Sia $f^{-1}: G_2 \to G_1$ la sua applicazione inversa. Poiché essa è bigettiva, resta da provare che essa è un omomorfismo. Siano $u, v \in G_2$, e siano $x = f^{-1}(u), y = f^{-1}(v)$. Allora, essendo *f* un omomorfismo,

$$f(x *_1 y) = f(x) *_2 f(y) = f(f^{-1}(u)) *_2 f(f^{-1}(v)) = u *_2 v.$$

Segue che

$$f^{-1}(u *_2 v) = x *_1 y = f^{-1}(u) *_1 f^{-1}(v).$$

Ciò prova che f^{-1} è un omomorfismo, e dunque un isomorfismo. □

Definizione 3.12 Si dice che il gruppo $(G_1, *_1)$ è *isomorfo* al gruppo $(G_2, *_2)$ se esiste un isomorfismo di gruppi $f: G_1 \to G_2$. In tal caso si scrive $G_1 \simeq G_2$. Scriveremo anche $G_1 \overset{f}{\simeq} G_2$, quando vorremo specificare l'isomorfismo.

La precedente definizione introduce, nella classe dei gruppi, una relazione binaria $\simeq$, detta di *isomorfismo.* Questa, in realtà, è una *relazione di equivalenza*.

Proposizione 3.13 *(Relazione di isomorfismo)* La relazione di isomorfismo per i gruppi è riflessiva, simmetrica e transitiva.

Dimostrazione: Per ogni gruppo G si ha $G \overset{id_G}{\simeq} G$, quindi $G \simeq G$. Ciò prova che $\simeq$ è riflessiva. Siano ora G_1, G_2 gruppi tali che $G_1 \overset{f}{\simeq} G_2$. Allora, in base alla Proposizione 3.11, $G_2 \overset{f^{-1}}{\simeq} G_1$, e quindi $G_2 \simeq G_1$. Ciò prova che $\simeq$ è simmetrica. Infine, siano G_1, G_2, G_3 gruppi tali che $G_1 \overset{f}{\simeq} G_2$, $G_2 \overset{g}{\simeq} G_3$. Allora, in base alla Proposizione 3.10, $G_1 \overset{g \circ f}{\simeq} G_3$. Ciò prova che $\simeq$ è transitiva. □

Nota La Proposizione 3.13 ci consente di dire, quando $G_1 \simeq G_2$, che G_1 e G_2 sono *gruppi isomorfi*, senza precisare alcun ordine tra i due gruppi, ossia senza specificare la direzione dell'isomorfismo esistente tra loro.

Esempio 3.14 I gruppi H_n, con $n \geq 1$, dell'Esempio 3.9 sono a due a due isomorfi. Infatti, per ogni $n \geq 1$, l'applicazione $f_n': H_1 = \mathbb{Z} \to H_n$ definita da $a \mapsto na$ per ogni $a \in \mathbb{Z}$ è un isomorfismo.

Quindi, per ogni $n, m \geq 1$, l'applicazione $f'_m \circ (f'_n)^{-1} : H_n \to H_m$, definita da $na \mapsto ma$ per ogni $a \in \mathbb{Z}$, è un isomorfismo.

Esempio 3.15
(a) I gruppi banali sono a due a due isomorfi. Infatti l'unica applicazione esistente tra due gruppi di cardinalità 1 è ovviamente un omomorfismo, e quindi un isomorfismo.
(b) I gruppi di cardinalità 2 sono a due a due isomorfi. Abbiamo visto nella Lezione 2 che, se $X = \{x, y\}$ è un insieme con due elementi, allora esiste (a meno di ridenominare gli elementi) un'unica operazione $*$ che lo renda un gruppo, precisamente quella data dalla tavola di composizione

$*$	x	y
x	y	x
y	x	y

ove abbiamo supposto che y sia l'elemento neutro. Dato un altro gruppo di cardinalità 2, costituito dall'insieme $U = \{u, v\}$ dotato dell'operazione $\vartriangle$, la sua tavola di composizione sarà, pertanto,

$\vartriangle$	u	v
u	v	u
v	u	v

supponendo che v sia l'elemento neutro. L'applicazione $f : X \to U$ definita da $f(x) = u$, $f(y) = v$, è allora evidentemente un omomorfismo di gruppi: rispetta le operazioni perché trasforma la tavola di composizione del primo gruppo nella tavola di composizione del secondo gruppo. Essendo bigettiva, è un isomorfismo.
Analogamente si conclude che anche i gruppi di cardinalità 3 sono a due a due isomorfi.

In generale, due gruppi isomorfi sono gruppi che hanno la stessa struttura su insiemi equipotenti. Nel caso di insiemi finiti, ciò avviene se e solo se le tavole di composizione dei due gruppi coincidono a meno di sostituire elementi uguali (del primo gruppo) con elementi uguali (del secondo gruppo).

Se, dunque, la relazione di isomorfismo equivale ad un'identità di struttura, le operazioni di due gruppi isomorfi devono godere delle stesse proprietà.

Proposizione 3.16 *(Commutatività e isomorfismo di gruppi)* Siano $(G_1, *_1)$ e $(G_2, *_2)$ gruppi isomorfi. Allora G_1 è abeliano se e solo se G_2 è abeliano.

Dimostrazione: Sia $f : G_1 \to G_2$ un isomorfismo di gruppi. Supponiamo che G_1 sia abeliano. Siano $u, v \in G_2$. Siano $x = f^{-1}(u)$ e $y = f^{-1}(v)$. Allora

$$u *_2 v = f(x) *_2 f(y) = f(x *_1 y) = f(y *_1 x) = f(y) *_2 f(x) = v *_2 u,$$

ove la seconda e la quarta uguaglianza seguono dalla definizione di omomorfismo, la terza dalla commutatività di $*_1$. Ciò prova che G_2 è abeliano. Invertendo i ruoli di G_1 e G_2 (ossia sostituendo, nel ragionamento, f con f^{-1}), si prova l'implicazione opposta. □

Esercizio 3.17* Dire quali delle seguenti applicazioni sono omomorfismi, monomorfismi, epimorfismi, isomorfismi di gruppi. Determinare, quando possibile, nucleo e immagine.

(a) $f : \mathbb{Q}^* \to \mathbb{Q}^*$ definita da $x \mapsto x^{-1}$ per ogni $x \in \mathbb{Q}^*$.
(b) $f : \mathbb{Z} \to \mathbb{Q}^*$ definita da $a \mapsto 2^a$ per ogni $a \in \mathbb{Z}$.
(c) $f : \mathbb{R}^* \to \mathbb{R}^*$ definita da $x \mapsto x^2$ per ogni $x \in \mathbb{R}^*$.
(d) $f : \mathbb{R}^* \to \mathbb{R}^*$ definita da $x \mapsto x^3$ per ogni $x \in \mathbb{R}^*$.
(e) $f : \mathbb{R} \to \mathbb{R}$ definita da $x \mapsto x+1$ per ogni $x \in \mathbb{R}$.
(f) $f : \mathbb{Z} \to R_2 = \{-1,1\}$ definita da $a \mapsto 1$ se a è pari, $a \mapsto -1$ se a è dispari, per ogni $a \in \mathbb{Z}$.