

AL210 - Appunti integrativi - 3

Prof. Stefania Gabelli - a.a. 2016-2017

Nello studio delle strutture algebriche, sono interessanti le relazioni che sono “compatibili con le operazioni”.

Vogliamo dimostrare che le relazioni di equivalenza su un gruppo $G = (G, *)$ che sono compatibili con l'operazione $*$ sono in corrispondenza biunivoca con certi sottogruppi particolari di G , che si chiamano *sottogruppi normali*. Questi sottogruppi sono stati considerati per la prima volta da J.-L. Lagrange nell'ambito dei suoi studi sulla risolubilità per radicali delle equazioni polinomiali (1770).

Vedremo in seguito che, analogamente, le relazioni di equivalenza su un anello $A = (A, +, \cdot)$ che sono compatibili con entrambe le operazioni di addizione e moltiplicazione sono in corrispondenza biunivoca con certi sottoanelli di A , che si chiamano *ideali*. Il concetto di ideale è nato nella metà del 1800, in seguito ai risultati di E. Kummer sull'Ultimo Teorema di Fermat.

Relazioni compatibili

Sia ρ una relazione sull'insieme X . Se $*$ è una operazione su X , ρ si dice *compatibile con $*$* se

$$x \rho x', y \rho y' \Rightarrow (x * y) \rho (x' * y').$$

Ad esempio:

L'ordinamento naturale in \mathbb{R} è compatibile con l'addizione e la moltiplicazione:

$$x \geq x', y \geq y' \Rightarrow x + y \geq x' + y', \quad xy \geq x'y'.$$

La congruenza modulo n in \mathbb{Z} è compatibile con l'addizione e la moltiplicazione:

$$x \equiv_n x', y \equiv_n y' \Rightarrow x + y \equiv_n x' + y', \quad xy \equiv_n x'y'.$$

Se ρ è una relazione di equivalenza compatibile con $*$, si può (ben) definire sull'insieme X/ρ delle classi di equivalenza, una operazione “indotta da $*$ ”, che si indica ancora con lo stesso simbolo, ponendo:

$$\bar{x} * \bar{y} = \overline{x * y}.$$

Infatti, se ρ è una relazione di equivalenza compatibile con l'operazione $*$, l'operazione indotta su A/ρ non dipende dai rappresentanti delle classi. Infatti:

$$\bar{x} = \bar{x'}; \bar{y} = \bar{y'} \Leftrightarrow x \rho x', y \rho y' \Rightarrow (x*y) \rho (x'*y') \Leftrightarrow \overline{x*y} = \overline{x'*y'}$$

È facile verificare che se le operazioni su X sono associative, commutative o distributive, anche le operazioni indotte (qualora siano definite) lo sono.

In particolare:

Se $(G, *)$ è un gruppo (rispettivamente, commutativo) e ρ è una relazione di equivalenza compatibile con l'operazione $*$, l'insieme quoziente G/ρ è ancora un gruppo (rispettivamente, commutativo) rispetto all'operazione indotta. Ovvero

(g1) $*$ è associativa su G/ρ ;

(g2) esistenza dell'elemento neutro: Se e è l'elemento neutro di G , \bar{e} è l'elemento neutro di G/ρ . Infatti

$$\bar{g} * \bar{e} = \overline{g * e} = \bar{g} = \overline{e * g} = \bar{e} * \bar{g},$$

per ogni $g \in G$.

(g3) esistenza del simmetrico: se $g' \in G$ è il simmetrico di g , allora $\bar{g'}$ è il simmetrico di \bar{g} . Infatti

$$\bar{g} * \bar{g'} = \overline{g * g'} = \bar{e} = \overline{g' * g} = \bar{g'} * \bar{g}.$$

Nello stesso modo, se $(A, +, \cdot)$ è un anello (rispettivamente, commutativo, unitario) e ρ è compatibile con le operazioni $+$ e \cdot , l'insieme quoziente A/ρ è ancora un anello (rispettivamente, commutativo, unitario) rispetto alle operazioni indotte. Infatti, come visto sopra,

(a1) $(A/\rho, +)$ è un gruppo commutativo;

(a2) $(A/\rho, \cdot)$ è un semigruppato (rispettivamente, commutativo, unitario);

(a3) valgono le proprietà distributive della moltiplicazione rispetto alla somma.

Esempio: La relazione \equiv_n di congruenza modulo n su l'anello degli interi \mathbb{Z} è compatibile sia con l'addizione che con la moltiplicazione, quindi, ponendo $\mathbb{Z}_n := \mathbb{Z}/\equiv_n$, si ha che $(\mathbb{Z}_n, +, \cdot)$ è un anello, detto l'*anello delle classi resto modulo n* .

Le operazioni indotte su \mathbb{Z}_n sono definite da:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Sottogruppi normali

Una famiglia $\{X_i\}_{i \in I}$ di sottoinsiemi di un insieme X è una *partizione* di X se (1) $X = \bigcup_{i \in I} X_i$, (2) comunque scelti $i, j \in I$, risulta $X_i = X_j$ oppure $X_i \cap X_j = \emptyset$.

Le partizioni di un insieme X sono in corrispondenza biunivoca con le relazioni di equivalenza definite sull'insieme stesso.

Infatti, se ρ è una relazione di equivalenza su X e \bar{x} è la classe di $x \in X$, si ha che $X = \bigcup_{x \in X} \bar{x}$ è una partizione. Viceversa, data una partizione $X = \bigcup_{i \in I} X_i$, la relazione $x \rho x'$ se e soltanto se x e x' appartengono ad uno stesso insieme X_i della partizione è una relazione di equivalenza su X .

Quindi due relazioni di equivalenza sono uguali se e soltanto se hanno le stesse classi di equivalenza.

Abbiamo già visto che importanti partizioni di un gruppo G sono date dalle classi laterali rispetto a un sottogruppo.

Sia G un gruppo (in notazione moltiplicativa) e sia $H \subseteq G$ un sottogruppo. Per ogni $g \in G$, definiamo i due sottoinsiemi:

$$gH = \{gh; h \in H\} \text{ (classe laterale sinistra di } H \text{ rispetto a } g\text{);}$$

$$Hg = \{hg; h \in H\} \text{ (classe laterale destra di } H \text{ rispetto a } g\text{)}.$$

Il sottogruppo H si dice *normale in* G se $gH = Hg$, per ogni $g \in G$, questo significa che, per ogni $g \in G$ ed $h \in H$, esiste $h' \in H$ tale che $gh = h'g$.

Se G è commutativo, $gh = hg$, per ogni $h \in H$ e $g \in G$, dunque ogni sottogruppo di un gruppo commutativo è normale.

Il sottogruppo $N := \langle (123) \rangle$ di S_3 è normale, mentre il sottogruppo $H := \langle (12) \rangle$ non lo è.

Sappiamo che:

Proposizione 3.1: L'insieme delle classi laterali sinistre (rispettivamente, destre) di H formano un *partizione* di G . Cioè:

(1) G è unione delle classi laterali sinistre (rispettivamente, destre) di H , ovvero $G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg$;

(2) Due classi laterali sinistre (rispettivamente, destre) di H coincidono oppure sono disgiunte, ovvero, se $g, g' \in G$, risulta $gH = g'H$ oppure $gH \cap g'H = \emptyset$ (rispettivamente, $Hg = Hg'$ oppure $Hg \cap Hg' = \emptyset$).

Possiamo allora definire due relazioni di equivalenza associate ad H ,

Relazione di congruenza sinistra modulo H :

$$x \sigma_H y \Leftrightarrow x, y \in gH, \text{ per qualche } g \in G.$$

Poiché $x = xe \in xH$, $y \in yH$ si ha:

$$x \sigma_H y \Leftrightarrow xH = yH \Leftrightarrow x^{-1}y \in H.$$

Relazione di congruenza destra modulo H :

$$x \delta_H y \Leftrightarrow x, y \in Hg, \text{ per qualche } g \in G.$$

Poiché $x = ex \in Hx$, $y \in Hy$ si ha

$$x \delta_H y \Leftrightarrow Hx = Hy \Leftrightarrow xy^{-1} \in H.$$

Per definizione, la classe di equivalenza dell'elemento $g \in G$ rispetto a σ_H è la classe laterale sinistra gH e, analogamente, la classe di equivalenze di g rispetto a δ_H è la classe laterale destra Hg . Allora, i rispettivi insiemi quozienti sono:

$$G/\sigma_H = \{gH; g \in G\}; \quad G/\delta_H = \{Hg; g \in G\}.$$

Segue subito dalle definizioni che $\sigma_H = \delta_H$ se e soltanto se H è un sottogruppo normale.

Teorema 3.2: Sia H un sottogruppo di G e siano σ_H , δ_H le relazioni associate ad H sopra definite. Le seguenti condizioni sono equivalenti:

- (i) H è un sottogruppo normale di G (cioè $gH = Hg$, per ogni $g \in G$);
- (ii) La relazione σ_H è compatibile;
- (iii) La relazione δ_H è compatibile;
- (iv) $\sigma_H = \delta_H$.

Dimostrazione: Poniamo $\sigma := \sigma_H$ e $\delta := \delta_H$.

(i) \Leftrightarrow (iv) Basta osservare che classi di equivalenza di σ sono le classi laterali sinistre e quelle di δ sono le classi laterali destre.

(i), (iv) \Rightarrow (ii), (iii). Sia $\rho := \sigma = \delta$. Dobbiamo far vedere che, se $x_1 \rho y_1$ e $x_2 \rho y_2$, allora $x_1 x_2 \rho y_1 y_2$.

Poiché per ipotesi $x_1 H = Hx_1$, possiamo scrivere $x_1 h = h' x_1$, $h, h' \in H$. Inoltre (poiché $\rho := \delta$) $x_1 y_1^{-1}, x_2 y_2^{-1} \in H$. Allora

$$(x_1 x_2)(y_1 y_2)^{-1} = (x_1 x_2)(y_2^{-1} y_1^{-1}) = x_1 (x_2 y_2^{-1}) y_1^{-1} = x_1 h y_1^{-1} = h' (x_1 y_1^{-1}) \in H.$$

(ii) \Rightarrow (iv). Sia $x \sigma y$. Poiché $y^{-1} \sigma y^{-1}$, per compatibilità $xy^{-1} \sigma yy^{-1} = e$. Dunque $xy^{-1} \in H$ e $x \delta y$.

Viceversa, sia $x \delta y$, ovvero $xy^{-1} \in H$. Allora $(xy^{-1}) \sigma e$ e poiché $y \sigma y$, per compatibilità risulta $x \sigma y$.

(iii) \Rightarrow (iv) Analogamente.

Se N è un sottogruppo normale di G , risulta $\sigma_N = \delta_N$. questa relazione si chiama semplicemente la relazione di *congruenza modulo N* (senza distinguere tra destra e sinistra) e verrà indicata con ρ_N . Dunque, se N è un sottogruppo normale di G ,

$$x \rho_N y \Leftrightarrow x^{-1} y \in H \Leftrightarrow xy^{-1} \in H.$$

Dimostriamo finalmente che le relazioni di equivalenza compatibili sono in corrispondenza biunivoca con i sottogruppi normali.

Proposizione 3.3: Sia ρ una relazione di equivalenza compatibile sul gruppo G . Allora l'insieme $N_\rho := \{x \in G; x \rho e\} = \bar{e}$ è un sottogruppo normale di G .

Dimostrazione: Sia $N := N_\rho$ e siano $x, y \in N$, ovvero $x \rho e$, $y \rho e$. Poiché $y^{-1} \rho y^{-1}$, per compatibilità abbiamo $xy^{-1} \rho y^{-1}$ ed $e \rho y^{-1}$. Dunque $xy^{-1} \rho e$, ovvero $xy^{-1} \in N$. Ne segue che N è un sottogruppo di G .

Inoltre, sempre per la compatibilità,

$$x \rho y \Leftrightarrow xy^{-1} \rho e \Leftrightarrow xy^{-1} \in N \Leftrightarrow x \sigma_N y.$$

Dunque σ_N coincide con ρ e perciò è compatibile. Allora, per il teorema precedente, N è normale.

Se ρ è una relazione compatibile su G e $N_\rho := \{x \in G; x \rho e\}$ è il sottogruppo normale di G associato a ρ , si ha che $\rho = \rho_{N_\rho}$ è la congruenza modulo N_ρ . Infatti:

$$x \rho_{N_\rho} y \Leftrightarrow xy^{-1} \in N_\rho \Leftrightarrow xy^{-1} \rho e \Leftrightarrow x \rho y.$$

Viceversa, se N è un sottogruppo normale di G e ρ_N è la congruenza modulo N , allora $N = N_{\rho_N}$. Infatti

$$N_{\rho_N} := \{x \in G; x \rho_N e\} = N.$$

Abbiamo allora il seguente risultato

Teorema 3.4: Sia G un gruppo. Indichiamo con \mathcal{R} l'insieme delle relazioni di equivalenza su G compatibili e con \mathcal{N} l'insieme dei sottogruppi normali di G . L'applicazione

$$\alpha : \mathcal{R} \longrightarrow \mathcal{N}; \quad \rho \mapsto N_\rho := \{x \in G; x \rho e\} = \bar{e}$$

è un'applicazione biunivoca, la cui inversa è l'applicazione

$$\beta : \mathcal{N} \longrightarrow \mathcal{R}; \quad N \mapsto \rho_N$$

che associa ad ogni sottogruppo normale N di G la relazione ρ_N di congruenza modulo N da esso definita.

Dimostrazione: Per quanto visto sopra, α e β sono ben definite. Inoltre $\beta(\alpha(\rho)) = \beta(N_\rho) = \rho_{N_\rho} = \rho$ e $\alpha(\beta(N)) = \alpha(\rho_N) = N_{\rho_N} = N$.

Se G è commutativo ogni suo sottogruppo è normale. In questo caso, tutte le relazioni di congruenza (destra o sinistra) modulo un sottogruppo H di G sono compatibili.

Se $N \subseteq G$ è un sottogruppo normale e ρ_N è la relazione di congruenza modulo N , l'insieme quoziente G/ρ_N viene indicato con G/N . Dunque si ha

$$G/N := G/\rho_N = \{gN; g \in G\} = \{Ng; g \in G\}.$$

Con questa notazione, per la compatibilità della relazione ρ_N , abbiamo:

Proposizione 3.5: Se $N \subseteq G$ è un sottogruppo normale del gruppo G , l'insieme quoziente G/N delle classi di congruenza modulo N è un gruppo, con l'operazione tra classi

$$(gN)(g'N) = (gg')N.$$

L'elemento neutro di G/N è la classe di e , cioè $eN = N$. Il simmetrico della classe gN è la classe del simmetrico di g , $(gN)^{-1} = g^{-1}N$.

Inoltre, se G è commutativo anche il gruppo quoziente G/N lo è.

Se N è un sottogruppo normale di G , il gruppo G/N si chiama il *gruppo quoziente modulo N* .

Omomorfismi

Ricordiamo che tutte le operazioni considerate sono associative. Quindi, se $(X, *_1, \dots, *_n)$ è una struttura algebrica, $(X, *_i)$ è un semigruppato, per ogni operazione $*_i$.

Nello studio delle strutture algebriche, sono interessanti le funzioni di insiemi che “conservano le operazioni”. Queste funzioni si chiamano *omomorfismi*.

Se $(G, *)$, $(G', *')$ sono (semi)gruppi, un *omomorfismo di (semi)gruppi* è una funzione $f : G \rightarrow G'$ tale che

$$f(g * h) = f(g) *' f(h), \text{ per ogni } g, h \in G.$$

Più in generale, se $(X, *_1, \dots, *_n)$ e $(X', *'_1, \dots, *'_n)$ sono strutture algebriche dello stesso tipo, un *omomorfismo* è una funzione $f : X \rightarrow X'$ tale che

$$f(x *_i y) = f(x) *'_i f(y), \text{ per ogni } x, y \in X : i = 1, \dots, n.$$

Cioè f è un omomorfismo di semigruppato, per ogni operazione $*_i$.

Un omomorfismo biiettivo si chiama un *isomorfismo*. Un omomorfismo di X in X si chiama un *endomorfismo* e un isomorfismo di X in X si chiama un *automorfismo*.

Notiamo che:

(1) La funzione identica $id_X : X \rightarrow X; x \mapsto x$ è un automorfismo di X . Inoltre se $Y \subseteq X$, la funzione identica su Y , $id_Y : Y \rightarrow X; y \mapsto y$ è un omomorfismo iniettivo di Y in X .

(2) Se $f : X \rightarrow X', g : X' \rightarrow X''$ sono omomorfismi (rispettivamente, isomorfismi), anche la loro composizione $f \circ g : X \rightarrow X''$ è un omomorfismo (rispettivamente, isomorfismo).

(3) Se $f : X \rightarrow X'$ è un isomorfismo, anche l'applicazione inversa $f^{-1} : X' \rightarrow X$ è un isomorfismo.

Infatti, se f è biettiva, è definita la funzione inversa f^{-1} , che è biettiva. Per vedere che f^{-1} è un omomorfismo, dobbiamo verificare che se $*$ è un'operazione su X e $*'$ è la corrispondente operazione su X' , risulta

$$f^{-1}(x' *' y') = f^{-1}(x') * f^{-1}(y')$$

Poiché f è un isomorfismo, esistono (e sono unici) $x, y \in X$ tali che $x' = f(x)$ e $y' = f(y)$ e inoltre $f(x * y) = f(x) *' f(y) = x' *' y'$. Allora

$$f^{-1}(x' *' y') = f^{-1}(f(x) *' f(y)) = f^{-1}(f(x * y)) = x * y = f^{-1}(x') * f^{-1}(y').$$

Ne segue che la relazione di isomorfismo tra strutture algebriche si comporta come una relazione di equivalenza. Infatti è *riflessiva*, per (1), *simmetrica*, per (3), e *transitiva*, per (2).

Le strutture algebriche si classificano *a meno di isomorfismi*; infatti due strutture algebriche isomorfe hanno le stesse proprietà caratterizzanti e quindi si considerano uguali.

L'insieme $Aut(X)$ degli automorfismi di X è un sottogruppo del gruppo $\mathcal{T}(X)$ delle trasformazioni su X , rispetto alla composizione di funzioni.

Infatti:

(sg0) La composizione di automorfismi è un automorfismo, per (2);

(sg1) La funzione identica $id_X : X \rightarrow X; x \mapsto x$ è un automorfismo, per (1);

(sg2) Se f è un automorfismo di X , anche f^{-1} lo è, per (3).

Proprietà degli omomorfismi

Siano X, X' strutture algebriche e $f : X \rightarrow X'$ un omomorfismo. Ovvero, se $*$ è un'operazione su X e $*'$ la corrispondente operazione su X' , si ha

$$f(x * y) = f(x) *' f(y), \text{ per ogni } x, y \in X.$$

Valgono le seguenti proprietà:

(1) Se $Y \subseteq X$ è un sottoinsieme chiuso rispetto a $*$, cioè $Y * Y \subseteq Y$, allora $f(Y)$ è un sottoinsieme di X' chiuso rispetto a $*'$, cioè $f(Y) *' f(Y) \subseteq f(Y)$. In altre parole, se Y è un sottosemigruppo di X rispetto a $*$, allora $f(Y)$ è un sottosemigruppo di X' rispetto a $*'$.

Infatti, se $y_1, y_2 \in Y$ e Y è chiuso, si ha $y_1 * y_2 \in Y$. Allora

$$f(y_1) *' f(y_2) = f(y_1 * y_2) \subseteq f(Y).$$

(2) Se e è l'elemento neutro di X rispetto a $*$, $f(e)$ è l'elemento neutro di $f(X)$ rispetto a $*'$. Inoltre, se X' ha un elemento neutro e' rispetto a $*'$ tale che $e' \in f(X)$, deve risultare $f(e) = e'$.

Infatti, se $e * x = x = x * e$, per ogni $x \in X$, deve essere

$$f(e) *' f(x) = f(e * x) = f(x) = f(x * e) = f(x) *' f(e)$$

per ogni $f(x) \in f(X)$.

Inoltre, se $e' \in f(X)$, e' è anche un elemento neutro di $f(X)$. Quindi, per l'unicità dell'elemento neutro in $f(X)$, deve essere $f(e) = e'$.

(3) Se $x \in X$ è simmetrizzabile rispetto a $*$, con simmetrico y , allora $f(x) \in f(X)$ è simmetrizzabile in $f(X)$ rispetto a $*'$, con simmetrico $f(y)$.

Infatti, se e è l'elemento neutro di X rispetto a $*$ e si ha $x * y = e = y * x$, allora $f(e)$ è l'elemento neutro di $f(X)$ rispetto a $*'$ (per (2)) e risulta

$$f(x) *' f(y) = f(e) = f(y) *' f(x).$$

Da queste proprietà segue subito che:

Proposizione 3.6: Se $f : G \rightarrow G'$ è un omomorfismo di gruppi e H è un sottogruppo di G , $f(H)$ è un sottogruppo di G' . In particolare, $\text{Im}(f) = f(G)$ è un sottogruppo di G' .

Inoltre, se e ed e' sono gli elementi neutri di G e G' rispettivamente, si ha $f(e) = e'$ e, in notazione moltiplicativa, $f(g^{-1}) = f(g)^{-1}$, per ogni $g \in G$.

Dimostrazione: $f(H)$ è chiuso per la proprietà (1). Dobbiamo far vedere che $e' \in f(H)$ e $f(h)^{-1} \in f(H)$, per ogni $h \in H$.

Per la proprietà (2), $f(e)$ è l'elemento neutro di $f(G)$. Allora, per ogni $g \in G$, si ha $f(g)f(e) = f(g) = f(g)e'$. Poiché $f(g)$ è simmetrizzabile in G' , cancellando $f(g)$ si ha $f(e) = e'$. In particolare, poiché $e \in H$, si ha $e' = f(e) \in f(H)$.

Infine, per ogni $g \in G$,

$$e' = f(e) = f(gg^{-1}) = f(g)f(g^{-1}); \quad e' = f(e) = f(g^{-1}g) = f(g^{-1})f(g).$$

Da cui, per l'unicità del simmetrico in G' , si ottiene $f(g)^{-1} = f(g^{-1})$. In particolare, poiché per ogni $h \in H$, si ha $h^{-1} \in H$, allora $f(h)^{-1} = f(h^{-1}) \in f(H)$.

La relazione nucleo

Se $f : X \rightarrow X'$ è un'applicazione di insiemi, la relazione definita su X da

$$x \nu_f y \Leftrightarrow f(x) = f(y)$$

è una relazione di equivalenza su X , chiamata la *relazione nucleo* associata ad f .

Teorema 3.7: Se $f : X \rightarrow X'$ è un omomorfismo di strutture algebriche, la relazione nucleo ν_f è compatibile con le operazioni di X .

Dimostrazione: Sia $*$ una operazione su X e sia $*'$ la rispettiva operazione su X' . Se f è un omomorfismo e $\nu := \nu_f$, si ha:

$$\begin{aligned} x \nu x', y \nu y' &\Rightarrow f(x) = f(x'), f(y) = f(y') \Rightarrow \\ f(x * y) &= f(x) *' f(y) = f(x') *' f(y') = f(x' * y') \Rightarrow . \\ (x * y) \nu &(x' * y') \end{aligned}$$

Per quanto visto nel Teorema 3.4, ad una relazione di equivalenza ρ compatibile su un gruppo G resta associato un sottogruppo normale di G , precisamente il sottogruppo $N = \bar{e}$ formato dagli elementi equivalenti all'elemento neutro $e \in G$. Inoltre le classi di equivalenza di G rispetto a ρ sono precisamente le classi laterali di N . Cioè, in notazione moltiplicativa,

$$g \rho h \Leftrightarrow gN = hN \quad \text{e} \quad G/\rho = G/N = \{gN; g \in G\}.$$

Allora se $f : G \rightarrow G'$ è un omomorfismo di gruppi, il sottoinsieme

$$N_f = \bar{e} = \{n \in G; n \nu_f e\} = \{n \in G; f(n) = f(e) = e'\}$$

è un sottogruppo normale di G .

Questo sottogruppo N_f si chiama il *nucleo* di f e si indica con $\text{Ker}(f)$. (La parola inglese *Kernel* significa *Nocciolo*.)

Allora

$$\text{Ker}(f) = \{n \in G; f(n) = e'\}$$

e

$$\begin{aligned} g \nu_f h &\Leftrightarrow f(g) = f(h) \Leftrightarrow \bar{g} = g \text{Ker}(f) = h \text{Ker}(f) = \bar{h} \\ &\Leftrightarrow gh^{-1} \in \text{Ker}(f) \Leftrightarrow f(gh^{-1}) = e'. \end{aligned}$$

Dunque, per $g \in G$,

$$g \text{Ker}(f) = \{gn; n \in \text{Ker}(f)\} = \{h \in G, h \nu_f g\} = \{h \in G, f(h) = f(g)\}.$$

e

$$G/\nu_f = G/\text{Ker}(f) = \{g \text{Ker}(f); g \in G\}.$$

Notiamo che $\text{Ker}(f) = G$ se e soltanto se $f(g) = e'$, per ogni $g \in G$, cioè f è l'omomorfismo banale. Da quanto abbiamo appena visto, otteniamo:

Proposizione 3.8: Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi. Allora, se $f(g) = g'$, la controimmagine di g' è $f^{-1}(g') = g \text{Ker}(f)$.

Quindi f è iniettivo se e soltanto se $\text{Ker}(f) = \{e\}$.

Vogliamo ora dimostrare che un sottogruppo N di un gruppo G è normale se e soltanto se è il nucleo di qualche omomorfismo di gruppi $f : G \longrightarrow G'$.

Ricordiamo che se ρ è una relazione di equivalenza sull'insieme X , l'applicazione sull'insieme quoziente X/ρ

$$\pi : X \longrightarrow X/\rho; \quad x \mapsto \bar{x}$$

è suriettiva (π si chiama la *proiezione canonica*).

Proposizione 3.9: Sia $(G, *)$ un gruppo e sia ρ una relazione di equivalenza compatibile su G . Allora G/ρ è un gruppo e la proiezione canonica $\pi : G \longrightarrow G/\rho$ è un omomorfismo suriettivo di gruppi.

Dimostrazione: Abbiamo visto che G/ρ è un gruppo rispetto all'operazione indotta. Per vedere che π è un omomorfismo, basta osservare che, per come sono definite le operazioni indotte su G/ρ , si ha

$$\pi(x * y) = \overline{x * y} = \bar{x} * \bar{y} = \pi(x) * \pi(y).$$

Corollario 3.10: Se G è un gruppo e N è un sottogruppo normale di G , la proiezione canonica sul gruppo quoziente G/N ,

$$\pi : G \longrightarrow G/N; \quad g \mapsto gN$$

è un omomorfismo suriettivo di gruppi il cui nucleo è N .

Dimostrazione: Se N è un sottogruppo normale di un gruppo G , la relazione $\rho = \rho_N$ di congruenza modulo N è compatibile. Allora $G/N = G/\rho$ è un gruppo e la proiezione canonica

$$\pi : G \longrightarrow G/N; \quad g \mapsto gN$$

è un omomorfismo di gruppi. Inoltre, poiché l'elemento neutro di G/N è la classe $eN = N$, si ha

$$g \in \text{Ker}(\pi) \iff \pi(g) = gN = N \iff g \in N.$$

Dunque $\text{Ker}(\pi) = N$.

Proposizione 3.8: Sia G un gruppo. Un sottoinsieme N di G è un sottogruppo normale se e soltanto se esistono un gruppo G' ed un omomorfismo di gruppi $f : G \longrightarrow G'$ il cui nucleo è $\text{Ker}(f) = N$.

Dimostrazione: Se $f : G \longrightarrow G'$ è un omomorfismo di gruppi, come visto sopra, $\text{Ker}(f)$ è un sottogruppo normale di G . Il viceversa segue dal Corollario 3.10.

Primo Teorema di Omomorfismo

Per le funzioni di insiemi, vale il seguente

Teorema di Decomposizione delle Funzioni: Siano $f : X \rightarrow X'$ un'applicazione di insiemi e ν_f la relazione nucleo associata ad f . Allora l'applicazione

$$\bar{f} : X/\nu_f \rightarrow \text{Im}(f) \quad \bar{x} \mapsto f(x)$$

è ben definita e biiettiva. Inoltre, se

$$\pi : X \rightarrow X/\nu_f \quad x \mapsto \bar{x}$$

è la proiezione canonica, si ha $f = \pi \circ \bar{f}$.

Dimostrazione: È una semplice verifica, ricordando che

$$x \nu_f y \Leftrightarrow f(x) = f(y).$$

Nel caso in cui f sia un omomorfismo di strutture algebriche, Il Teorema di Decomposizione delle Funzioni diventa il così detto *Teorema Fondamentale di Omomorfismo*.

Teorema Fondamentale di Omomorfismo per i Gruppi: Sia $f : G \rightarrow G'$ un omomorfismo di gruppi. Allora:

- (1) $G/\text{Ker}(f)$ è un gruppo e la proiezione canonica

$$\pi : G \rightarrow G/\text{Ker}(f); \quad g \mapsto g \text{Ker}(f)$$

è un omomorfismo suriettivo di gruppi;

- (2) $\text{Im}(f)$ è un gruppo e l'applicazione

$$\bar{f} : G/\text{Ker}(f) \rightarrow \text{Im}(f) \quad \bar{g} \text{Ker}(f) \mapsto f(g)$$

è un (ben definito) isomorfismo di gruppi.

- (3) Risulta $f = \pi \circ \bar{f}$.

Dimostrazione: (1) segue dal Corollario 3.4, perché $\text{Ker}(f)$ è un sottogruppo normale di G .

(2) $\text{Im}(f)$ è un gruppo per la Proposizione 3.1. L'applicazione di insiemi \bar{f} è una (ben definita) funzione biiettiva. Inoltre, poiché f è un omomorfismo,

$$\bar{f}(g \text{Ker}(f) h \text{Ker}(f)) = \bar{f}(gh \text{Ker}(f)) = f(gh) = f(g)f(h) = \bar{f}(g \text{Ker}(f))\bar{f}(h \text{Ker}(f)).$$

- (3) segue dal Teorema per le Funzioni.