

CAPITOLO 6

[indice](#)

PROPRIETA' CHE SI CONSERVANO

1. Omomorfismi nella logica del primo ordine

Le nozioni di omomorfismo, congruenza, quoziente che abbiamo già definito nel Capitolo 2 per le strutture del primo ordine possono essere riformulate in modo da poterle applicare alle interpretazioni di un linguaggio del primo ordine. In questo paragrafo cominciamo con la nozione di omomorfismo.

Definizione 1.1. Siano (D, I) e (D', I') due interpretazioni di un linguaggio del primo ordine Λ , allora chiamiamo *omomorfismo* di (D, I) in (D', I') ogni funzione $f: D \rightarrow D'$ tale che, per ogni nome di operazione n -aria o , per ogni costante c e per ogni nome di relazione n -aria r in Λ risulti :

- (1) $f(I(o)(d_1, \dots, d_n)) = I'(o)(f(d_1), \dots, f(d_n))$;
- (2) $f(I(c)) = I'(c)$;
- (3) $(d_1, \dots, d_n) \in I(r) \Rightarrow (f(d_1), \dots, f(d_n)) \in I'(r)$,

per ogni d_1, \dots, d_n in D . Un omomorfismo è un *isomorfismo* se è invertibile ed il suo inverso è ancora un omomorfismo.

Nella seguente definizione si elencano alcuni tipi di omomorfismo.

Definizione 1.2. Nel seguito diciamo che un omomorfismo f

- è un *epimorfismo* se è suriettivo,
- è un *endomorfismo* se è un omomorfismo di I in se stesso
- è un *automorfismo* se è un isomorfismo di I in se stesso.
- è *pieno* se, per ogni nome di relazione r diversa dall'identità¹, risulta

$$(d_1, \dots, d_n) \in I(r) \Leftrightarrow (f(d_1), \dots, f(d_n)) \in I'(r).$$
- è una *immersione* se è un omomorfismo pieno per cui tale equivalenza vale anche per $=$,

$$(d_1, d_2) \in I(=) \Leftrightarrow (f(d_1), f(d_2)) \in I'(=).$$

Se (D, I) è una sottostruttura di una interpretazione (D', I') allora l'applicazione identica $i: D \rightarrow D'$ definita dall'essere $i(x) = x$ per ogni $x \in D$ è una immersione di I in I' .

Proposizione 1.3. Valgono le seguenti proposizioni:

- i) Ogni isomorfismo è una immersione (e quindi un omomorfismo pieno).
- ii) Nelle strutture algebriche, in cui l'unico nome di relazione è $=$, la nozione di omomorfismo pieno e quella di omomorfismo coincidono.
- iii) Nelle strutture normali le immersioni sono funzioni iniettive
- iv) Nelle strutture normali una funzione è un isomorfismo se e solo se è una immersione suriettiva.

Dim. Ci limitiamo a provare la iv), cioè che nelle strutture normali una immersione è iniettiva. Infatti basta osservare che se denotiamo con \equiv e \equiv' le interpretazioni di $=$ in I ed I' , rispettivamente allora un omomorfismo pieno f è una immersione se e solo se

$$d_1 \equiv d_2 \Leftrightarrow f(d_1) \equiv' f(d_2).$$

¹ Il motivo per cui si è supposto che r sia diverso da $=$ è che altrimenti si dovrebbe accettare che nei modelli normali tutti gli omomorfismi pieni siano iniettivi. In particolare si dovrebbe accettare che nella teoria delle strutture algebriche (che non può fare a meno dell'uguaglianza) siano considerati solo omomorfismi iniettivi.

Nel caso di strutture normali ciò equivale a dire che d_1 è identico a d_2 se e solo se $f(d_1)$ è identico a $f(d_2)$ e quindi equivale a dire che f è iniettiva.

Sappiamo che per definizione un omomorfismo conserva le operazioni delle due strutture coinvolte (l'immagine del composto è uguale al composto delle immagini). Il seguente teorema mostra che un omomorfismo conserva anche tutte le funzioni che si possono calcolare tramite tali operazioni, cioè tutte le funzioni che sono interpretazione di un termine.

Teorema 1.4. Siano I ed I' due interpretazioni, f un omomorfismo di I in I' , e t un termine le cui variabili libere sono tra x_1, \dots, x_n . Allora

$$f(I(t)(d_1, \dots, d_n)) = I'(t)(f(d_1), \dots, f(d_n)). \tag{1.1}$$

Dim. Si procede per induzione sulla complessità di t . Precisamente:

1. proviamo che il teorema vale per i termini che sono costanti o variabili
2. dimostriamo che se h è il nome di una operazione e se il teorema vale per i termini t_1, \dots, t_h allora il teorema vale anche per $t = h(t_1, \dots, t_h)$.

Infatti se t è la costante c allora

$$f(I(c)(d_1, \dots, d_n)) = f(I(c)) = I'(c) = I'(c)(f(d_1), \dots, f(d_n)).$$

Se t è la variabile x_i allora

$$f(I(x_i)(d_1, \dots, d_n)) = f(d_i) = I'(x_i)(f(d_1), \dots, f(d_n)).$$

Sia $t = h(t_1, \dots, t_h)$, allora

$$\begin{aligned} f(I(t)(d_1, \dots, d_n)) &= f(I(o)(I(t_1)(d_1, \dots, d_n), \dots, I(t_h)(d_1, \dots, d_n))) \\ &= I'(o)(f(I(t_1)(d_1, \dots, d_n)), \dots, f(I(t_h)(d_1, \dots, d_n))) \\ &= I'(o)(I'(t_1)(f(d_1), \dots, f(d_n)), \dots, I'(t_h)(f(d_1), \dots, f(d_n))) = I'(t)(f(d_1), \dots, f(d_n)). \quad \square \end{aligned}$$

Da notare che un termine è in un certo senso la descrizione di un algoritmo che utilizza le operazioni della struttura algebrica che stiamo considerando. Allora la proposizione ora dimostrata dice che:

- se applicando l'algoritmo t agli elementi d_1, \dots, d_n si ottiene l'elemento d
- allora applicando lo stesso algoritmo agli elementi $f(d_1), \dots, f(d_n)$ si ottiene $f(d)$.

Possiamo visualizzare al modo seguente questo fenomeno.

$input(d_1, \dots, d_n)$	$input(f(d_1), \dots, f(d_n))$
·	·
·	·
·	·
·	·
$write(d)$	$write(f(d))$

Esempio. Consideriamo il linguaggio additivo della teoria dei gruppi e come interpretazione il gruppo additivo dei reali $(R, +, -, 0)$. Allora la funzione $f(x) = 2 \cdot x$ è un endomorfismo in quanto

$$f(x+y) = 2 \cdot (x+y) = 2 \cdot x + 2 \cdot y = f(x) + f(y) ; f(0) = 0.$$

Questo significa che se, ad esempio, consideriamo il termine $t(x_1, x_2, x_3) = ((x_1 - x_2) + x_3) + x_1$ e lo applichiamo ad alcuni numeri, ad esempio 2, 4, 6 risulta

$$f(I(t)(2, 4, 6)) = I(t)(f(2), f(4), f(6))$$

oppure, equivalentemente,

$$2 \cdot ((2-4)+6)+2 = ((2 \cdot 2 - 2 \cdot 4) + 2 \cdot 6) + 2 \cdot 2.$$

Esempio. Siano G e G' due gruppi ed $f : G \rightarrow G'$ un omomorfismo di G in G' . Applicando la proposizione al termine $t(x, y, z) = (x \cdot y) \cdot (z^{-1} \cdot x)$ ed alla terna a, b, c di elementi di G , otterremo che

$$f((a \cdot b) \cdot (c^{-1} \cdot a)) = (f(a) \cdot f(b)) \cdot (f(c)^{-1} \cdot f(a)).$$

2. Un automorfismo per le radici complesse di un polinomio

Passiamo ora ad una semplice applicazione del teorema 1.4. Ci riferiamo al linguaggio della teoria degli anelli ed all'interpretazione (D, I) di tale linguaggio definita dal campo dei numeri complessi. Ricordiamo la definizione del campo dei numeri complessi.

Definizione 2.1. Il *campo dei numeri complessi* è l'interpretazione (C, I) del linguaggio della teoria degli anelli definita dal porre, detto R il campo dei numeri reali,

$$\begin{aligned} C &= \{(x, y) : x \in R \text{ e } y \in R\}, \\ I(+)((x, y), (x', y')) &= (x+x', y+y') \\ I(\cdot)((x, y), (x', y')) &= (x \cdot x' - y \cdot y', x \cdot y' + x' \cdot y) \\ I(0) &= (0, 0) \\ I(1) &= (1, 0). \end{aligned}$$

Si dimostra che la struttura ora definita è effettivamente un campo. Inoltre la funzione $f : R \rightarrow C$ definita ponendo $f(x) = (x, 0)$ è una immersione del campo dei numeri reali nel campo dei numeri complessi. Pertanto il campo dei numeri complessi è una estensione del campo dei numeri reali. Ciò permette, dato un numero reale x di scrivere x per denotare il numero complesso $(x, 0)$. In particolare scriveremo 0 ed 1 al posto di $(0, 0)$ e $(1, 0)$, rispettivamente. Se si indica con i il numero complesso $(0, 1)$, è subito visto che $i^2 = -1$ e $i \cdot (x, y) = (-y, x)$. Inoltre

$$(x, y) = (x, 0) + i \cdot (y, 0).$$

Pertanto, se identifichiamo $(x, 0)$ e $(y, 0)$ con x ed y , rispettivamente, possiamo scrivere ogni numero complesso nella forma $x+i \cdot y$.

Definizione 2.2. Chiamiamo *coniugio* la funzione $con : C \rightarrow C$ che associa ad ogni un numero complesso (x, y) il numero $con(x, y) = (x, -y)$.

In altre parole con è definito dall'equazione $con(x+iy) = x-iy$. La verifica della seguente proposizione è il risultato di semplici calcoli.

Proposizione 2.3. La funzione $con : C \rightarrow C$ è un automorfismo del campo dei numeri complessi.

Da tale proposizione segue che, qualunque sia il termine t ed i numeri complessi c_1, \dots, c_n ,

$$con((I(t)(c_1, \dots, c_n)) = I(t)(con(c_1), \dots, con(c_n))). \quad (2.1)$$

Pertanto, dovendo calcolare il coniugato del risultato di un algoritmo t applicato ai numeri c_1, \dots, c_n posso semplicemente applicare lo stesso algoritmo ai coniugati di c_1, \dots, c_n . Ad esempio, il coniugato del numero $(7-i) \cdot ((5+3i) \cdot (7-3i) - (8+3i))$ sarà il numero $(7+i) \cdot ((5-3i) \cdot (7+3i) - (8-3i))$. In questo caso si è applicata (2.1) al termine $t(x_1, x_2, x_3, x_4) = x_1 \cdot (x_2 \cdot x_3 - x_4)$ ed ai numeri complessi $c_1 = 7-i$, $c_2 = 5+3i$, $c_3 = 7-3i$, $c_4 = 8+3i$.

Esercizio. Calcolare il coniugato di $(5-3i)^3 + 5 + (3-5i)$ specificando a quale termine t ed a quali elementi c_1, \dots, c_n si applica la (2.1).

Consideriamo la formula risolutiva che fornisce le due soluzioni dell'equazione di secondo grado $ax^2 + bx + c = 0$ a coefficienti reali:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Nel caso in cui $b^2 - 4ac$ sia negativo tale formula fornisce due soluzioni complesse coniugate

$$\frac{-b + i\sqrt{4ac - b^2}}{2a} \text{ e } \frac{-b - i\sqrt{4ac - b^2}}{2a}.$$

Pertanto una equazione di secondo grado se ammette una radice complessa allora ammette come radice anche la sua coniugata. Utilizzando la proposizione 2.3, una tale proprietà può essere estesa a tutte le equazioni algebriche a coefficienti reali.

Teorema 2.4. Se un polinomio a coefficienti reali in n variabili ammette come radici la n -pla c_1, \dots, c_n allora ammette come radici anche la n -upla $\text{con}(c_1), \dots, \text{con}(c_n)$.

Dim. Supponiamo, per semplificare, che il polinomio sia di una sola variabile, cioè che $p(z) = a_n \cdot z^n + a_{n-1} \cdot z^{n-1} + \dots + a_0$ e che c sia una radice di tale polinomio, cioè

$$a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + a_0 = 0.$$

Allora il valore $a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + a_0$ può essere interpretato come il valore del termine

$$t(x_n, x_{n-1}, \dots, x_0, z) = x_n \cdot z^n + x_{n-1} \cdot z^{n-1} + \dots + x_0$$

nelle variabili $x_n, x_{n-1}, \dots, x_0, z$ negli elementi a_n, a_{n-1}, \dots, c . D'altra parte

$$\text{con}(I(t)(a_n, a_{n-1}, \dots, c)) = I(t)(\text{con}(a_n), \text{con}(a_{n-1}) \dots, \text{con}(a_0), \text{con}(c)).$$

e quindi, più esplicitamente,

$$\text{con}(a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + a_0) = \text{con}(a_n) \cdot \text{con}(c)^n + \text{con}(a_{n-1}) \cdot \text{con}(c)^{n-1} + \dots + \text{con}(a_0).$$

Tenendo conto che per ogni numero reale x $\text{con}(x) = x$, otteniamo

$$\text{con}(a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + a_0) = a_n \cdot \text{con}(c)^n + a_{n-1} \cdot \text{con}(c)^{n-1} + \dots + a_0.$$

D'altra parte essendo $a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + a_0 = 0$ è anche $\text{con}(a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + a_0) = \text{con}(0) = 0$. Pertanto, in conclusione,

$$a_n \cdot \text{con}(c)^n + a_{n-1} \cdot \text{con}(c)^{n-1} + \dots + a_0 = 0$$

e questo prova che $\text{con}(c)$ è ancora una radice del polinomio p . □

3. Proprietà che si conservano per isomorfismi: l'equivalenza elementare

Nel paragrafo 2 abbiamo visto che un omomorfismo, che per definizione conserva le operazioni primitive, in realtà riesce a fare molto di più. Infatti conserva tutte le funzioni definibili tramite le operazioni primitive, cioè tutte le funzioni che sono interpretazioni di un termine. Un discorso analogo può essere fatto per quanto riguarda le relazioni. Si pone il problema se un omomorfismo conservi tutte le relazioni definibili, cioè il problema se per un omomorfismo f valga una equivalenza del tipo

$$I \models \alpha [d_1, \dots, d_m] \Leftrightarrow I' \models \alpha [f(d_1), \dots, f(d_m)] \quad (3.1)$$

per ogni possibile formula α . Nel seguente teorema si mostra che nel caso di un isomorfismo la risposta è positiva. Si noti che nella dimostrazione sono evidenziate le ipotesi che si debbono assumere sulla funzione f perché i vari passi del ragionamento siano giustificati.

Teorema 3.1. Se f è una immersione suriettiva di I in I' allora, per ogni formula α ,

$$I \models \alpha [d_1, \dots, d_n] \Leftrightarrow I' \models \alpha [f(d_1), \dots, f(d_n)]. \quad (3.2)$$

In particolare tale equivalenza vale per ogni isomorfismo.

Dim. Procediamo per induzione sulla complessità delle formule.

1. (3.2) vale per le formule atomiche. Sia α uguale alla formula atomica $r(t_1, \dots, t_h)$, allora

$$\begin{aligned} I \models r(t_1, \dots, t_h) [d_1, \dots, d_m] &\Leftrightarrow (I(t_1)(d_1, \dots, d_m), \dots, I(t_h)(d_1, \dots, d_m)) \in I(r) \\ &\Leftrightarrow (f(I(t_1)(d_1, \dots, d_m)), \dots, f(I(t_h)(d_1, \dots, d_m))) \in I'(r) \\ &\Leftrightarrow (I'(t_1)(f(d_1), \dots, f(d_m)), \dots, I'(t_h)(f(d_1), \dots, f(d_m))) \in I'(r) \\ &\Leftrightarrow I' \models r(t_1, \dots, t_h) [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Da notare che la prima equivalenza vale per il modo in cui viene definite la relazione \models per le formule atomiche. La seconda equivalenza vale perché f è una immersione. La terza equivalenza vale per il teorema 1.4. La quarta equivalenza vale per il modo in cui è definita \models . In definitiva in tale passo della dimostrazione si utilizza solo l'ipotesi che f sia una immersione. E' possibile anche effettuare tale passo nel caso in cui f sia un omomorfismo pieno ma è necessario escludere il caso in cui in α sia presente il simbolo $=$.

2. Se (3.2) vale per α e β allora vale anche per $\alpha \wedge \beta$.

Supponiamo che α e β verifichino (3.2), allora

$$\begin{aligned} I \models \alpha \wedge \beta [d_1, \dots, d_n] &\Leftrightarrow I \models \alpha [d_1, \dots, d_m] \text{ e } I \models \beta [d_1, \dots, d_m] \\ &\Leftrightarrow I' \models \alpha [f(d_1), \dots, f(d_m)] \text{ e } I' \models \beta [f(d_1), \dots, f(d_m)] \\ &\Leftrightarrow I' \models \alpha \wedge \beta [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Pertanto anche $\alpha \wedge \beta$ verifica (3.2).

3. Se (3.2) vale per α e β allora vale anche per $\alpha \vee \beta$.

Supponiamo che α e β verifichino (3.2), allora

$$\begin{aligned} I \models \alpha \vee \beta [d_1, \dots, d_n] &\Leftrightarrow I \models \alpha [d_1, \dots, d_m] \text{ oppure } I \models \beta [d_1, \dots, d_m] \\ &\Leftrightarrow I' \models \alpha [f(d_1), \dots, f(d_m)] \text{ oppure } I' \models \beta [f(d_1), \dots, f(d_m)] \\ &\Leftrightarrow I' \models \alpha \vee \beta [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Pertanto anche $\alpha \vee \beta$ verifica (3.2).

4. Se (3.2) vale per α allora vale anche per $\neg \alpha$.

Supponiamo che α verifichi (3.2), allora

$$\begin{aligned} I \models \neg \alpha [d_1, \dots, d_m] &\Leftrightarrow \text{non } I \models \alpha [d_1, \dots, d_m] \Leftrightarrow \text{non } I' \models \alpha [f(d_1), \dots, f(d_m)] \\ &\Leftrightarrow I' \models \neg \alpha [f(d_1), \dots, f(d_m)]. \end{aligned}$$

5. Se (3.2) vale per α allora vale anche per $\exists x_i \alpha$.

Supponiamo che (3.2) valga per α allora

$$\begin{aligned} I \models \exists x_i \alpha [d_1, \dots, d_m] &\Leftrightarrow \text{esiste } d \in D \text{ tale che } I \models \alpha [d_1, \dots, d_{i-1}, d, d_{i+1}, \dots, d_m] \\ &\Leftrightarrow \text{esiste } d \in D \text{ tale che } I' \models \alpha [f(d_1), \dots, f(d), \dots, f(d_m)] \\ &\Leftrightarrow \text{esiste } d' \in D' \text{ tale che } I' \models \alpha [f(d_1), \dots, d', \dots, f(d_m)] \\ &\Leftrightarrow I' \models \exists x_i \alpha [f(d_1), \dots, f(d_m)] \end{aligned}$$

dove il passaggio dalla seconda alla terza equivalenza è giustificato dal fatto che, essendo f suriettiva, ogni elemento $d' \in D'$ sarà del tipo $f(d)$. Pertanto si utilizza l'ipotesi che f è suriettiva

Corollario 3.2. Se f è una immersione suriettiva (in particolare un isomorfismo) di I in I' allora, per ogni formula chiusa α ,

$$I \models \alpha \Leftrightarrow I' \models \alpha. \quad (3.3)$$

Dim. Si deve osservare che se in α non ci sono variabili libere allora $I \models \alpha [d_1, \dots, d_m]$ equivale a $I \models \alpha$ ed $I' \models \alpha [f(d_1), \dots, f(d_m)]$ equivale a $I' \models \alpha$.

Tale corollario assicura che due interpretazioni isomorfe sono indistinguibili nel senso che ogni proprietà verificata da una interpretazione è anche verificata dall'altra e viceversa. Un modo più elegante di esprimere tale situazione si ottiene tramite la nozione di equivalenza elementare.

Definizione 3.3. Diciamo che due interpretazioni sono *elementarmente equivalenti* se per ogni formula chiusa α ,

$$I \models \alpha \Leftrightarrow I' \models \alpha.$$

Allora i risultati di questo paragrafo possono essere enunciati al modo seguente:

Teorema 3.4. Due strutture isomorfe sono elementarmente equivalenti.

Si osservi che esistono anche interpretazioni che sono elementarmente equivalenti ma che non sono isomorfe (si veda il paragrafo sulla logica monadica ed il capitolo sulla la teoria degli ultra-prodotti)².

² Per rendersi conto del significato della nozione di equivalenza elementare facciamo un semplice esempio è confrontiamo l'insieme ordinato $((-1,+1),\leq)$ e l'insieme ordinato (R,\leq) . Un isomorfismo sarà una funzione biettiva $f: (-1,+1) \rightarrow R$ tale che

$$x \leq y \Leftrightarrow f(x) \leq f(y).$$

Pertanto non è difficile mostrare che tali strutture sono isomorfe. Ad esempio un isomorfismo è costituito dalla funzione $f: (-1,+1) \rightarrow R$ definita dall'equazione $f(x) = x/(x^2-1)$. Ne segue che la struttura $((-1,+1),\leq)$ è elementarmente equivalente alla struttura (R,\leq) . Pertanto

non esiste nessuna asserzione nel linguaggio degli insiemi ordinati che permetta di distinguere le due strutture poiché tutto quello che si può dire di una è vero anche per l'altra.

Questo fatto crea uno strano problema di "comunicazione" tra persone che si può esprimere dicendo:

quando parlano due persone ed una descrive un oggetto fino a che punto l'altra può capire di quale oggetto si parla ?

Supponiamo infatti di avere due interlocutori A e B che si scrivono per posta elettronica in un linguaggio molto povero in cui è ammesso solo il simbolo \leq oltre gli usuali simboli della logica (variabili, quantificatori, connettivi del calcolo proposizionale). Supponiamo che A abbia in mente l'insieme ordinato $(-1,1)$ e che B cerchi di capire quale sia la struttura matematica di cui parla A . Allora B può fare, ad esempio, una domanda del tipo

$\exists x \forall y (x \leq y)$? (in altre parole: esiste un minimo ?).

Naturalmente la risposta sarà negativa, ma tale risposta non consente di capire se A ha in mente $(-1,1)$ oppure R , oppure l'insieme ordinato Z dei numeri interi oppure altro. Allora B può chiedere

$\forall x \forall y \exists z (x < z < y)$? (l'insieme è denso ?)

dove $x_1 < x_2$ significa come al solito $(x_1 \leq x_2) \wedge \neg(x_1 = x_2)$. In questo caso la risposta sarà positiva e ciò consente, ad esempio, di escludere che A abbia in mente Z . Tuttavia non gli consente di capire se A ha in mente $(-1,1)$ oppure R . In effetti in questo *gioco*, stante l'isomorfismo tra gli insiemi ordinati $(-1,1)$ ed R , non è possibile in alcun modo per B di capire con sicurezza quali dei due insiemi ordinati è nella mente di A .

4. Verificare se due strutture sono isomorfe e calcolare il gruppo degli automorfismi

I teoremi ora dimostrati sono utili per verificare l'esistenza o meno di isomorfismi. Infatti se due strutture sono isomorfe devono verificare le stesse proprietà esprimibili nel linguaggio del primo ordine considerato.

Esempio. Confrontiamo il campo Q dei razionali con l'anello Z degli interi relativi visti entrambi come interpretazioni del linguaggio della teoria degli anelli. Tali strutture non possono essere isomorfe poiché Q verifica la formula $\forall x(\neg x=0 \Rightarrow \exists y(x \cdot y = 1))$ mentre Z non verifica tale formula.

Esempio. Consideriamo le due strutture ordinate $(\{0,1,2,3\}, \leq)$ e $(\Pi(\{a,b\}), \subseteq)$ e chiediamoci se esiste un isomorfismo tra esse. La risposta è negativa in quanto, ad esempio, il primo insieme verifica la proprietà $\forall x \forall y((x \leq y) \vee (y \leq x))$ (cioè è totalmente ordinato) mentre il secondo non verifica tale proprietà.

Esempio. Chiediamoci ora se (R, \leq) possa essere isomorfo all'insieme ordinato $[0,1]$. Anche in questo caso la risposta è negativa. Infatti il primo insieme non ammette minimo e quindi verifica la proprietà $\forall x \exists y(y \leq x \wedge \neg y=x)$.

Ricordiamo anche che due strutture per potere essere isomorfe devono essere interpretazioni di uno stesso linguaggio. Pertanto non ha senso chiedersi se l'anello dei reali sia isomorfo al gruppo additivo dei numeri complessi in quanto nella prima struttura sono definite oltre alle operazioni del gruppo additivo anche il prodotto e nella seconda struttura sono definite solo le operazioni di gruppo additivo. Infine è evidente che due strutture isomorfe hanno la stessa cardinalità in quanto un isomorfismo è anche una funzione biunivoca. Allora è evidente che, ad esempio, il campo dei razionali (che è numerabile) non può essere isomorfo al campo dei reali (che ha cardinalità maggiore del numerabile).

Problemi:

- (R, \leq) è isomorfo all'insieme ordinato $(0,1]$?
- (R, \leq) è isomorfo all'insieme ordinato dei numeri razionali ?
- gli interi modulo 5 costituiscono un campo isomorfo agli interi modulo 7 ?
- l'anello degli interi modulo 5 è isomorfo ad un gruppo di ordine 5 ?

Un'altra applicazione dei teoremi di conservazione riguarda la determinazione del gruppo degli automorfismi di una struttura. Diamo alcune definizioni.

Definizione 4.1. Nel seguito chiameremo *rigida* una struttura il cui gruppo degli automorfismi si riduce all'applicazione identica. Diciamo che un elemento d di una interpretazione (D,I) è *caratterizzabile* se $\{d\}$ è definibile.

In altri termini un elemento è caratterizzabile se esiste una formula α con una variabile libera x tale che l'unico elemento che verifica $\alpha(x)$ è d . Ad esempio il minimo di una struttura ordinata è unico ed è caratterizzato dalla formula $\alpha(x) = \forall y(y \geq x)$. Il massimo è caratterizzato dalla formula $\alpha(x) = \forall y(x \geq y)$.

Proposizione 4.2. Se un elemento è caratterizzabile allora è un punto fisso³ di ogni automorfismo. Pertanto se tutti gli elementi sono caratterizzabili la struttura è rigida.

³ Un *punto fisso* di una funzione h è un elemento d tale che $h(d) = d$. E' evidente che un funzione h è l'applicazione identica se e solo tutti i punti sono fissi per h .

Dim. Sia d caratterizzabile dalla formula α , allora d verifica α e quindi, essendo f un isomorfismo, $f(d)$ verifica α . Esistendo un solo elemento che verifica α , possiamo concludere che $f(d) = d$. \square

Pertanto in insieme ordinato il minimo (se esiste) è punto fisso di ogni automorfismo della struttura. Lo stesso si può dire del massimo.

Esempio. Consideriamo ad esempio la struttura $(\Pi(\{a,b\}), \subseteq)$ e sia f un suo automorfismo. Allora poiché \emptyset è il minimo e $\{a,b\}$ è il massimo, deve essere $f(\emptyset) = \emptyset$ e $f(\{a,b\}) = \{a,b\}$. Resta da dire quale è il comportamento di f in $\{a\}$ e $\{b\}$ ed in effetti è facile verificare che o $f(\{a\}) = \{a\}$ e $f(\{b\}) = \{b\}$ (automorfismo identico) oppure $f(\{a\}) = \{b\}$ e $f(\{b\}) = \{a\}$. In definitiva il gruppo degli automorfismi è costituito da due elementi e quindi la struttura $(\Pi(\{a,b\}), \subseteq)$ non è rigida.

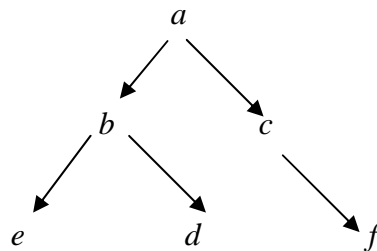
Proposizione 4.3. Ogni insieme finito totalmente ordinato (D, \leq) è una struttura rigida, cioè il gruppo degli automorfismi è identico.

Dim. Consideriamo nel linguaggio delle strutture ordinate la formula, che indichiamo con $cat_n(x_n)$,

$$\exists x_1 \dots \exists x_{n-1} (x_1 < x_2) \wedge \dots \wedge (x_{n-1} < x_n).$$

Tale formula è verificata da d se esistono $n-1$ elementi distinti d_1, \dots, d_{n-1} che precedono d . Siano $d_1 < \dots < d_i$ gli elementi di D scritti in ordine crescente ed f un automorfismo. Allora ogni elemento d_i è caratterizzato dalla formula $cat_i(x_{i-1}) \wedge \neg cat_i(x_i)$ che esprime il fatto che esistono $i-1$ elementi in catena prima di d_i ma non ne esistono i . Questo prova che tutti i punti sono fissi e che quindi un automorfismo deve coincidere con l'applicazione identica. \square

Esempio. Si consideri il seguente grafo



che supponiamo interpretazione di un linguaggio con un predicato binario r . Supponiamo cioè che $D = \{a,b,c,d,e,f\}$ e $I(r) = \{(a,b), (a,c), (b,e), (b,d), (c,e)\}$. Supponiamo che h sia un automorfismo di tale grafo. Allora poiché

a è l'unico punto che non ha precedenti

b è l'unico punto che ha un precedente e due successivi

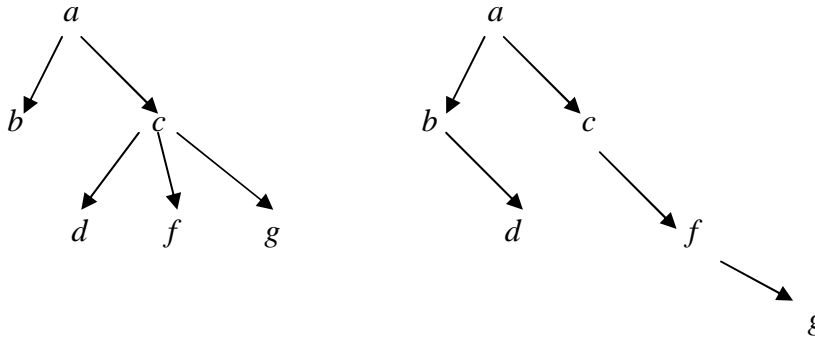
c è l'unico punto che ha un precedente ed un successivo,

risulta che $h(a) = a$, $h(b) = b$, $h(c) = c$. Inoltre, poiché f ha c come precedente $h(f)$ deve avere $h(c) = c$ come precedente. Ciò comporta che $h(f) = f$. In conclusione si vede che h o coincide con l'applicazione identica oppure con l'applicazione che scambia e con d .

Si osservi che la nozione di *caratterizzabile* si riferisce ad un dato linguaggio. Se ad esempio interpreto i punti del grafo come stanze di un labirinto e mettesi in c e d delle trappole, allora sicuramente d sarebbe distinguibile dai rimanenti punti. Infatti si può caratterizzare d come un elemento *finale* in cui esiste una trappola. In tale caso però mi riferirei ad un linguaggio diverso da quello del grafo, un linguaggio contenente oltre al

simbolo r anche un simbolo tr per il predicato monadico “contiene una trappola”. L'interpretazione I associa a tr l'insieme $I(tr) = \{c, d\}$.

Esercizio. Calcolare il gruppo degli automorfismi dei seguenti grafi.



Problema. Determinare il gruppo degli automorfismi di (N, \leq) .
 Determinare il gruppo degli automorfismi di (Z, \leq) .

5. Principio di dualità in un algebra di Boole

Consideriamo un linguaggio \mathcal{A} il cui alfabeto è costituito dai simboli $+, \cdot, -, 0, 1$. Una interpretazione di tale linguaggi si ottiene considerando un insieme non vuoto S e la corrispondente algebra di Boole $\mathbf{B} = (\Pi(S), \cup, \cap, -, \emptyset, S)$. Più precisamente tale struttura definisce una interpretazione (D, I) in cui

- $D = \Pi(S)$,
- $I(+)$ è uguale all'operazione di unione,
- $I(\cdot)$ è uguale all'operazione di intersezione,
- $I(-)$ è uguale all'operazione complemento,
- $I(0) = \emptyset$,
- $I(1) = S$.

Lo stesso linguaggio tuttavia può essere interpretato anche dalla struttura $\mathbf{B}^d = (\Pi(S), \cap, \cup, -, S, \emptyset)$ che si ottiene da \mathbf{B} scambiando le operazioni di unione ed intersezione e scambiando S con \emptyset . Questo significa che possiamo considerare l'interpretazione (D, I^d) tale che

- $D = \Pi(S)$,
- $I(+)$ è uguale all'operazione di intersezione,
- $I(\cdot)$ è uguale all'operazione di unione,
- $I(-)$ è uguale all'operazione complemento,
- $I(0) = S$,
- $I(1) = \emptyset$.

Le due interpretazioni sono diverse tra loro⁴, tuttavia la seguente proposizione mostra che sono isomorfe.

Proposizione 5.1. Sia $compl : P(S) \rightarrow P(S)$ la funzione complemento, cioè sia $compl(X) = -X$ per ogni elemento sottoinsieme X di D . Allora $compl$ è un isomorfismo tra \mathbf{B} e \mathbf{B}^d . Pertanto, per ogni formula α ,

$$\mathbf{B} \models \alpha \Leftrightarrow \mathbf{B}^d \models \alpha$$

⁴ Se una struttura algebrica si definisse come un dominio più un insieme di operazioni non potremmo esprimere il fatto che tali strutture sono diverse.

Proof. Per provare che compl è un isomorfismo basta utilizzare alcune ben note proprietà del complemento. Infatti

$$\text{compl}(I(+)(X,Y)) = -(X \cup Y) = (-X) \cap (-Y) = I^d(+)(\text{compl}(X), \text{compl}(Y))$$

$$\text{compl}(I(\cdot)(X,Y)) = -(X \cap Y) = (-X) \cup (-Y) = I^d(\cdot)(\text{compl}(X), \text{compl}(Y))$$

$$\text{compl}(I(-)(X)) = -(-X) = I^d(-)(\text{compl}(X))$$

$$\text{compl}(I(1)) = -S = \emptyset = I^d(1)$$

$$\text{compl}(I(1)) = -S = \emptyset = I^d(1).$$

Si pone il problema di vedere che cosa significhi $\mathbf{B}^d \models \alpha$. A tale scopo se α è una formula, chiameremo *duale* di α la formula α^d che si ottiene sostituendo ad ogni occorrenza di $+$ il simbolo \cdot , ad ogni occorrenza di \cdot il simbolo $+$, ad ogni 0 il simbolo 1 ed ad ogni 1 il simbolo 0 . Ad esempio, se α è la formula $x \cdot 1 = x$, la sua duale è la formula $x + 0 = x$. Se α è la formula $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ esprime la proprietà distributiva di \cdot rispetto a $+$, allora α^d sarà la formula $x + (y \cdot z) = (x + y) \cdot (x + z)$ esprime la proprietà distributiva dell'operazione $+$ rispetto all'operazione \cdot . Ovviamente $(\alpha^d)^d = \alpha$.

Teorema 5.2 (Principio di dualità per l'algebra \mathbf{B} degli insiemi). Sia \mathbf{B} l'algebra di Boole dei sottoinsiemi di S , allora per ogni formula α

$$\mathbf{B} \models \alpha \Leftrightarrow \mathbf{B} \models \alpha^d.$$

Dim. Basta osservare che $\mathbf{B}^d \models \alpha$ se e solo se $\mathbf{B} \models \alpha^d$ ed applicare la proposizione 5.1.

Se analizziamo la dimostrazione della proposizione 5.1 ci accorgiamo che vale per ogni possibile algebra di Boole. Inoltre anche il teorema 5.2 di fatto è stato dimostrato per ogni algebra di Boole e quindi può essere generalizzato al modo seguente.

Teorema 5.3 (Principio di dualità per le algebre di Boole). Sia \mathbf{B} una qualsiasi algebra di Boole, allora per ogni formula α

$$\mathbf{B} \models \alpha \Leftrightarrow \mathbf{B} \models \alpha^d.$$

Da ciò è possibile derivare il seguente teorema.

Teorema 5.4. (Principio di dualità per la teoria delle algebre di Boole). Sia T il sistema di assiomi per le algebre di Boole (si veda nel capitolo 2). Allora, per ogni formula α ,

$$T \models \alpha \Leftrightarrow T \models \alpha^d.$$

Dim. Supponiamo che $T \models \alpha$, allora per dimostrare che $T \models \alpha^d$ consideriamo un modello di T , cioè un algebra di Boole \mathbf{B} . Per l'ipotesi $T \models \alpha$, \mathbf{B} verificherà α e quindi per il teorema 5.3 verificherà α^d . In definitiva ogni modello di T è un modello di α^d e ciò prova che $T \models \alpha^d$.

6. La classe dei modelli di una teoria non è un insieme

In questo paragrafo vogliamo mostrare che, data una interpretazione, se ne possono fare quante copie isomorfe si vuole.

Definizione 6.1. Data una interpretazione (D, I) , un insieme D' equipotente a D ed una funzione biettiva $f: D \rightarrow D'$, chiamiamo *fotocopia* di (D, I) in D' tramite f , l'interpretazione (D', I') definita dal porre:

- $I'(c) = f(I(c))$ per ogni costante c
- $I'(o)(d_1', \dots, d_n') = f(I(o)(f^{-1}(d_1'), \dots, f^{-1}(d_n')))$ per ogni nome di operazione o
- $(d_1', \dots, d_n') \in I'(r) \Leftrightarrow (f^{-1}(d_1'), \dots, f^{-1}(d_n')) \in I(r)$ per ogni nome di relazione r .

Per fare un esempio, supponiamo di considerare il gruppo additivo degli interi modulo 3 individuato dagli elementi 0, 1, 2 ed in cui si pone

$$x+0 = 0+x = x, 1+1=2, 2+2 = 1, 1+2 = 2+1 = 0.$$

Consideriamo un qualunque insieme con tre elementi, ad esempio l'insieme $\{a,b,c\}$, allora possiamo dare a tale insieme una struttura isomorfa a tale gruppo considerando la funzione $f: \{0,1,2\} \rightarrow \{a,b,c\}$ definita dal porre $f(0) = a, f(1) = b, f(2) = c$. Se denotiamo con g l'inversa di f , l'operazione di addizione in $\{a,b,c\}$ è definita al modo seguente.

$$a \oplus x = f(0+g(x)) = f(g(x)) = x$$

$$x \oplus a = f(g(x)+0) = f(g(x)) = x$$

$$b \oplus b = f(1+1) = f(2) = c$$

$$b \oplus c = f(1+2) = f(3) = a$$

$$c \oplus b = f(2+1) = f(3) = a$$

$$c \oplus c = f(2+2) = f(1) = b$$

In definitiva si ha la tabellina

\oplus	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Proposizione 6.2. Consideriamo una interpretazione (D,I) , un insieme D' equipotente a D ed una funzione biettiva $f: D \rightarrow D'$. Allora f è un isomorfismo tra (D,I) e la sua fotocopia in D' .

Dim. Per provare che f è un isomorfismo tra (D',I') e (D,I) è sufficiente osservare che se si pone $d_1 = g(d_1'), \dots, d_n = g(d_n')$ allora le equazioni con cui abbiamo definito I' diventano:

$$- I'(c) = f(I(c)) \text{ per ogni costante } c$$

$$- I'(o)(f(d_1), \dots, f(d_n)) = f(I(o)(d_1, \dots, d_n)) \text{ per ogni nome di operazione } o$$

$$- (f(d_1), \dots, f(d_n)) \in I'(r) \Leftrightarrow (d_1, \dots, d_n) \in I(r) \text{ per ogni nome di relazione } r.$$

Possiamo esprimere tale proposizione dicendo che data una interpretazione comunque si consideri un "foglio" D' di opportune dimensioni allora è possibile fotocopiare (D,I) su D' .

Nelle proposizioni successive affrontiamo problemi del tipo:

Esistono teorie con un solo modello?

La classe dei gruppi è equipotente alla classe degli anelli?

Vedremo come la risposta alla prima domanda è negativa mentre la seconda domanda non è sensata. Esaminiamo infatti due risultati "paradossali".

Teorema 6.3. (Teorema della fotocopiatrice). Sia (D,I) una interpretazione e sia S un qualunque insieme, la classe delle interpretazioni isomorfe a (D,I) ha cardinalità maggiore di quella di S .

Dim. Per ogni $s \in S$, consideriamo l'insieme $D_s = D \times \{s\} = \{(d,s) \mid d \in D\}$. Ovviamente D_s è equipotente a D in quanto la funzione $f : D \rightarrow D_s$ definita ponendo $f(d) = (d,s)$ è biettiva. Pertanto possiamo “fotocopiare” D in D_s tramite la funzione f . Precisamente otteniamo una interpretazione I_s ponendo

$$D_s = D \times \{s\} \quad ; \quad I_s(c) = (I(c), s) \quad ; \quad I_s(o)((d_1, s), \dots, (d_n, s)) = (I(o)(d_1, \dots, d_n), s) ; \\ I_s(r) = \{(d_1, s), \dots, (d_n, s) \mid (d_1, \dots, d_n) \in I(r)\}.$$

ed f è un isomorfismo di (D, I) in (D_s, I_s) .

Considerando il fatto che la corrispondenza che associa ad ogni $s \in S$ l'interpretazione (D_s, I_s) è iniettiva, la proposizione è provata. \square

Possiamo interpretare tale proposizione al modo seguente. Supponiamo che I sia una fotografia, ad esempio la foto della mia gatta Titti e che in fondo alla foto ci sia una striscia bianca in cui è possibile scrivere qualche cosa. Sia inoltre S un insieme, ad esempio $S = \{1, 2, 3, 4, 5\}$. Allora posso fare cinque fotocopie di I inserendo nella striscia bianca in basso i numeri progressivi 1, 2, 3, 4, 5 ed ottenendo le foto I_1, \dots, I_5 . E' ragionevole chiamare ancora “foto di Titti” le foto ottenute in questo modo. Quindi:

esistono almeno 5 foto di Titti.

Supponiamo ora di considerare Z uguale ad N ed indichiamo, per ogni $n \in N$, con I_n una fotocopia di I con su stampato il numeretto n nella striscia bianca. Questo procedimento permette di dimostrare che:

esiste almeno una quantità numerabile di foto di Titti.

Naturalmente l'espressione “esiste” deve essere intesa come esistenza nel mondo della matematica, non nel mondo che ci circonda. E' chiaro che la stessa argomentazione può essere fatta per qualunque tipo di cardinalità.

Esercizio. Dato l'insieme ordinato $\{1, 2, 3\}$ poniamo S uguale all'insieme dei numeri reali. Provare che, per ogni numero reale x , $\{1, 2, 3\}$ è isomorfo alla “fotocopia” $\{(1, x), (2, x), (3, x)\}$ e quindi che la cardinalità della classe degli insiemi con tre elementi è maggiore o uguale alla potenza del continuo.

Proposizione 6.4. Sia T una teoria soddisfacibile ed S un insieme, allora la classe dei modelli di T ha cardinalità maggiore o uguale a quella di S .

Dim. Sia I un modello di T . Poiché due interpretazioni isomorfe verificano le stesse formule, ciascun I_s della proposizione precedente è anche un modello di T . \square

Con riferimento agli esempi precedenti possiamo dire che:

per ogni insieme S esiste una quantità di foto di Titti maggiore della cardinalità di S ,

e quindi che

la classe delle possibili foto di Titti è tanto grande da avere una cardinalità maggiore di quella di qualunque insieme.

Tale proposizione conduce al seguente interessante paradosso della teoria degli insiemi. Ricordiamo che il teorema di Cantor afferma che, dato un insieme S , la cardinalità di $\Pi(S)$ è strettamente maggiore di quella di S .

Proposizione 6.5. La classe $M(T)$ dei modelli di una teoria T del primo ordine non verifica il teorema di Cantor.

Dim. La dimostrazione segue dalla proposizione 6.4 ponendo $S = M(T)$. \square

Ad esempio possiamo considerare la teoria T avente come assioma la formula

$$\exists x \exists y ((x \neq y) \wedge \forall z (z = x \vee z = y))$$

esprimente la proprietà "avere esattamente due elementi". Abbiamo allora che anche una collezione apparentemente naturale come "la totalità di tutti gli insiemi con due elementi" non verifica il teorema di Cantor. La stessa cosa si può dire per la classe dei gruppi, degli anelli e così via.

Uno dei modi per risolvere tale paradosso consiste nella *teoria delle classi*. In tale teoria si propone come concetto primitivo quello di *classe* e definendo *insieme* ogni classe che appartiene ad un'altra classe. Le classi che non sono insiemi vengono chiamate *classi proprie*. Per le classi proprie, cioè che non sono insiemi, non sono applicabili le usuali nozioni della teoria degli insiemi. Ad esempio,

non ha senso parlare di cardinalità di una classe propria,

non ha senso ad esempio dire che la cardinalità della classe dei gruppi è minore della cardinalità della classe degli anelli. Pertanto il paradosso prova semplicemente che la totalità dei modelli di una teoria del primo ordine costituisce una classe propria.

Teorema 6.6. La classe $\mathcal{M}(T)$ dei modelli di una teoria T del primo ordine è una classe propria che non è un insieme.

Il teorema della fotocopiatrice mette anche in evidenza che non esistono teorie con un solo modello. Tuttavia esistono teorie i cui modelli sono tutti isomorfi tra loro.

Definizione 6.7. Chiamiamo *categorica* una teoria che abbia almeno un modello e tutti i suoi modelli sono isomorfi tra loro.

Un matematico tende ad identificare due modelli isomorfi, pertanto una teoria categorica viene vista come una teoria avente un solo modello. Infatti a volte per una teoria categorica si dice che ha un "*solo modello a meno di isomorfismi*".

La teoria dei gruppi di ordine 5. Ad esempio consideriamo la teoria T dei gruppi di ordine 5 e sia G è un modello di tale teoria. Allora se g è un elemento G diverso dall'elemento neutro, è subito visto che l'applicazione $f: \mathbb{Z} \rightarrow G$ che associa ad ogni intero relativo n l'elemento g^n è un epimorfismo del gruppo additivo \mathbb{Z} su G . Per il teorema fondamentale sugli omomorfismi il quoziente di \mathbb{Z} modulo il nucleo di tale omomorfismo è isomorfo a G . Tale quoziente, che ha cardinalità 5, non può che coincidere con il gruppo degli interi modulo 5. Pertanto ogni gruppo di ordine 5 è isomorfo a $\mathbb{Z}/5$. Ne segue ancora che tutti i modelli della teoria T sono isomorfi tra loro e quindi che la teoria T è categorica.

Esercizio. Dire quali delle seguenti teorie sono categoriche: La teoria dei gruppi abeliani, la teoria dei gruppi di ordine 3, la teoria degli insiemi ordinati con tre elementi, la teoria dell'ordine lineare con tre elementi, la teoria dei campi, la teoria degli anelli.

7. Proprietà conservate da omomorfismi che non sono necessariamente isomorfismi

Il teorema 3.1 è stato dimostrato supponendo che f sia un isomorfismo (o, più in generale, una immersione che sia anche un epimorfismo). Nel caso in cui f non verifichi tali proprietà è possibile comunque provare risultati più deboli. A tale scopo basta riesaminare la dimostrazione di tale teorema per vedere fino a quale punto può andare avanti senza supporre le proprietà di isomorfismo. Il seguente teorema mostra ad esempio che un qualunque omomorfismo conserva tutte le relazioni che siano definibili a partire dalle relazioni primitive utilizzando i connettivi logici di \wedge ed \vee .

Teorema 7.1. Sia $f : D \rightarrow D'$ un omomorfismo di (D, I) in (D', I') ed α una matrice positiva (cioè senza negazione), allora

$$I \models \alpha [d_1, \dots, d_m] \Rightarrow I' \models \alpha [f(d_1), \dots, f(d_m)]. \quad (7.1)$$

Dim. Osserviamo che le matrici positive sono le formule che si ottengono a partire dalle formule atomiche utilizzando i soli connettivi \wedge e \vee . Pertanto, per dimostrare (7.1) possiamo procedere per induzione sulla complessità di α provando che

- (7.1) vale per le formule atomiche e che
- se (7.1) vale per due formule α e β allora vale anche per $\alpha \wedge \beta$ e $\alpha \vee \beta$.

Ora, il punto 1 nella dimostrazione del teorema 3.1, che riguarda il caso delle formule atomiche, continua a valere purché si sostituisca alla seconda equivalenza una implicazione. Più esplicitamente:

$$\begin{aligned} I \models r(t_1, \dots, t_n) [d_1, \dots, d_m] &\Leftrightarrow (I(t_1)(d_1, \dots, d_m), \dots, I(t_n)(d_1, \dots, d_m)) \in I(r) \\ &\Rightarrow (f(I(t_1)(d_1, \dots, d_m)), \dots, f(I(t_n)(d_1, \dots, d_m))) \in I'(r) \\ &\Leftrightarrow (I'(t_1)(f(d_1), \dots, f(d_m)), \dots, I'(t_n)(f(d_1), \dots, f(d_m))) \in I'(r) \\ &\Leftrightarrow I' \models r(t_1, \dots, t_n) [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Pertanto (7.1) vale per α atomica. Si osservi che tale ragionamento comprende anche il caso in cui r coincide con $=$. Anche i punti 2 e 3 si ripetono allo stesso modo, sostituendo anche in questo caso, per poter applicare l'ipotesi di induzione, alla seconda equivalenza una implicazione. Pertanto,

$$\begin{aligned} I \models \alpha \wedge \beta [d_1, \dots, d_m] &\Leftrightarrow I \models \alpha [d_1, \dots, d_m] \text{ e } I \models \beta [d_1, \dots, d_m] \\ &\Rightarrow I' \models \alpha [f(d_1), \dots, f(d_m)] \text{ e } I' \models \beta [f(d_1), \dots, f(d_m)] \\ &\Leftrightarrow I' \models \alpha \wedge \beta [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Allo stesso modo si procede per provare che $\alpha \vee \beta$ verifica (7.1). □

Il seguente corollario mostra che il teorema 2.4 relativo alle radici complesse può essere esteso anche ai sistemi di equazioni ed agli endomorfismi.

Corollario 7.2. Sia f un endomorfismo in una struttura (D, I) e consideriamo un sistema di equazioni

$$\begin{cases} t_1(x_1, \dots, x_m) = s_1(x_1, \dots, x_m) \\ \dots \\ t_n(x_1, \dots, x_m) = s_n(x_1, \dots, x_m) \end{cases}$$

dove $t_1, \dots, t_n, s_1, \dots, s_n$ sono termini in m variabili. Allora, se d_1, \dots, d_m sono radici di tale sistema anche $f(d_1), \dots, f(d_m)$ sono radici dello stesso sistema.

E' anche molto importante esaminare le asserzioni che si conservano per epimorfismi pieni. Infatti, come vedremo, ciò equivale ad esaminare le proprietà che si conservano per quozienti.

Teorema 7.3. Sia $f : D \rightarrow D'$ un epimorfismo pieno di (D, I) in (D', I') e $\forall x_1 \dots \forall x_n \alpha$ una proprietà universale positiva, allora

$$I \models \forall x_1 \dots \forall x_n \alpha \Rightarrow I' \models \forall x_1 \dots \forall x_n \alpha. \quad (7.2)$$

Dim. Supponiamo che f sia suriettiva e supponiamo che valga $I \models \forall x_1 \dots \forall x_n \alpha$. Per provare che $I' \models \forall x_1 \dots \forall x_n \alpha$ dobbiamo provare che se d_1', \dots, d_m' sono elementi qualunque di D' , allora $I' \models \alpha [d_1', \dots, d_m']$. Ora, essendo f suriettiva, esistono d_1, \dots, d_m per cui $f(d_1) = d_1', \dots, f(d_m) = d_m'$. D'altra parte l'ipotesi per cui $I \models \forall x_1 \dots \forall x_n \alpha$ comporta che, in particolare $I \models \alpha [d_1, \dots, d_m]$. Ne segue che per (7.1) sarà $I \models \alpha [f(d_1), \dots, f(d_m)]$ e quindi $I' \models \alpha [d_1', \dots, d_m']$. \square

Da notare che (7.2) non è valida se si considerano matrici che non siano positive. Ad esempio possiamo considerare l'epimorfismo canonico di Z sull'anello $Z/3$ degli interi modulo 3. In tale caso la formula $\forall x (\neg(x=x+3))$ vale in Z ma non vale per la sua immagine epimorfa $Z/3$.

Teorema 7.3. Se f è un epimorfismo pieno di I in I' allora per ogni formula α che non contiene $=$ risulta che

$$I \models \alpha [d_1, \dots, d_n] \Leftrightarrow I' \models \alpha [f(d_1), \dots, f(d_n)] \quad (7.3)$$

e quindi, per ogni formula chiusa α non contenente $=$,

$$I \models \alpha \Leftrightarrow I' \models \alpha. \quad (7.4)$$

Dim. Per provare (7.3) dobbiamo provare che:

- (7.3) vale per le formule atomiche che non contengono $=$

- se (7.3) vale per α e β allora (7.3) vale anche per $\alpha \wedge \beta$, $\alpha \vee \beta$, $\neg \alpha$ e $\exists x_i \alpha$.

Infatti sia α uguale alla formula atomica $r(t_1, \dots, t_h)$. Avremo:

$$\begin{aligned} I \models r(t_1, \dots, t_h) [d_1, \dots, d_m] &\Leftrightarrow (I(t_1)(d_1, \dots, d_m), \dots, I(t_h)(d_1, \dots, d_m)) \in I(r) \\ &\Leftrightarrow (f(I(t_1)(d_1, \dots, d_m)), \dots, f(I(t_h)(d_1, \dots, d_m))) \in I'(r) \\ &\Leftrightarrow (I'(t_1)(f(d_1), \dots, f(d_m)), \dots, I'(t_h)(f(d_1), \dots, f(d_m))) \in I'(r) \\ &\Leftrightarrow I' \models r(t_1, \dots, t_h) [f(d_1), \dots, f(d_m)].^5 \end{aligned}$$

Supponiamo che α e β verifichino (7.3), allora

$$\begin{aligned} I \models \alpha \wedge \beta [d_1, \dots, d_m] &\Leftrightarrow I \models \alpha [d_1, \dots, d_m] \text{ e } I \models \beta [d_1, \dots, d_m] \\ &\Leftrightarrow I' \models \alpha [f(d_1), \dots, f(d_m)] \text{ e } I' \models \beta [f(d_1), \dots, f(d_m)] \\ &\Leftrightarrow I' \models \alpha \wedge \beta [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Pertanto anche $\alpha \wedge \beta$ verifica (7.3). Allo stesso modo si procede per provare che se α e β verificano (7.3) anche $\alpha \vee \beta$ verifica (7.3).

Supponiamo che α verifichi (7.3) allora

$$\begin{aligned} I \models \neg \alpha [d_1, \dots, d_m] &\Leftrightarrow \text{non } I \models \alpha [d_1, \dots, d_m] \Leftrightarrow \text{non } I' \models \alpha [f(d_1), \dots, f(d_m)] \\ &\Leftrightarrow I' \models \neg \alpha [f(d_1), \dots, f(d_m)]. \end{aligned}$$

Ciò prova (7.3).

Supponiamo che (7.3) valga per α allora

$$\begin{aligned} I \models \exists x_i \alpha [d_1, \dots, d_m] &\Leftrightarrow \text{esiste } d \in D \text{ tale che } I \models \alpha [d_1, \dots, d_{i-1}, d, d_{i+1}, \dots, d_m] \\ &\Leftrightarrow \text{esiste } d \in D \text{ tale che } I' \models \alpha [f(d_1), \dots, f(d), \dots, f(d_m)] \\ &\Leftrightarrow \text{esiste } d' \in D' \text{ tale che } I' \models \alpha [f(d_1), \dots, d', \dots, f(d_m)] \\ &\Leftrightarrow I' \models \exists x_i \alpha [f(d_1), \dots, f(d_m)] \end{aligned}$$

⁵ La prima equivalenza vale per la definizione data di "essere vero in I' " per la formula atomica $r(t_1, \dots, t_h)$. La seconda equivalenza vale per il fatto che f è un omomorfismo pieno e, nel caso in cui r coincide con $=$, in quanto f è iniettiva. La terza equivalenza vale per la proposizione 2.1. L'ultima equivalenza vale per la definizione di "essere vero in I' " della formula $r(t_1, \dots, t_h)$.

dove il passaggio dalla seconda alla terza equivalenza è giustificato dal fatto che, essendo f suriettiva, ogni elemento $d' \in D'$ sarà del tipo $f(d)$.