

CAPITOLO 7

[indice](#)

PROPRIETA' CHE SI CONSERVANO: QUOZIENTI, PRODOTTI DIRETTI ED ULTRAPRODOTTI

1. Congruenze, quozienti ed epimorfismi canonici

Anche le nozioni di congruenza e di quoziente, che abbiamo dato per le strutture matematiche del primo ordine possono essere riformulate in modo più preciso per le interpretazioni di una logica del primo ordine.

Definizione 1.1. Chiamiamo *congruenza* in una interpretazione (D, I) una relazione di equivalenza \equiv in D che sia compatibile con tutte le operazioni $I(o)$ e con tutte le relazioni $I(r)$ in cui r sia diverso da $=$. Il *quoziente modulo* \equiv di (D, I) si definisce come l'interpretazione normale (D_{\equiv}, I_{\equiv}) tale che

- D_{\equiv} è uguale al quoziente di D modulo \equiv ,
- $I_{\equiv}(o)([d_1], \dots, [d_n]) = [I(o)(d_1, \dots, d_n)]$,
- $I_{\equiv}(r) = \{([d_1], \dots, [d_n]) \mid (d_1, \dots, d_n) \in I(r)\}$,
- $I_{\equiv}(c) = [I(c)]$.

Si osservi che il motivo per cui non abbiamo supposto che la relazione \equiv sia compatibile con il simbolo $=$ e perché in tale caso in una struttura normale l'unica congruenza possibile sarebbe la relazione l'identità. Infatti supposto che \equiv verifichi l'implicazione

$$d_1 \equiv d_1' \text{ e } d_2 \equiv d_2' \Rightarrow ((d_1, d_2) \in I(=) \Leftrightarrow (d_1', d_2') \in I(=)).$$

Allora se $d \equiv d'$, poiché $d \equiv d$ si avrebbe $(d', d) \in I(=)$. Nelle strutture normali ciò comporterebbe la coincidenza di d con d' .

Come abbiamo già visto nel capitolo 2, la nozione di quoziente è strettamente collegata con quella di epimorfismo.

Proposizione 1.2. La funzione $f : D \rightarrow D_{\equiv}$ che ad ogni elemento x in D associa la classe $[x] \in D_{\equiv}$ è un epimorfismo pieno (chiamato *epimorfismo canonico*).

Dim. Che f conservi le operazioni e le costanti segue direttamente dal modo in cui è stato definito il quoziente. D'altra parte, poiché per definizione per ogni simbolo di relazione r abbiamo posto $I_{\equiv}(r) = \{([d_1], \dots, [d_n]) \mid (d_1, \dots, d_n) \in I(r)\}$, risulta

$$(d_1, \dots, d_n) \in I(r) \Leftrightarrow ([d_1], \dots, [d_n]) \in I_{\equiv}(r) \Leftrightarrow (f(d_1), \dots, f(d_n)) \in I_{\equiv}(r).$$

L'epimorfismo canonico non è in generale una immersione. Infatti vale la seguente proposizione.

Proposizione 1.3. Sia \equiv una congruenza in (D, I) , allora le seguenti asserzioni sono equivalenti:

- i) L'epimorfismo canonico è una immersione
- ii) \equiv coincide con $I(=)$.

Quando ciò avviene \equiv è una congruenza compatibile anche con $=$

Dim. Sappiamo che dire che l'epimorfismo canonico sia una immersione equivale a dire che

$$(d_1, d_2) \in I(=) \Leftrightarrow [d_1] = [d_2]$$

e quindi che

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

D'altra parte se \equiv coincide con $I(=)$ allora la compatibilità di \equiv con $I(=)$ equivale alla ovvia implicazione

$$d_1 \equiv d_1' \text{ e } d_2 \equiv d_2' \Rightarrow (d_1 \equiv d_2 \Leftrightarrow d_1' \equiv d_2').$$

Teorema 1.4. Sia \equiv una congruenza in una interpretazione (D, I) ed (D_{\equiv}, I_{\equiv}) il relativo quoziente modulo \equiv . Allora

$$[I(t)(d_1, \dots, d_n)] = I_{\equiv}(t)([d_1], \dots, [d_n]) \tag{1.1}$$

e quindi

$$d_1 \equiv d_1', \dots, d_n \equiv d_n' \Rightarrow I(t)(d_1, \dots, d_n) \equiv I(t)(d_1', \dots, d_n'). \tag{1.2}$$

Dim. Per provare (1.1) applichiamo il teorema 1.4 del Capitolo 6 al caso in cui f è l'epimorfismo canonico. Per provare (1.2) osserviamo che

$$\begin{aligned} d_1 \equiv d_1', \dots, d_n \equiv d_n' &\Rightarrow [d_1] = [d_1'], \dots, [d_n] = [d_n'] \\ &\Rightarrow I_{\equiv}(t)([d_1], \dots, [d_n]) = I_{\equiv}(t)([d_1'], \dots, [d_n']) \\ &\Rightarrow [I(t)(d_1, \dots, d_n)] = [I(t)(d_1', \dots, d_n')] \\ &\Rightarrow I(t)(d_1, \dots, d_n) \equiv I(t)(d_1', \dots, d_n'). \end{aligned}$$

L'equazione (1.1) si può leggere dicendo che:

“la classe del composto secondo l'algoritmo t è uguale al composto delle classi”

L'implicazione (1.2) ci dice che:

- se un “calcolo” descritto dal termine t viene applicato invece che agli elementi d_1, \dots, d_n agli elementi equivalenti d_1', \dots, d_n'

- allora i risultati che si ottengono sono equivalenti.

Poiché possiamo interpretare un termine come un programma, possiamo visualizzare tale fenomeno al modo seguente:

<i>input</i> d_1, \dots, d_n	<i>input</i> d_1', \dots, d_n'	Se $d_1 \equiv d_1', \dots, d_n \equiv d_n'$
·	·	
·	·	
·	·	
<i>output</i> d	<i>output</i> d'	allora $d \equiv d'$.

2. Una applicazione: la prova del nove.

Una applicazione interessante di quanto dimostrato nel paragrafo precedente è fornita dalla famosa “*prova del nove*”¹. Tale prova viene spesso insegnata nelle scuole medie come metodo per controllare l'esattezza di una moltiplicazione. Essa si basa sulla nozione di *ridotto* di un numero.

Definizione 2.1. Dato un numero intero n indichiamo con $s(n)$ la somma delle sue cifre in una rappresentazione decimale di n . Indichiamo con $r(n)$ il *ridotto* di n cioè il numero che si ottiene applicando più volte la funzione r fino ad ottenere un numero di una sola cifra.

¹ La prova del nove ha origini antichissime. E' presente ad esempio nel libro del 1202 *Liber A baci* di Fibonacci.

Ad esempio se $n = 3456$ allora $s(n) = 3+4+5+6 = 18$ e quindi $r(n) = s(18) = 1+8 = 9$. Se $n = 463.465$ allora $s(n) = 4+6+3+4+6+5 = 28$ e quindi $s(s(n)) = s(28) = 10$ e quindi ancora $r(n) = s(s(s(n))) = s(10) = 1$.²

Allora la prova del nove consiste nella seguente procedura. Supponiamo di avere moltiplicato i due numeri interi a e b ottenendo il risultato c , $a \cdot b = c$. Allora

1. calcoliamo il ridotto $r(a)$ e lo moltiplichiamo per il ridotto $r(b)$
2. riduciamo ulteriormente il numero ottenuto
3. verifichiamo che quello che si ottiene è il ridotto di c .

Se questo avviene diciamo che la prova del nove è riuscita e questo “ci rassicura” in qualche modo che la moltiplicazione è stata eseguita bene.

Ad esempio partiamo dal prodotto $233 \times 521 = 121393$ e sostituiamo al numero 233 il numero $2+3+3 = 8$, al numero 521 il numero $5+2+1 = 8$. Effettuiamo poi la moltiplicazione di tali numeri ottenendo il numero 64 che viene ridotto al numero $6+4 = 10$ e quindi al numero $1+0 = 1$. D'altra parte il numero 121393 viene ridotto al numero $1+2+1+3+9+3 = 19$ che a sua volta viene ridotto al numero $1+9 = 10$ e quindi al numero 1. In definitiva dall'equazione di partenza si giunge all'equazione $1=1$ e quindi possiamo affermare che la prova del nove è riuscita.

La correttezza di questo procedimento è conseguenza della seguente proposizione.

Proposizione 2.2. Ogni numero intero n è congruo modulo 9 alla somma $s(n)$ delle sue cifre. Pertanto ogni numero è congruo al proprio ridotto.

Dim. Sia n un numero intero e scriviamo n in base 10

$$n = a_n a_{n-1} \dots a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0 \cdot 10^0.$$

Allora possiamo vedere tale numero come il risultato della applicazione del termine $t(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_0 \cdot x^0$ al numero 10^3 . Infatti,

$$I(t)(10) = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0 \cdot 10^0 = n$$

Se ora indichiamo con \equiv la congruenza modulo 9, avremo che $10 \equiv 1$. D'altra parte per il teorema 1.3 sappiamo che

$$d \equiv d' \Rightarrow I(t)(d) \equiv I(t)(d')$$

e quindi, essendo $10 \equiv 1$, possiamo dire che $I(t)(1) \equiv I(t)(10)$. Essendo $I(t)(1) = a_n \cdot 1^n + a_{n-1} \cdot 1^{n-1} + \dots + a_0 \cdot 1^0 = a_n + a_{n-1} + \dots + a_0$, la prima parte della proposizione è provata.

Per dimostrare che $n \equiv r(n)$ è sufficiente applicare la proprietà transitiva dell'equivalenza ed osservare che, detto k un intero tale che $s^k(n)$, risulta che $n \equiv s(n)$, $s(n) \equiv s^2(n)$, ..., $s^{k-1}(n) \equiv s^k(n) = r(n)$.

Proposizione 2.3. (La prova del nove). Vale l'implicazione

$$c = a \cdot b \Rightarrow s(c) \equiv s(a) \cdot s(b),$$

e quindi $r(r(a) \cdot r(b)) = r(c)$.

² Il calcolo del ridotto di un numero può essere anche inquadrato nell'ambito della teoria dei punti fissi. Ricordiamo che se f è una funzione allora un punto fisso di f è un elemento x tale che $f(x) = x$. Spesso i punti fissi di f vengono trovati fissando un qualunque elemento \underline{x} e calcolando la successione $f(\underline{x})$, $f^2(\underline{x})$, ... che prende il nome di *orbita* di \underline{x} . Nel nostro caso i punti fissi di s sono tutti e solo i numeri di una sola cifra (cioè minori o uguali a 9). D'altra parte, se invece n non è un punto fisso allora $s(n) < n$. Pertanto in ogni caso $s(n) \leq n$. Calcoliamo all'ora l'orbita di n , cioè la successione $s(n) \geq s^2(n) \geq \dots$. Poiché in N ogni sottoinsieme ammette minimo esisterà un k tale che $s^{k+1}(n) = s^k(n)$. Questo significa che $s^k(n)$ è un punto fisso di s , cioè $s^k(n) = r(n)$.

³ Per la struttura Z utilizziamo il linguaggio degli anelli costituito dalla relazione di identità $=$, dai simboli $+$, \cdot per le operazioni e dalle costanti 0 ed 1 . Con 2 indichiamo il termine $1+1$, con 3 il termine $(1+1)+1$, ... Pertanto, ad esempio, $3 \cdot x + 2$ è il termine $((1+1)+1) \cdot x + (1+1)$.

Dim. Essendo \equiv una congruenza, per definizione sappiamo che se $a \equiv a'$ e $b \equiv b'$ allora $a \cdot b \equiv a' \cdot b'$. Poiché $a \equiv s(a)$ e $b \equiv s(b)$, possiamo concludere che $s(c) \equiv s(a \cdot b) \equiv a \cdot b \equiv s(a) \cdot s(b)$. Similmente, poiché $a \equiv r(a)$ e $b \equiv r(b)$, possiamo concludere che $r(c) \equiv r(a \cdot b) \equiv a \cdot b \equiv r(a) \cdot r(b)$ e quindi $r(c) = r(r(c)) \equiv r(r(a) \cdot r(b))$.

Da notare che il procedimento della prova del nove può essere applicato ad ogni base. Infatti se la base con cui si rappresenta un numero n è b allora la somma delle cifre di n è un numero congruo ad n modulo $b-1$. Da notare ancora che poiché tale proposizione è una implicazione e non una equivalenza, risulta che:

Proposizione 2.4. Se la prova del nove fallisce allora la moltiplicazione è sbagliata, tuttavia se la prova del nove riesce questo non comporta che la moltiplicazione sia fatta bene.

Ad esempio poiché risulta $34 \times 27 = 918$ per tale prodotto la prova del nove riesce. D'altra parte se permuti le cifre di 918 allora essendo il ridotto di 189 uguale al ridotto di 918, deve riuscire anche la prova del nove per il calcolo sbagliato $34 \times 27 = 189$. Similmente, poiché due numeri le cui cifre differiscono solo per la presenza di zeri hanno lo stesso ridotto, allora la prova del nove riuscirà anche per calcoli sbagliati $34 \times 27 = 9018$, $34 \times 207 = 918$, $340000 \times 27 = 918$ e così via.

In realtà la prova del nove non vale solo per il prodotto ma per qualunque tipo di calcolo algebrico.

Proposizione 2.5. (Prova del nove estesa) Supponiamo di avere un algoritmo algebrico espresso tramite un termine $t(x_1, \dots, x_n)$ e che, applicato questo algoritmo a valori n_1, \dots, n_p si ottenga il risultato $n = t(n_1, \dots, n_p)$. Allora nel caso il calcolo sia esatto deve risultare $r(n) = r(t(r(d_1), \dots, r(d_n)))$.

Ad esempio, supponiamo di dover verificare il calcolo $234 \times (23+12+15)+71 = 47573$, allora sostituendo ad ogni numero il relativo ridotto calcoliamo $9 \times (5+3+6)+8$ e quindi $9 \times 5+8$ e quindi $9+8 = 17$ e quindi 8. D'altra parte possiamo ridurre il numero 47573 nel numero 26 e quindi nel numero 8. Quindi la prova del nove riesce.

Esercizio. Inventarsi una prova dell'undici. Si suggerisce di sfruttare il fatto che 10 è congruo a -1 modulo 11.

3. Proprietà che si conservano per passaggio a quoziente

Se applichiamo il teorema 7.3 del Capitolo 6 agli epimorfismi canonici otteniamo il seguente teorema.

Teorema 3.1. Tutte le proprietà universali positive sono conservate nel passaggio a quoziente. In particolare tutte le equazioni si conservano per passaggio a quoziente.

Se, ad esempio, applichiamo tale proposizione alla teoria dei gruppi, abbiamo la seguente proposizione.

Proposizione 3.2. Il quoziente G' di un gruppo G modulo una data congruenza è ancora un gruppo. Se G è abeliano, allora anche G' è abeliano. La proprietà $\forall x((x+x=0) \rightarrow x=0)$ è un esempio di proprietà universale (non positiva) che non si conserva per quoziente.

Dim. Una struttura algebrica G è un gruppo se e solo se verifica le equazioni

$$(x+y)+z = z+(y+z), x+1 = x, 1+x = x, x+(-x) = 0, (-x)+x = 0.$$

Poiché nel passaggio a quoziente tali equazioni continuano a valere, anche G' continua ad essere un gruppo. Per lo stesso motivo se G è commutativo, cioè verifica l'equazione $x+y = y+x$ anche G' è commutativo perché verifica la stessa equazione.

Consideriamo la proprietà $\forall x((x+x=0) \rightarrow x=0)$ che è universale ma non positiva in quanto coincidente con $\forall x(x=0 \vee \neg(x+x=0))$. Consideriamo il gruppo additivo $(\mathbb{Z}, +, -, 0)$ degli interi relativi e la congruenza modulo 2 in cui si pone $x \equiv x'$ se $x-x'$ è un multiplo di 2. Allora il quoziente è il gruppo con due elementi, $[0]$ ed $[1]$ e risulta evidente che $[1]+[1] = [0]$ mentre $[1] \neq [0]$.

Un esempio ulteriore è fornito dalla teoria degli anelli.

Proposizione 3.3. Il quoziente di un anello modulo una congruenza è ancora un anello. In particolare, dato un intero m , il quoziente Z/m di Z modulo m è un anello. Tuttavia, se m è un numero non primo, la formula

$$\forall x \forall y((x \cdot y = 0) \rightarrow (x = 0) \vee (y = 0))$$

che esprime il non avere divisori dello zero è una proprietà universale non positiva che, pur essendo verificata da Z non è verificata dal quoziente Z/m .

Dim. Che il quoziente di un anello sia un anello deriva dal fatto che il passaggio a quoziente conserva tutte le equazioni e quindi anche tutti gli assiomi della teoria degli anelli. E' noto che in Z non esistono divisori dello zero. D'altra parte se $m = p \cdot q$ con p e q divisori propri, allora $[p] \cdot [q] = [m] = [0]$. Essendo sia p che q diversi da m e minori o uguali ad m risulta anche che $[p] \neq [0]$ e $[q] \neq [0]$. Pertanto Z/m ammette come divisori dello zero $[p]$ e $[q]$. Da notare che $\forall x \forall y((x \cdot y = 0) \rightarrow (x = 0) \vee (y = 0))$ è universale non positiva in quanto coincide con la formula $\forall x \forall y(\neg(x \cdot y = 0) \vee (x = 0) \vee (y = 0))$.

Nel capitolo 5 quando abbiamo parlato di logiche con uguaglianza abbiamo supposto che la relazione $=$ soddisfacesse alcuni assiomi. Tuttavia tali assiomi, oltre ad essere verificati dalla identità, sono verificati anche da una qualunque congruenza. Si pone allora il problema se aggiungendo ulteriori assiomi non sia possibile fare in modo che l'unica interpretazione possibile di $=$ sia l'identità. Il seguente teorema mostra che ciò non è possibile.

Teorema 3.4. Il quoziente normale di una interpretazione (D, I) è elementarmente equivalente a (D, I) . Pertanto non esiste un sistema di assiomi capace di caratterizzare l'identità.

Dim. Sappiamo che $I(=)$ è una congruenza e che, in base alla proposizione 1.3, il corrispondente epimorfismo canonico è una immersione suriettiva. Pertanto, per il teorema 3.1 del capitolo 6, possiamo concludere che (D, I) è elementarmente equivalente al suo quoziente normale.

Se esistesse un sistema di assiomi T capace di caratterizzare l'identità, allora data una interpretazione non normale (D, I) il sistema T sarebbe verificato dal quoziente normale di (D, I) . Stante il fatto che tale quoziente è elementarmente equivalente a (D, I) , ciò comporterebbe che anche (D, I) verifica T . Ma allora (D, I) sarebbe un modello normale in contrasto con le ipotesi.

Se applichiamo il teorema 7.3 del capitolo 6 agli epimorfismi canonici, otteniamo il seguente teorema che mostra che ogni proprietà esprimibile senza l'utilizzo del simbolo di identità si conserva per quoziente.

Teorema 3.5. Sia (D,I) una interpretazione e sia (D_{\equiv},I_{\equiv}) il suo quoziente modulo una relazione di congruenza \equiv . Allora per ogni formula α in cui non compare il simbolo $=$ risulta

$$I \models \alpha [d_1, \dots, d_n] \Leftrightarrow I_{\equiv} \models \alpha [[d_1'], \dots, [d_n']] \tag{3.1}$$

Pertanto se $d_1 \equiv d_1', \dots, d_n \equiv d_n'$ allora

$$I \models \alpha [d_1, \dots, d_n] \Leftrightarrow I \models \alpha [d_1', \dots, d_n'] \tag{3.2}$$

Ne segue che nei linguaggi senza uguaglianza ogni quoziente di una struttura è elementarmente equivalente alla struttura stessa.

Dim. Per provare la seconda parte del teorema, supponiamo che $d_1 \equiv d_1', \dots, d_n \equiv d_n'$. Allora,

$$I \models \alpha [d_1, \dots, d_n] \Leftrightarrow I_{\equiv} \models \alpha [[d_1], \dots, [d_n]] \Leftrightarrow I_{\equiv} \models \alpha [[d_1'], \dots, [d_n']] \Leftrightarrow I \models \alpha [d_1', \dots, d_n']$$

Come è noto il quoziente dell'anello Z modulo m nel caso in cui m sia un numero primo risulta essere un campo. Pertanto la proprietà

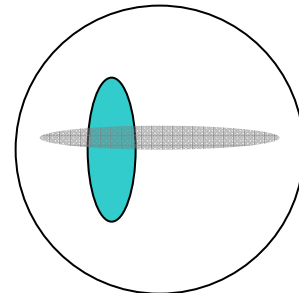
$$\exists x(x \neq 0) \wedge (\forall y(x \cdot y \neq 1))$$

di “non essere un campo” non si conserva per quoziente coerentemente con il fatto che tale proprietà coinvolge il simbolo $=$.

4. La logica monadica: la logica di Aristotele è decidibile.

Applichiamo il teorema ora dimostrato alle *logiche monadiche* cioè alle logiche il cui linguaggio contenga solo predicati *monadici*, cioè predicati di arità 1, e costanti. In tale logica invece non sono presenti simboli di funzioni e non è presente il simbolo $=$. L'interesse di tale logica risiede nel fatto che, come abbiamo visto nel primo capitolo, Aristotele considerava nella sua logica solo predicati monadici e mai relazioni di arità maggiore o uguale a 2. Se indichiamo con r_1, \dots, r_n i nomi dei predicati monadici allora una interpretazione (D,I) è definita da un dominio D e dai sottoinsiemi $S_1 = I(r_1), \dots, S_n = I(r_n)$. Possiamo indicare allora con (D, S_1, \dots, S_n) una tale interpretazione.

Ad esempio nella figura affianco è definito un modello di una logica con due predicati monadici r_1, r_2 in cui D è l'insieme dei punti interni al cerchio e gli insiemi $S_1 = I(r_1), S_2 = I(r_2)$ sono rappresentati dai punti interni alle due ellissi.



In ogni interpretazione di un linguaggio monadico esiste una congruenza definita in modo naturale.

Definizione 4.2. Sia (D,I) una interpretazione di un linguaggio monadico. Chiamiamo *indiscernibili*⁴ due elementi d e d' di D tali che, per ogni predicato monadico r ,

$$(D,I) \models r(x) [d] \Leftrightarrow (D,I) \models r(x) [d']$$

Pertanto due elementi sono indiscernibili se tutto quello che si può dire di uno lo si può dire di un altro. Indichiamo con \equiv la relazione di indiscernibilità.

Teorema 4.3. La relazione di indiscernibilità è una congruenza in (D,I) . Il relativo quoziente prende il nome di *ridotto* di (D,I) . Se il linguaggio contiene solo n predicati monadici, il ridotto di (D,I) ha un numero di elementi minore o uguale a 2^n .

⁴ Questo tipo di relazione di equivalenza è molto importante ed è legata al principio degli indiscernibili di Leibniz secondo cui due elementi sono uguali se tutto ciò che si può dire di uno si può dire dell'altro. Se si specifica in quale linguaggio viene intesa l'espressione “si può dire”, allora in un linguaggio molto povero è evidente che due oggetti potrebbero essere non distinguibili pur non essendo uguali.

Dim. Che la relazione \equiv sia una congruenza è vero perché, per definizione, per ogni r ,

$$d \equiv d' \Rightarrow d \in I(\alpha) \Leftrightarrow d' \in I(\alpha).$$

Inoltre, se $M = \{r_1, \dots, r_n\}$ è l'insieme dei predicati monadici, allora \equiv può anche essere vista come il nucleo della funzione $h : D \rightarrow P(M)$ che associa ad ogni elemento $d \in D$ la classe $h(d)$ dei predicati in M che sono verificati da d . Da ciò segue che il quoziente (D', I') di (D, I) modulo \equiv ha un numero di elementi minore o uguale a quelli di $P(A)$ e quindi minore o uguale a 2^n .

Teorema 4.4. Data una interpretazione (D, I) di un linguaggio monadico con n predicati monadici. Allora il suo ridotto è una interpretazione elementarmente equivalente a (D, I) che ha un numero di elementi minore o uguale a 2^n .

Dim. Basta osservare che poiché il linguaggio monadico non contiene l'identità, per il teorema 4.1 il ridotto di (D, I) è elementarmente equivalente a (D, I) .

Il seguente corollario mostra che possono esistere interpretazioni elementarmente equivalenti ma non isomorfe.

Corollario 4.5. Supponiamo che una interpretazione (D, I) di una logica monadica ad n predicati abbia più di 2^n elementi. Allora il suo ridotto è una interpretazione elementarmente equivalente a (D, I) non isomorfa a (D, I) .

Dim. Basta osservare che il ridotto di (D, I) non può essere isomorfo a (D, I) poiché strutture isomorfe hanno lo stesso numero di elementi.

Corollario 4.6. Sia T una teoria in una logica del primo ordine con solo n predicati monadici. Allora:

- a) T ha un modello se e solo se ha un modello con un numero di elementi minore o uguale a 2^n .
- b) se α è una formula chiusa, allora $T \models \alpha$ se e solo se ogni modello di T con un numero di elementi minore o uguale a 2^n è anche un modello di α ,
- c) due formule α e α' sono logicamente equivalenti se ammettono gli stessi modelli con un numero di elementi minore o uguale a 2^n .

Dim. La proposizione a) è evidente. Per provare b) supponiamo che ogni modello di T con un numero di elementi minore o uguale a 2^n sia anche un modello di α . Sia ora (D, I) un qualunque modello di T e supponiamo per assurdo che α sia false, allora (D, I) sarebbe un modello di $T \cup \{\neg\alpha\}$. Esisterebbe allora un modello di tale teoria con un numero di elementi minore o uguale a 2^n . Ciò è in contrasto con l'ipotesi. L'implicazione inversa è evidente.

Per provare c) osserviamo che α è logicamente equivalente ad α' se e solo se $\alpha \leftrightarrow \alpha'$ è una tautologia. D'altra parte $\alpha \leftrightarrow \alpha'$ è vera in tutte le interpretazioni se e solo se è vera in tutte le interpretazioni con un numero di elementi minore o uguale a 2^n . Ciò implica c).

Corollario 4.7. Ogni teoria finita è decidibile. In altri termini esiste un procedimento effettivo che permette di stabilire se una formula α è una conseguenza logica o meno di T .

Dim. Supponiamo di dovere stabilire se α sia una conseguenza logica di T oppure no. Possiamo mettere in moto il seguente algoritmo.

1. fissiamo $m = 1$ e $D_m = \{1\}$

2. calcoliamo l'insieme I_m delle possibili interpretazioni con dominio D_m
3. isoliamo quelle interpretazioni in I_m che sono modelli di T e verifichiamo che siano anche modelli di α . Se questo non avviene ci fermiamo e concludiamo che α non è conseguenza logica di T . Altrimenti incrementiamo m di una unità ed aggiungiamo a D_m il numero m (in breve $m := m+1$ e $D_m = D_m \cup \{m\}$).
4. Successivamente andiamo all'istruzione 2 e ripetiamo il ciclo fino a quando m non superi 2^n
5. Se il ciclo non è stato interrotto prima (per aver trovato un modello di T che non verifica α) possiamo concludere che α è conseguenza logica di T .

Naturalmente un tale tipo di algoritmo è altamente “pesante” e richiede un tempo di calcolo enorme. Tuttavia in linea di principio può essere implementato in un qualunque linguaggio di programmazione. Come vedremo nell'ultimo capitolo è invece stato scoperto che in generale le logiche che coinvolgono relazioni binarie non sono decidibili.

A titolo di esercizio possiamo studiare cosa succede in una logica il cui linguaggio ha un solo predicato monadico r . Per tale logica un modello è costituito da una coppia (D, I) con $I(r)$ sottoinsieme S di D , cioè da una coppia costituita da un insieme e da un sottoinsieme.

Inoltre per quanto riguarda la nozione di isomorfismo vale la seguente proposizione.

Proposizione 4.8. Due modelli (D, S) e (D', S') di una logica con un solo predicato monadico sono isomorfi se e solo se D è equipotente a D' ed S è equipotente ad S' .

D.im Se $f : D \rightarrow D'$ è un isomorfismo allora è anche una funzione biettiva tra D e D' che quindi sono equipotenti. Inoltre poiché per ogni $x \in D$,

$$x \in S \Leftrightarrow f(x) \in S',$$

la restrizione di f ad S è una applicazione biettiva tra S ed S' e questo prova che anche i sottoinsiemi S ed S' sono equipotenti.

Viceversa supponiamo che D sia equipotente a D' ed S equipotente ad S' , allora anche $D-S$ è equipotente a $D'-S'$. Siano $f_1 : S \rightarrow S'$ ed $f_2 : D-S \rightarrow D'-S'$ due funzioni biettive. Allora è subito visto che $f = f_1 \cup f_2$ è un isomorfismo tra (D, S) e (D', S') .

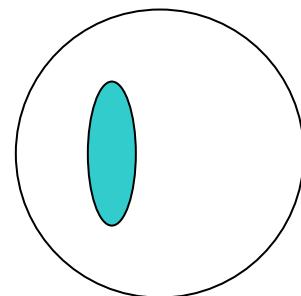
In un linguaggio tanto povero naturalmente possono essere espresse poche proprietà. Ad esempio possiamo considerare la formula $\exists x r(x)$ che esprime il fatto che S è non vuoto oppure la formula $\exists x \neg r(x)$ per esprimere il fatto che $-S$ è non vuoto. In base al Corollario 4.5 per tale logica possiamo riferirci solo ad interpretazioni il cui dominio D ha uno o due elementi. Non è difficile elencarle tutte:

1. Caso un solo elemento. Supponendo ad esempio che $D = \{a\}$, in $P(D)$ vi sono solo due sottoinsiemi, \emptyset e $\{a\}$. Pertanto vi sono solo due possibili interpretazioni $(\{a\}, I_1)$ e $(\{a\}, I_2)$ che si ottengono ponendo $I_1(r) = \emptyset$ e $I_2(r) = \{a\}$, rispettivamente.

2. Caso due elementi. Supponendo ad esempio che $D = \{a, b\}$, in $P(D)$ vi sono solo quattro sottoinsiemi a cui corrispondono solo quattro possibili interpretazioni $(\{a, b\}, I_3)$, $(\{a, b\}, I_4)$, $(\{a, b\}, I_5)$, $(\{a, b\}, I_6)$ che si ottengono ponendo $I_3(r) = \emptyset$, $I_4(r) = D$, $I_5(r) = \{a\}$, $I_6(r) = \{b\}$.

Si noti comunque che la quinta e la sesta interpretazione sono isomorfe tra loro e quindi in definitiva ogni questione in tale logica può essere verificata facendo riferimento solo alle prime cinque interpretazioni ora elencate.

Ad esempio consideriamo l'interpretazione che si ottiene ponendo D uguale l'insieme dei punti del cerchio ed $I(r)$ uguale all'insieme dei punti interni all'ellisse. Allora due elementi sono equivalenti solo se appartengono entrambi all'ellisse oppure se



entrambi non appartengono all'ellisse. Allora il suo ridotto è costituito solo da classi $a = I(r)$ e $b = -I(r)$. E' evidente che non essendo equipotenti le due interpretazioni, pur essendo elementarmente equivalenti non possono essere isomorfe.

5. Prodotto diretto di due interpretazioni

Date due interpretazioni (D_1, I_1) e (D_2, I_2) di un linguaggio L , ci poniamo il problema di definire la nozione di *prodotto* di tali interpretazioni, cioè di definire in modo adeguato una interpretazione che abbia come dominio il prodotto cartesiano $D_1 \times D_2$. Questo può essere fatto in vari modi come mostriamo negli esempi seguenti.

Prodotto di due insiemi ordinati: Ad esempio supponiamo che in L ci sia solo il simbolo di relazione binaria \leq e che (D_1, \leq_1) e (D_2, \leq_2) siano due interpretazioni di L tali che \leq_1 e \leq_2 siano due relazioni d'ordine. Allora possiamo definire nel prodotto $D_1 \times D_2$ la relazione \leq ottenuta ponendo

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 < y_1 \text{ oppure } x_1 = y_1 \text{ e } x_2 \leq y_2.$$

In altre parole dovendo confrontare (x_1, x_2) con (y_1, y_2) effettuiamo il confronto prima tra le prime componenti, se le prime componenti coincidono allora si procede al confronto delle seconde componenti. Ad esempio supponiamo che entrambi gli ordinamenti coincidano con l'insieme ordinato N dei numeri naturali. Allora, ad esempio, avremmo che $(1, 2) \leq (2, 1)$ e $(1, 2) \leq (1, 3)$. Questo modo di fare il prodotto, che prende il nome di *lessicografico*, ha l'importante proprietà per cui il prodotto di due totali è ancora un ordine totale. Una ovvia estensione di tale procedimento lo rende utile ad esempio per inserire le parole in un vocabolario in modo che l'ordinamento delle lettere dell'alfabeto (che è totale) diventi un ordinamento (totale) dell'insieme delle parole. Ad esempio la parola *do* viene messa prima della parola *mi* in quanto *d* precede in *m*, la parola *do* viene invece messa dopo la parola *da* (ricordiamo che una parola di due lettere può essere vista come una coppia).

Un modo diverso di effettuare il prodotto di due insiemi ordinati si ottiene ponendo :

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 \leq y_1 \text{ e } x_2 \leq y_2.$$

Rispetto a tale modo di definire l'ordinamento abbiamo che $(1, 2)$ non è confrontabile con $(2, 1)$ mentre $(1, 2) \leq (1, 3)$. Tranne il caso banale in cui uno degli insiemi abbia un solo elemento, questo tipo di ordinamento non è totale.

Prodotto di due campi. Sia L il linguaggio della teoria degli anelli unitari e sia $(R, +, \cdot, 0, 1)$ il campo dei numeri reali. Vogliamo definire una interpretazione di L che abbia come dominio il prodotto cartesiano $R \times R$. Un primo modo di fare questo può essere suggerito dalla definizione di numero complesso (si veda il capitolo 6) ponendo

$$(x, y) + (x', y') = (x + x', y + y') ; (x, y) \cdot (x', y') = (x \cdot x' - y \cdot y', x \cdot y' + y \cdot x').$$

Come è noto in questo modo si ottiene il campo dei numeri reali.

Un modo diverso di effettuare il prodotto consiste nel definire oltre la somma anche il prodotto "componente per componente" ponendo

$$(x, y) \cdot (x', y') = (x \cdot x', y \cdot y').$$

Inoltre la costante 0 viene interpretata ancora con la coppia $(0, 0)$, mentre la costante 1 con la coppia $(1, 1)$. In questo modo $R \times R$ non risulta più essere un campo. Infatti se si considerano due elementi del tipo $(x, 0)$ e $(0, y)$ risulta che

$$(x, 0) \cdot (0, y) = (0, 0)$$

Questo significa che in $R \times R$ esistono divisori dello zero e quindi elementi non nulli che non sono invertibili.

Si pone allora il seguente problema:

quale è il modo migliore di definire il prodotto di due interpretazioni ?

Per dare una risposta a tale domanda ricordiamo che prendono il nome di *proiezioni* le due funzioni $Pr_1: D_1 \times D_2 \rightarrow D_1$ e $Pr_2: D_1 \times D_2 \rightarrow D_2$ definite dall'essere:

$$Pr_1(x_1, x_2) = x_1 \quad ; \quad Pr_2(x_1, x_2) = x_2.$$

La parola *proiezione* si giustifica dal fatto che se (x_1, x_2) si interpreta come un punto di un piano le cui coordinate sono x_1 e x_2 (in un sistema di assi cartesiani ortogonali) allora le proiezioni si possono interpretare come proiezioni ortogonali sugli assi cartesiani.

In matematica usa applicare il seguente principio:

“il prodotto di due strutture deve essere definito in modo tale che le proiezioni siano degli epimorfismi”.

In base a tale principio date le due strutture ordinate (D_1, \leq_1) e (D_2, \leq_2) deve risultare che

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow Pr_1(x_1, x_2) \leq Pr_1(y_1, y_2) \Leftrightarrow x_1 \leq y_1$$

e

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow Pr_2(x_1, x_2) \leq Pr_2(y_1, y_2) \Leftrightarrow x_2 \leq y_2.$$

Queste due equivalenze sono appunto soddisfatte solo se si segue il secondo modo di definire il prodotto di due ordinamenti cioè solo se si pone

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 \leq y_1 \text{ e } x_2 \leq y_2.$$

Problema: Dimostrare con un esempio che nel prodotto lexicografico le proiezioni non sono omomorfismi.

Considerando invece il caso del prodotto del campo dei numeri reali per se stesso, risulterà che

$$Pr_1((x_1, x_2) + (y_1, y_2)) = Pr_1(x_1, x_2) + Pr_1(y_1, y_2) = x_1 + y_1$$

e

$$Pr_2((x_1, x_2) + (y_1, y_2)) = Pr_2(x_1, x_2) + Pr_2(y_1, y_2) = x_2 + y_2.$$

Questo comporta che necessariamente

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2).$$

In altri termini il prodotto di due coppie deve essere fatto moltiplicando le prime e le seconde. Ciò coincide con la definizione di somma di due numeri complessi. Similmente se consideriamo il prodotto allora deve essere

$$Pr_1((x_1, x_2) \cdot (y_1, y_2)) = Pr_1(x_1, x_2) \cdot Pr_1(y_1, y_2) = x_1 \cdot y_1$$

e

$$Pr_2((x_1, x_2) \cdot (y_1, y_2)) = Pr_2(x_1, x_2) \cdot Pr_2(y_1, y_2) = x_2 \cdot y_2.$$

Pertanto anche il prodotto viene definito componente per componente. Per quanto riguarda l'interpretazione $I(0)$ della costante 0, se vogliamo che le proiezioni siano omomorfismi allora deve risultare che

$$Pr_1(I(0)) = I_1(0) \text{ e } Pr_2(I(0)) = I_2(0)$$

e quindi che $I(0) = (I_1(0), I_2(0)) = (0, 0)$. Similmente:

$$Pr_1(I(1)) = I_1(1) \text{ e } Pr_2(I(1)) = I_2(1)$$

e quindi che $I(1) = (I_1(1), I_2(1)) = (1, 1)$.

Problema: Dimostrare con un esempio il fatto che la funzione che associa ad ogni numero complesso la sua parte reale non è un omomorfismo.

Queste considerazioni suggeriscono la seguente definizione:

Definizione 5.1. Siano (D_1, I_1) e (D_2, I_2) due interpretazioni di un linguaggio L , allora chiamiamo *prodotto diretto* di (D_1, I_1) e (D_2, I_2) l'interpretazione (D, I) tale che:

- $D = D_1 \times D_2$

- $I(o)((d_1, d_1'), \dots, (d_n, d_n')) = (I_1(o)(d_1, \dots, d_n), I_2(o)(d_1', \dots, d_n'))$

- $((d_1, d_1'), \dots, (d_n, d_n')) \in I(r) \Leftrightarrow (d_1, \dots, d_n) \in I_1(r) \text{ e } (d_1', \dots, d_n') \in I_2(r)$

- $I(c) = (I_1(c), I_2(c))$.

Esempio. Consideriamo gli insiemi ordinati $\{a,b,c\}$ e $\{1,2,3\}$, cioè le interpretazioni (D_1, I_1) e (D_2, I_2) con

$$D_1 = \{a,b,c\}, I_1(\leq) = \{(a,b), (b,c), (a,c), (a,a), (b,b), (c,c)\}$$

$$D_2 = \{1,2,3\}, I_2(\leq) = \{(1,2), (2,3), (1,3), (1,1), (2,2), (3,3)\}$$

allora il prodotto diretto di tali insiemi ha come dominio $D = \{a,b,c\} \times \{1,2,3\}$ mentre la relazione \leq è definita ponendo, per ogni coppia (x,n) e (x',n') ,

$$(x,n) \leq (x',n') \text{ se e solo se } x \leq x' \text{ e } n \leq n'.$$

6. Proprietà che si conservano per prodotti diretti: classi equazionali

Per esaminare le proprietà che si conservano per prodotti diretti sono utili le seguenti due proposizioni.

Proposizione 6.1. Date due interpretazioni (D_1, I_1) e (D_2, I_2) ed il relativo prodotto diretto (D, I) , la prima e seconda proiezione sono epimorfismi. Conseguentemente, per ogni termine t ,

$$I(t)((d_1, d_1'), \dots, (d_n, d_n')) = (I_1(t)(d_1, \dots, d_n), I_2(t)(d_1', \dots, d_n')). \quad (6.1)$$

Dim. Ripetendo quanto detto all'inizio del paragrafo, osserviamo che se h è il nome di una operazione n -aria, allora

$$Pr_1(I(o)((d_1, d_1'), \dots, (d_n, d_n'))) = I_1(o)(d_1, \dots, d_n) = I_1(o)(Pr_1(d_1, d_1'), \dots, Pr_1(d_n, d_n')).$$

Se c è una costante allora

$$Pr_1(I(c)) = I_1(c).$$

Infine, se r è il nome di una relazione n -aria, allora

$$((d_1, d_1'), \dots, (d_n, d_n')) \in I(r) \Rightarrow (d_1, \dots, d_n) \in I_1(r) \Leftrightarrow (Pr_1(d_1, d_1'), \dots, Pr_1(d_n, d_n')) \in I_1(r).$$

Ciò prova che Pr_1 è un omomorfismo. Analogo discorso vale per la seconda proiezione.

Per provare (6.1) osserviamo che, in base al teorema 1.4 del capitolo 6,

$$Pr_1(I(t)((d_1, d_1'), \dots, (d_n, d_n'))) = I_1(t)(Pr_1(d_1, d_1'), \dots, Pr_1(d_n, d_n')) = I_1(t)(d_1, \dots, d_n).$$

e

$$Pr_2(I(t)((d_1, d_1'), \dots, (d_n, d_n'))) = I_2(t)(Pr_2(d_1, d_1'), \dots, Pr_2(d_n, d_n')) = I_2(t)(d_1, \dots, d_n). \quad \square$$

In altre parole tale proposizione afferma che se si deve applicare un algoritmo t ad elementi del prodotto, allora il risultato sarà una coppia che si ottiene operando separatamente sulla prima e sulla seconda componente secondo l'algoritmo t . Ad esempio se si considera il prodotto diretto $Z \times Z$ ed il termine $(x+y) \cdot z$ allora se si applica tale termine alle coppie $(2,3)$, $(2,-6)$, $(5,4)$ allora il risultato sarà $((2+2) \cdot 5, (3-6) \cdot 4)$.

Teorema 6.2. Sia β una formula atomica, allora

$$(D_1, I_1) \models \beta, (D_2, I_2) \models \beta \Leftrightarrow (D, I) \models \beta.$$

Dim. Dobbiamo provare che vale l'equivalenza

$$(D_1, I_1) \models \beta [d_{1,1}, \dots, d_{1,n}], (D_2, I_2) \models \beta [d_{2,1}, \dots, d_{2,n}] \\ \Leftrightarrow (D, I) \models \beta [(d_{1,1}, d_{2,n}), \dots, (d_{1,n}, d_{2,n})]$$

Per ogni $d_{1,1}, \dots, d_{1,n}$ in D_1 e $d_{2,1}, \dots, d_{2,n}$ in D_2 . D'altra parte, supposto che β sia del tipo $r(t_1, \dots, t_m)$,

$$(D_1, I_1) \models r(t_1, \dots, t_m) [d_{1,1}, \dots, d_{1,n}], (D_2, I_2) \models r(t_1, \dots, t_m) [d_{2,1}, \dots, d_{2,n}] \\ \Leftrightarrow (I_1(t_1)(d_{1,1}, \dots, d_{1,n}), \dots, I_1(t_m)(d_{1,1}, \dots, d_{1,n})) \in I_1(r) \\ \text{e } (I_2(t_1)(d_{2,1}, \dots, d_{2,n}), \dots, I_2(t_m)(d_{2,1}, \dots, d_{2,n})) \in I_2(r) \\ \Leftrightarrow (I(t_1)((d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n})), \dots, I(t_m)((d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n}))) \in I(r)$$

$$\Leftrightarrow (D, I) \models r(t_1, \dots, t_m) [(d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n})].$$

In particolare possiamo applicare tale teorema alle formule che sono equazioni. Ciò è importante poiché moltissime teorie matematiche sono costituite da assiomi che sono equazioni. Basta osservare che la proprietà associativa, quella per cui un dato elemento è elemento neutro, l' invertibilità, la proprietà commutativa, l' idempotenza, la distributività, sono tutte esprimibili tramite equazioni. Ad esempio la teoria dei gruppi è definita dalle seguenti equazioni:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad ; \quad x \cdot (x^{-1}) = 1 \quad ; \quad (x^{-1}) \cdot x = 1 \quad ; \quad x \cdot 1 = x \quad ; \quad 1 \cdot x = x.$$

Per ottenere la teoria dei gruppi abeliani è sufficiente aggiungere l'equazione $x \cdot y = y \cdot x$. Altri esempi di sono la teoria dei monoidi, la teoria dei reticoli, la teoria degli anelli, la teoria delle algebre di Boole.

Definizione 6.3. Chiamiamo *equazionale* una teoria per le strutture algebriche che sia costituita da sole equazioni. Chiamiamo *classe equazionale* o *varietà* la classe dei modelli di una teoria equazionale.

L'importanza delle classi equazionali è quella di essere chiuse rispetto le principali costruzioni algebriche. Ciò rende più agevole lo studio dei gruppi, degli anelli, dei reticoli e di molte altre classi di strutture equazionali studiate dai matematici.

Teorema 6.4. Sia C una classe di strutture algebriche. Allora C è equazionale se e solo se è chiusa per quozienti, per sottoalgebre, per copie isomorfe e per prodotti diretti.

Dim. Sia T un sistema di assiomi per la classe C costituito da sole equazioni. Dal teorema 3.1 segue che il quoziente di un modello di T è ancora un modello di T . Dal teorema 8.2 del capitolo 6 segue che se I è un modello di T allora ogni sua sottostruttura è un modello di T . Dal corollario 3.2 del capitolo 6 segue che ogni copia isomorfa di un modello di T è un modello di T . Infine con il teorema 6.2 abbiamo già provato che il prodotto di due modelli di T è ancora un modello di T .

La dimostrazione della parte inversa del teorema (che è meno immediata) non viene fatta. \square

Ad esempio, poiché la classe dei gruppi è una varietà, abbiamo che

- ogni sottostruttura di un gruppo è ancora un gruppo
- il quoziente di un gruppo è ancora un gruppo
- il prodotto diretto di una famiglia di gruppi è ancora un gruppo.
- ogni copia isomorfa di un gruppo è ancora un gruppo.

Per la classe degli anelli, che costituisce una varietà, valgono le stesse proprietà. Si osservi che invece la classe dei campi non è una varietà. Infatti, come abbiamo già visto, il prodotto diretto di due campi non è un campo.

Proposizione 6.5. La classe dei campi non è equazionale, non è possibile quindi assiomatizzare la nozione di campo tramite sole equazioni come nel caso dei gruppi e degli anelli.

Nota. Si osservi che il fatto che la teoria dei campi utilizzi la formula $\forall x(\neg(x=0) \rightarrow \exists y(x \cdot y=1))$ esprime l'esistenza dell'inverso e che tale formula non è una equazione non per se stessa una prova che la classe dei campi non è equazionale. Infatti niente esclude che si possa riformulare tale assioma tramite opportune equazioni.

Nota. Anche l'eliminazione del quantificatore esistenziale tramite una funzione opportuna non migliora la situazione. Infatti riduciamo $\forall x(\neg(x=0) \rightarrow \exists y(x \cdot y=1))$ nella forma normale premessa $\forall x \exists y(\neg(x=0) \rightarrow (x \cdot y=1))$ e quindi, tramite una funzione *inv*, riscriviamo tale formula in $\forall x(\neg(x=0) \rightarrow (x \cdot \text{inv}(x)=1))$ o, se si vuole, $\forall x((x=0) \vee (x \cdot \text{inv}(x)=1))$. Otteniamo una formula che, per quanto universale, non è una equazione.

Problema. Dimostrare che la classe dei gruppi di ordine minore di 100 non è una varietà.

Problema. Esiste una teoria equazionale categorica (cioè i cui modelli sono tutti isomorfi tra loro) ?

La classe delle formule che si conservano per prodotti diretti è molto più ampia di quella delle sole formule atomiche. Per mostrare questo fatto introduciamo un po' di nomenclatura chiamando:

- *clausola di Horn* ogni clausola con al più un letterale positivo
- *formula di Horn* Ogni formula in forma normale premessa $Q_1 x_1 \dots Q_n x_n (\alpha)$ con α congiunzione di clausole di Horn

Pertanto o una clausola di Horn non contiene letterali positivi ed allora è del tipo $\neg(\alpha_1 \wedge \dots \wedge \alpha_n)$ oppure è una clausola di programma.

Teorema 6.6. Siano (D_1, I_1) e (D_2, I_2) due interpretazioni e sia (D, I) il relativo prodotto diretto, allora per ogni formula di Horn β

$$(D_1, I_1) \models \beta, (D_2, I_2) \models \beta \Rightarrow (D, I) \models \beta.$$

Dim. Abbiamo già dimostrato che il teorema vale per le formule atomiche. Supponiamo che β sia la congiunzione di formule atomiche $\beta_1 \wedge \dots \wedge \beta_n$. Allora,

$$\begin{aligned} & (D_1, I_1) \models \beta_1 \wedge \dots \wedge \beta_n, (D_2, I_2) \models \beta_1 \wedge \dots \wedge \beta_n \\ \Leftrightarrow & (D_1, I_1) \models \beta_1 \dots (D_1, I_1) \models \beta_n, (D_2, I_2) \models \beta_1, \dots, (D_2, I_2) \models \beta_n \\ \Leftrightarrow & (D, I) \models \beta_1, \dots, (D, I) \models \beta_n \Leftrightarrow (D, I) \models \beta_1 \wedge \dots \wedge \beta_n. \end{aligned}$$

Se β è del tipo $\neg(\beta_1 \wedge \dots \wedge \beta_n)$,

$$\begin{aligned} & (D_1, I_1) \models \neg(\beta_1 \wedge \dots \wedge \beta_n), (D_2, I_2) \models \neg(\beta_1 \wedge \dots \wedge \beta_n) \\ \Leftrightarrow & \text{non } (D_1, I_1) \models \beta_1 \wedge \dots \wedge \beta_n, \text{ non } (D_2, I_2) \models \beta_1 \wedge \dots \wedge \beta_n \\ \Rightarrow & \text{non } (D, I) \models \beta_1 \wedge \dots \wedge \beta_n \Leftrightarrow (D, I) \models \neg(\beta_1 \wedge \dots \wedge \beta_n). \end{aligned}$$

Consideriamo ora il caso in cui β sia una qualunque formula di Horn $\forall x_1 \dots \forall x_n (\alpha_1 \wedge \dots \wedge \alpha_k)$ dove $\alpha_1, \dots, \alpha_k$ sono clausole di Horn. Per la legge della distributività del quantificatore universale rispetto alla congiunzione, tale formula equivale all'insieme di formule $\forall x_1 \dots \forall x_n (\alpha_1), \dots, \forall x_1 \dots \forall x_n (\alpha_k)$. Pertanto è sufficiente provare il teorema solo per formule del tipo $\forall x_1 \dots \forall x_n (\beta)$ con β clausola di Horn. Supponiamo che β coincida con una clausola del tipo $\alpha_1 \wedge \dots \wedge \alpha_m \rightarrow \alpha$, siano $(d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n})$ elementi di $D_1 \times D_2$ e supponiamo che per tutti gli α_i ,

$$(D, I) \models \alpha_i [(d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n})].$$

Allora,

$$(D_1, I_1) \models \alpha_i [d_{1,1}, \dots, d_{1,n}] \text{ e } (D_2, I_2) \models \alpha_i [d_{2,1}, \dots, d_{2,n}]$$

e quindi

$$(D_1, I_1) \models \alpha [d_{1,1}, \dots, d_{1,n}] \text{ e } (D_2, I_2) \models \alpha [d_{2,1}, \dots, d_{2,n}].$$

Essendo α atomica, abbiamo già provato che ciò comporta che $(D, I) \models \alpha [(d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n})]$. Possiamo pertanto concludere che

$$(D, I) \models \alpha_1 \wedge \dots \wedge \alpha_m \rightarrow \alpha \quad [(d_{1,1}, d_{2,1}), \dots, (d_{1,n}, d_{2,n})]. \quad \square$$

7. Prodotto diretto di una qualunque famiglia di interpretazioni

La definizione di prodotto di due interpretazioni può essere facilmente estesa al prodotto di un numero finito di interpretazioni. Volendo dare una nozione di prodotto per una qualunque famiglia (eventualmente infinita) di interpretazioni ricordiamo per prima cosa come si estende la nozione di prodotto cartesiano. A tale proposito osserviamo che, dati gli insiemi D_1, \dots, D_n , il prodotto cartesiano $D_1 \times \dots \times D_n$ è definito come l'insieme delle n -ple (d_1, \dots, d_n) . Ora fissare una n -pla significa dire quale è il primo elemento (scelto in D_1), quale è il secondo elemento (scelto in D_2) ... e così via. Allora una n -pla può essere vista come una funzione $f: \{1, \dots, n\} \rightarrow D_1 \cup \dots \cup D_n$ tale che $f(i) \in D_i$. Ad esempio se si pone $D_1 = \{x, y, z\}$, $D_2 = \{a, b, c\}$, $D_3 = \{2, 3\}$, allora un elemento di $D_1 \times D_2 \times D_3$ è ad esempio $(2, b, 2)$. Questo elemento può essere visto come l'applicazione $f: \{1, 2, 3\} \rightarrow \{x, y, z, a, b, c, 2, 3\}$ che associa

- ad 1 il valore 2,
- a 2 il valore b ,
- a 3 il valore 2.

Ne segue che il prodotto cartesiano può essere definito come l'insieme

$$D_1 \times \dots \times D_n = \{f \in (D_1 \cup \dots \cup D_n)^{\{1, \dots, n\}} : f(i) \in D_i\}$$

Questo modo di definire il prodotto cartesiano rende possibile la seguente generalizzazione al caso di infiniti insiemi.

Definizione 7.1. Se $(D_j)_{j \in J}$ è una famiglia di insiemi chiamiamo *prodotto cartesiano*, l'insieme $\prod_{j \in J} D_j$ delle funzioni $f: I \rightarrow \cup_{j \in J} D_j$ tali che $f(j) \in D_j$ per ogni $j \in J$. Chiamiamo *proiezione j -esima* la funzione $pr_j: \prod_{j \in J} D_j \rightarrow D_j$ definita dal porre

$$pr_j(f) = f(j).$$

Come al solito, una funzione $f: I \rightarrow \cup_{j \in J} D_j$ a volte viene indicata scrivendo $(f(i))_{i \in I}$. Se tutti gli elementi di tale famiglia coincidono con l'insieme D allora indichiamo con D^J il prodotto cartesiano e diciamo che D^J è la *potenza cartesiana* di D con insieme di indici J . Naturalmente, D^J coincide con l'insieme delle funzioni di J in D .

Definizione 7.2. Sia $(I_j)_{j \in J}$ una famiglia di interpretazioni di un linguaggio \mathcal{L} con $I_j = (D_j, I_j)$. Chiamiamo *prodotto diretto* di $(I_j)_{j \in J}$ l'interpretazione $\prod_{j \in J} I_j = (D, I)$ tale che:

- $D = \prod_{j \in J} D_j$
- $I(o)(f_1, \dots, f_i)(j) = (I_j(o)(f_1(j), \dots, f_i(j)))$ per ogni $j \in J$
- $I(r) = \{(f_1, \dots, f_s) \mid (f_1(j), \dots, f_s(j)) \in I_j(r) \text{ per ogni } j \in J\}$
- $I(c) = (I_j(c))_{j \in J}$.

Se tutti gli elementi della famiglia $(I_j)_{j \in J}$ coincidono con una stessa interpretazione I , allora preferiamo parlare di *potenza diretta di I con insieme di indici in J* e scriveremo I^J per indicare tale potenza.

Esempio. Sia $(R, \leq, +, \cdot, 0, 1)$ il campo ordinato dei numeri reali e sia $I = N$. Allora la potenza diretta di tale struttura con insieme di indici N è la struttura $(R^N, \leq, +, \cdot, \mathbf{u}, \mathbf{z})$ in cui si pone

- $(x_n)_{n \in N} \leq (y_n)_{n \in N}$ se e solo se $x_n \leq y_n$ per ogni $n \in N$
- $(x_n)_{n \in N} + (y_n)_{n \in N} = (x_n + y_n)_{n \in N}$
- $(x_n)_{n \in N} \cdot (y_n)_{n \in N} = (x_n \cdot y_n)_{n \in N}$
- \mathbf{u} è la successione costantemente uguale ad 1
- \mathbf{z} è la successione costantemente uguale a zero.

E' da notare che tale struttura è un anello unitario il cui zero è z e la cui unità è u . Tuttavia R^N non è un campo in quanto esistono elementi che sono divisori dello zero e quindi non invertibili. Infatti sia

- $p = (p_n)_{n \in \mathbb{N}}$ la successione che assume valore 1 se n è pari e 0 se n è dispari

- $d = (d_n)_{n \in \mathbb{N}}$ la successione che assume valore 0 se n è pari ed 1 se n è dispari.

Allora il prodotto $p \cdot d$ è uguale a zero pur essendo p e d diversi da zero.

Le proposizioni dimostrate per il prodotto di due interpretazioni possono essere estese facilmente al prodotto di una famiglia di interpretazioni.

Proposizione 7.3. Per ogni $j \in J$ la j -proiezione $pr_j : D \rightarrow D_j$ è un omomorfismo suriettivo del prodotto diretto (D, I) nella componente (D_j, I_j) . Conseguentemente, per ogni termine t e per ogni $j \in J$

$$I(t)(f_1, \dots, f_i)(j) = I_j(t)(f_1(j), \dots, f_i(j)). \quad (7.1)$$

Proof. Sia h il nome di una operazione n -aria, allora

$$pr_j(I(o)(f_1, \dots, f_n)) = I_j(o)(f_1(j), \dots, f_n(j)) = I_j(h)(pr(f_1), \dots, pr(f_n)).$$

Se c è una costante allora

$$pr_j(I(c)) = I_j(c).$$

Infine, se r è il nome di una relazione n -aria, allora

$$(f_1, \dots, f_n) \in I(r) \Rightarrow (f_1(j), \dots, f_n(j)) \in I_j(r) \Leftrightarrow (pr_j(f_1), \dots, pr_j(f_n)) \in I_j(r).$$

Ciò prova che pr_j è un omomorfismo. Considerando la (2.1) della proposizione 2.1 abbiamo che

$$I(t)(f_1, \dots, f_i)(j) = pr_j(I(t)(f_1, \dots, f_i)) = I_j(t)(pr_j(f_1), \dots, pr_j(f_i)) = I_j(t)(f_1(j), \dots, f_i(j)). \quad \square$$

Teorema 7.4. Sia C una classe equazionale, allora C è chiusa per quozienti, per sottoalgebre, per copie isomorfe e per prodotti diretti di famiglie di elementi di C .

Il seguente teorema, di cui omettiamo la dimostrazione, permette di invertire tale teorema. Esso fornisce una caratterizzazione delle varietà non in termini del tipo di assiomi usati (equazioni) ma in termini di chiusura rispetto alcune operazioni di carattere algebrico sulle strutture che compongono la varietà.

Teorema 7.5. (Teorema fondamentale sulle classi equazionali). Sia C una classe di interpretazioni chiusa per sottostrutture, quozienti, prodotti diretti di famiglie e copie isomorfe. Allora tale classe è una varietà e pertanto esiste un sistema di assiomi per C espressi tramite equazioni.

8. Ultraprodotto: una costruzione che conserva tutte le proprietà

Sia S un insieme, allora chiamiamo *filtro* su S un sottoinsieme \mathcal{F} di $\mathcal{P}(S)$ tale che:

i) $X \in \mathcal{F}$ e $Y \in \mathcal{F} \Rightarrow X \cap Y \in \mathcal{F}$

ii) $X \in \mathcal{F}, Y \supseteq X \Rightarrow Y \in \mathcal{F}$

iii) $S \in \mathcal{F}$.

Un filtro si dice *proprio* se non coincide con $\mathcal{P}(S)$. Una classe di filtri si ottiene fissando un sottoinsieme C di S e ponendo $\mathcal{F} = \{X \in \mathcal{P}(S) : X \supseteq C\}$. I filtri ottenuti in questo modo si dicono filtri *principali*.

Esempi. Sia $p : \mathcal{P}(S) \rightarrow [0,1]$ è una probabilità finitamente additiva e poniamo $\mathcal{F} = \{X \subseteq S : p(X) = 1\}$ allora \mathcal{F} è un filtro. Infatti le condizioni ii) e iii) sono evidenti

$$X \in \mathcal{F} \text{ e } Y \in \mathcal{F} \Rightarrow p(X) = 1 \text{ e } p(Y) = 1$$

$$\Rightarrow p(X \cap Y) = p(X) + p(Y) - p(X \cup Y) = 1 + 1 - 1 = 1 \Rightarrow X \cap Y \in \mathcal{F}.$$

Se S è infinito un esempio importante di filtro è il filtro degli insiemi *cofiniti*, cioè $\mathcal{F} = \{X : S - X \text{ è finito o vuoto}\}$. L'ipotesi che S sia infinito è essenziale poiché altrimenti \mathcal{F} coinciderebbe con $\mathcal{P}(S)$. Un altro esempio è il filtro degli intorni di un punto in uno spazio topologico.

Esercizio. Dimostrare che tutti gli esempi esposti sono filtri.

Diciamo che un filtro proprio \mathcal{F} è un *ultrafiltro* o che \mathcal{F} è un *filtro primo* se

iv) per ogni $X \in \mathcal{P}(S)$, o $X \in \mathcal{F}$ oppure $-X \in \mathcal{F}$.

Il filtro dei cofiniti non è un ultrafiltro poiché se X è un insieme che sia infinito ed il cui complemento è infinito allora sia X che $-X$ non appartengono a \mathcal{F} . Neanche il filtro degli intorni di un punto risulta essere un ultrafiltro. Si noti che se \mathcal{F} è un ultrafiltro allora, per ogni X e Y in $\mathcal{P}(S)$,

v) $X \cup Y \in \mathcal{F} \Leftrightarrow X \in \mathcal{F}$ oppure $Y \in \mathcal{F}$.

Infatti, supposto $X \cup Y \in \mathcal{F}$, se non fosse $X \in \mathcal{F}$ dovrebbe essere $-X \in \mathcal{F}$ e quindi $(X \cup Y) \cap -X = Y \cap -X \in \mathcal{F}$. Essendo $Y \supseteq Y \cap -X$, ciò comporterebbe che $Y \in \mathcal{F}$.

Esercizio. Provare che se S è un insieme finito allora tutti i filtri su S sono principali.

Esercizio. Sia \mathcal{F} un filtro.

- Provare che \emptyset non può appartenere ad un filtro \mathcal{F} .
- Provare che non esiste X tale che $X \in \mathcal{F}$ e $-X \in \mathcal{F}$.

Nel seguito saremo interessati agli ultrafiltri che non siano principali. La seguente proposizione mostra come sono fatti gli ultrafiltri principali.

Proposizione 8.1. Le seguenti asserzioni sono equivalenti:

- a) \mathcal{F} è un ultrafiltro principale.
- b) \mathcal{F} è generato da un singoletto $\{x\}$, cioè $\mathcal{F} = \{X \in \mathcal{P}(S) : x \in X\}$.
- c) \mathcal{F} è un ultrafiltro che non contiene il filtro dei cofiniti.
- d) \mathcal{F} è un ultrafiltro che contiene un insieme finito

Dim. a) \Rightarrow b). Sia \mathcal{F} un ultrafiltro e sia \mathcal{F} generato dall'insieme X . Se X non fosse un singoletto si potrebbe "spezzare" in due insiemi non vuoti X_1 e X_2 , cioè $X = X_1 \cup X_2$ con $X_1 \cap X_2 = \emptyset$. Allora avremmo che $X_1 \cup X_2 \in \mathcal{F}$ ma $X_1 \notin \mathcal{F}$ e $X_2 \notin \mathcal{F}$, in contrasto con l'ipotesi che \mathcal{F} sia primo.

b) \Rightarrow c) Evidente in quanto $S - \{x\}$ è un cofinito non appartenente ad \mathcal{F} .

c) \Rightarrow d) Supponiamo che \mathcal{F} sia primo e sia C un cofinito che non appartiene ad \mathcal{F} . L'ipotesi che \mathcal{F} sia principale comporta allora che il complemento di C sia un insieme finito Z appartenente ad \mathcal{F} .

d) \Rightarrow a) Sia Z un insieme finito appartenente ad \mathcal{F} . Poiché Z è unione finita dei suoi singoletti, dalla proprietà v) segue che almeno un singoletto $\{x\}$ con $x \in Z$ appartiene a \mathcal{F} . Ne segue che $\mathcal{F} \supseteq \{X \in \mathcal{P}(S) : x \in X\}$. D'altra parte se $X \in \mathcal{F}$, poiché anche $X \cap \{x\} \in \mathcal{F}$ dovrà essere $X \cap \{x\} \neq \emptyset$ e quindi $x \in X$. Ciò prova che $\mathcal{F} = \{X \in \mathcal{P}(S) : x \in X\}$ da cui segue immediatamente a). \square

Definizione 8.2. Sia $(I_j)_{j \in S}$ una famiglia di strutture dello stesso tipo ed \mathcal{F} un filtro in S . Per ogni coppia f e g in $\prod_{j \in S} D_j$ poniamo $E(f, g) = \{j \in S \mid f(j) = g(j)\}$. Allora definiamo una relazione binaria $\equiv_{\mathcal{F}}$ in $\prod_{j \in S} D_j$ ponendo

$$f \equiv_{\mathcal{F}} g \Leftrightarrow E(f, g) \in \mathcal{F}.$$

Se $f \equiv_{\mathcal{F}} g$ allora diciamo anche che f e g *coincidono quasi ovunque rispetto* \mathcal{F} .

Esempi. Se \mathcal{F} è il filtro dei cofiniti allora f e g sono equivalenti se coincidono a meno di un numero finito di punti. Sia \mathcal{F} il filtro determinato da una probabilità p . Allora $f \equiv_{\mathcal{F}} g$ se e solo se la probabilità che $f(x)$ coincida con $g(x)$ è uno. Se \mathcal{F} è il filtro principale generato da X allora $f \equiv_{\mathcal{F}} g$ se e solo se f e g coincidono negli elementi di X . Nel caso $X=S$ allora $f \equiv_{\mathcal{F}} g$ se e solo se f e g coincidono in tutto S . Pertanto in tale caso $\equiv_{\mathcal{F}}$ coincide con l'identità.

Proposizione 8.3. Sia $(I_j)_{j \in S}$ una famiglia di interpretazioni ed \mathcal{F} un filtro su S ed indichiamo con (D, I) l'interpretazione tale che

- $D = \prod_{j \in J} D^j$
- $I(o)(f_1, \dots, f_i)(j) = (I_j(o)(f_1(j), \dots, f_i(j)))$ per ogni $j \in J$
- $I(r) = \{(f_1, \dots, f_s) \mid (f_1(j), \dots, f_s(j)) \in I_j(r) \text{ quasi ovunque rispetto ad } \mathcal{F}\}$
- $I(c) = (I_j(c))_{j \in J}$.

Allora la relazione $\equiv_{\mathcal{F}}$ è una congruenza in (D, I) .

Dim. La proprietà riflessiva e simmetrica di $\equiv_{\mathcal{F}}$ è evidente. Per provare la proprietà transitiva, supponiamo che $f \equiv_{\mathcal{F}} g$ e $g \equiv_{\mathcal{F}} s$ e quindi che $E(f, g) \in \mathcal{F}$ e $E(g, s) \in \mathcal{F}$. Allora, $E(f, g) \cap E(g, s) \in \mathcal{F}$ e quindi, poiché $E(f, s) \supseteq E(f, g) \cap E(g, s)$ risulta che $E(f, s) \in \mathcal{F}$ e quindi che $f \equiv_{\mathcal{F}} s$.

Sia h il nome di una operazione n -aria ed f_1, \dots, f_n e g_1, \dots, g_n elementi di $\prod_{j \in S} D_j$ tali che $f_i \equiv_{\mathcal{F}} g_i$. Vogliamo provare che $I(o)(f_1, \dots, f_n) \equiv_{\mathcal{F}} I(o)(g_1, \dots, g_n)$. Infatti per ipotesi

$$E(f_1, g_1) \in \mathcal{F}, \dots, E(f_n, g_n) \in \mathcal{F}$$

e quindi, per i),

$$E(f_1, g_1) \cap \dots \cap E(f_n, g_n) = \{j \in S \mid f_1(j) = g_1(j), \dots, f_n(j) = g_n(j)\} \in \mathcal{F}.$$

Poiché

$$\begin{aligned} \{j \in S \mid I(o)(f_1, \dots, f_n)(j) = I(o)(g_1, \dots, g_n)(j)\} &= \{j \in S \mid I_j(o)(f_1(j), \dots, f_n(j)) = I_j(o)(g_1(j), \dots, g_n(j))\} \\ &\supseteq \{j \in S \mid f_1(j) = g_1(j), \dots, f_n(j) = g_n(j)\}. \end{aligned}$$

Per ii) abbiamo che $\{j \in S \mid I(o)(f_1, \dots, f_n)(j) = I(o)(g_1, \dots, g_n)(j)\} \in \mathcal{F}$.

Sia r il nome di una relazione n -aria, e siano f_1, \dots, f_n e g_1, \dots, g_n elementi di $\prod_{j \in S} D_j$ tali che $f_i \equiv g_i$. Allora

$$\begin{aligned} (f_1, \dots, f_n) \in I(r) &\Leftrightarrow \{j \in S : (f_1(j), \dots, f_n(j)) \in I_j(r)\} \in \mathcal{F} \\ &\Leftrightarrow E(f_1, g_1) \cap \dots \cap E(f_n, g_n) \cap \{j \in S : (f_1(j), \dots, f_n(j)) \in I_j(r)\} \in \mathcal{F} \\ &\Leftrightarrow \{j \in S \mid (g_1(j), \dots, g_n(j)) \in I_j(r)\} \in \mathcal{F} \Leftrightarrow (g_1, \dots, g_n) \in I(r). \quad \square \end{aligned}$$

Si osservi che l'interpretazione (D, I) differisce dal prodotto diretto solo per il modo come sono definite le relazioni. Ad esempio, considerando R^N ed il filtro dei cofiniti, in (D, I) la relazione d'ordine porrà $(a_n)_{n \in N} \leq (b_n)_{n \in N}$ se $a_n \leq b_n$ tranne che per un numero finito di interi n . Se non esistono relazioni, cioè le strutture I_j sono strutture algebriche, allora (D, I) coincide con il prodotto diretto e quindi $\equiv_{\mathcal{F}}$ è una congruenza in tale prodotto.

Nota. Se nelle strutture I_j esistono anche relazioni allora $\equiv_{\mathcal{F}}$ pur essendo compatibile con le operazioni nel prodotto diretto non è in generale compatibile con le relazioni e quindi non è una congruenza. Ad esempio, consideriamo il prodotto diretto R^N dove R è il campo ordinato dei numeri reali e sia \mathcal{F} il filtro dei cofiniti. Siano $a = (a_n)_{n \in N}$ e $b = (b_n)_{n \in N}$ due successioni tali che $a_n \leq b_n$ per ogni $n \in N$. Supponiamo che $a' = (a'_n)_{n \in N}$ sia la successione ottenuta ponendo $a'_1 = 2$ e $a'_n = a_n$ per ogni intero $n \neq 1$ e che $b' = (b'_n)_{n \in N}$ sia tale che $b'_1 = 1$ e $b'_n = b_n$ per ogni $n \neq 1$. Allora risulta che $a \leq b$ ma che, pur essendo $a \equiv_{\mathcal{F}} a'$, $b \equiv_{\mathcal{F}} b'$, non è vero che $a \leq b$.

Definizione 8.4. Chiamiamo *prodotto ridotto* di $(I_j)_{j \in S}$ modulo \mathcal{F} il quoziente della interpretazione definita in Proposizione 8.3 modulo \mathcal{F} . Se \mathcal{F} è un ultrafiltro allora il prodotto ridotto è chiamato *ultraprodotto*. Se inoltre tutte le strutture della famiglia coincidono allora parleremo di *ultrapotenza*.

In definitiva abbiamo che il prodotto ridotto $M^* = (D^*, I^*)$ è l'interpretazione tale che:

- D^* è il quoziente di $\prod_{j \in S} D_j$ modulo $\equiv_{\mathcal{F}}$
- $I^*(c) = [(I_j(c))_{j \in S}]$,
- $I^*(h)([f_1], \dots, [f_n]) = [(I_j(h)(f_1(j), \dots, f_n(j)))_{j \in S}]$
- $I^*(r) = \{([f_1], \dots, [f_n]) \mid (f_1(j), \dots, f_n(j)) \in I_j(r) \text{ quasi ovunque}\}$.

Supponiamo che \mathcal{F} sia un filtro principale generato da un sottoinsieme X di S allora (D^*, I^*) coincide, a meno di isomorfismi, con il prodotto diretto $\prod_{j \in T} I_j$ dove $T = S - X$. Infatti non è difficile provare che la corrispondenza che associa ad ogni $[f] \in D^*$ la restrizione di f a T è un isomorfismo tra (D^*, I^*) e $\prod_{j \in T} I_j$. In particolare, se $\mathcal{F} = \{S\}$, allora la nozione di prodotto ridotto coincide con quella di prodotto diretto. Questo significa che la nozione di prodotto ridotto non è interessante nel caso dei filtri principali. Per questo motivo nel seguito considereremo solo filtri non principali.

Esempio. Torniamo all'esempio delle successioni di numeri reali e consideriamo come filtro la classe dei cofiniti. In tale caso due successioni sono equivalenti se e solo se coincidono da un certo indice in poi. Se $a = (a_n)_{n \in N}$ e $b = (b_n)_{n \in N}$ sono due successioni di reali allora $[a] \leq [b]$ se e solo se esiste m tale che $a_n \leq b_n$ per ogni $n \geq m$. Inoltre lo zero $[z]$ può essere rappresentato da una qualunque successione che sia uguale a zero da un opportuno indice in poi. Anche in questo caso R^N / \equiv è un anello avente divisori dello zero e quindi non è un campo. Infatti con riferimento alle notazioni dell'esempio precedente, $[p] \cdot [q] = [z]$ pur essendo

$[p] \neq [z]$ e $[q] \neq [z]$. Supponiamo invece che \mathcal{F} sia un ultrafiltro. Allora continua ad essere $[p] \cdot [q] = [z]$. In questo caso però o risulta $[p] = [z]$ oppure risulta $[q] = [z]$. Infatti, essendo \mathcal{F} primo, o risulta che l'insieme dei pari appartiene ad \mathcal{F} oppure l'insieme dei dispari appartiene ad \mathcal{F} . Nel primo caso risulta che $p=z$, nel secondo caso risulta che $q=z$. In definitiva $[p]$ e $[q]$ non sono una coppia di divisori dello zero. In realtà come vedremo nel seguito l'ultrapotenza di un campo è ancora un campo e quindi non può possedere divisori dello zero.

Esponiamo ora il teorema fondamentale sugli ultraprodotti che asserisce che tutte le proprietà esprimibili tramite una formula del primo ordine si conservano per ultraprodotti.

Teorema 8.5. (Teorema fondamentale sugli ultraprodotti). Sia $(I_j)_{j \in S}$ una famiglia di interpretazioni di un linguaggio \mathcal{L} , \mathcal{U} un ultrafiltro su S ed $I^* = (D^*, I^*)$ l'ultraprodotto di tale famiglia tramite \mathcal{U} . Allora

(i) per ogni termine $t(x_1, \dots, x_n)$ e $[f_1], \dots, [f_n] \in D^*$ risulta

$$I^*(t)([f_1], \dots, [f_n]) = [(I_j(t)(f_1(j), \dots, f_n(j)))_{j \in J}]$$

(ii) per ogni formula $\alpha(x_1, \dots, x_n)$ e $[f_1], \dots, [f_n] \in D^*$ risulta

$$I \models \alpha [[f_1], \dots, [f_n]] \Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}$$

(iii) per ogni formula chiusa α

$$I \models \alpha \Leftrightarrow \{j \in J \mid I_j \models \alpha\} \in \mathcal{U}.$$

Dim. Indichiamo con I la struttura definita in proposizione 7.3. Allora essendo $\equiv_{\mathcal{F}}$ una congruenza, per la proposizione 2.1 abbiamo che:

$$I^*(t)([f_1], \dots, [f_n]) = [I(t)(f_1, \dots, f_n)] = [(I_j(t)(f_1(j), \dots, f_n(j)))_{j \in J}].$$

Ciò prova (i). Per provare (ii) procediamo per induzione sulla complessità della formula α . Se α è la formula atomica $r(t_1, \dots, t_m)$ allora

$$\begin{aligned} I^* \models r(t_1, \dots, t_m) [[f_1], \dots, [f_n]] &\Leftrightarrow (I^*(t_1)([f_1], \dots, [f_n]), \dots, I^*(t_m)([f_1], \dots, [f_n])) \in I^*(r) \\ &\Leftrightarrow ([I(t_1)(f_1, \dots, f_n)], \dots, [I(t_m)(f_1, \dots, f_n)]) \in I^*(r) \Leftrightarrow (I(t_1)(f_1, \dots, f_n), \dots, I(t_m)(f_1, \dots, f_n)) \in I(r) \\ &\Leftrightarrow \{j \in J \mid (I_j(t_1)(f_1(j), \dots, f_n(j)), \dots, I_j(t_m)(f_1(j), \dots, f_n(j))) \in I_j(r)\} \in \mathcal{U} \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}. \end{aligned}$$

Supponiamo che (ii) sia vera per le formule α e β , allora, ricordando che

$$X \in \mathcal{U} \text{ e } Y \in \mathcal{U} \Rightarrow X \cap Y \in \mathcal{U},$$

$$\begin{aligned} I \models \alpha \wedge \beta [[f_1], \dots, [f_n]] &\Leftrightarrow I \models \alpha [[f_1], \dots, [f_n]] \text{ e } I \models \beta [[f_1], \dots, [f_n]] \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \text{ e } \{j \in J \mid I_j \models \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)]\} \cap \{j \in J \mid I_j \models \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)] \text{ e } I_j \models \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha \wedge \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}. \end{aligned}$$

Utilizzando la proprietà

$$X \in \mathcal{U} \text{ o } Y \in \mathcal{U} \Rightarrow X \cup Y \in \mathcal{U},$$

$$\begin{aligned} I \models \alpha \vee \beta [[f_1], \dots, [f_n]] &\Leftrightarrow I \models \alpha [[f_1], \dots, [f_n]] \text{ oppure } I \models \beta [[f_1], \dots, [f_n]] \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \text{ oppure } \{j \in J \mid I_j \models \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)]\} \cup \{j \in J \mid I_j \models \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \\ &\Leftrightarrow \{j \in J \mid I_j \models \alpha [f_1(j), \dots, f_n(j)] \text{ oppure } I_j \models \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \end{aligned}$$

$$\Leftrightarrow \{j \in J \mid I_j \vDash \alpha \wedge \beta [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}.$$

Inoltre, ricordando che in ogni ultrafiltro

$$X \notin \mathcal{U} \Rightarrow X^c \in \mathcal{U}.$$

$$I \vDash \neg \alpha [[f_1], \dots, [f_n]] \Leftrightarrow \text{non } I \vDash \alpha [[f_1], \dots, [f_n]] \Leftrightarrow \text{non } \{j \in J \mid I_j \vDash \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}$$

$$\Leftrightarrow \{j \in J \mid \text{non } I_j \vDash \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U} \Leftrightarrow \{j \in J \mid I_j \vDash \neg \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}.$$

Infine per una formula del tipo $\exists x_i \alpha$ osserviamo che per ipotesi di induzione

$$I \vDash \exists x_i \alpha [[f_1], \dots, [f_n]] \Leftrightarrow \text{esiste } [f] \in D^* \text{ tale che } I \vDash \alpha [[f_1], \dots, [f], \dots, [f_n]]$$

$$\Leftrightarrow \text{esiste } [f] \in D^* \text{ tale che } \{j \in J \mid I_j \vDash \alpha [f_1(j), \dots, f(j), \dots, f_n(j)]\} \in \mathcal{U}$$

D'altra parte, poiché $f(j)$ è un elemento di D_j ,

$$\text{esiste } [f] \in D^* \text{ tale che } \{j \in J \mid I_j \vDash \alpha [f_1(j), \dots, f(j), \dots, f_n(j)]\} \in \mathcal{U}$$

$$\Rightarrow \{j \in J \mid \text{esiste } d_j \in D_j \text{ tale che } I_j \vDash \alpha [f_1(j), \dots, d_j, \dots, f_n(j)]\} \in \mathcal{U}$$

$$\Leftrightarrow \{j \in J \mid I_j \vDash \exists x_i \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}.$$

Viceversa, supponiamo che $\{j \in J \mid I_j \vDash \exists x_i \alpha [f_1(j), \dots, f_n(j)]\} \in \mathcal{U}$ e che quindi $\{j \in J \mid \text{esiste}$

$d_j \in D_j$ tale che $I_j \vDash \alpha [f_1(j), \dots, d_j, \dots, f_n(j)]\} \in \mathcal{U}$. Allora possiamo definire f ponendo, per ogni

$j \in J$, $f(j)$ uguale ad un elemento $d_j \in D_j$ tale che $I_j \vDash \alpha [f_1(j), \dots, d_j, \dots, f_n(j)]$ se tale elemento esiste e ponendo $f(j)$ uguale ad un qualsiasi elemento di D_j altrimenti. Allora $[f]$ è un elemento di D^* tale che $\{j \in J \mid I_j \vDash \alpha [f_1(j), \dots, f(j), \dots, f_n(j)]\} \in \mathcal{U}$. Ciò implica che $I \vDash \exists x_i \alpha [[f_1], \dots, [f_n]]$. \square

Da quanto ora provato consegue immediatamente il seguente teorema.

Teorema 8.6. Se una proprietà vale per tutte le componenti di un ultraprodotto allora vale anche per l'ultraprodotto. In particolare, un ultraprodotto di una famiglia di modelli di una teoria del primo ordine T è ancora un modello di T .

Ne segue che, ad esempio, un ultraprodotto di una famiglia di campi è ancora un campo. Si osservi che invece un prodotto diretto di una famiglia di campi è solo un anello come mostra l'esempio delle successioni di numeri reali.

9. Applicazioni della teoria degli ultraprodotti.

Una ovvia conseguenza del teorema 3.6 è il seguente teorema.

Teorema 9.1. Data una interpretazione (D, I) , ogni ultrapotenza di (D, I) è elementarmente equivalente a (D, I) , cioè verifica le stesse proprietà del primo ordine di (D, I) .

Nel capitolo 6 abbiamo visto che due strutture isomorfe sono elementarmente equivalenti. Poiché in generale la potenza di un modello infinito ??Il seguente corollario mostra che il viceversa non è vero.

Corollario 9.2. Dato un modello infinito (D, I) esiste un modello elementarmente equivalente a (D, I) ma non isomorfo a (D, I) .

Omettiamo la dimostrazione della seguente proposizione.

Proposizione 9.3. Dato un insieme S ogni filtro su S si può estendere ad un ultrafiltro su S . In particolare, se S è infinito il filtro dei cofiniti si può estendere ad un ultrafiltro che non è principale.

E' possibile ora provare uno dei principali teoremi della logica matematica.

Teorema 9.4. (Teorema di compattezza). Sia T un insieme di formule, allora
 T ammette un modello \Leftrightarrow ogni parte finita di T ammette un modello.

Dim. E' evidente che se T ammette un modello (D,I) allora ogni parte finita di T ammette (D,I) come modello. Viceversa, supponiamo che ogni parte finita di T ammette un modello e supponiamo che T sia ordinato in una successione $\alpha_1, \alpha_2, \dots$. Per ogni $j \in S$ sia (D_j, I_j) un modello di $T_j = \{\alpha_1, \dots, \alpha_j\}$ e sia \mathcal{U} un ultrafiltro (non principale) di N . Voglio provare che l'ultraprodotto (D, I) della famiglia $((D_j, I_j))_{j \in N}$ è un modello di T . Infatti se $\alpha \in T$ allora risulta che $\alpha \in T_j$ e quindi $(D_j, I_j) \models \alpha$ per ogni indice j maggiore di un opportuno intero m . Ne segue che l'insieme $\{j \in N : (D_j, I_j) \models \alpha\}$ è cofinito e quindi appartiene ad \mathcal{U} . Per il teorema fondamentale sugli ultraprodotti ne segue che α è vera in (D, I) . \square

Definizione 9.5. Indichiamo con $alm(n)$ la formula $\exists x_1 \dots \exists x_n ((x_1 \neq x_2) \wedge \dots \wedge (x_i \neq x_j) \wedge \dots)$ e con Inf l'insieme di formule $\{alm(n) : n \in N\}$.

La formula $alm(n)$ afferma l'esistenza di almeno n elementi distinti. L'insieme Inf di formule esprime il fatto che un modello è infinito nel senso che una interpretazione (D, I) è un modello dell'insieme Inf di formule se e solo se D è infinito.

Teorema 9.6. Sia T una teoria tale che per ogni intero n esiste un modello finito di cardinalità maggiore di n . Allora T ammette un modello infinito.

Dim. Consideriamo la teoria $T \cup Inf$. Ogni parte finita di tale teoria ammette un modello e quindi l'intera teoria ammette un modello. Ma un modello di $T \cup Inf$ è un modello di T che sia infinito e quindi T ammette un modello infinito.

Un modo più diretto di costruire un modello infinito di T è il seguente. Per ogni intero n sia (D_n, I_n) un modello di T di cardinalità maggiore di n , sia \mathcal{U} un ultrafiltro non principale su N e sia (D, I) il relativo ultraprodotto. Voglio provare che (D, I) ha cardinalità infinita. Sappiamo che $alm(n)$ è vera in tutti i modelli (D_m, I_m) con $m \geq n$ e che quindi $\{m : I_m \models alm(n)\} \in \mathcal{U}$. Ciò comporta che per ogni n la formula $alm(n)$ è vera in (D, I) . In definitiva (D, I) è un modello di Inf e quindi è infinito. \square

Proposizione 9.7. Non esiste un insieme di formule capace di esprimere la proprietà di essere finito. Pertanto la teoria dei gruppi finiti non è assiomatizzabile al primo ordine.

10. Ultraprodotti, infinitesimi ed infiniti

Una applicazione molto interessante della teoria degli ultraprodotti è legata al campo dei numeri reali. Ricordiamo che un *anello unitario commutativo* è una struttura algebrica $(D, +, \cdot, 0, 1)$ tale che:

- 1) $(D, +, 0)$ è un gruppo commutativo
- 2) $(D, \cdot, 1)$ è una operazione associativa e commutativa con 1 come elemento neutro
3. vale la proprietà distributiva cioè

$$(a+b) \cdot c = a \cdot c + b \cdot c$$

In ogni anello unitario commutativo risulta che:

- i) $x \cdot 0 = 0$.
- ii) $x \cdot (-y) = -x \cdot y$.
- iii) $x \cdot (-1)$ è l'opposto di x .
- iv) $(-1)^2 = 1$.

Infatti, per provare i) osserviamo che per la proprietà distributiva $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$ da cui, sottraendo da entrambi i membri $x \cdot 0$, si ricava che $0 \cdot x = 0$. Per provare ii) osserviamo che $x \cdot (-y) + x \cdot y = x \cdot (-y+y) = x \cdot 0 = 0$. Le rimanenti proprietà sono ovvie.

Definizione 10.1. Un anello unitario commutativo $(D, +, \cdot, 0, 1)$ è chiamato *campo* se $(D \setminus \{0\}, \cdot, 1)$ è un gruppo. Chiamiamo *campo ordinato* una struttura $(D, +, \cdot, 0, 1, \leq)$ tale che $(D, +, \cdot, 0, 1)$ sia un campo e \leq una relazione d'ordine totale tale che:

- 1) $a \leq b \Rightarrow a+c \leq b+c$,
- 2) $c \geq 0, a \leq b \Rightarrow ac \leq bc$.

Chiamiamo *positivi* gli elementi maggiori di 0 e *negativi* gli elementi minori di 0.

Proposizione 10.2. In ogni campo ordinato risulta che:

- i) $a \leq b \Rightarrow a-b \leq 0$,
- ii) $a \leq b \Rightarrow 0 \leq b-a$.
- iii) $b \geq 0 \Leftrightarrow -b \leq 0$.
- iv) $c \geq 0, b \geq 0 \Rightarrow b \cdot c \geq 0$
- v) $c \geq 0, a \leq 0 \Rightarrow ac \leq 0$
- vi) $c \leq 0, b \leq 0 \Rightarrow b \cdot c \geq 0$
- v) $1 \geq 0, -1 \leq 0$.

Dim. L'implicazione i) si ottiene ponendo $c = -b$ in 1). La ii) si ottiene ponendo $c = -a$. Se in i) si pone $a = 0$ allora si ottiene $b \geq 0 \Rightarrow -b \leq 0$. Se in ii) si pone $b = 0$ si ottiene $a \leq 0 \Rightarrow 0 \leq -a$. In questo modo la iii) è dimostrata. Le rimanenti proprietà si dimostrano in modo analogo.

La struttura algebrica definita dai razionali è un tipico esempio di campo ordinato.

Definizione 10.3. Un elemento x di un campo ordinato si chiama *infinito positivo* se risulta che $x \geq p \cdot 1$ qualunque sia l'intero p . Chiamiamo *infinito negativo* l'opposto di un infinito positivo. Chiamiamo *infinitesimo positivo (negativo)* un elemento x che sia l'inverso di un elemento infinito positivo (negativo).

Pertanto un elemento positivo di un campo è un infinitesimo positivo se $x \leq 1/p$ per ogni naturale p . Un elemento negativo x è un infinitesimo negativo se $x \geq -1/p$ per ogni naturale p .

Definizione 10.4. Un campo ordinato $(D, +, \cdot, 0, 1, \leq)$ si dice *archimedeo* se non ammette elementi infiniti positivi, cioè se $\forall x \in D \exists p \in \mathbb{N}$ tale che $p \cdot 1 \geq x$.

Da notare che un assioma simile lo abbiamo già visto quando abbiamo definito la classe di grandezze omogenee. Il campo dei numeri razionali ed il campo dei numeri reali risulta essere archimedeo. I campi non archimedei sono molto affascinanti perché in essi è possibile sviluppare una teoria degli infiniti e degli infinitesimi. Ad esempio possiamo dire che due elementi x ed y di un campo ordinato sono *infinitamente vicini* se $x-y$ è un infinitesimo. Per gli infinitesimi e gli infiniti valgono molte proprietà che sono in accordo con la nostra intuizione di infinito ed infinitesimo. Ad esempio la seguente proposizione mette in rilievo che se sottraggo 1 da un elemento infinito positivo allora ottengo ancora un elemento infinito positivo.

Proposizione 10.5. Indichiamo con I^+ l'insieme degli infiniti positivi. Allora

$$x \in I^+ \Rightarrow x-1 \in I^+$$

e pertanto I^+ non ammette minimo.

Dim. Poniamo $x' = x-1$, allora poiché per ogni n vale $(n+1) \cdot 1 \leq x$ risulta che $n \cdot 1 + 1 \leq x$ e quindi che $n \cdot 1 \leq x'$. Pertanto x' è un infinito.

Infine arriviamo alla più importante proprietà dei campi ordinati, la completezza. Nel seguito dati due sottoinsiemi A e B di un insieme ordinato scriveremo $A \leq B$ per indicare che ogni elemento di A è minore di ogni elemento di B . In tale caso si dice anche che A e B sono *separati*. Chiameremo "elemento separatore" della coppia A e B un elemento u tale $A \leq \{u\} \leq B$ cioè un elemento u maggiore di tutti gli elementi di A e minore di tutti gli elementi di B .

Definizione 10.6. Un campo ordinato si dice *completo* se ogni coppia A e B di sottoinsiemi di D tali che $A \leq B$ ammette un elemento separatore.

Come per l'assioma di Archimede abbiamo già considerato la proprietà di completezza nella teoria delle grandezze omogenee sotto il nome di *continuità*. La cosa non deve sorprendere perché la teoria delle grandezze omogenee costituiva appunto un sostituto della teoria dei numeri reali.

Proposizione 10.7. Ogni campo completo è archimedeo.

Dim. Supponiamo che $(D, +, \cdot, 0, 1, \leq)$ sia un campo completo e poniamo

$$A = \{n \cdot 1 : n \in \mathbb{N}\}; B = \{x \in D : x \text{ è infinito positivo}\}.$$

Supponiamo per assurdo che tale campo non sia archimedeo, allora B è non vuoto. Inoltre, per definizione di elemento infinito positivo abbiamo che $A \leq B$. Sia u un elemento separatore di tale coppia di insiemi, allora u in quanto maggiorante di A è un infinito e quindi appartiene a B . Inoltre u , che è anche minorante di B , appartenendo a B è un minimo di B in contrasto con la proposizione 5.

Teorema 10.8. Ogni ultrapotenza del campo ordinato dei numeri reali è un campo ordinato. Esiste una ultrapotenza del campo ordinato dei numeri reali che non è archimedeo e quindi ammette infiniti ed infinitesimi.

Dim. Consideriamo l'insieme R^N delle successioni $(r_n)_{n \in \mathbb{N}}$ di numeri reali e sia \mathcal{F} un ultrafiltro in N che contiene il filtro dei cofiniti. Consideriamo inoltre la successione $(n^2)_{n \in \mathbb{N}}$ ed indichiamo con i la relativa classe di equivalenza $i = [(n^2)_{n \in \mathbb{N}}]$. Allora se m è un qualunque

intero l'insieme $\{n : n^2 < m\}$ è finito e quindi non appartiene ad \mathcal{F} . Ne segue che la formula $i < m$ risulta falsa e quindi che i è un infinito. \square

Ogni ultrapotenza del campo dei numeri reali che non sia archimedea viene detta anche *modello non standard dell'analisi*. Il motivo di tale nomenclatura è che è possibile fondare tutta l'analisi matematica utilizzando infiniti ed infinitesimi. Se ci riferiamo

Si ricordi che il campo dei numeri reali si può caratterizzare come un campo che sia completo ed archimedeo. La nozione "essere completo" non è del primo ordine perché si riferisce ai sottoinsiemi di R e non agli elementi di R . Si pone allora il problema se sia possibile trovare un sistema di assiomi del primo ordine capace di caratterizzare tale campo. La risposta è negativa.

Corollario 10.9. Non è possibile assiomatizzare nella logica del primo ordine il campo ordinato dei numeri reali.

Dim. Se esistesse un sistema T di assiomi del primo ordine avente come unico modello (a meno di isomorfismi) il campo dei numeri reali allora ogni ultrapotenza di R , essendo un modello di T , dovrebbe essere isomorfa a T . Poiché sappiamo che esiste una ultrapotenza che è un campo non archimedeo, ciò è assurdo. \square