

Elementi di Algebra Universale

Uno degli obiettivi dell'algebra universale è quello di individuare ed estrarre, laddove possibile, gli elementi comuni a molte strutture algebriche anche apparentemente molto diverse tra loro. In quest'ottica si scoprono concetti generali, costruzioni e risultati che, oltre a generalizzare ed unificare situazioni particolari già note consentendone una presentazione più agevole, possono essere applicati a situazioni completamente nuove, essendo ad un livello di astrazione più elevato, fornendo informazioni significative e nuove direzioni di sviluppo.

Nel presente capitolo descriveremo alcuni di questi concetti e le loro interrelazioni. Di primaria importanza è il concetto di algebra; incentrando la trattazione su di esso, discuteremo le nozioni isomorfismo, sottoalgebra, congruenza, algebra quoziente, omomorfismo, prodotto diretto, prodotto sottodiretto, termine, identità ed algebra libera.

1 Definizioni ed esempi di algebre.

La definizione di algebra che daremo di seguito comprende la maggior parte delle più note strutture algebriche, come vedremo, oltre a numerose altre strutture, meno note, che sono recentemente oggetto di ricerca. Sebbene diversi matematici - come Whitehead nel 1898 e, più tardi, Noether - avessero ravvisato la necessità di una tale definizione, il merito di averla formulata è da attribuirsi a Birkhoff (1933). Si potrebbe osservare che recenti ricerche hanno rivelato che la nozione di algebra data originariamente da Birkhoff potrebbe essere estesa in maniera proficua fino a comprendere, ad esempio, le algebre parziali e le algebre eterogenee. Tuttavia tali strutture esulano dai nostri obiettivi.

Definizione 1.1. Sia A un insieme non vuoto e sia n un intero non negativo. Poniamo $A^0 = \{\emptyset\}$ e, per $n \geq 0$, $A^n = \{(x_1, \dots, x_n) \mid x_i \in A, \forall i = 1, \dots, n\}$. Una *operazione* (o *funzione*) n -aria su A è una qualunque funzione f di A^n a valori in A . L'intero n si dice *arità* (o *rango*) di f .

Un'operazione *finitaria* è un'operazione n -aria, per qualche n . L'immagine di (a_1, \dots, a_n) mediante un'operazione n -aria f si denota con $f(a_1, \dots, a_n)$. Un'operazione f su A si dice un'operazione *nullaria* (o una *costante*) se la sua arità è zero. Essa è individuata univocamente dall'immagine $f(\emptyset)$ in A dell'unico elemento di A^0 ed è pertanto conveniente identificare l'operazione stessa con l'elemento $f(\emptyset)$. Quindi un'operazione nullaria è pensata come un elemento di A .

Infine un'operazione si dice *unaria*, *binaria* o *ternaria* se il suo rango è, rispettivamente, 1, 2 o 3.

Definizione 1.2. Un *linguaggio* (o *tipo*) di algebre è un insieme \mathcal{F} di *simboli funzionali* tale che un intero non negativo n sia assegnato ad ogni elemento f di \mathcal{F} . Tale intero è chiamato *arietà* (o *rango*) di f , ed f si dice un *simbolo funzionale n -ario*. Il sottoinsieme di \mathcal{F} costituito dai simboli funzionali n -ari s'indica con \mathcal{F}_n .

Definizione 1.3. Sia \mathcal{F} un linguaggio di algebre. Un'*algebra \mathbf{A} di tipo \mathcal{F}* è una coppia del tipo (A, F) , dove A è un insieme non vuoto, ed F una famiglia di operazioni finitarie su A indicizzate mediante il linguaggio \mathcal{F} in modo tale che, ad ogni simbolo funzionale n -ario $f \in \mathcal{F}$, corrisponda un'operazione n -aria $f^{\mathbf{A}}$ su A . L'insieme A si dice l'*universo* (o il *sostegno*) di $\mathbf{A} = (A, F)$, e le operazioni $f^{\mathbf{A}}$ si dicono *operazioni fondamentali di \mathbf{A}* (spesso scriveremo f in luogo di $f^{\mathbf{A}}$).

Se \mathcal{F} è finito, diciamo $\mathcal{F} = \{f_1, \dots, f_k\}$, spesso scriveremo (A, f_1, \dots, f_k) invece di (A, F) , adottando - in genere - la convenzione seguente:

$$\text{arity}f_1 \geq \text{arity}f_2 \geq \dots \geq \text{arity}f_k.$$

Un'algebra \mathbf{A} è *unaria* se ogni sua operazione è unaria, ed è *mono-unaria* se è dotata di una sola operazione e tale operazione è unaria. \mathbf{A} è un *gruppoide* se ha una sola operazione binaria (solitamente denotata con $+ o \cdot$); in tal caso indicheremo con $a+b$ o $a \cdot b$ (o semplicemente ab) l'immagine della coppia (a, b) tramite quest'operazione, e chiameremo tale immagine - rispettivamente - *somma* o *prodotto* di a e b .

Un'algebra \mathbf{A} si dice *finita* se A è un insieme finito, e si dice *banale* se $|A| = 1$.

Vale la pena osservare che le algebre più conosciute e studiate non hanno operazioni di arità maggiore di due.

Presenteremo ora alcuni esempi di algebre. Alcune di esse sono probabilmente meno note, ma di grande attualità nell'ambito della ricerca. In particolare cercheremo di evidenziare il ruolo svolto da alcuni orientamenti della logica moderna che hanno l'obiettivo di fornire modelli algebrici per

certi sistemi logici. Il lettore noterà che tutti i diversi tipi di algebre che elencheremo si distinguono tra loro attraverso le operazioni fondamentali e le identità che soddisfano. Uno dei primi successi di Birkhoff fu proprio quello di chiarire il ruolo delle identità.

ESEMPLI.

1. GRUPPI.

Un *gruppo* \mathbf{G} è un'algebra $(G, \cdot, ^{-1}, 1)$ con un'operazione binaria, una unaria ed una nullaria, tali che siano soddisfatte le seguenti identità:

$$(G1): x \cdot (y \cdot z) \approx (x \cdot y) \cdot z;$$

$$(G2): x \cdot 1 \approx 1 \cdot x \approx x;$$

$$(G3): x \cdot x^{-1} \approx x^{-1} \cdot x \approx 1.$$

Un gruppo \mathbf{G} si dice *abeliano* (o *commutativo*) se vale la seguente identità:

$$(G4): x \cdot y \approx y \cdot x.$$

Quello di gruppo fu uno dei primi concetti studiati in algebra (i gruppi di sostituzioni apparvero circa duecento anni fa). La definizione qui proposta non è quella riportata nei testi di teoria dei gruppi; essi, infatti, usano una sola operazione (binaria) ed assiomi contenenti i quantificatori. Il motivo di questa scelta sarà chiarito nel paragrafo 2.

Il concetto di gruppo si generalizza a quelli di semigruppato e di monoide in una direzione e a quelli di quasigruppato e ciclo in un'altra.

2. SEMIGRUPPI E MONOIDI.

Un *semigruppato* è un'algebra (G, \cdot) che soddisfa l'identità (G1). Esso si dice *abeliano* (o *commutativo*) se vale la (G4). Un *monoide* è un'algebra $(M, \cdot, 1)$ con un'operazione binaria ed una nullaria soddisfacenti (G1) e (G2).

3. QUASIGRUPPI E CICLI.

Un *quasigruppato* è un'algebra $(Q, /, \cdot, \backslash)$ con tre operazioni binarie soddisfacenti le seguenti identità:

$$(Q1): x \backslash (x \cdot y) \approx y; (x \cdot y) / y \approx x;$$

$$(Q2): x \cdot (x \backslash y) \approx y; (x / y) \cdot y \approx x.$$

Un *ciclo* è un quasigruppo unitario, cioè un'algebra $(Q, /, \cdot, \backslash, 1)$ che soddisfa (Q1), (Q2) e (G2).

4. ANELLI.

Un *anello* è un'algebra $(R, +, \cdot, -, 0)$, dove $+$ e \cdot sono operazioni binarie, $-$ è unaria e 0 ed 1 sono costanti, soddisfacente le seguenti condizioni:

(R1): $(R, +, -, 0)$ è un gruppo abeliano;

(R2): (R, \cdot) è un semigruppo;

(R3): $x \cdot (y + z) \approx (x \cdot y) + (x \cdot z)$; $(x + y) \cdot z \approx (x \cdot z) + (y \cdot z)$.

Un *anello unitario* è un'algebra $(R, +, \cdot, -, 0, 1)$ che soddisfa le (R1)-(R3) e la (G2).

5. MODULI SU UN ANELLO.

Sia \mathbf{R} un anello. Un \mathbf{R} -modulo (*sinistro*) è una struttura algebrica $(M, +, -, 0, (f_r)_{r \in R})$, dove $+$ è un'operazione binaria, $-$ è unaria, 0 è nullaria ed f_r è unaria per ogni $r \in R$, soddisfacente le seguenti condizioni:

(M1): $(M, +, -, 0)$ è un gruppo abeliano;

(M2): $f_r(x + y) \approx f_r(x) + f_r(y)$ per ogni $r \in R$;

(M3): $f_{r+s}(x) \approx f_r(x) + f_s(x)$ per ogni $r, s \in R$;

(M4): $f_r(f_s(x)) \approx f_{rs}(x)$ per ogni $r, s \in R$.

Sia \mathbf{R} un anello unitario. Un \mathbf{R} -modulo *unitario* è un modulo che soddisfa, oltre alle (M1)-(M4), anche la

(M5): $f_1(x) \approx x$.

Gli \mathbf{R} -moduli *destri* si definiscono in maniera del tutto analoga agli \mathbf{R} -moduli sinistri (la (M4) diventa: $f_r(f_s(x)) \approx f_{sr}(x)$).

6. ALGEBRE SU UN ANELLO.

Sia \mathbf{R} un anello unitario. Un'algebra *su* \mathbf{R} è una struttura algebrica $(A, +, \cdot, -, 0, (f_r)_{r \in R})$ tale che valgano le seguenti condizioni:

(A1): $(A, +, -, 0, (f_r)_{r \in R})$ è un \mathbf{R} -modulo unitario;

(A2): $(A, +, \cdot, -, 0)$ è un anello;

(A3): $f_r(x \cdot y) \approx (f_r(x)) \cdot y \approx x \cdot f_r(y)$ per $r \in R$.

7. SEMIRETICOLI.

Un *semireticolo* è un semigruppò (S, \cdot) che soddisfa la proprietà commutativa (G4) e quella d'idempotenza:

$$(S1): x \cdot x \approx x.$$

8. RETICOLI.

Un *reticolo* è un'algebra (L, \vee, \wedge) con due operazioni binarie che soddisfano le seguenti proprietà:

(L1): proprietà commutative

$$\text{a) } x \vee y \approx y \vee x,$$

$$\text{b) } x \wedge y \approx y \wedge x;$$

(L2): proprietà associative

$$\text{a) } x \vee (y \vee z) \approx (x \vee y) \vee z,$$

$$\text{b) } x \wedge (y \wedge z) \approx (x \wedge y) \wedge z;$$

(L3): leggi d'idempotenza

$$\text{a) } x \vee x \approx x,$$

$$\text{b) } x \wedge x \approx x;$$

(L4): leggi d'assorbimento

$$\text{a) } x \approx x \vee (x \wedge y),$$

$$\text{b) } x \approx x \wedge (x \vee y).$$

9. RETICOLI LIMITATI.

Un'algebra $(L, \vee, \wedge, 0, 1)$ con due operazioni binarie e due nullarie è un *reticolo limitato* se soddisfa le due seguenti condizioni:

(BL1): (L, \vee, \wedge) è un reticolo;

(BL2): $x \vee 1 \approx 1, \quad x \wedge 0 \approx 0.$

10. ALGEBRE DI BOOLE.

Un'algebra booleana (o algebra di Boole) è un'algebra $(B, \vee, \wedge, ', 0, 1)$ con due operazioni binarie, una unaria e due nullarie soddisfacenti le seguenti condizioni:

(B1): (B, \vee, \wedge) è un reticolo distributivo (ovvero un reticolo in cui ciascuna delle operazioni \vee e \wedge sia distributiva rispetto all'altra);

(B2): $x \wedge 0 \approx 0, \quad x \vee 1 \approx 1;$

$$(B3): x \wedge x' \approx 0, \quad x \vee x' \approx 1.$$

11. ALGEBRE DI HEYTING.

Un'algebra $(H, \vee, \wedge, \rightarrow, 0, 1)$ con tre operazioni binarie e due costanti, è un'algebra di Heyting se soddisfa le condizioni:

(H1): (H, \vee, \wedge) è un reticolo distributivo;

(H2): $x \wedge 0 \approx 0, \quad x \vee 1 \approx 1$;

(H3): $x \rightarrow x \approx 1$;

(H4): $(x \rightarrow y) \wedge y \approx y, \quad x \wedge (x \rightarrow y) \approx x \wedge y$;

(H5): $x \rightarrow (y \wedge z) \approx (x \rightarrow y) \wedge (x \rightarrow z), \quad (x \vee y) \rightarrow z \approx (x \rightarrow z) \wedge (y \rightarrow z)$.

Le algebre di Heyting furono introdotte da Birkhoff con il nome di *algebre brouweriane*, con la notazione “ $y : x$ ” invece di “ $x \rightarrow y$ ”.

12. ALGEBRE DI POST AD n VALORI.

Un'algebra $(A, \vee, \wedge, ', 0, 1)$ con due operazioni binarie, una unaria e due nullarie, è un'algebra di Post ad n valori se soddisfa ogni identità soddisfatta dall'algebra

$$\mathbf{P}_n = (\{0, 1, \dots, n-1\}, \vee, \wedge, ', 0, 1)$$

dove $(\{0, 1, \dots, n-1\}, \vee, \wedge, 0, 1)$ è una catena limitata, con $0 < n-1 < n-2 < \dots < 2 < 1$ e $1' = 2, 2' = 3, \dots, (n-2)' = n-1, (n-1)' = 0$, e $0' = 1$.

13. ALGEBRE CILINDRICHE DI DIMENSIONE n .

Sia n un numero naturale. Una struttura algebrica

$$(A, \vee, \wedge, ', c_0, \dots, c_{n-1}, 0, 1, d_{00}, \dots, d_{0(n-1)}, \dots, d_{(n-1)0}, \dots, d_{(n-1)(n-1)})$$

con due operazioni binarie, $n+1$ unarie e n^2+2 costanti, è un'algebra ciclica di dimensione n se soddisfa le seguenti condizioni, dove $0 \leq i, j, k < n$:

(C1): $(A, \vee, \wedge, ', 0, 1)$ è un'algebra di Boole;

(C2): $c_i 0 \approx 0$;

(C3): $x \leq c_i x$;

(C4): $c_i(x \wedge c_i y) \approx (c_i x) \wedge (c_i y)$;

(C5): $c_i c_j x \approx c_j c_i x$;

(C6): $d_{ii} \approx 1$;

(C7): $d_{ik} \approx c_j(d_{ij} \wedge d_{jk})$ se $i \neq j \neq k$;

(C8): $c_i(d_{ij} \wedge x) \wedge c_i(d_{ij} \wedge x') \approx 0$ se $i \neq j$.

Le algebre cilindriche furono introdotte da Tarski e Thompson con lo scopo di fornire una versione algebrica della logica dei predicati.

14. ORTORETICOLI.

Un'algebra $(L, \vee, \wedge, ', 0, 1)$ con due operazioni binarie, una unaria e due costanti, è un *ortoreticolo* se soddisfa le seguenti condizioni:

(Q1): $(L, \vee, \wedge, 0, 1)$ è un reticolo limitato;

(Q2): $x \wedge x' \approx 0, x \vee x' \approx 1$;

(Q3): $(x \wedge y)' \approx x' \vee y', (x \vee y)' \approx x' \wedge y'$;

(Q4): $(x')' \approx x$.

Un *reticolo ortomodulare* è un ortoreticolo che soddisfa la

(Q5): $x \leq y \rightarrow x \vee (x' \wedge y) \approx y$.

2 Algebre isomorfe. Sottoalgebre.

I concetti d'isomorfismo in teoria dei gruppi, teoria degli anelli e teoria dei reticoli sono casi particolari della nozione d'isomorfismo tra algebre.

Definizione 2.1. Siano \mathbf{A} e \mathbf{B} due algebre dello stesso tipo \mathcal{F} . Una funzione $\alpha : A \rightarrow B$ è un *isomorfismo* tra \mathbf{A} e \mathbf{B} se α è biettiva e, per ogni simbolo funzionale n -ario $f \in \mathcal{F}$, si ha

$$(1) \quad \alpha f^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n).$$

Diremo che \mathbf{A} è isomorfa a \mathbf{B} , e scriveremo $\mathbf{A} \cong \mathbf{B}$, se esiste un isomorfismo tra \mathbf{A} e \mathbf{B} .

L'Algebra è spesso considerata come lo studio di quelle proprietà delle strutture algebriche che sono invarianti per isomorfismi. Tali proprietà delle algebre si dicono, appunto, *proprietà algebriche*. Pertanto, in quest'ambito, strutture isomorfe possono essere trattate come se fossero lo stesso oggetto. Per questi motivi si usa spesso dire che due strutture "sono uguali a meno d'isomorfismi".

Esistono diversi metodi per costruire nuove algebre a partire da strutture date. Tre dei più importanti sono: la costruzione delle sottoalgebre, le immagini omomorfe e i prodotti diretti. Nei successivi paragrafi ci occuperemo di tali costruzioni.

Definizione 2.2. Siano \mathbf{A} e \mathbf{B} due algebre dello stesso tipo. Diremo allora che \mathbf{B} è una *sottoalgebra* di \mathbf{A} se $B \subseteq A$ e ciascuna delle operazioni di \mathbf{B} è la restrizione della corrispondente operazione di \mathbf{A} , cioè, per ogni simbolo funzionale f , $f^{\mathbf{B}}$ è $f^{\mathbf{A}}$ ristretto a B . Se \mathbf{B} è una sottoalgebra di \mathbf{A} , scriveremo $\mathbf{B} \leq \mathbf{A}$. Un *sottouniverso* di \mathbf{A} è un sottoinsieme B di A chiuso rispetto alle operazioni fondamentali di \mathbf{A} , cioè, se f è un'operazione n -aria fondamentale di \mathbf{A} ed $a_1, \dots, a_n \in B$, allora deve risultare $f(a_1, \dots, a_n) \in B$.

Dunque se \mathbf{B} è una sottoalgebra di \mathbf{A} , allora B è un sottouniverso di \mathbf{A} . Osserviamo che l'insieme vuoto può essere un sottouniverso ma non è il sostegno di alcuna sottoalgebra. Se \mathbf{A} ha delle costanti, allora esse devono appartenere ad ogni suo sottouniverso.

La scelta delle operazioni fondamentali negli esempi del paragrafo precedente è motivata proprio dalla definizione di sottoalgebra che abbiamo dato. Ad esempio, secondo la definizione, una sottoalgebra di un gruppo è ancora un gruppo. Se avessimo considerato un gruppo \mathbf{G} come un'algebra (G, \cdot) dotata della sola consueta operazione binaria, le sue sottoalgebre sarebbero state tutti i suoi sottosemigruppi, in quanto sottoinsiemi chiusi rispetto all'unica operazione fondamentale di \mathbf{G} . In altre parole tale definizione ci assicura che una struttura algebrica e le sue sottostrutture sono sempre algebre dello stesso tipo.

Definizione 2.3. Siano \mathbf{A} e \mathbf{B} algebre dello stesso tipo. Una funzione $\alpha : A \rightarrow B$ è un'*immersione* (o un *monomorfismo*) se α è iniettiva e soddisfa la (1). Per ragioni di brevità diremo talvolta che $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ è un'immersione. Diremo inoltre che \mathbf{A} è *immergibile* in \mathbf{B} se esiste un'immersione di \mathbf{A} in \mathbf{B} .

Teorema 2.4. Se $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ è un'immersione, allora $\alpha(A)$ è un sottouniverso di \mathbf{B} .

Dimostrazione. Sia dunque $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un'immersione. Allora, per ogni simbolo funzionale n -ario f ed $a_1, \dots, a_n \in A$,

$$f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n) = \alpha f^{\mathbf{A}}(a_1, \dots, a_n) \in \alpha(A).$$

Ne segue l'asserto. □

Se $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ è un'immersione, indicheremo con $\alpha(\mathbf{A})$ la sottoalgebra di \mathbf{B} il cui sostegno è $\alpha(A)$.

Un problema d'interesse generale per gli algebristi può essere formulato come segue.

Sia K una classe di algebre e sia K_1 una sottoclasse propria di K . Due questioni basilari sorgono nella ricerca di teoremi di struttura.

- (1) Ogni elemento di K è isomorfo a qualche elemento di K_1 ?
- (2) Ogni elemento di K è immergibile in qualche elemento di K_1 ?

Ad esempio, ogni algebra di Boole è isomorfa ad un'algebra d'insiemi, ogni gruppo è isomorfo ad un gruppo di permutazioni, un gruppo abeliano finito è isomorfo ad un prodotto diretto di gruppi ciclici, e un reticolo distributivo finito può essere immerso in una potenza del reticolo distributivo a due elementi.

3 Reticoli algebrici e sottouniversi.

Definizione 3.1. Data un'algebra \mathbf{A} definiamo, per ogni $X \subseteq A$,

$$\text{Sg}(X) = \bigcap \{B : X \subseteq B \text{ e } B \text{ è un sottouniverso di } \mathbf{A}\}.$$

Diremo che $\text{Sg}(X)$ è il *sottouniverso generato da X* .

Teorema 3.2. Per ogni algebra \mathbf{A} , Sg è un operatore di chiusura algebrica su A .

Dimostrazione. Osserviamo innanzitutto che l'intersezione di sottouniversi di \mathbf{A} è ancora un sottouniverso di \mathbf{A} , per cui Sg è un operatore di chiusura su A i cui insiemi chiusi sono esattamente i sottouniversi di A . Ora, per ogni $X \subseteq A$, definiamo

$$E(X) = X \cup \{f(a_1, \dots, a_n) : f \text{ è un'operazione } n\text{-aria fondamentale su } A \text{ e } a_1, \dots, a_n \in X\}.$$

Definiamo poi, per ogni $n \in \mathbb{N}_0$, $E^n(X)$ come segue:

$$\begin{aligned} E^0(X) &= X \\ E^{n+1}(X) &= E(E^n(X)). \end{aligned}$$

Poiché tutte le operazioni fondamentali su A sono finitarie e

$$X \subseteq E(X) \subseteq E^2(X) \subseteq \dots$$

si può dimostrare facilmente che

$$\text{Sg}(X) = X \cup E(X) \cup E^2(X) \cup \dots,$$

e da ciò segue che, se $a \in \text{Sg}(X)$, allora $a \in E^n(X)$ per qualche $n \in \mathbb{N}_0$. Pertanto per qualche $Y \subseteq X$, Y finito, $a \in E^n(Y)$, e quindi $a \in \text{Sg}(Y)$. Ma ciò significa che Sg è un operatore di chiusura algebrica, che è quanto volevamo dimostrare. \square

Corollario 3.3. *Se \mathbf{A} è un'algebra, allora \mathbf{L}_{Sg} , il reticolo dei sottouniversi di \mathbf{A} , è un reticolo algebrico.*

Il corollario precedente afferma che i sottouniversi di \mathbf{A} , parzialmente ordinati mediante la relazione d'inclusione, costituiscono un reticolo algebrico.

Definizione 3.4. Data un'algebra \mathbf{A} , indicheremo con $\text{Sub}(\mathbf{A})$ l'insieme dei sottouniversi di \mathbf{A} e con $\mathbf{Sub}(\mathbf{A})$ il corrispondente reticolo algebrico, il *reticolo dei sottouniversi di \mathbf{A}* . Per $X \subseteq A$ diremo che X genera \mathbf{A} (o che \mathbf{A} è generato da X , o - ancora - che X è un sistema di generatori di \mathbf{A}) se $\text{Sg}(X) = A$. L'algebra \mathbf{A} si dice *finitamente generata* se ha un insieme finito di generatori.

Teorema 3.5. (Birkhoff - Frink). *Se \mathbf{L} è un reticolo algebrico, allora $\mathbf{L} \cong \mathbf{Sub}(\mathbf{A})$, per qualche algebra \mathbf{A} .*

Dimostrazione. Sia C un operatore di chiusura algebrica su un insieme A tale che $\mathbf{L} \cong \mathbf{L}_C$. Per ogni sottoinsieme finito B di A , e per ogni $b \in C(B)$, definiamo una funzione n -aria $f_{B,b}$ su A , dove $n = |B|$, come segue:

$$f_{B,b}(a_1, \dots, a_n) = \begin{cases} b & \text{se } B = \{a_1, \dots, a_n\} \\ a_1 & \text{altrimenti} \end{cases},$$

ed indichiamo con \mathbf{A} l'algebra risultante. Allora ovviamente

$$\text{Sg}(X) \subseteq C(X).$$

D'altra parte

$$C(X) = \bigcup \{C(B) : B \subseteq X, B \text{ finito}\}$$

e, per B finito,

$$C(B) = \{f_{B,b}(a_1, \dots, a_n) : B = \{a_1, \dots, a_n\}, b \in C(B)\}$$

$$\begin{aligned} &\subseteq \text{Sg}(B) \\ &\subseteq \text{Sg}(X) \end{aligned}$$

implica

$$C(X) \subseteq \text{Sg}(X);$$

e quindi

$$C(X) = \text{Sg}(X).$$

Pertanto $\mathbf{L}_C = \mathbf{Sub}(\mathbf{A})$, da cui segue l'asserto: $\mathbf{Sub}(\mathbf{A}) \cong \mathbf{L}$. □

Il seguente risultato di teoria degli insiemi è utile per giustificare certe costruzioni in algebra universale. In particolare esso prova che non possono esistere “troppe” algebre (a meno d'isomorfismi) di un dato tipo, generate da insiemi non più grandi di una data cardinalità. Ricordiamo che ω è il più piccolo cardinale infinito.

Corollario 3.6. *Se \mathbf{A} è un'algebra e $X \subseteq A$, allora $|\text{Sg}(X)| \leq |X| + |\mathcal{F}| + \omega$.*

Dimostrazione. Procedendo per induzione su n , si ha $|E^n(X)| \leq |X| + |\mathcal{F}| + \omega$, e quindi la tesi segue dalla dimostrazione del Teorema 3.2. □

4 Il Teorema della base irridondante.

Negli spazi vettoriali finitamente generati, tutti i sistemi di generatori minimali hanno la stessa cardinalità, detta la dimensione dello spazio. Tuttavia quella di avere una dimensione è una caratteristica piuttosto rara tra le strutture algebriche. Ad esempio il gruppo abeliano \mathbf{Z}_6 ammette sia $\{1\}$ che $\{2, 3\}$ come sistemi di generatori.

Definizione 4.1. Sia C un operatore di chiusura su A . Per $n < \omega$, sia C_n la funzione definita su $\mathcal{P}(A)$ da

$$C_n(X) = \bigcup \{C(Y) : Y \subseteq X, |Y| \leq n\}.$$

Diremo che C è *n-ario* se

$$C(X) = C_n(X) \cup C_n^2(X) \cup \dots,$$

dove

$$\begin{aligned} C_n^1 &= C_n(X), \\ C_n^{k+1}(X) &= C_n(C_n^k(X)). \end{aligned}$$

Lemma 4.2. *Sia \mathbf{A} un'algebra le cui operazioni fondamentali abbiano arità $\leq n$. Allora Sg è un operatore di chiusura n -ario su A .*

Dimostrazione. Consideriamo l'operatore E introdotto nella dimostrazione del Teorema 3.2, ed osserviamo che

$$E(X) \subseteq (\text{Sg})_n(X) \subseteq \text{Sg}(X);$$

per cui

$$\begin{aligned} \text{Sg}(X) &= X \cup E(X) \cup E^2(X) \cup \dots \\ &\subseteq (\text{Sg})_n(X) \cup (\text{Sg})_n^2(X) \cup \dots \\ &\subseteq \text{Sg}(X), \end{aligned}$$

e quindi

$$\text{Sg}(X) = (\text{Sg})_n(X) \cup (\text{Sg})_n^2(X) \cup \dots$$

□

Definizione 4.3. Sia C un operatore di chiusura su S . Un insieme di generatori minimale di S si dice una *base irridondante*. Definiamo inoltre

$$\text{IrB}(C) = \{n < \omega : S \text{ ha una base irridondante di ordine } n\}.$$

Teorema 4.4. (Tarski). *Se C è un operatore di chiusura n -ario su S , con $n \geq 2$, e se $i < j$ con $i, j \in \text{IrB}(C)$ tali che*

$$(2) \quad \{i + 1, \dots, j - 1\} \cap \text{IrB}(C) = \emptyset,$$

allora $j - i \leq n - 1$. In particolare, se $n = 2$ allora $\text{IrB}(C)$ è un sottoinsieme convesso di ω , cioè una sequenza di numeri consecutivi.

Dimostrazione. Sia B una base irridondante di ordine j e sia K l'insieme delle basi irridondanti di ordine $\leq i$:

$$K = \{A : A \text{ è base irridondante, } |A| \leq i\}.$$

L'idea della dimostrazione è semplice. Penseremo a B come al "centro" di S e misureremo la distanza degli elementi di K da B usando gli "anelli" $C_n^{k+1}(B) - C_n^k(B)$. Vogliamo scegliere una base A_0 in K che sia quanto più possibile "vicina" a B , e tale che l'ultimo anello contenente elementi di A_0 , ne contenga il minor numero possibile. Sceglieremo uno di questi elementi a_0 e lo sostituiremo con n - o meno - elementi più vicini b_1, \dots, b_m per ottenere un nuovo insieme di generatori A_1 , con $|A_1| < i + n$. Allora A_1 contiene una

base irridondante A_2 . Per la condizione di “distanza minimale” su A_0 , si ha che $A_2 \notin K$, da cui $|A_2| > i$, e quindi $|A_2| \geq j$ per la (2). Pertanto $j < i + n$.

Ora, in dettaglio, scegliamo $A_0 \in K$ tale che

$$A_0 \not\subseteq C_n^k(B) \quad \text{implichi} \quad A \not\subseteq C_n^k(B)$$

per $A \in K$. Sia t tale che

$$A_0 \subseteq C_n^{t+1}(B), \quad A_0 \not\subseteq C_n^t(B).$$

Possiamo assumere che

$$|A_0 \cap (C_n^{t+1}(B) - C_n^t(B))| \leq |A \cap (C_n^{t+1}(B) - C_n^t(B))|$$

per ogni $A \in K$ con $A \subseteq C_n^{t+1}(B)$. Scegliamo

$$a_0 \in [C_n^{t+1}(B) - C_n^t(B)] \cap A_0.$$

Allora devono esistere $b_1, \dots, b_m \in C_n^t(B)$, per qualche $m \leq n$, con

$$a_0 \in C_n(\{b_1, \dots, b_m\}),$$

quindi

$$A_0 \subseteq C_n(A_1),$$

dove $A_1 = (A_0 - \{a_0\}) \cup \{b_1, \dots, b_m\}$.

Pertanto $C(A_0) \subseteq C(A_1)$, il che significa che A_1 è un insieme di generatori di S . Di conseguenza esiste una base irridondante $A_2 \subseteq A_1$, e si ha: $|A_2| < |A_0| + n$. Se $|A_0| + n \leq j$, l'esistenza di A_2 è in contraddizione con la scelta di A_0 perché in tal caso avremmo

$$A_2 \in K, \quad A_2 \subseteq C_n^{t+1}(B)$$

e

$$|A_2 \cap (C_n^{t+1}(B) - C_n^t(B))| < |A_0 \cap (C_n^{t+1}(B) - C_n^t(B))|.$$

Allora $|A_0| + n > j$ e, essendo $|A_0| \leq i$, abbiamo $j - i < n$. □

Se \mathbf{A} è un'algebra in cui tutte le operazioni fondamentali hanno arità ≤ 2 , allora $\text{IrB}(\text{Sg})$ è un insieme convesso. Questo si applica a tutti gli esempi presentati nel paragrafo 1.

5 Congruenze ed algebre quozienti.

I concetti di congruenza, algebra quoziente ed omomorfismo sono strettamente correlati tra loro. Ci occuperemo di tali concetti in questo paragrafo e nel successivo.

I sottogruppi normali, introdotti da Galois all'inizio del diciannovesimo secolo, giocano un ruolo fondamentale nella definizione dei gruppi quoziente e nei cosiddetti teoremi di omomorfismo e di isomorfismo che sono importantissimi nello studio della teoria dei gruppi. Analogamente gli ideali, introdotti da Dedekind nella seconda metà dello stesso secolo, sono fondamentali per la definizione degli anelli quoziente e per i corrispondenti teoremi di omomorfismo e di isomorfismo nella teoria degli anelli. È quindi naturale che i matematici, partendo dall'osservazione di situazioni analoghe come queste, abbiano cercato di definire tali concetti in maniera più generale.

Definizione 5.1. Sia \mathbf{A} un'algebra di tipo \mathcal{F} e sia $\theta \in \text{Eq}(A)$, dove $\text{Eq}(A)$ è l'insieme di tutte le relazioni d'equivalenza su A . Allora θ è una *congruenza* su \mathbf{A} se soddisfa la seguente *proprietà di compatibilità*:

(CP): Per ogni simbolo funzionale n -ario $f \in \mathcal{F}$, e qualunque siano $a_i, b_i \in A$, $i = 1, \dots, n$, tali che $a_i \theta b_i$, si ha

$$f^{\mathbf{A}}(a_1, \dots, a_n) \theta f^{\mathbf{A}}(b_1, \dots, b_n).$$

La proprietà di compatibilità è una condizione necessaria per l'introduzione di una struttura algebrica indotta da \mathbf{A} sull'insieme delle classi d'equivalenza A/θ .

Definizione 5.2. Indichiamo con $\text{Con } \mathbf{A}$ l'insieme di tutte le congruenze sull'algebra \mathbf{A} , e sia $\theta \in \text{Con } \mathbf{A}$. Allora l'*algebra quoziente di \mathbf{A} rispetto a θ* , che indicheremo con \mathbf{A}/θ , è l'algebra il cui sostegno è A/θ e le cui operazioni soddisfano la seguente identità:

$$f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta) = f^{\mathbf{A}}(a_1, \dots, a_n)/\theta,$$

dove $a_1, \dots, a_n \in A$ ed f è un simbolo funzionale n -ario in \mathcal{F} .

Ovviamente le algebre quozienti di \mathbf{A} sono dello stesso tipo di \mathbf{A} .

Riprenderemo lo studio delle algebre quozienti nel prossimo paragrafo. Ora, invece, analizzeremo la struttura reticolare di $\text{Con } \mathbf{A}$.

Teorema 5.3. $(\text{Con } \mathbf{A}, \subseteq)$ è un sottoreticolo completo di $(\text{Eq}(A), \subseteq)$, il reticolo delle relazioni d'equivalenza su A .

Dimostrazione. La verifica del fatto che $\text{Con } \mathbf{A}$ è chiuso rispetto all'intersezione è immediata. Per verificare la stabilità rispetto all'unione, consideriamo una famiglia $\{\theta_i\}_{i \in I}$ di elementi di $\text{Con } \mathbf{A}$. Allora, se f è un'operazione fondamentale n -aria di \mathbf{A} e

$$(a_1, b_1), \dots, (a_n, b_n) \in \bigvee_{i \in I} \theta_i,$$

dove \bigvee è l'unione in $\text{Eq}(A)$, allora segue da una proprietà dei reticoli l'esistenza di $k + 1$ indici $i_0, \dots, i_k \in I$ tali che

$$(a_i, b_i) \in \theta_{i_0} \circ \dots \circ \theta_{i_k}, \quad 0 \leq i \leq n.$$

Da ciò segue semplicemente

$$(f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta_{i_0} \circ \dots \circ \theta_{i_k}.$$

Pertanto $\bigvee_{i \in I} \theta_i$ è una congruenza in \mathbf{A} , e l'asserto è provato. \square

Definizione 5.4. Il reticolo delle congruenze di \mathbf{A} , che indicheremo con $\text{Con } \mathbf{A}$, è l'algebra che ha come sostegno $\text{Con } \mathbf{A}$ ed è dotata delle operazioni di unione ed intersezione indotte dal reticolo delle relazioni d'equivalenza.

Il teorema seguente fornisce una caratterizzazione astratta dei reticoli delle congruenze sulle strutture algebriche.

Teorema 5.5. Sia \mathbf{A} un'algebra. Allora esiste un operatore di chiusura algebrica Θ su $A \times A$ tale che i sottoinsiemi chiusi di $A \times A$ sono esattamente le congruenze su \mathbf{A} . Pertanto $\text{Con } \mathbf{A}$ è un reticolo algebrico.

Dimostrazione. Innanzitutto definiamo un'appropriata struttura algebrica su $A \times A$. Per ogni simbolo funzionale n -ario f nel linguaggio di \mathbf{A} , definiamo una corrispondente funzione n -aria f su $A \times A$ come segue:

$$f((a_1, b_1), \dots, (a_n, b_n)) = (f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)).$$

Ora aggiungiamo le costanti (a, a) per ogni $a \in A$, un'operazione unaria s definita come

$$s((a, b)) = (b, a),$$

e un'operazione binaria t definita come segue:

$$t((a, b), (c, d)) = \begin{cases} (a, d) & \text{se } b = c \\ (a, b) & \text{altrimenti.} \end{cases}$$

Osserviamo che è semplice verificare che B è un sottouniverso di questa nuova algebra se e solo se B è una congruenza su \mathbf{A} . Sia Θ l'operatore di chiusura Sg su $A \times A$ per l'algebra appena definita. Allora, per il Corollario 3.3, $\text{Con } \mathbf{A}$ è un reticolo algebrico. \square

Definizione 5.6. Siano \mathbf{A} un'algebra ed $a_1, \dots, a_n \in A$. Indicheremo con $\Theta(a_1, \dots, a_n)$ la congruenza generata da $\{(a_i, a_j) : 1 \leq i, j \leq n\}$, ovvero la più piccola congruenza rispetto alla quale a_1, \dots, a_n sono nella stessa classe d'equivalenza. Una congruenza del tipo $\Theta(a_1, a_2)$ si dice una *congruenza principale*. Per ogni sottoinsieme X di A indicheremo semplicemente con $\Theta(X)$ la congruenza generata da $X \times X$.

Le congruenze finitamente generate ci torneranno molto utili nel paragrafo 12.

Teorema 5.7. *Sia \mathbf{A} un'algebra, e siano $a_1, b_1, \dots, a_n, b_n \in A$ e $\theta \in \text{Con } \mathbf{A}$. Allora:*

- (a) $\Theta(a_1, b_1) = \Theta(b_1, a_1)$;
- (b) $\Theta((a_1, b_1), \dots, (a_n, b_n)) = \Theta(a_1, b_1) \vee \dots \vee \Theta(a_n, b_n)$;
- (c) $\Theta(a_1, \dots, a_n) = \Theta(a_1, a_2) \vee \Theta(a_2, a_3) \vee \dots \vee \Theta(a_{n-1}, a_n)$;
- (d) $\theta = \bigcup \{\Theta(a, b) : (a, b) \in \theta\} = \bigvee \{\Theta(a, b) : (a, b) \in \theta\}$;
- (e) $\theta = \bigcup \{\Theta((a_1, b_1), \dots, (a_n, b_n)) : (a_i, b_i) \in \theta, n \geq 1\}$.

Dimostrazione. (a) Poiché $(b_1, a_1) \in \Theta(a_1, b_1)$, si ha che

$$\Theta(b_1, a_1) \subseteq \Theta(a_1, b_1)$$

e quindi, per simmetria, $\Theta(a_1, b_1) = \Theta(b_1, a_1)$.

(b) Per $1 \leq i \leq n$, si ha $(a_i, b_i) \in \Theta((a_1, b_1), \dots, (a_n, b_n))$. Allora

$$\Theta(a_i, b_i) \subseteq \Theta((a_1, b_1), \dots, (a_n, b_n)),$$

per cui

$$\Theta(a_1, b_1) \vee \dots \vee \Theta(a_n, b_n) \subseteq \Theta((a_1, b_1), \dots, (a_n, b_n)).$$

D'altra parte, per $1 \leq i \leq n$,

$$(a_i, b_i) \in \Theta(a_i, b_i) \subseteq \Theta(a_1, b_1) \vee \dots \vee \Theta(a_n, b_n),$$

e quindi

$$\{(a_1, b_1), \dots, (a_n, b_n)\} \subseteq \Theta(a_1, b_1) \vee \dots \vee \Theta(a_n, b_n).$$

Ne segue che

$$\Theta((a_1, b_1), \dots, (a_n, b_n)) \subseteq \Theta(a_1, b_1) \vee \dots \vee \Theta(a_n, b_n),$$

e quindi

$$\Theta((a_1, b_1), \dots, (a_n, b_n)) = \Theta(a_1, b_1) \vee \dots \vee \Theta(a_n, b_n).$$

(c) Per $1 \leq i \leq n-1$,

$$(a_i, a_{i+1}) \in \Theta(a_1, \dots, a_n),$$

cioè

$$\Theta(a_i, a_{i+1}) \subseteq \Theta(a_1, \dots, a_n),$$

e quindi

$$\Theta(a_1, a_2) \vee \dots \vee \Theta(a_{n-1}, a_n) \subseteq \Theta(a_1, \dots, a_n).$$

Reciprocamente, per $1 \leq i < j \leq n$,

$$(a_i, a_j) \in \Theta(a_i, a_{i+1}) \circ \dots \circ \Theta(a_{j-1}, a_j),$$

da cui segue

$$(a_i, a_j) \in \Theta(a_i, a_{i+1}) \vee \dots \vee \Theta(a_{j-1}, a_j)$$

e quindi anche

$$(a_i, a_j) \in \Theta(a_1, a_2) \vee \dots \vee \Theta(a_{n-1}, a_n).$$

Tenendo conto anche della (a), segue allora

$$\Theta(a_1, \dots, a_n) \subseteq \Theta(a_1, a_2) \vee \dots \vee \Theta(a_{n-1}, a_n),$$

e pertanto

$$\Theta(a_1, \dots, a_n) = \Theta(a_1, a_2) \vee \dots \vee \Theta(a_{n-1}, a_n).$$

(d) Per $(a, b) \in \theta$ ovviamente si ha

$$(a, b) \in \Theta(a, b) \subseteq \theta;$$

dunque

$$\theta \subseteq \bigcup \{\Theta(a, b) : (a, b) \in \theta\} \subseteq \bigvee \{\Theta(a, b) : (a, b) \in \theta\} \subseteq \theta.$$

Pertanto si ha

$$\theta = \bigcup \{\Theta(a, b) : (a, b) \in \theta\} = \bigvee \{\Theta(a, b) : (a, b) \in \theta\}.$$

(e) Del tutto analoga alla (d).

□

Non è possibile aggiungere ulteriori proprietà alla caratterizzazione astratta dei reticoli delle congruenze di un'algebra (Teorema 5.5). Nel 1963, infatti, Grätzer e Schmidt dimostrarono che per ogni reticolo algebrico \mathbf{L} esiste un'algebra \mathbf{A} tale che $\mathbf{L} \cong \mathbf{Con A}$. Ovviamente, per particolari classi di algebre, è possibile trovare altre proprietà di cui siano dotate le rispettive classi dei reticoli di congruenze. Ad esempio i reticoli delle congruenze dei reticoli sono distributivi, quelli dei gruppi e degli anelli sono modulari.

Definizione 5.8. Un'algebra \mathbf{A} è *congruenze-distributiva* (rispettivamente: *congruenze-modulare*) se $\mathbf{Con A}$ è un reticolo distributivo (rispettivamente: modulare).

Se $\theta_1, \theta_2 \in \mathbf{Con A}$ e

$$\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1,$$

diremo allora che θ_1 e θ_2 sono *permutabili* (o che θ_1 e θ_2 *permutano*). \mathbf{A} si dice *congruenze-permutabile* se ogni coppia di congruenze su \mathbf{A} permuta. Una classe K di algebre è *congruenze-distributiva*, *congruenze-modulare* o *congruenze-permutabile*, rispettivamente, se e solo se lo è ciascuna delle algebre in essa contenute.

Concludiamo il presente paragrafo enunciando due risultati riguardanti le congruenze permutabili.

Teorema 5.9. Siano \mathbf{A} una struttura algebrica e $\theta_1, \theta_2 \in \mathbf{Con A}$. Sono equivalenti le seguenti affermazioni:

(a) $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1;$

(b) $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2;$

(c) $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1.$

Teorema 5.10. (Birkhoff). Se \mathbf{A} è *congruenze-permutabile*, allora \mathbf{A} è *congruenze-modulare*.

6 Omomorfismi ed isomorfismi.

Definizione 6.1. Siano \mathbf{A} e \mathbf{B} due algebre dello stesso tipo \mathcal{F} . Una funzione $\alpha : A \rightarrow B$ si dice un *omomorfismo* di \mathbf{A} in \mathbf{B} se

$$\alpha f^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n),$$

per ogni operazione n -aria $f \in \mathcal{F}$, qualunque siano $a_1, \dots, a_n \in A$. Se, inoltre, α è suriettiva, allora diremo che \mathbf{B} è una *immagine omomorfa* di

\mathbf{A} , ed α si dice un *epimorfismo*. Un omomorfismo iniettivo si dice anche un *monomorfismo* o una *immersione*. Un omomorfismo biiettivo si dice un *isomorfismo*. Un omomorfismo di \mathbf{A} in sé si dice un *endomorfismo* e, se biiettivo, un *automorfismo*.

Teorema 6.2. *Sia \mathbf{A} un'algebra generata da un insieme X . Se $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ e $\beta : \mathbf{A} \rightarrow \mathbf{B}$ sono due omomorfismi che coincidono su X (ovvero tali che $\alpha(a) = \beta(a) \forall a \in X$), allora $\alpha = \beta$.*

Dimostrazione. Richiamiamo la definizione dell'operatore E data nel paragrafo 3. Osserviamo che se α e β coincidono su X , allora coincidono anche su $E(X)$. Infatti, se f è un simbolo funzionale n -ario ed $a_1, \dots, a_n \in X$, allora

$$\begin{aligned} \alpha f^{\mathbf{A}}(a_1, \dots, a_n) &= f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n) \\ &= f^{\mathbf{B}}(\beta a_1, \dots, \beta a_n) = \beta f^{\mathbf{A}}(a_1, \dots, a_n). \end{aligned}$$

Ne segue per induzione che, se α e β coincidono su X , allora coincidono su $E^n(X)$ per $n < \omega$, e pertanto essi coincidono su $\text{Sg}(X)$. \square

Teorema 6.3. *Sia $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un omomorfismo. Allora l'immagine mediante α di un sottouniverso di \mathbf{A} è un sottouniverso di \mathbf{B} , e la controimmagine mediante α di un sottouniverso di \mathbf{B} è un sottouniverso di \mathbf{A} .*

Dimostrazione. Sia S un sottouniverso di \mathbf{A} , e siano f un simbolo funzionale n -ario di \mathcal{F} e $a_1, \dots, a_n \in S$. Allora

$$f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n) = \alpha f^{\mathbf{A}}(a_1, \dots, a_n) \in \alpha(S),$$

e quindi $\alpha(S)$ è un sottouniverso di \mathbf{B} . Supponiamo ora che S sia un sottouniverso di \mathbf{B} e siano $\alpha(a_1), \dots, \alpha(a_n) \in S$. Allora segue dalla precedente uguaglianza che $\alpha f^{\mathbf{A}}(a_1, \dots, a_n) \in S$, e pertanto $f^{\mathbf{A}}(a_1, \dots, a_n) \in \alpha^{-1}(S)$. Ne segue che $\alpha^{-1}(S)$ è un sottouniverso di \mathbf{A} . \square

Definizione 6.4. Siano $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un omomorfismo e $\mathbf{C} \leq \mathbf{A}, \mathbf{D} \leq \mathbf{B}$. Indicheremo con $\alpha(\mathbf{C})$ la sottoalgebra di \mathbf{B} il cui sostegno è $\alpha(C)$, e con $\alpha^{-1}(\mathbf{D})$ la sottoalgebra di \mathbf{A} il cui sostegno è $\alpha^{-1}(D)$ (con $\alpha^{-1}(D) \neq \emptyset$).

Il seguente risultato è di verifica immediata.

Teorema 6.5. *Siano $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ e $\beta : \mathbf{B} \rightarrow \mathbf{C}$ omomorfismi. Allora $\beta \circ \alpha : \mathbf{A} \rightarrow \mathbf{C}$ è un omomorfismo.*

Teorema 6.6. *Se $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ è un omomorfismo ed $X \subseteq A$, allora*

$$\alpha \text{Sg}(X) = \text{Sg}(\alpha X).$$

Dimostrazione. Dalla definizione dell'operatore E e dal fatto che α è un omomorfismo, si ha subito

$$\alpha E(Y) = E(\alpha Y),$$

per ogni $Y \subseteq A$. Pertanto, procedendo per induzione su n ,

$$\alpha E^n(X) = E^n(\alpha X)$$

per $n \geq 1$. Ne segue che

$$\begin{aligned} \alpha \text{Sg}(X) &= \alpha(X \cup E(X) \cup E^2(X) \cup \dots) \\ &= \alpha X \cup \alpha E(X) \cup \alpha E^2(X) \cup \dots \\ &= \alpha X \cup E(\alpha X) \cup E^2(\alpha X) \cup \dots \\ &= \text{Sg}(\alpha X). \end{aligned}$$

□

Definizione 6.7. Sia $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un omomorfismo. Si definisce il *nucleo* $\ker \alpha$ di α come l'insieme

$$\ker \alpha = \{(a, b) \in A^2 : \alpha(a) = \alpha(b)\}.$$

Teorema 6.8. Sia $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un omomorfismo. Allora $\ker \alpha$ è una congruenza su \mathbf{A} .

Dimostrazione. Se $(a_i, b_i) \in \ker \alpha$, $1 \leq i \leq n$, ed $f \in \mathcal{F}$ è un simbolo funzionale n -ario, allora

$$\begin{aligned} \alpha f^{\mathbf{A}}(a_1, \dots, a_n) &= f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n) \\ &= f^{\mathbf{B}}(\alpha b_1, \dots, \alpha b_n) \\ &= \alpha f^{\mathbf{A}}(b_1, \dots, b_n); \end{aligned}$$

per cui

$$(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \ker \alpha.$$

D'altra parte $\ker \alpha$ è banalmente una relazione d'equivalenza. Ne segue l'asserto. □

Nello studio dei gruppi, quando si parla del nucleo di un omomorfismo α , ci si riferisce al sottogruppo normale del dominio, costituito dalle controimmagini tramite α dell'unità del codominio. Questo fatto non causa particolari problemi perché, come abbiamo già osservato nel paragrafo 5, ogni

congruenza in un gruppo è determinata univocamente dalla classe d'equivalenza dell'unità, che è un sottogruppo normale. Analogamente, nello studio degli anelli, il nucleo di un omomorfismo è un ideale.

Ora siamo in grado di fornire una diretta generalizzazione, alle algebre astratte, dei teoremi d'isomorfismo e di omomorfismo che normalmente si studiano in teoria dei gruppi, teoria degli anelli eccetera.

Definizione 6.9. Sia \mathbf{A} un'algebra e sia $\theta \in \text{Con } \mathbf{A}$. La *proiezione canonica* $\nu_\theta : A \rightarrow A/\theta$ è definita da $\nu_\theta(a) = a/\theta$.

Teorema 6.10. Per ogni algebra \mathbf{A} e per ogni $\theta \in \text{Con } \mathbf{A}$, la proiezione canonica ν_θ è un epimorfismo.

Dimostrazione. Sia f un simbolo funzionale n -ario e siano $a_1, \dots, a_n \in A$. Si ha:

$$\begin{aligned} \nu_\theta f^{\mathbf{A}}(a_1, \dots, a_n) &= f^{\mathbf{A}}(a_1, \dots, a_n)/\theta \\ &= f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta) \\ &= f^{\mathbf{A}/\theta}(\nu_\theta a_1, \dots, \nu_\theta a_n), \end{aligned}$$

e quindi ν_θ è un omomorfismo ed è, banalmente, suriettivo. \square

Definizione 6.11. In base al Teorema 6.10, chiameremo ν_θ *epimorfismo canonico di A su A/θ* .

Teorema 6.12. (Teorema di Omomorfismo). Sia $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un epimorfismo. Allora esiste un isomorfismo β tra $\mathbf{A}/\ker \alpha$ e \mathbf{B} , definito da $\alpha = \beta \circ \nu$, dove $\nu = \nu_{\ker \alpha}$.

Dimostrazione. Osserviamo innanzitutto che, se $\alpha = \beta \circ \nu$, allora $\beta(a/\theta) = \alpha(a)$. Tale uguaglianza definisce una funzione β e, banalmente, si ha $\alpha = \beta \circ \nu$. È immediato verificare che β è effettivamente una biezione. Resta da provare il fatto che β è un omomorfismo. Supponiamo allora che f sia un simbolo funzionale n -ario, e siano $a_1, \dots, a_n \in A$. Si ha:

$$\begin{aligned} \beta(f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta)) &= \beta(f^{\mathbf{A}}(a_1, \dots, a_n)/\theta) \\ &= \alpha f^{\mathbf{A}}(a_1, \dots, a_n) \\ &= f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n) \\ &= f^{\mathbf{B}}(\beta(a_1/\theta), \dots, \beta(a_n/\theta)). \end{aligned}$$

\square

Dai Teoremi 6.5 e 6.12 segue che un'algebra è immagine omomorfa di un'altra algebra \mathbf{A} se e solo se essa è isomorfa ad un quoziente di \mathbf{A} . Pertanto il problema “esterno” consistente nel trovare tutte le immagini omomorfe di \mathbf{A} si riduce al problema “interno” dell'individuazione di tutte le congruenze su \mathbf{A} . Il Teorema d'Omomorfismo è anche detto Primo Teorema di Omomorfismo.

Definizione 6.13. Siano \mathbf{A} un'algebra e $\phi, \theta \in \text{Con } \mathbf{A}$, con $\theta \subseteq \phi$. Allora poniamo

$$\phi/\theta = \{(a/\theta, b/\theta) \in (a/\theta)^2 : (a, b) \in \phi\}.$$

Lemma 6.14. Se $\phi, \theta \in \text{Con } \mathbf{A}$ e $\theta \subseteq \phi$, allora ϕ/θ è una congruenza su \mathbf{A}/θ .

Dimostrazione. Sia f un simbolo funzionale n -ario e siano $(a_i/\theta, b_i/\theta) \in \phi/\theta$, $1 \leq i \leq n$. Allora $(a_i, b_i) \in \phi$ e quindi

$$(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \phi.$$

Pertanto

$$(f^{\mathbf{A}}(a_1, \dots, a_n)/\theta, f^{\mathbf{A}}(b_1, \dots, b_n)/\theta) \in \phi/\theta,$$

e da ciò segue

$$(f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta), f^{\mathbf{A}/\theta}(b_1/\theta, \dots, b_n/\theta)) \in \phi/\theta.$$

L'asserto è provato. □

Teorema 6.15. (Secondo Teorema di Omomorfismo). Se $\phi, \theta \in \text{Con } \mathbf{A}$ e $\theta \subseteq \phi$, allora la funzione

$$\alpha : (\mathbf{A}/\theta)/(\phi/\theta) \rightarrow \mathbf{A}/\phi,$$

definita da

$$\alpha((a/\theta)/(\phi/\theta)) = a/\phi,$$

è un isomorfismo tra $(\mathbf{A}/\theta)/(\phi/\theta)$ e \mathbf{A}/ϕ .

Dimostrazione. Siano $a, b \in \mathbf{A}$. Allora da

$$(a/\theta)/(\phi/\theta) = (b/\theta)/(\phi/\theta) \quad \text{sse} \quad a/\phi = b/\phi$$

segue che α è un'applicazione biettiva ben definita. Ora, se f è un simbolo funzionale n -ario ed $a_1, \dots, a_n \in A$, si ha

$$\begin{aligned}
& \alpha f^{(\mathbf{A}/\theta)/(\phi/\theta)}((a_1/\theta)/(\phi/\theta), \dots, (a_n/\theta)/(\phi/\theta)) \\
&= \alpha(f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta)/(\phi/\theta)) \\
&= \alpha((f^{\mathbf{A}}(a_1, \dots, a_n)/\theta)/(\phi/\theta)) \\
&= f^{\mathbf{A}}(a_1, \dots, a_n)/\phi \\
&= f^{\mathbf{A}/\phi}(a_1/\phi, \dots, a_n/\phi) \\
&= f^{\mathbf{A}/\phi}(\alpha((a_1/\theta)/(\phi/\theta)), \dots, \alpha((a_n/\theta)/(\phi/\theta))).
\end{aligned}$$

Dunque α è un isomorfismo. \square

Definizione 6.16. Siano B un sottoinsieme di A e θ una congruenza su \mathbf{A} , e si consideri l'insieme $B^\theta = \{a \in A : B \cap a/\theta \neq \emptyset\}$. Indicheremo con \mathbf{B}^θ la sottoalgebra di \mathbf{A} generata da B^θ . Indicheremo, inoltre, con $\theta|_B$ la restrizione $\theta \cap B^2$ di θ a B .

Lemma 6.17. Siano \mathbf{B} una sottoalgebra di \mathbf{A} e $\theta \in \text{Con } \mathbf{A}$. Allora

- (a) il sostegno di \mathbf{B}^θ è B^θ ;
- (b) $\theta|_B$ è una congruenza su \mathbf{B} .

Dimostrazione. Sia f un simbolo funzionale n -ario e siano $a_1, \dots, a_n \in B^\theta$. Allora possiamo trovare $b_1, \dots, b_n \in B$ tali che

$$(a_i, b_i) \in \theta, \quad 1 \leq i \leq n,$$

per cui

$$(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \theta,$$

e quindi

$$f^{\mathbf{A}}(a_1, \dots, a_n) \in B^\theta.$$

Pertanto B^θ è un sottouniverso di \mathbf{A} . È poi immediato verificare che $\theta|_B$ è una congruenza su \mathbf{B} . \square

Teorema 6.18. (Terzo Teorema di Omomorfismo). Se \mathbf{B} è una sottoalgebra di \mathbf{A} e $\theta \in \text{Con } \mathbf{A}$, allora

$$\mathbf{B}/\theta|_B \cong \mathbf{B}^\theta/\theta|_{B^\theta}.$$

Dimostrazione. Non è difficile verificare che l'applicazione

$$\alpha : b/\theta|_B \in \mathbf{B}/\theta|_B \mapsto \mathbf{B}^\theta/\theta|_{B^\theta} \in b/\theta|_{B^\theta}$$

è effettivamente un isomorfismo. \square

Il Teorema 6.20 risulterà importante nello studio delle algebre sottodirettamente irriducibili. Prima di enunciarlo, però, osserviamo che, se \mathbf{L} è un reticolo e $a, b \in L$ con $a \leq b$, allora l'intervallo $[a, b]$ è un sottouniverso di \mathbf{L} .

Definizione 6.19. Se $[a, b]$ è un intervallo chiuso di un reticolo \mathbf{L} , con $a \leq b$, indicheremo con $[a, b]^*$ il sottoreticolo di \mathbf{L} che ha $[a, b]$ come sostegno.

Teorema 6.20. (Teorema di Corrispondenza). *Siano \mathbf{A} un'algebra e $\theta \in \text{Con } \mathbf{A}$. Allora la funzione α definita su $[\theta, \nabla_{\mathbf{A}}]$ da*

$$\alpha(\phi) = \phi/\theta$$

è un isomorfismo tra i reticoli $[\theta, \nabla_{\mathbf{A}}]^$ e $\text{Con } \mathbf{A}/\theta$, dove $[\theta, \nabla_{\mathbf{A}}]^*$ è un sottoreticolo di $\text{Con } \mathbf{A}$.*

7 Prodotti diretti, congruenze-fattore, algebre direttamente indecomponibili.

Le costruzioni che abbiamo esaminato finora, come quelle delle sottoalgebre e delle algebre quozienti, non permettono di creare algebre di cardinalità maggiore rispetto a quella dell'algebra di partenza, né di combinare in qualche modo diverse algebre per ottenerne una nuova.

Definizione 7.1. Siano \mathbf{A}_1 ed \mathbf{A}_2 due algebre dello stesso tipo \mathcal{F} . Definiamo il *prodotto diretto* $\mathbf{A}_1 \times \mathbf{A}_2$ delle due algebre come l'algebra il cui universo è l'insieme $A_1 \times A_2$, e tale che per $f \in \mathcal{F}_n$, e $a_i \in A_1, a'_i \in A_2, 1 \leq i \leq n$,

$$f^{\mathbf{A}_1 \times \mathbf{A}_2}((a_1, a'_1), \dots, (a_n, a'_n)) = (f^{\mathbf{A}_1}(a_1, \dots, a_n), f^{\mathbf{A}_2}(a'_1, \dots, a'_n)).$$

In generale \mathbf{A}_1 ed \mathbf{A}_2 non sono immergibili in $\mathbf{A}_1 \times \mathbf{A}_2$, anche se ciò è possibile in casi speciali come avviene, ad esempio, per i gruppi (in quanto dotati sempre di una sottostruttura banale). Sia \mathbf{A}_1 che \mathbf{A}_2 sono, però, immagini omomorfe di $\mathbf{A}_1 \times \mathbf{A}_2$.

Definizione 7.2. La funzione

$$\pi_i : A_1 \times A_2 \rightarrow A_i, \quad i \in \{1, 2\},$$

definita da

$$\pi_i((a_1, a_2)) = a_i,$$

si dice *proiezione i -esima di $A_1 \times A_2$* o *proiezione di $A_1 \times A_2$ su A_i* o, ancora, *proiezione di $A_1 \times A_2$ sull' i -esima coordinata*.

Teorema 7.3. Per $i \in \{1, 2\}$, la funzione $\pi_i : A_1 \times A_2 \rightarrow A_i$ è un epimorfismo di $\mathbf{A} = \mathbf{A}_1 \times \mathbf{A}_2$ su \mathbf{A}_i . Inoltre, in $\mathbf{Con} \mathbf{A}_1 \times \mathbf{A}_2$, si ha:

$$\ker \pi_1 \cap \ker \pi_2 = \Delta,$$

$\ker \pi_1$ e $\ker \pi_2$ permutano,

e

$$\ker \pi_1 \vee \ker \pi_2 = \nabla.$$

Dimostrazione. La funzione π_i è chiaramente suriettiva. Se $f \in \mathcal{F}_n$, e $a_i \in A_1, a'_i \in A_2, 1 \leq i \leq n$, allora

$$\begin{aligned} \pi_1(f^{\mathbf{A}}((a_1, a'_1), \dots, (a_n, a'_n))) &= \pi_1((f^{\mathbf{A}_1}(a_1, \dots, a_n), f^{\mathbf{A}_2}(a'_1, \dots, a'_n))) \\ &= f^{\mathbf{A}_1}(a_1, \dots, a_n) \\ &= f^{\mathbf{A}_1}(\pi_1((a_1, a'_1), \dots, \pi_1((a_n, a'_n))), \end{aligned}$$

e quindi π_1 è un omomorfismo. Analogamente si prova che anche π_2 è un omomorfismo.

Si ha, ora,

$$\begin{aligned} &((a_1, a_2), (b_1, b_2)) \in \ker \pi_i \\ \text{sse} \quad &\pi_i((a_1, a_2)) = \pi_i((b_1, b_2)) \\ \text{sse} \quad &a_i = b_i. \end{aligned}$$

Pertanto

$$\ker \pi_1 \cap \ker \pi_2 = \Delta.$$

Se $(a_1, a_2), (b_1, b_2)$ sono due qualunque elementi di $A_1 \times A_2$, allora

$$(a_1, a_2) \ker \pi_1(a_1, b_2) \ker \pi_2(b_1, b_2),$$

e quindi

$$\nabla = \ker \pi_1 \circ \ker \pi_2.$$

Ma allora $\ker \pi_1$ e $\ker \pi_2$ permutano e $\ker \pi_1 \vee \ker \pi_2 = \nabla$. □

La seconda parte del Teorema 7.3 ci permette di dare la seguente

Definizione 7.4. Una congruenza θ su \mathbf{A} è una *congruenza-fattore* se esiste una congruenza θ^* su \mathbf{A} tale che

$$\theta \cap \theta^* = \Delta,$$

$$\theta \vee \theta^* = \nabla,$$

e

θ permuta con θ^* .

La coppia (θ, θ^*) si dice una *coppia di congruenze-fattore* su \mathbf{A} .

Teorema 7.5. Se (θ, θ^*) è una coppia di congruenze-fattore su \mathbf{A} , allora

$$\mathbf{A} \cong \mathbf{A}/\theta \times \mathbf{A}/\theta^*$$

mediante la funzione definita da

$$\alpha(a) = (a/\theta, a/\theta^*).$$

Dimostrazione. Se $a, b \in A$ e $\alpha(a) = \alpha(b)$, allora $a/\theta = b/\theta$ e $a/\theta^* = b/\theta^*$. Allora $(a, b) \in \theta$ e $(a, b) \in \theta^*$, cioè $a = b$. Dunque α è iniettiva.

Siano ora $a, b \in A$; esiste allora $c \in A$ tale che

$$a\theta c\theta^* b,$$

e quindi

$$\alpha(c) = (c/\theta, c/\theta^*) = (a/\theta, b/\theta^*).$$

Ne segue che α è suriettiva.

Siano, infine, $f \in \mathcal{F}$ ed $a_1, \dots, a_n \in A$. Si ha:

$$\begin{aligned} \alpha f^{\mathbf{A}}(a_1, \dots, a_n) &= (f^{\mathbf{A}}(a_1, \dots, a_n)/\theta, f^{\mathbf{A}}(a_1, \dots, a_n)/\theta^*) \\ &= (f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta), f^{\mathbf{A}/\theta^*}(a_1/\theta^*, \dots, a_n/\theta^*)) \\ &= f^{\mathbf{A}/\theta \times \mathbf{A}/\theta^*}((a_1/\theta, a_1/\theta^*), \dots, (a_n/\theta, a_n/\theta^*)) \\ &= f^{\mathbf{A}/\theta \times \mathbf{A}/\theta^*}(\alpha a_1, \dots, \alpha a_n); \end{aligned}$$

e quindi α è proprio un isomorfismo. □

Definizione 7.6. Un'algebra \mathbf{A} si dice (*direttamente*) *indecomponibile* se \mathbf{A} non è isomorfa al prodotto diretto di algebre non banali.

Il seguente risultato è diretta conseguenza dei Teoremi 7.3 e 7.5.

Corollario 7.7. \mathbf{A} è *direttamente indecomponibile* se e solo se le uniche congruenze-fattore su \mathbf{A} sono Δ e ∇ .

La definizione di prodotto diretto di due algebre si generalizza nel modo seguente:

Definizione 7.8. Sia $(\mathbf{A}_i)_{i \in I}$ una famiglia, con insieme di indici I , di algebre di tipo \mathcal{F} . Il *prodotto (diretto)* $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ è un'algebra il cui universo è $\prod_{i \in I} A_i$ e tale che, per $f \in \mathcal{F}_n$ ed $a_1, \dots, a_n \in \prod_{i \in I} A_i$,

$$f^{\mathbf{A}}(a_1, \dots, a_n)(i) = f^{\mathbf{A}_i}(a_1(i), \dots, a_n(i))$$

per $i \in I$. Il prodotto vuoto $\prod \emptyset$ è l'algebra banale il cui universo è $\{\emptyset\}$. Come nel caso del prodotto di due algebre abbiamo le *proiezioni*

$$\pi_j : a \in \prod_{i \in I} A_i \mapsto \pi_j(a) = a(j) \in A_j$$

da cui si ha l'*epimorfismo canonico*

$$\pi_j : \prod_{i \in I} \mathbf{A}_i \rightarrow \mathbf{A}_j.$$

Se $I = \{1, \dots, n\}$, indicheremo il prodotto diretto delle algebre $\mathbf{A}_1, \dots, \mathbf{A}_n$ anche con $\mathbf{A}_1 \times \dots \times \mathbf{A}_n$. Se $\mathbf{A}_i = \mathbf{A}$ per ogni $i \in I$, scriveremo \mathbf{A}^I invece che $\prod_{i \in I} \mathbf{A}_i$, e chiameremo tale prodotto diretto, la *potenza (diretta)* di \mathbf{A} . \mathbf{A}^\emptyset è un'algebra banale.

Teorema 7.9. *Se $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$ sono algebre dello stesso tipo \mathcal{F} , allora:*

- (i) $\mathbf{A}_1 \times \mathbf{A}_2 \cong \mathbf{A}_2 \times \mathbf{A}_1$ mediante l'isomorfismo $\alpha((a_1, a_2)) = (a_2, a_1)$;
- (ii) $\mathbf{A}_1 \times (\mathbf{A}_2 \times \mathbf{A}_3) \cong \mathbf{A}_1 \times \mathbf{A}_2 \times \mathbf{A}_3$, con $\alpha((a_1, (a_2, a_3))) = (a_1, a_2, a_3)$ isomorfismo tra le due strutture.

Teorema 7.10. *Ogni algebra finita è isomorfa ad un prodotto diretto di algebre direttamente indecomponibili.*

Dimostrazione. Sia \mathbf{A} un'algebra finita. Se \mathbf{A} è banale, allora è indecomponibile. Procediamo ora per induzione sulla cardinalità di A . Supponiamo quindi che \mathbf{A} sia un'algebra finita non banale tale che ogni algebra \mathbf{B} , il cui universo abbia cardinalità minore di $|A|$, è isomorfa ad un prodotto diretto di algebre direttamente indecomponibili. Se \mathbf{A} è indecomponibile, non c'è nulla da dimostrare. Se, invece, \mathbf{A} non è indecomponibile, allora $\mathbf{A} \cong \mathbf{A}_1 \times \mathbf{A}_2$ con $1 < |A_1|, |A_2| < |A|$. Allora, per l'ipotesi d'induzione,

$$\mathbf{A}_1 \cong \mathbf{B}_1 \times \dots \times \mathbf{B}_m,$$

$$\mathbf{A}_2 \cong \mathbf{C}_1 \times \dots \times \mathbf{C}_n,$$

dove \mathbf{B}_i e \mathbf{C}_j sono indecomponibili. Ne segue che

$$\mathbf{A} \cong \mathbf{B}_1 \times \dots \times \mathbf{B}_m \times \mathbf{C}_1 \times \dots \times \mathbf{C}_n,$$

cioè l'asserto. □

Definizione 7.11. Date delle funzioni $\alpha_i : A \rightarrow A_i$, $i \in I$, l'applicazione naturale

$$\alpha : A \rightarrow \prod_{i \in I} A_i$$

tra A e $\prod_{i \in I} A_i$, è definita da

$$(\alpha a)(i) = \alpha_i a.$$

Date delle funzioni $\alpha_i : A_i \rightarrow B_i$, $i \in I$, l'applicazione naturale

$$\alpha : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$$

tra $\prod_{i \in I} A_i$ e $\prod_{i \in I} B_i$, è definita da

$$(\alpha a)(i) = \alpha_i(a(i)).$$

Teorema 7.12. (i) Se $\alpha_i : \mathbf{A} \rightarrow \mathbf{A}_i$, $i \in I$, è una famiglia di omomorfismi, allora l'applicazione naturale α è un omomorfismo tra \mathbf{A} ed $\mathbf{A}^* = \prod_{i \in I} \mathbf{A}_i$.

(ii) Se $\alpha_i : \mathbf{A}_i \rightarrow \mathbf{B}_i$, $i \in I$, è una famiglia di omomorfismi, allora l'applicazione naturale α è un omomorfismo tra \mathbf{A}^* e \mathbf{B}^* .

Dimostrazione. Siano $a_1, \dots, a_n \in A$ e sia $f \in \mathcal{F}_n$; allora, per ogni $i \in I$, si ha:

$$\begin{aligned} (\alpha f^{\mathbf{A}}(a_1, \dots, a_n))(i) &= \alpha_i f^{\mathbf{A}}(a_1, \dots, a_n) \\ &= f^{\mathbf{A}_i}(\alpha_i a_1, \dots, \alpha_i a_n) \\ &= f^{\mathbf{A}_i}((\alpha a_1)(i), \dots, (\alpha a_n)(i)) \\ &= f^{\mathbf{A}^*}(\alpha a_1, \dots, \alpha a_n)(i); \end{aligned}$$

e quindi

$$\alpha f^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{A}^*}(\alpha a_1, \dots, \alpha a_n).$$

Ne segue la tesi (i).

La (ii) discende immediatamente dalla (i); basta, infatti, considerare l'omomorfismo $\alpha_i \circ \pi_i$. \square

Definizione 7.13. Siano $a_1, a_2 \in A$ ed $\alpha : A \rightarrow B$ una funzione. Diremo che α separa a_1 ed a_2 se

$$\alpha a_1 \neq \alpha a_2.$$

Diremo anche che le funzioni $\alpha_i : A \rightarrow A_i$, $i \in I$, separano i punti se, qualunque siano gli elementi distinti $a_1, a_2 \in A$, esiste un indice i tale che

$$\alpha_i(a_1) \neq \alpha_i(a_2).$$

Lemma 7.14. Per una famiglia di funzioni $\alpha_i : A \rightarrow A_i$, $i \in I$, sono equivalenti le seguenti condizioni:

(a) le funzioni α_i separano i punti;

(b) l'applicazione naturale $\alpha : A \rightarrow A^*$ è iniettiva;

(c) $\bigcap_{i \in I} \ker \alpha_i = \Delta$.

Dimostrazione. (a) \Rightarrow (b). Siano $a_1, a_2 \in A$, con $a_1 \neq a_2$. Allora, per qualche $i \in I$,

$$\alpha_i(a_1) \neq \alpha_i(a_2),$$

e quindi

$$(\alpha a_1)(i) \neq (\alpha a_2)(i).$$

Ne segue la (b):

$$\alpha a_1 \neq \alpha a_2.$$

(b) \Rightarrow (c). Per $a_1, a_2 \in A$, con $a_1 \neq a_2$, si ha

$$\alpha a_1 \neq \alpha a_2.$$

Pertanto

$$(\alpha a_1)(i) \neq (\alpha a_2)(i)$$

per qualche i , cioè

$$\alpha_i a_1 \neq \alpha_i a_2.$$

Allora $(a_1, a_2) \notin \ker \alpha_i$, il che implica la (c):

$$\bigcap_{i \in I} \ker \alpha_i = \Delta.$$

(c) \Rightarrow (a). Siano a_1, a_2 elementi distinti di A ; si ha

$$(a_1, a_2) \notin \bigcap_{i \in I} \ker \alpha_i$$

e quindi, per qualche i ,

$$(a_1, a_2) \notin \ker \alpha_i.$$

Allora vale la (a):

$$\alpha_i a_1 \neq \alpha_i a_2.$$

□

Il risultato seguente è conseguenza immediata del Lemma 7.14.

Teorema 7.15. *Data una famiglia di omomorfismi $\alpha_i : \mathbf{A} \rightarrow \mathbf{A}_i$, $i \in I$, l'omomorfismo naturale $\alpha : \mathbf{A} \rightarrow \mathbf{A}^*$ è un'immersione se e solo se $\bigcap_{i \in I} \ker \alpha_i = \Delta$ se e solo se le funzioni α_i separano i punti.*

8 Prodotti sottodiretti, algebre sottodirettamente irriducibili, algebre semplici.

Sebbene ogni algebra finita sia isomorfa ad un prodotto diretto di algebre direttamente indecomponibili, altrettanto non si può dire - in generale - per le algebre infinite. Ad esempio, si vede facilmente che uno spazio vettoriale numerabile, su un campo finito, non può essere isomorfo ad un prodotto diretto di spazi di dimensione uno. Queste considerazioni portarono Birkhoff a definire e studiare algebre sottodirettamente irriducibili.

Definizione 8.1. Un'algebra \mathbf{A} è un *prodotto sottodiretto* di una famiglia $(\mathbf{A}_i)_{i \in I}$ di algebre se

- (i) $\mathbf{A} \leq \prod_{i \in I} \mathbf{A}_i$,
- (ii) $\pi_i(\mathbf{A}) = \mathbf{A}_i$ per ogni $i \in I$.

Un'immersione $\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}_i$ è *sottodiretta* se $\alpha(\mathbf{A})$ è un prodotto sottodiretto degli \mathbf{A}_i .

Osserviamo che se $I = \emptyset$, allora \mathbf{A} è un prodotto sottodiretto di \emptyset se e solo se $\mathbf{A} = \prod \emptyset$, cioè \mathbf{A} è un'algebra banale.

Lemma 8.2. *Se $\theta_i \in \text{Con } \mathbf{A}$ per $i \in I$ e $\bigcap_{i \in I} \theta_i = \Delta$, allora l'omomorfismo naturale*

$$\nu : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}/\theta_i$$

definito da

$$\nu(a)(i) = a/\theta_i$$

è un'immersione sottodiretta.

Dimostrazione. Sia ν_i l'omomorfismo naturale tra \mathbf{A} e \mathbf{A}/θ_i , per $i \in I$. Poiché $\ker \nu_i = \theta_i$, segue dal Teorema 7.15 che ν è un'immersione. Essendo, poi, ν_i suriettiva per ogni i , ν è un'immersione sottodiretta. \square

Definizione 8.3. Una struttura algebrica \mathbf{A} è *sottodirettamente irriducibile* se per ogni immersione sottodiretta

$$\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}_i$$

esiste un indice $i \in I$ tale che

$$\pi_i \circ \alpha : \mathbf{A} \rightarrow \mathbf{A}_i$$

è un isomorfismo.

La seguente caratterizzazione delle algebre sottodirettamente irriducibili è molto utile in pratica.

Teorema 8.4. *Un'algebra \mathbf{A} è sottodirettamente irriducibile se e solo se \mathbf{A} è banale o esiste una congruenza minima in $\text{Con } \mathbf{A} - \{\Delta\}$. Nel secondo caso, il minimo elemento è $\bigcap(\text{Con } \mathbf{A} - \{\Delta\})$, una congruenza principale.*

Dimostrazione. Se \mathbf{A} è non banale e $\text{Con } \mathbf{A} - \{\Delta\}$ non ha minimo, allora $\bigcap(\text{Con } \mathbf{A} - \{\Delta\}) = \Delta$. Sia $I = \text{Con } \mathbf{A} - \{\Delta\}$. Allora l'applicazione naturale $\alpha : \mathbf{A} \rightarrow \prod_{\theta \in I} \mathbf{A}/\theta$ è un'immersione sottodiretta per il Lemma 8.2 e, poiché l'applicazione naturale $\mathbf{A} \rightarrow \mathbf{A}/\theta$ non è iniettiva per ogni $\theta \in I$, segue che \mathbf{A} non è sottodirettamente irriducibile.

Viceversa, se \mathbf{A} è banale ed $\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}_i$ è un'immersione sottodiretta, allora ogni \mathbf{A}_i è banale. Quindi ciascuno degli omomorfismi $\pi_i \circ \alpha$ è un isomorfismo. Supponiamo dunque che \mathbf{A} sia non banale, e sia $\theta = \bigcap(\text{Con } \mathbf{A} - \{\Delta\}) \neq \Delta$. Scegliamo $(a, b) \in \theta$, con $a \neq b$. Se $\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}_i$ è un'immersione sottodiretta, allora $(\alpha a)(i) \neq (\alpha b)(i)$ per qualche i ; dunque $(\pi_i \circ \alpha)(a) \neq (\pi_i \circ \alpha)(b)$. Pertanto $(a, b) \notin \ker(\pi_i \circ \alpha)$ e quindi $\theta \not\subseteq \ker(\pi_i \circ \alpha)$. Ma ciò implica che $\ker(\pi_i \circ \alpha) = \Delta$, e quindi $\pi_i \circ \alpha : \mathbf{A} \rightarrow \mathbf{A}_i$ è un isomorfismo. Di conseguenza \mathbf{A} è sottodirettamente irriducibile.

Se $\text{Con } \mathbf{A} - \{\Delta\}$ è dotato di minimo θ , allora se $a \neq b$ e $(a, b) \in \theta$, si ha $\Theta(a, b) \subseteq \theta$, e quindi $\theta \subseteq \Theta(a, b)$. \square

ESEMPLI.

1. Un gruppo abeliano finito \mathbf{G} è sottodirettamente irriducibile se e solo se è ciclico e $|G| = p^n$ per qualche primo p .
2. Il gruppo \mathbf{Z}_{p^∞} è sottodirettamente irriducibile.
3. Ogni gruppo semplice è sottodirettamente irriducibile.

4. Uno spazio vettoriale su un campo F è sottodirettamente irriducibile se e solo se è banale o ha dimensione uno.
5. Ogni algebra a due elementi è sottodirettamente irriducibile.

Teorema 8.5. *Un'algebra sottodirettamente irriducibile è direttamente indecomponibile.*

Dimostrazione. Chiaramente le uniche congruenze-fattore su un'algebra sottodirettamente irriducibile sono Δ e ∇ . Dunque, per il Corollario 7.7, una tale algebra è direttamente indecomponibile. \square

Osserviamo esplicitamente che non vale, in generale, l'inverso del Teorema 8.5, cioè un'algebra direttamente indecomponibile non è necessariamente anche sottodirettamente irriducibile.

Teorema 8.6. (Birkhoff). *Ogni algebra \mathbf{A} è isomorfa ad un prodotto sottodiretto di algebre sottodirettamente irriducibili (che sono immagini omomorfe di \mathbf{A}).*

Dimostrazione. Poiché le algebre banali sono sottodirettamente irriducibili, ci basterà provare il teorema nel caso di un'algebra non banale \mathbf{A} . Siano a e b elementi distinti di A ; mediante il Lemma di Zorn possiamo trovare una congruenza $\theta_{a,b}$ su \mathbf{A} che sia massimale rispetto alla condizione $(a, b) \notin \theta_{a,b}$. Allora, ovviamente, $\Theta(a, b) \vee \theta_{a,b}$ è la più piccola congruenza in $[\theta_{a,b}, \nabla] - \{\theta_{a,b}\}$ e quindi, per i Teoremi 6.20 e 8.4, $\mathbf{A}/\theta_{a,b}$ è sottodirettamente irriducibile. Poiché $\bigcap \{\theta_{a,b} : a \neq b\} = \Delta$, possiamo applicare il Lemma 8.2 per provare che \mathbf{A} è sottodirettamente immergibile nel prodotto della famiglia di algebre sottodirettamente irriducibili $(\mathbf{A}/\theta_{a,b})_{a \neq b}$. \square

Il corollario seguente è un'immediata conseguenza del Teorema 8.6.

Corollario 8.7. *Ogni algebra finita è isomorfa ad un prodotto sottodiretto di un numero finito di algebre finite sottodirettamente irriducibili.*

Ora ci occuperemo di un particolare tipo di algebre sottodirettamente irriducibili. La seguente definizione estende le nozioni di gruppo semplice ed anello semplice ad un'arbitraria struttura algebrica.

Definizione 8.8. Un'algebra \mathbf{A} si dice *semplice* se $\text{Con } \mathbf{A} = \{\Delta, \nabla\}$. Una congruenza θ su un'algebra \mathbf{A} è *massimale* se l'intervallo $[\theta, \nabla]$ di $\text{Con } \mathbf{A}$ ha esattamente due elementi.

Teorema 8.9. *Sia $\theta \in \text{Con } \mathbf{A}$. Allora \mathbf{A}/θ è semplice se e solo se θ è una congruenza massimale su \mathbf{A} oppure $\theta = \nabla$.*

Dimostrazione. Dal Teorema 6.20 sappiamo che

$$\mathbf{Con} \mathbf{A}/\theta \cong [\theta, \nabla_{\mathbf{A}}],$$

e quindi la tesi è un'immediata conseguenza della Definizione 8.8. \square

9 Operatori di classe e varietà.

Un tema importante in algebra universale è lo studio delle classi di algebre che sono chiuse rispetto a certe costruzioni.

Definizione 9.1. Introduciamo i seguenti operatori tra classi di algebre dello stesso tipo:

$\mathbf{A} \in I(K)$ sse \mathbf{A} è isomorfa a qualche elemento di K ,

$\mathbf{A} \in S(K)$ sse \mathbf{A} è una sottoalgebra di qualche elemento di K ,

$\mathbf{A} \in H(K)$ sse \mathbf{A} è immagine omomorfa di qualche elemento di K ,

$\mathbf{A} \in P(K)$ sse \mathbf{A} è prodotto diretto di una famiglia non vuota di algebre di K ,

$\mathbf{A} \in P_S(K)$ sse \mathbf{A} è un prodotto sottodiretto di una famiglia non vuota di algebre di K .

Se O_1 e O_2 sono operatori su classi di algebre, indicheremo con $O_1 O_2$ l'operatore composto. Indicheremo inoltre con \leq la relazione d'ordine parziale definita da

$$O_1 \leq O_2 \quad \text{sse} \quad O_1(K) \subseteq O_2(K) \quad \text{per ogni classe } K \text{ di algebre.}$$

Un operatore O si dice *idempotente* se $O^2 = O$. Una classe K di algebre è *chiusa* rispetto all'operatore O se $O(K) \subseteq K$.

Lemma 9.2. *Valgono le seguenti relazioni: $SH \leq HS$, $PS \leq SP$ e $PH \leq HP$. Inoltre gli operatori H, S ed IP sono idempotenti.*

Dimostrazione. Supponiamo che $\mathbf{A} = SH(K)$. Allora esiste $\mathbf{B} \in K$ ed esiste un epimorfismo $\alpha : \mathbf{B} \rightarrow \mathbf{C}$, tali che $\mathbf{A} \leq \mathbf{C}$. Quindi $\alpha^{-1}(\mathbf{A}) \leq \mathbf{B}$, e poiché $\alpha(\alpha^{-1}(\mathbf{A})) = \mathbf{A}$, abbiamo $\mathbf{A} \in HS(K)$.

Se $\mathbf{A} \in PS(K)$ allora $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ per opportuni $\mathbf{A}_i \leq \mathbf{B}_i \in K$, $i \in I$. Poiché $\prod_{i \in I} \mathbf{A}_i \leq \prod_{i \in I} \mathbf{B}_i$, abbiamo $\mathbf{A} \in SP(K)$.

Se $\mathbf{A} \in PH(K)$, allora esistono algebre $\mathbf{B}_i \in K$ ed epimorfismi $\alpha_i : \mathbf{B}_i \rightarrow \mathbf{A}_i$ tali che $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$. È facile provare che la funzione $\alpha :$

$\prod_{i \in I} \mathbf{B}_i \rightarrow \prod_{i \in I} \mathbf{A}_i$, definita da $\alpha(b)(i) = \alpha_i(b(i))$, è un epimorfismo, per cui $\mathbf{A} \in HP(K)$.

Infine l'idempotenza di H, S ed IP si prova banalmente. \square

Definizione 9.3. Una classe non vuota K di algebre di tipo \mathcal{F} si dice una *varietà* se è chiusa per passaggio alle sottoalgebre, per immagini omomorfe e per prodotti diretti.

Poiché l'intersezione di una classe di varietà di algebre di tipo \mathcal{F} è ancora una varietà, e poiché tutte le algebre di un dato tipo \mathcal{F} costituiscono una varietà, possiamo concludere che per ogni classe K di algebre dello stesso tipo, esiste la più piccola varietà contenente K .

Definizione 9.4. Se K è una classe di algebre dello stesso tipo, sia $V(K)$ la più piccola varietà contenente K , che chiameremo la *varietà generata da K* . Se $K = \{\mathbf{A}\}$ scriveremo semplicemente $V(\mathbf{A})$. Una varietà V si dice che è *finitamente generata* se $V = V(K)$ con K insieme finito di algebre.

Teorema 9.5. (Tarski). $V = HSP$.

Dimostrazione. Da $HV = SV = IPV = V$ e $I \leq V$, segue

$$HSP \leq HSPV = V.$$

Dal Lemma 9.2 si ha che

$$\begin{aligned} H(HSP) &= HSP, \\ S(HSP) &\leq HSSP = HSP \end{aligned}$$

e

$$\begin{aligned} P(HSP) &\leq HPSP \leq HSPP \leq HSIPIPI \\ &= HSIP \leq HSHP \leq HHSP = HSP. \end{aligned}$$

Quindi per ogni K , $HSP(K)$ è chiuso rispetto ad H, S e P . Poiché $V(K)$ è la più piccola classe contenente K e chiusa rispetto ad H, S e P , si ha $V = HSP$. \square

Un'altra caratterizzazione dell'operatore V sarà data alla fine del paragrafo 11. La seguente versione del Teorema 8.6 di Birkhoff è utile nello studio delle varietà.

Teorema 9.6. *Se K è una varietà, allora ogni elemento di K è isomorfo ad un prodotto sottodiretto di algebre sottodirettamente irriducibili di K .*

Corollario 9.7. *Una varietà è determinata dai suoi elementi sottodirettamente irriducibili.*

10 Termini ed algebre di termini. Algebre libere.

Data un'algebra \mathbf{A} , solitamente esistono molte funzioni - oltre alle operazioni fondamentali - che sono compatibili con le congruenze in \mathbf{A} e che "preservano" le sottoalgebre di \mathbf{A} . Le più ovvie tra queste funzioni si ottengono mediante la composizione delle operazioni fondamentali. Questo ci porta allo studio dei termini.

Definizione 10.1. Sia X un insieme di oggetti (distinti) chiamati *variabili*, e sia \mathcal{F} un tipo di algebre. L'insieme $T(X)$ di *termini di tipo \mathcal{F} su X* è il più piccolo insieme tale che

- (i) $X \cup \mathcal{F}_0 \subseteq T(X)$,
- (ii) se $p_1, \dots, p_n \in T(X)$ e $f \in \mathcal{F}_n$, allora la "stringa" $f(p_1, \dots, p_n) \in T(X)$.

Per un simbolo funzionale binario \cdot , preferiremo di solito scrivere $p_1 \cdot p_2$ piuttosto che $\cdot(p_1, p_2)$. Per $p \in T(X)$ scriveremo spesso $p(x_1, \dots, x_n)$ per indicare che le variabili che occorrono in p sono in $\{x_1, \dots, x_n\}$. Un termine p è *n-ario* se il numero di variabili che appaiono esplicitamente in p è $\leq n$.

ESEMPLI.

1. Sia \mathcal{F} costituito da un solo simbolo funzionale binario \cdot , e sia $X = \{x, y, z\}$. Allora

$$x, y, z, x \cdot y, y \cdot z, x \cdot (y \cdot z), (x \cdot y) \cdot z$$

sono alcuni dei termini su X .

2. Sia \mathcal{F} costituito da due simboli funzionali binari $+$ e \cdot , e sia X lo stesso insieme dell'esempio 1. Allora

$$x, y, z, x \cdot (y + z), (x \cdot y) + (x \cdot z)$$

sono termini su X .

3. I polinomi a coefficienti nel campo reale \mathbf{R} sono termini su \mathbb{R} , con \mathcal{F} costituito da $+$, \cdot , $-$ ed un simbolo funzionale nullario r per ogni $r \in \mathbb{R}$.

In algebra elementare si può spesso pensare ai polinomi a coefficienti in \mathbb{R} come funzioni di \mathbb{R}^n in \mathbb{R} per qualche n . Lo stesso si può dire per i termini.

Definizione 10.2. Dato un termine $p(x_1, \dots, x_n)$ di tipo \mathcal{F} su un insieme X e un'algebra \mathbf{A} di tipo \mathcal{F} , definiamo una funzione $p^{\mathbf{A}} : A^n \rightarrow A$ come segue:

(i) se p è una variabile x_i , allora

$$p^{\mathbf{A}}(a_1, \dots, a_n) = a_i$$

per $a_1, \dots, a_n \in A$, cioè $p^{\mathbf{A}}$ è la proiezione i -esima;

(ii) se p è della forma $f(p_1(x_1, \dots, x_n), \dots, p_k(x_1, \dots, x_n))$, dove $f \in \mathcal{F}_k$, allora

$$p^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{A}}(p_1^{\mathbf{A}}, \dots, p_k^{\mathbf{A}}(a_1, \dots, a_n)).$$

In particolare se $p = f \in \mathcal{F}$ allora $p^{\mathbf{A}} = f^{\mathbf{A}} \cdot p^{\mathbf{A}}$ è la *funzione di termine* su \mathbf{A} corrispondente al termine p (nel seguito ometteremo spesso l'apice \mathbf{A}).

Teorema 10.3. Per ogni linguaggio \mathcal{F} , qualunque siano le algebre \mathbf{A}, \mathbf{B} di tipo \mathcal{F} , valgono le seguenti proprietà.

(a) Siano p un termine n -ario di tipo \mathcal{F} e $\theta \in \text{Con } \mathbf{A}$, e supponiamo che $(a_i, b_i) \in \theta$ per $1 \leq i \leq n$. Allora

$$p^{\mathbf{A}}(a_1, \dots, a_n) \theta p^{\mathbf{A}}(b_1, \dots, b_n).$$

(b) Se p è un termine n -ario di tipo \mathcal{F} ed $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ è un omomorfismo, allora

$$\alpha p^{\mathbf{A}}(a_1, \dots, a_n) = p^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n)$$

per $a_1, \dots, a_n \in A$.

(c) Sia S è un sottoinsieme di A . Allora

$$\text{Sg}(S) = \{p^{\mathbf{A}}(a_1, \dots, a_n) : p \text{ è un termine } n\text{-ario di tipo } \mathcal{F}, \\ n < \omega, a_1, \dots, a_n \in S\}.$$

Dimostrazione. Dato un termine p , definiamo la lunghezza $l(p)$ di p come il numero di occorrenze in p di simboli operazionali n -ari, per $n \geq 1$. Osserviamo che $l(p) = 0$ se e solo se $p \in X \cup \mathcal{F}_0$.

(a) Procediamo per induzione su $l(p)$. Se $l(p) = 0$, allora o $p = x_i$ per qualche i , e quindi

$$(p^{\mathbf{A}}(a_1, \dots, a_n), p^{\mathbf{A}}(b_1, \dots, b_n)) = (a_i, b_i) \in \theta,$$

oppure $p = a$ per qualche $a \in \mathcal{F}_0$, da cui

$$(p^{\mathbf{A}}(a_1, \dots, a_n), p^{\mathbf{A}}(b_1, \dots, b_n)) = (a^{\mathbf{A}}, a^{\mathbf{A}}) \in \theta.$$

Supponiamo ora che $l(p) > 0$ e che l'asserto sia vero per ogni termine q di lunghezza $l(q) < l(p)$. Allora sappiamo che p è della forma

$$f(p_1(x_1, \dots, x_n), \dots, p_k(x_1, \dots, x_n)),$$

e poiché $l(p_i) < l(p)$, abbiamo, per $1 \leq i \leq k$,

$$(p_i^{\mathbf{A}}(a_1, \dots, a_n), p_i^{\mathbf{A}}(b_1, \dots, b_n)) \in \theta.$$

Allora

$$(p^{\mathbf{A}}(a_1, \dots, a_n), p^{\mathbf{A}}(b_1, \dots, b_n)) \in \theta.$$

(b) Anche in questo caso l'asserto si prova in maniera abbastanza semplice ragionando per induzione su $l(p)$.

(c) Con riferimento al paragrafo 3 si prova, per induzione su k ($k \geq 1$), che

$$E^k(S) = \{p^{\mathbf{A}}(a_1, \dots, a_n) : p \text{ è un termine } n\text{-ario, } l(p) \leq k, \\ n < \omega, a_1, \dots, a_n \in S\},$$

e quindi

$$\text{Sg}(S) = \bigcup_{k < \omega} E^k(S) = \{p^{\mathbf{A}}(a_1, \dots, a_n) : p \text{ è un termine } n\text{-ario,} \\ n < \omega, a_1, \dots, a_n \in S\}.$$

□

Definizione 10.4. Sia \mathcal{F} un linguaggio e sia X un insieme. Se $T(X) \neq \emptyset$, allora l'algebra dei termini $\mathbf{T}(X)$ di tipo \mathcal{F} su X ha l'insieme $T(X)$ come universo e le operazioni fondamentali soddisfano la seguente condizione:

$$f^{\mathbf{T}(X)} : (p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n)$$

per $f \in \mathcal{F}_n$ e $p_i \in T(X)$, $1 \leq i \leq n$. ($\mathbf{T}(\emptyset)$ esiste se e solo se $\mathcal{F}_0 \neq \emptyset$.)

Osserviamo che $\mathbf{T}(X)$ è di fatto generata da X .

Definizione 10.5. Sia K una classe di algebre di tipo \mathcal{F} e sia $\mathbf{U}(X)$ un'algebra di tipo \mathcal{F} generata da X . Se per ogni $\mathbf{A} \in K$ e per ogni funzione $\alpha : X \rightarrow A$ esiste un omomorfismo

$$\beta : \mathbf{U}(X) \rightarrow \mathbf{A}$$

che estende α (cioè tale che $\beta(x) = \alpha(x)$ per $x \in X$), allora diremo che $\mathbf{U}(X)$ ha la *proprietà universale delle applicazioni per K su X* . Diremo inoltre che X è un *insieme di generatori liberi* di $\mathbf{U}(X)$, e che $\mathbf{U}(X)$ è *liberamente generata* da X .

Lemma 10.6. *Supponiamo che $\mathbf{U}(X)$ abbia la proprietà universale delle applicazioni per K su X . Allora, fissate $\mathbf{A} \in K$ ed $\alpha : X \rightarrow A$, esiste un'unica estensione β di α tale β sia un omomorfismo tra $\mathbf{U}(X)$ ed \mathbf{A} .*

Dimostrazione. Basta osservare che un omomorfismo è univocamente determinato dalla maniera con cui agisce su di un insieme di generatori del dominio (cfr. Teorema 6.2). \square

Il prossimo risultato afferma che per un dato numero cardinale m esiste, a meno d'isomorfismi, al più un'algebra in una classe K che ha la proprietà universale delle applicazioni per K su un insieme di generatori liberi di cardinalità m .

Teorema 10.7. *Siano $\mathbf{U}_1(X_1)$ ed $\mathbf{U}_2(X_2)$ due algebre in una classe K con la proprietà universale delle applicazioni per K su un insieme fissato. Se $|X_1| = |X_2|$, allora $\mathbf{U}_1(X_1) \cong \mathbf{U}_2(X_2)$.*

Dimostrazione. Osserviamo innanzitutto che la funzione identica

$$\iota_j : X_j \rightarrow X_j, \quad j = 1, 2,$$

ha la funzione identica di $\mathbf{U}_j(X_j)$ in sé come unica estensione ad un omomorfismo.

Sia ora

$$\alpha : X_1 \rightarrow X_2$$

una biezione. Allora abbiamo un omomorfismo

$$\mathbf{U}_1(X_1) \rightarrow \mathbf{U}_2(X_2)$$

che estende α , ed un omomorfismo

$$\gamma : \mathbf{U}_2(X_2) \rightarrow \mathbf{U}_1(X_1)$$

che estende α^{-1} . Poiché $\beta \circ \gamma$ è un endomorfismo di $\mathbf{U}_2(X_2)$ che estende ι_2 , allora $\beta \circ \gamma$ è l'identità di $\mathbf{U}_2(X_2)$. Analogamente si prova che $\gamma \circ \beta$ è l'identità di $\mathbf{U}_1(X_1)$. Ne segue che l'omomorfismo β è biiettivo e pertanto $\mathbf{U}_1(X_1) \cong \mathbf{U}_2(X_2)$. \square

Teorema 10.8. *Per ogni linguaggio \mathcal{F} e per ogni insieme non vuoto X di variabili, se $\mathcal{F}_0 = \emptyset$, l'algebra dei termini $\mathbf{T}(X)$ ha la proprietà universale delle applicazioni per la classe di tutte le algebre di tipo \mathcal{F} su X .*

Dimostrazione. Sia $\alpha : X \rightarrow A$ un'applicazione, dove \mathbf{A} è di tipo \mathcal{F} . Definiamo

$$\beta : T(X) \rightarrow A$$

ricorsivamente mediante le seguenti posizioni:

$$\beta x = \alpha x$$

per $x \in X$,

$$\beta(f(p_1, \dots, p_n)) = f^{\mathbf{A}}(\beta p_1, \dots, \beta p_n)$$

per $p_1, \dots, p_n \in T(X)$ e $f \in \mathcal{F}_n$. Allora $\beta(p(x_1, \dots, x_n)) = p^{\mathbf{A}}(\alpha x_1, \dots, \alpha x_n)$, e β è l'omomorfismo che estende α che cercavamo. \square

Dunque, data una classe di algebre K , le algebre dei termini sono esempi di algebre con la proprietà universale delle applicazioni per K . Per studiare le proprietà delle classi di algebre si cerca spesso di individuare particolari tipi di algebre, all'interno di dette classi, che siano in grado di fornire le informazioni desiderate. Le algebre direttamente indecomponibili e quelle sottodirettamente irriducibili sono i due esempi già incontrati. Per trovare algebre con la proprietà universale delle applicazioni per K , che siano più significative, introdurremo le algebre K -libere. Sfortunatamente non tutte le classi contengono algebre con la proprietà universale delle applicazioni. Proveremo, però, che ogni classe K , chiusa rispetto ad I , S e P , contiene algebre K -libere. Per molte classi risulta difficile dare una descrizione completa di tali algebre; comunque la maggior parte delle applicazioni delle algebre K -libere, derivano direttamente dalla proprietà universale delle applicazioni, dalla loro stessa esistenza nelle varietà, e dalle loro relazioni con le identità che valgono in K (che esamineremo nel prossimo paragrafo). Il ruolo delle algebre libere è di fondamentale importanza nello sviluppo degli argomenti che stiamo trattando. Ad esempio useremo le algebre libere per provare che le varietà sono classi definite mediante equazioni (Birkhoff), per dare utili caratterizzazioni (condizioni di Mal'cev) di importanti proprietà delle varietà, e per provare che ogni varietà non banale contiene un'algebra semplice non banale (Magari).

Definizione 10.9. Sia K una famiglia di algebre di tipo \mathcal{F} . Dato un insieme X di variabili, definiamo la cangrenza $\theta_K(X)$ su $\mathbf{T}(X)$ come segue:

$$\theta_K(X) = \bigcap \Phi_K(X),$$

dove

$$\Phi_K(X) = \{\phi \in \text{Con } \mathbf{T}(X) : \mathbf{T}(X)/\phi \in IS(K)\};$$

e successivamente definiamo $\mathbf{F}_K(\overline{X})$, l'algebra K -libera su \overline{X} , come

$$\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\theta_K(X),$$

dove

$$\overline{X} = X/\theta_K(X).$$

Per $x \in X$ scriveremo \bar{x} per indicare la classe $x/\theta_K(X)$, e per $p = p(x_1, \dots, x_n) \in T(X)$ scriveremo \bar{p} per $p^{\mathbf{F}_K(\overline{X})}(\bar{x}_1, \dots, \bar{x}_n)$. Se X è finito, diciamo $X = \{x_1, \dots, x_n\}$, scriveremo spesso $\mathbf{F}_K(\bar{x}_1, \dots, \bar{x}_n)$ invece di $\mathbf{F}_K(\overline{X})$. $\mathbf{F}_K(\overline{X})$ è il sostegno di $\mathbf{F}_K(\overline{X})$.

Osservazioni.

- (1) $\mathbf{F}_K(\overline{X})$ esiste sse esiste $\mathbf{T}(X)$ sse $X \neq \emptyset$ o $\mathcal{F}_0 \neq \emptyset$.
- (2) Se $\mathbf{F}_K(\overline{X})$ esiste, allora - poiché X genera $\mathbf{T}(X)$ - \overline{X} è un insieme di generatori di $\mathbf{F}_K(\overline{X})$.
- (3) Se $\mathcal{F}_0 \neq \emptyset$, allora l'algebra $\mathbf{F}_K(\overline{\emptyset})$ è spesso chiamata *oggetto iniziale*.
- (4) Se $K = \emptyset$ o K è costituita esclusivamente da algebre banali, allora $\mathbf{F}_K(\overline{X})$ è un'algebra banale, essendo $\theta_K(X) = \nabla$.
- (5) Se K ha un'algebra non banale \mathbf{A} e $\mathbf{T}(X)$ esiste, allora elementi distinti x, y di X possono essere separati da un omomorfismo $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ e quindi $X \cap (x/\theta_K(X)) = \{x\}$. In tal caso $|\overline{X}| = |X|$.
- (6) Se $|X| = |Y|$ e $\mathbf{T}(X)$ esiste, allora chiaramente $\mathbf{F}_K(\overline{X}) \cong \mathbf{F}_K(\overline{Y})$ tramite un isomorfismo che manda \overline{X} in \overline{Y} e $\mathbf{T}(X) \cong \mathbf{T}(Y)$ tramite un isomorfismo che manda X in Y . Pertanto $\mathbf{F}_K(\overline{X})$ è determinata, a meno d'isomorfismi, da K e $|X|$.

Teorema 10.10. (Birkhoff). *Supponiamo che esista $\mathbf{T}(X)$. Allora $\mathbf{F}_K(\overline{X})$ ha la proprietà universale delle applicazioni per K su \overline{X} .*

Dimostrazione. Siano $\mathbf{A} \in K$ ed α una funzione da \overline{X} ad \mathbf{A} . Sia $\nu : \mathbf{T}(X) \rightarrow \mathbf{F}_K(\overline{X})$ l'omomorfismo naturale. Allora $\alpha \circ \nu$ immerge X in \mathbf{A} e quindi per la proprietà universale delle applicazioni di $\mathbf{T}(X)$, esiste un omomorfismo $\mu : \mathbf{T}(X) \rightarrow \mathbf{A}$ che estende $\alpha \circ \nu|_X$. Dalla definizione di $\theta_K(X)$ segue

subito che $\theta_K(X) \subseteq \ker \mu$ ($\ker \mu \in \Phi_K(X)$). Allora esiste un omomorfismo $\beta : \mathbf{F}_K(\overline{X}) \rightarrow \mathbf{A}$ tale che $\mu = \beta \circ \nu$ e $\ker \nu = \theta_K(X)$. Ma allora, per $x \in X$,

$$\begin{aligned}\beta(\overline{x}) &= \beta \circ \nu(x) \\ &= \mu(x) \\ &= \alpha \circ \nu(x) \\ &= \alpha(\overline{x}),\end{aligned}$$

e quindi β estende α . Pertanto $\mathbf{F}_K(\overline{X})$ ha la proprietà universale delle applicazioni per K su \overline{X} . \square

Corollario 10.11. *Se K è una classe di algebre di tipo \mathcal{F} ed $\mathbf{A} \in K$, allora per un insieme X sufficientemente grande, $\mathbf{A} \in H(\mathbf{F}_K(\overline{X}))$.*

Dimostrazione. Scegliamo $|X| \geq |A|$ e sia

$$\alpha : \overline{X} \rightarrow A$$

un'applicazione suriettiva. Allora

$$\beta : \mathbf{F}_K(\overline{X}) \rightarrow \mathbf{A}$$

è un omomorfismo che estende α . \square

In generale $\mathbf{F}_K(\overline{X})$ non è isomorfa ad un elemento di K , ma può essere immersa in un prodotto di elementi di K .

Teorema 10.12. (Birkhoff). *Supponiamo che $\mathbf{T}(X)$ esista. Allora per $K \neq \emptyset$, $\mathbf{F}_K(\overline{X}) \in ISP(K)$. Allora se K è chiusa rispetto ad I , S e P - in particolare se K è una varietà - $\mathbf{F}_K(\overline{X}) \in K$.*

Dimostrazione. Poiché $\theta_K(X) = \bigcap \Phi_K(X)$, segue che

$$\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\theta_K(X) \in IP_S(\{\mathbf{T}(X)/\theta : \theta \in \Phi_K(X)\}),$$

e quindi

$$\mathbf{F}_K(\overline{X}) \in IP_SIS(K).$$

Ne segue, per il Lemma 9.2 e poiché $P_S \leq SP$,

$$\mathbf{F}_K(\overline{X}) \in ISP(K).$$

\square

Da un precedente teorema di Birkhoff sappiamo che se una varietà contiene un'algebra non banale, allora essa deve contenere anche un'algebra non banale sottodirettamente irriducibile. Il prossimo risultato mostra che una tale varietà deve anche contenere un'algebra semplice non banale.

Teorema 10.13. (Magari). *Data una varietà V dotata di un elemento non banale, V contiene un'algebra semplice non banale.*

Dimostrazione. Sia $X = \{x, y\}$ e sia

$$S = \{p(\bar{x}) : p \in T(\{x\})\},$$

un sottoinsieme di $F_V(\bar{X})$. Supponiamo innanzitutto che $\Theta(S) \neq \nabla$ in $\text{Con } \mathbf{F}_V(\bar{X})$. Allora per il Lemma di Zorn esiste un elemento massimale in $[\Theta(S), \nabla] - \{\nabla\}$. Infatti si prova facilmente che, per $\theta \in [\Theta(S), \nabla]$,

$$\theta = \nabla \quad \text{sse} \quad (\bar{x}, \bar{y}) \in \theta.$$

Sia θ_0 un elemento massimale in $[\Theta(S), \nabla] - \{\nabla\}$. Allora $\mathbf{F}_V(\bar{X})/\theta_0$ è un'algebra semplice per il Teorema 8.9, ed è in V .

Se, comunque, $\Theta(S) = \nabla$, poiché Θ è un operatore di chiusura algebrica per il Teorema 5.5, si ha che per qualche sottoinsieme finito S_0 di S avremo $(\bar{x}, \bar{y}) \in \Theta(S_0)$. Sia \mathbf{S} la sottoalgebra di $\mathbf{F}_V(\bar{X})$ di sostegno S (si osservi che $S = \text{Sg}(\{\bar{x}\})$ per il Teorema 10.3(c)). Poiché V è non banale, avremo $\bar{x} \neq \bar{y}$ in $\mathbf{F}_V(\bar{X})$, e poiché $(\bar{x}, \bar{y}) \in \Theta(S)$, segue che S è non banale.

Ora diciamo che $\nabla_S = \Theta(S_0)$, dove per Θ s'intende - in questo caso - l'opportuno operatore di chiusura su S . Per provare quest'uguaglianza, sia $p(\bar{x}) \in S$ e sia

$$\alpha : \mathbf{F}_V(\bar{X}) \rightarrow \mathbf{S}$$

l'omomorfismo definito da

$$\begin{aligned} \alpha(\bar{x}) &= \bar{x} \\ \alpha(\bar{y}) &= p(\bar{x}). \end{aligned}$$

Essendo

$$(\bar{x}, \bar{y}) \in \Theta(S_0) \quad \text{in } \mathbf{F}_V(\bar{X}),$$

segue dal Teorema 6.6 che

$$(\bar{x}, p(\bar{x})) \in \Theta(S_0) \quad \text{in } \mathbf{S}$$

e

$$\alpha(S_0) = S_0.$$

Quindi $\nabla_S = \Theta(S_0)$, come dicevamo.

Ora usando il Lemma di Zorn possiamo trovare una congruenza massimale θ su \mathbf{S} , essendo ∇_S finitamente generata. Pertanto \mathbf{S}/θ è un'algebra semplice in V . \square

Passiamo ora ad un'altra applicazione delle algebre libere.

Definizione 10.14. Un'algebra \mathbf{A} è *localmente finita* se ogni sua sottoalgebra finitamente generata è finita. Una classe K di algebre è *localmente finita* se ogni suo elemento è localmente finito.

Teorema 10.15. *Una varietà V è localmente finita se e solo se*

$$|X| < \omega \Rightarrow |F_V(\overline{X})| < \omega.$$

Dimostrazione. Poiché \overline{X} genera $\mathbf{F}_V(\overline{X})$, è chiaro che la condizione è necessaria. Per provare la sufficienza, sia \mathbf{A} un'algebra finitamente generata di V , e sia $B \subseteq \mathbf{A}$ un insieme finito di generatori. Scegliamo X in modo da avere una biezione

$$\alpha : \overline{X} \rightarrow B.$$

Estendiamo α ad un omomorfismo

$$\beta : \mathbf{F}_V(\overline{X}) \rightarrow \mathbf{A}.$$

Poiché $\beta(\mathbf{F}_V(\overline{X}))$ è una sottoalgebra di \mathbf{A} contenente B , essa deve coincidere con \mathbf{A} . Pertanto β è suriettiva e, essendo $\mathbf{F}_V(\overline{X})$ finita, tale è anche \mathbf{A} . \square

Teorema 10.16. *Sia K un insieme finito di algebre finite. Allora $V(K)$ è una varietà localmente finita.*

Dimostrazione. Innanzitutto verifichiamo che $P(K)$ è localmente finita. A tale scopo definiamo una relazione d'equivalenza \sim su $T(\{x_1, \dots, x_n\})$: $p \sim q$ se le funzioni di termine corrispondenti a p e q sono uguali per ogni elemento di K . Usando le condizioni di finitezza si prova che \sim ha un numero finito di classi d'equivalenza. Questo, insieme al Teorema 10.3(c), è sufficiente. Segue allora facilmente che V è localmente finita perché ogni elemento finitamente generato di $HSP(K)$ è immagine omomorfa di un elemento finitamente generato di $SP(K)$. \square

11 Identità, algebre libere, il Teorema di Birkhoff.

Uno dei più importanti risultati di Birkhoff afferma che le classi di algebre definite mediante identità sono esattamente quelle chiuse rispetto ad H , S e P . In questo paragrafo studieremo le identità e le loro relazioni con le algebre libere, ed inoltre vedremo molte loro applicazioni, incluso il Teorema di Birkhoff.

Abbiamo già visto alcuni particolari esempi di identità come la proprietà associativa, quella commutativa etc. Formalizziamo ora la nozione generale di identità.

Definizione 11.1. Un'identità di tipo \mathcal{F} su X è un'espressione della forma

$$p \approx q$$

dove $p, q \in T(X)$. Indicheremo con $\text{Id}(X)$ l'insieme delle identità di tipo \mathcal{F} su X . Diremo che un'algebra \mathbf{A} di tipo \mathcal{F} *soddisfa* un'identità

$$p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n)$$

(o che l'identità è *vera in* \mathbf{A} , o *vale in* \mathbf{A}), e scriveremo

$$\mathbf{A} \models p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n),$$

o, più brevemente,

$$\mathbf{A} \models p \approx q$$

se per ogni scelta di $a_1, \dots, a_n \in A$ si ha

$$p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n).$$

Si dice che una classe K di algebre soddisfa $p \approx q$, e si scrive

$$K \models p \approx q,$$

se ogni elemento di K soddisfa $p \approx q$. Se Σ è un insieme di identità, diremo che K soddisfa Σ , e scriveremo

$$K \models \Sigma,$$

se $K \models p \approx q$ per ogni $p \approx q \in \Sigma$. Fissata una classe K ed un insieme di identità Σ , poniamo

$$\text{Id}_K(X) = \{p \approx q \in \text{Id}(X) : K \models p \approx q\}.$$

Useremo il simbolo $\not\models$ per “non soddisfa”.

Possiamo riformulare la precedente definizione di soddisfacimento usando la nozione di omomorfismo.

Lemma 11.2. *Se K è una classe di algebre di tipo \mathcal{F} e $p \approx q$ è un'identità di tipo \mathcal{F} su X , allora*

$$K \models p \approx q$$

se e solo se per ogni $\mathbf{A} \in K$ e per ogni omomorfismo $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ abbiamo

$$\alpha p = \alpha q.$$

Dimostrazione. (\Rightarrow) Siano $p = p(x_1, \dots, x_n), q = q(x_1, \dots, x_n)$. Supponiamo che $K \models p \approx q$, $\mathbf{A} \in K$, e sia $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ un omomorfismo. Allora

$$\begin{aligned} p^{\mathbf{A}}(\alpha x_1, \dots, \alpha x_n) &= q^{\mathbf{A}}(\alpha x_1, \dots, \alpha x_n) \\ \Rightarrow \alpha p^{\mathbf{T}(X)}(x_1, \dots, x_n) &= \alpha q^{\mathbf{T}(X)}(x_1, \dots, x_n) \\ \Rightarrow \alpha p &= \alpha q. \end{aligned}$$

(\Leftarrow) Scegliamo $\mathbf{A} \in K$ ed $a_1, \dots, a_n \in A$. Per la proprietà universale delle applicazioni di $\mathbf{T}(X)$ esiste un omomorfismo $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ tale che

$$\alpha x_i = a_i, \quad 1 \leq i \leq n.$$

Ma allora

$$\begin{aligned} p^{\mathbf{A}}(a_1, \dots, a_n) &= p^{\mathbf{A}}(\alpha x_1, \dots, \alpha x_n) \\ &= \alpha p \\ &= \alpha q \\ &= q^{\mathbf{A}}(\alpha x_1, \dots, \alpha x_n) \\ &= q^{\mathbf{A}}(a_1, \dots, a_n), \end{aligned}$$

quindi $K \models p \approx q$. □

Lemma 11.3. *Per ogni classe K di tipo \mathcal{F} , tutte le classi $K, I(K), S(K), H(K), P(K)$ e $V(K)$ soddisfano le stesse identità su ogni insieme di variabili X .*

Dimostrazione. K ed $I(K)$ banalmente soddisfano le stesse identità. Poiché

$$I \leq IS, \quad I \leq H, \quad I \leq IP,$$

dobbiamo avere

$$\text{Id}_K(X) \supseteq \text{Id}_{S(K)}(X), \text{Id}_{H(K)}(X), \text{Id}_{P(K)}(X).$$

Supponiamo che

$$K \models p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n).$$

Allora, se $\mathbf{B} \leq \mathbf{A} \in K$ e $b_1, \dots, b_n \in B$, poiché $b_1, \dots, b_n \in A$, abbiamo

$$p^{\mathbf{A}}(b_1, \dots, b_n) = q^{\mathbf{A}}(b_1, \dots, b_n),$$

da cui segue

$$p^{\mathbf{B}}(b_1, \dots, b_n) = q^{\mathbf{B}}(b_1, \dots, b_n)$$

e quindi

$$\mathbf{B} \models p \approx q.$$

Pertanto $\text{Id}_K(X) = \text{Id}_{S(K)}(X)$.

Supponiamo ora che $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ sia un epimorfismo, con $\mathbf{A} \in K$. Se $b_1, \dots, b_n \in B$, scegliamo $a_1, \dots, a_n \in A$ in modo che

$$\alpha(a_1) = b_1, \dots, \alpha(a_n) = b_n.$$

Allora da

$$p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$$

segue

$$\alpha p^{\mathbf{A}}(a_1, \dots, a_n) = \alpha q^{\mathbf{A}}(a_1, \dots, a_n),$$

e quindi

$$p^{\mathbf{B}}(b_1, \dots, b_n) = q^{\mathbf{B}}(b_1, \dots, b_n).$$

Allora

$$\mathbf{B} \models p \approx q,$$

cioè

$$\text{Id}_K(X) = \text{Id}_{H(K)}(X).$$

Infine consideriamo una famiglia $\{A_i\}_{i \in I}$ di algebre di K . Allora per $a_1, \dots, a_n \in A = \prod_{i \in I} A_i$ abbiamo

$$p^{\mathbf{A}^i}(a_1(i), \dots, a_n(i)) = q^{\mathbf{A}^i}(a_1(i), \dots, a_n(i));$$

ne segue

$$p^{\mathbf{A}}(a_1, \dots, a_n)(i) = q^{\mathbf{A}}(a_1, \dots, a_n)(i), \quad \forall i \in I$$

e quindi

$$p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n).$$

Allora

$$\text{Id}_K(X) = \text{Id}_{P(K)}(X).$$

Essendo $V = HSP$ (cfr. Teorema 9.5), la dimostrazione è completa. \square

Teorema 11.4. *Sia K una classe di algebre di tipo \mathcal{F} , e siano $p, q \in T(X)$ termini di tipo \mathcal{F} . Allora*

$$\begin{aligned} & K \models p \approx q \\ \Leftrightarrow & \mathbf{F}_K(\overline{X}) \models p \approx q \\ \Leftrightarrow & \bar{p} = \bar{q} \quad \text{in} \quad \mathbf{F}_K(\overline{X}) \\ \Leftrightarrow & (p, q) \in \theta_K(X). \end{aligned}$$

Dimostrazione. Poniamo $\mathbf{F} = \mathbf{F}_K(\overline{X})$, $p = p(x_1, \dots, x_n)$, $q = q(x_1, \dots, x_n)$, e sia

$$\nu : \mathbf{T}(X) \rightarrow \mathbf{F}$$

l'omomorfismo naturale. Chiaramente $K \models p \approx q$ implica $\mathbf{F} \models p \approx q$, essendo $\mathbf{F} \in ISP(K)$.

Supponiamo ora che $\mathbf{F} \models p \approx q$. Allora

$$p^{\mathbf{F}}(\overline{x}_1, \dots, \overline{x}_n) = q^{\mathbf{F}}(\overline{x}_1, \dots, \overline{x}_n),$$

da cui segue $\overline{p} = \overline{q}$. Sia ora $\overline{p} = \overline{q}$ in \mathbf{F} . Allora

$$\nu(p) = \overline{p} = \overline{q} = \nu(q),$$

e quindi

$$(p, q) \in \ker \nu = \theta_K(X).$$

Infine supponiamo che $(p, q) = \theta_K(X)$. Se $\mathbf{A} \in K$ e $a_1, \dots, a_n \in A$, scegliamo $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ in modo che $\alpha x_i = a_i$, $1 \leq i \leq n$. Poiché $\ker \alpha \in \Phi_K(X)$, abbiamo

$$\ker \alpha \supseteq \ker \nu = \theta_K(X),$$

e quindi segue l'esistenza di un omomorfismo $\beta : \mathbf{F} \rightarrow \mathbf{A}$ tale che $\alpha = \beta \circ \nu$. Allora

$$\alpha(p) = \beta \circ \nu(p) = \beta \circ \nu(q) = \alpha(q).$$

Ne segue

$$K \models p \approx q$$

per il Lemma 11.2. □

Corollario 11.5. *Sia K una classe di algebre di tipo \mathcal{F} , e supponiamo che $p, q \in T(X)$. Allora per ogni insieme di variabili Y - con $|Y| \geq |X|$ - si ha:*

$$K \models p \approx q \quad \text{sse} \quad \mathbf{F}_K(\overline{Y}) \models p \approx q.$$

Dimostrazione. L'implicazione " \Rightarrow " è ovvia, essendo $\mathbf{F}_K(\overline{Y}) \in ISP(K)$. Per provare l'altra implicazione scegliamo $X_0 \supseteq X$ in modo che $|X_0| = |Y|$. Allora

$$\mathbf{F}_K(\overline{X}_0) \cong \mathbf{F}_K(\overline{Y}),$$

e poiché

$$K \models p \approx q \quad \text{sse} \quad \mathbf{F}_K(\overline{X}_0) \models p \approx q,$$

dal Teorema 11.4 segue che

$$K \models p \approx q \quad \text{sse} \quad \mathbf{F}_K(\overline{Y}) \models p \approx q.$$

□

Corollario 11.6. *Siano K una classe di algebre di tipo \mathcal{F} e X un insieme di variabili. Allora, per ogni insieme infinito Y di variabili,*

$$\text{Id}_K(X) = \text{Id}_{\mathbf{F}_K(\overline{Y})}(X).$$

Dimostrazione. Per $p \approx q \in \text{Id}_K(X)$, diciamo

$$p = p(x_1, \dots, x_n), \quad q = q(x_1, \dots, x_n),$$

abbiamo $p, q \in T(\{x_1, \dots, x_n\})$. Poiché $|\{x_1, \dots, x_n\}| < |Y|$, per il Teorema 11.5

$$K \models p \approx q \quad \text{sse} \quad \mathbf{F}_K(\overline{Y}) \models p \approx q,$$

e l'asserto è provato. □

Come abbiamo visto nel paragrafo 1, molte delle classi di algebre più note sono definite mediante identità.

Definizione 11.7. Sia Σ un insieme di identità di tipo \mathcal{F} , e definiamo $M(\Sigma)$ come la classe delle algebre che soddisfano Σ . Una classe K di algebre è una *classe equazionale* se esiste un insieme Σ di identità tale che $K = M(\Sigma)$. In tal caso diremo che K è *definita*, o *assiomatizzata*, da Σ .

Lemma 11.8. *Se V è una varietà e X è un insieme infinito di variabili, allora $V = M(\text{Id}_V(X))$.*

Dimostrazione. Sia $V' = M(\text{Id}_V(X))$. Chiaramente V' è una varietà per il Lemma 11.3, $V' \supseteq V$, e $\text{Id}_{V'}(X) = \text{Id}_V(X)$.

Allora, per il Teorema 11.4,

$$\mathbf{F}_{V'}(\overline{X}) = \mathbf{F}_V(\overline{X}).$$

Ora, dato un insieme infinito Y di variabili, abbiamo per il Corollario 11.6

$$\text{Id}_{V'}(Y) = \text{Id}_{\mathbf{F}_{V'}(\overline{X})}(Y) = \text{Id}_{\mathbf{F}_V(\overline{X})}(Y) = \text{Id}_V(Y).$$

Pertanto, ancora per il Teorema 11.4,

$$\theta_{V'}(Y) = \theta_V(Y);$$

e quindi

$$\mathbf{F}_{V'}(\overline{Y}) = \mathbf{F}_V(\overline{Y}).$$

Ora per $\mathbf{A} \in V'$ abbiamo (per il Corollario 10.11), per un opportuno Y infinito,

$$\mathbf{A} \in H(\mathbf{F}_{V'}(\overline{Y}));$$

ne segue

$$\mathbf{A} \in H(\mathbf{F}_V(\overline{Y})),$$

e quindi $\mathbf{A} \in V$.

Ne segue che $V' \subseteq V$ e pertanto $V' = V$. \square

Ora abbiamo gli strumenti necessari per dimostrare il Teorema di Birkhoff.

Teorema 11.9. (Birkhoff). *K è una classe equazionale se e solo se K è una varietà.*

Dimostrazione. (\Rightarrow) Supponiamo che $K = M(\Sigma)$. Allora, per il Lemma 11.3, $V(K) \models \Sigma$; quindi $V(K) \subseteq M(\Sigma)$.

Allora $V(K) = K$, cioè K è una varietà.

(\Leftarrow) Segue dal Lemma 11.8. \square

Grazie al Teorema 11.4 possiamo anche ottenere un'estensione del Teorema 10.12.

Corollario 11.10. *Sia K una classe di algebre di tipo \mathcal{F} . Se $\mathbf{T}(X)$ esiste e K' è una qualunque classe di algebre tale che $K \subseteq K' \subseteq V(K)$, allora*

$$\mathbf{F}_{K'}(\overline{X}) = \mathbf{F}_K(\overline{X}).$$

In particolare si ha

$$\mathbf{F}_{K'}(\overline{X}) \in ISP(K).$$

Dimostrazione. Poiché $\text{Id}_K(X) = \text{Id}_{V(K)}(X)$ per il Lemma 11.3, segue che $\text{Id}_K(X) = \text{Id}_{K'}(X)$. Allora $\theta_{K'}(X) = \theta_K(X)$, da cui segue $\mathbf{F}_{K'}(\overline{X}) = \mathbf{F}_K(\overline{X})$. L'ultima parte dell'asserto segue poi dal Teorema 10.12. \square

Teorema 11.11. *Sia K una classe non vuota di algebre di tipo \mathcal{F} . Allora, per qualche cardinale m , se $|X| \geq m$ si ha*

$$\mathbf{F}_K(\overline{X}) \in IP_S(K).$$

Dimostrazione. Per prima cosa scegliamo un sottoinsieme K^* di K tale che per ogni X , $\text{Id}_{K^*}(X) = \text{Id}_K(X)$. Ad esempio si può trovare un tale K^* prendendo un insieme infinito Y di variabili e poi selezionando, per ogni identità $p \approx q$ in $\text{Id}(Y) - \text{Id}_K(Y)$, un'algebra $\mathbf{A} \in K$ tale che $\mathbf{A} \not\models p \approx q$. Sia m un maggiorante infinito di $\{|A| : \mathbf{A} \in K^*\}$ (tale m deve esistere, essendo K^* un insieme).

Sia ora, per qualunque X ,

$$\Psi_{K^*}(X) = \{\phi \in \text{Con } \mathbf{T}(X) : \mathbf{T}(X)/\phi \in I(K^*)\}.$$

Allora $\Psi_{K^*}(X) \subseteq \Phi_{K^*}(X)$, da cui si ha che $\bigcap \Psi_{K^*}(X) \supseteq \theta_{K^*}(X)$.

Per provare l'uguaglianza di queste due congruenze per $|X| \geq m$, supponiamo $(p, q) \notin \theta_{K^*}(X)$. Allora $K^* \not\approx p \approx q$ per il Teorema 11.4; pertanto per qualche $\mathbf{A} \in K^*$, $\mathbf{A} \not\approx p \approx q$. Se $p = p(x_1, \dots, x_n)$, $q = q(x_1, \dots, x_n)$, scegliamo $a_1, \dots, a_n \in A$ in modo che $p^{\mathbf{A}}(a_1, \dots, a_n) \neq q^{\mathbf{A}}(a_1, \dots, a_n)$. Poiché $|X| \geq |A|$, possiamo trovare una funzione $\alpha : X \rightarrow A$ che è suriettiva e tale che $\alpha x_i = a_i$, per ogni $i = 1, \dots, n$. Allora α può essere prolungata ad un epimorfismo $\beta : \mathbf{F}_{K^*}(\overline{X}) \rightarrow \mathbf{A}$, e $\beta(p) \neq \beta(q)$.

Quindi $(p, q) \notin \ker \beta \in \Psi_{K^*}(X)$, cioè $(p, q) \notin \bigcap \Psi_{K^*}(X)$. Di conseguenza $\bigcap \Psi_{K^*}(X) = \theta_{K^*}(X)$. Essendo $\mathbf{F}_K(\overline{X}) = \mathbf{F}_{K^*}(\overline{X})$ per il Teorema 11.4, segue che $\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\bigcap \Psi_{K^*}(X)$. Allora $\mathbf{F}_K(\overline{X}) \in IP_S(K^*) \subseteq IP_S(K)$. \square

Teorema 11.12. $V = HP_S$.

Dimostrazione. Poiché $P_S \leq SP$, si ha

$$HP_S \leq HSP = V.$$

Data una classe K di algebre ed un insieme X sufficientemente grande, abbiamo

$$\mathbf{F}_{V(K)}(\overline{X}) \in IP_S(K)$$

per il teorema precedente; dunque

$$V(K) \subseteq HP_S(K)$$

per il Corollario 10.11. Ne segue l'asserto. \square

12 Condizioni di Mal'cev.

Un importante filone di ricerca fu inaugurato da Mal'cev negli anni '50 del secolo scorso, allorché mostrò il legame esistente tra la permutabilità delle congruenze per tutte le algebre in una varietà V e l'esistenza di un termine ternario p tale che V soddisfi certe identità che coinvolgono p . La caratterizzazione di proprietà delle varietà mediante l'esistenza di certi termini coinvolge delle identità che chiameremo *condizioni di Mal'cev*. Tale argomento è stato notevolmente sviluppato negli ultimi anni da Taylor.

Lemma 12.1. *Sia V una varietà di tipo \mathcal{F} , e siano*

$$p(x_1, \dots, x_m, y_1, \dots, y_n),$$

$$q(x_1, \dots, x_m, y_1, \dots, y_n)$$

termini tali che in $\mathbf{F} = \mathbf{F}_V(\overline{X})$, dove

$$X = \{x_1, \dots, x_m, y_1, \dots, y_n\},$$

si abbia

$$(p^{\mathbf{F}}(\overline{x}_1, \dots, \overline{x}_m, \overline{y}_1, \dots, \overline{y}_n), q^{\mathbf{F}}(\overline{x}_1, \dots, \overline{x}_m, \overline{y}_1, \dots, \overline{y}_n)) \in \Theta(\overline{y}_1, \dots, \overline{y}_n).$$

Allora

$$V \models p(x_1, \dots, x_m, y, \dots, y) \approx q(x_1, \dots, x_m, y, \dots, y).$$

Dimostrazione. L'omomorfismo

$$\alpha : \mathbf{F}_V(\overline{x}_1, \dots, \overline{x}_m, \overline{y}_1, \dots, \overline{y}_n) \rightarrow \mathbf{F}_V(\overline{x}_1, \dots, \overline{x}_m, \overline{y})$$

definito da

$$\alpha(\overline{x}_i) = \overline{x}_i, \quad 1 \leq i \leq m,$$

e

$$\alpha(\overline{y}_i) = \overline{y}, \quad 1 \leq i \leq n,$$

è tale che

$$\Theta(\overline{y}_1, \dots, \overline{y}_n) \subseteq \ker \alpha;$$

quindi

$$\alpha p(\overline{x}_1, \dots, \overline{x}_m, \overline{y}_1, \dots, \overline{y}_n) = \alpha q(\overline{x}_1, \dots, \overline{x}_m, \overline{y}_1, \dots, \overline{y}_n).$$

Allora

$$p(\overline{x}_1, \dots, \overline{x}_m, \overline{y}, \dots, \overline{y}) = q(\overline{x}_1, \dots, \overline{x}_m, \overline{y}, \dots, \overline{y})$$

in $\mathbf{F}_V(\overline{x}_1, \dots, \overline{x}_m, \overline{y})$, e quindi

$$V \models p(x_1, \dots, x_m, y, \dots, y) \approx q(x_1, \dots, x_m, y, \dots, y).$$

□

Teorema 12.2. (Mal'cev). *Sia V una varietà di tipo \mathcal{F} . La varietà V è congruenze-permutabile se e solo se esiste un termine $p(x, y, z)$ tale che*

$$V \models p(x, x, y) \approx y$$

e

$$V \models p(x, y, y) \approx x.$$

Dimostrazione. (\Rightarrow) Se V è congruenze-permutabile, allora in $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ si ha

$$(\bar{x}, \bar{z}) \in \Theta(\bar{x}, \bar{y}) \circ \Theta(\bar{y}, \bar{z}),$$

quindi

$$(\bar{x}, \bar{z}) \in \Theta(\bar{y}, \bar{z}) \circ \Theta(\bar{x}, \bar{y}).$$

Per il Lemma 12.1

$$V \models p(x, y, y) \approx x$$

e

$$V \models p(x, x, z) \approx z.$$

(\Leftarrow) Sia $\mathbf{A} \in V$ e siano $\phi, \psi \in \text{Con } \mathbf{A}$. Se

$$(a, b) \in \phi \circ \psi,$$

diciamo $a\phi c\psi b$, allora

$$b = p(c, c, b)\phi p(a, c, b)\psi p(a, b, b) = a,$$

quindi

$$(b, a) \in \phi \circ \psi.$$

Allora per il Teorema 5.9

$$\phi \circ \psi = \psi \circ \phi.$$

□

ESEMPLI.

- (1) I gruppi $(G, \cdot, {}^{-1}, 1)$ sono congruenze-permutabili; basta considerare il termine $p(x, y, z)$ dato da $x \cdot y^{-1} \cdot z$.
- (2) Gli anelli $(R, +, \cdot, -, 0)$ sono congruenze-permutabili, posto $p(x, y, z) = x - y + z$.
- (3) I quasigruppi $(Q, /, \cdot, \backslash)$ sono congruenze-permutabili. Si consideri il termine $p(x, y, z) = (x/(y \backslash y))$.

Teorema 12.3. *Supponiamo che V sia una varietà per la quale esiste un termine ternario $M(x, y, z)$ tale che*

$$V \models M(x, x, y) \approx M(x, y, x) \approx M(y, x, x) \approx x.$$

Allora V è congruenze-distributiva.

Dimostrazione. Siano $\phi, \psi, \chi \in \text{Con } \mathbf{A}$, con $\mathbf{A} \in V$. Se

$$(a, b) \in \phi \wedge (\psi \vee \chi)$$

allora $(a, b) \in \phi$ ed esistono c_1, \dots, c_n tali che

$$a\psi c_1\chi c_2 \dots \psi c_n\chi b.$$

Ma allora, essendo

$$M(a, c_i, b)\phi M(a, c_i, a) = a,$$

per ogni i abbiamo

$$a = M(a, a, b)(\phi \wedge \psi)M(a, c_1, b)(\phi \wedge \chi)M(a, c_2, b) \dots M(a, c_n, b)$$

$$(\phi \wedge \chi)M(a, b, b) = b,$$

e quindi

$$(a, b) \in (\phi \wedge \psi) \vee (\phi \wedge \chi).$$

Questo mostra dunque che

$$\phi \wedge (\psi \vee \chi) = (\phi \wedge \psi) \vee (\phi \wedge \chi).$$

Ne segue l'asserto. □

Ad esempio i reticoli sono congruenze-distributivi, essendo

$$M(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z).$$

Definizione 12.4. Diremo che una varietà V è *aritmetica* se è congruenze-distributiva e congruenze-permutabile.

Teorema 12.5. (Pixley). *Una varietà V è aritmetica se e solo se soddisfa le seguenti condizioni, tra loro equivalenti*

(a) *Esistono un termine p come nel Teorema 12.2 ed un termine M come nel Teorema 12.3.*

(b) *Esiste un termine $m(x, y, z)$ tale che*

$$V \models m(x, y, x) \approx m(x, y, y) \approx m(y, y, x) \approx x.$$

Dimostrazione. Se V è aritmetica allora esiste un termine p come nel Teorema 12.2. Sia $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ l'algebra libera, in V , liberamente generata da $\{\bar{x}, \bar{y}, \bar{z}\}$. Allora poiché

$$(\bar{x}, \bar{z}) \in \Theta(\bar{x}, \bar{z}) \cap [\Theta(\bar{x}, \bar{y}) \vee \Theta(\bar{y}, \bar{z})],$$

segue che

$$(\bar{x}, \bar{z}) \in [\Theta(\bar{x}, \bar{z}) \cap \Theta(\bar{x}, \bar{y})] \vee [\Theta(\bar{x}, \bar{z}) \cap \Theta(\bar{y}, \bar{z})];$$

quindi

$$(\bar{x}, \bar{z}) \in [\Theta(\bar{x}, \bar{z}) \cap \Theta(\bar{x}, \bar{y})] \circ [\Theta(\bar{x}, \bar{z}) \cap \Theta(\bar{y}, \bar{z})].$$

Scegliamo $M(\bar{x}, \bar{y}, \bar{z}) \in F_V(\bar{x}, \bar{y}, \bar{z})$ in modo che

$$\bar{x}[\Theta(\bar{x}, \bar{z}) \cap \Theta(\bar{x}, \bar{y})]M(\bar{x}, \bar{y}, \bar{z})[\Theta(\bar{x}, \bar{z}) \cap \Theta(\bar{y}, \bar{z})]\bar{z}.$$

Allora, per il Lemma 12.1,

$$V \models M(x, x, y) \approx M(x, y, x) \approx M(y, x, x) \approx x.$$

Se vale la (a), allora poniamo $m(x, y, z) = p(x, M(x, y, z), z)$. Infine se vale la (b), basta porre $p(x, y, z) = m(x, y, z)$ e $M(x, y, z) = m(x, m(x, y, z), z)$, ed usare i Teoremi 12.2 e 12.3. \square

ESEMPLI.

(1) Le algebre di Boole sono aritmetiche; si pone:

$$m(x, y, z) = (x \wedge z) \vee (x \wedge y' \wedge z') \vee (x' \wedge y' \wedge z).$$

(2) Le algebre di Heyting sono aritmetiche:

$$m(x, y, z) = [(x \rightarrow y) \rightarrow z] \wedge [(z \rightarrow y) \rightarrow x] \wedge [x \vee z].$$

Osserviamo che il Teorema 12.3 non è una condizione di Mal'cev perché è un'implicazione e non una caratterizzazione. Jónsson scoprì una condizione di Mal'cev per le varietà congruenze-distributive.

Teorema 12.6. (Jónsson). *Una varietà V è congruenze-distributiva se e solo se esiste un numero n e dei termini $p_0(x, y, z), \dots, p_n(x, y, z)$ tali che V soddisfi le condizioni seguenti:*

$$\begin{array}{ll} p_i(x, y, x) \approx x & 0 \leq i \leq n \\ p_0(x, y, z) \approx x, & p_n(x, y, z) \approx z \\ p_i(x, x, y) \approx p_{i+1}(x, x, y) & \text{per } i \text{ pari} \\ p_i(x, y, y) \approx p_{i+1}(x, y, y) & \text{per } i \text{ dispari} \end{array}$$

Dimostrazione. (\Rightarrow) Poiché

$$\Theta(\bar{x}, \bar{z}) \wedge [\Theta(\bar{x}, \bar{y}) \vee \Theta(\bar{y}, \bar{z})] = [\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{x}, \bar{y})] \vee [\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{y}, \bar{z})],$$

in $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ avremo

$$(\bar{x}, \bar{z}) \in [\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{x}, \bar{y})] \vee [\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{y}, \bar{z})].$$

Allora per qualche $p_1(\bar{x}, \bar{y}, \bar{z}), \dots, p_{n-1}(\bar{x}, \bar{y}, \bar{z}) \in F_V(\bar{x}, \bar{y}, \bar{z})$, si ha

$$\begin{aligned} & \bar{x}[\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{x}, \bar{y})]p_1(\bar{x}, \bar{y}, \bar{z}) \\ & p_1(\bar{x}, \bar{y}, \bar{z})[\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{y}, \bar{z})]p_2(\bar{x}, \bar{y}, \bar{z}) \\ & \quad \vdots \\ & p_{n-1}(\bar{x}, \bar{y}, \bar{z})[\Theta(\bar{x}, \bar{z}) \wedge \Theta(\bar{y}, \bar{z})]\bar{z}, \end{aligned}$$

e da queste seguono le condizioni dell'enunciato.

(\Leftarrow) Per $\phi, \psi, \chi \in \text{Con } \mathbf{A}$, dove $\mathbf{A} \in V$, dobbiamo provare che

$$\phi \wedge (\psi \vee \chi) \subseteq (\phi \wedge \psi) \vee (\phi \wedge \chi),$$

e quindi sia

$$(a, b) \in \phi \wedge (\psi \vee \chi).$$

Allora $(a, b) \in \phi$, e per qualche c_1, \dots, c_t si ha

$$a\psi c_1\chi \dots c_t\chi b.$$

Da ciò segue, per $0 \leq i \leq n$,

$$p_i(a, a, b)\psi p_i(a, c_1, b)\chi \dots p_i(a, c_t, b)\chi p_i(a, b, b);$$

quindi

$$p_i(a, a, b)(\phi \wedge \psi)p_i(a, c_1, b)(\phi \wedge \chi) \dots p_i(a, c_t, b)(\phi \wedge \chi)p_i(a, b, b),$$

e pertanto

$$p_i(a, a, b)[(\phi \wedge \psi) \vee (\phi \wedge \chi)]p_i(a, b, b),$$

$0 \leq i \leq n$. Allora, per le equazioni date nell'enunciato, si ha $a[(\phi \wedge \psi) \vee (\phi \wedge \chi)]b$, e V è congruenze-distributiva.

□

Dalle dimostrazioni dei Teoremi 12.2 e 12.6 si deduce facilmente il seguente risultato.

Teorema 12.7. *Una varietà V è congruenze-permutabile (rispettivamente, congruenze-distributiva) se e solo se $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ ha congruenze permutabili (rispettivamente, distributive).*

Definizione 12.8. Un termine ternario p soddisfacente le condizioni del Teorema 12.2 per una varietà V , si dice un *termine di Mal'cev* per V , un termine ternario M come descritto nel Teorema 12.3 è un *termine maggioritario* per V , e un termine ternario m come descritto nel Teorema 12.5 si dice un *termine $\frac{2}{3}$ -minoritario* per V .

13 Il Centro di un'algebra.

Smith introdusse una generalizzazione del concetto di commutatore, proprio della teoria dei gruppi, a qualunque algebra contenuta in una varietà congruenze-permutabile. Successivamente Hagemann e Hermann dimostrarono che tali commutatori esistono in qualunque algebra contenuta in una varietà congruenze-modulare. Usando i commutatori è possibile definire il centro di tali algebre. Un'altra semplice definizione di centro, valida per ogni algebra, fu data da Freese e McKenzie, ed è quella che useremo qui.

Definizione 13.1. Sia \mathbf{A} un'algebra di tipo \mathcal{F} . Il *centro* di \mathbf{A} è la relazione binaria $Z(\mathbf{A})$ definita da:

$$(a, b) \in Z(\mathbf{A})$$

se e solo se, per ogni $p(x, y_1, \dots, y_n) \in T(x, y_1, \dots, y_n)$ e qualunque siano $c_1, \dots, c_n, d_1, \dots, d_n \in A$,

$$p(a, c_1, \dots, c_n) = p(a, d_1, \dots, d_n) \quad \text{sse} \quad p(b, c_1, \dots, c_n) = p(b, d_1, \dots, d_n).$$

Teorema 13.2. *Per ogni algebra \mathbf{A} , il centro $Z(\mathbf{A})$ è una congruenza su \mathbf{A} .*

Dimostrazione. Certamente $Z(\mathbf{A})$ è riflessiva, simmetrica e transitiva, e quindi è una relazione d'equivalenza su A . Sia ora f un simbolo funzionale n -ario, e siano $(a_i, b_i) \in Z(\mathbf{A}), 1 \leq i \leq n$. Dato un termine $p(x, y_1, \dots, y_m)$ e degli

elementi $c_1, \dots, c_m, d_1, \dots, d_m$ di A , dalla definizione di $Z(\mathbf{A})$ si ha

$$\begin{aligned} & p(f(a_1, a_2, \dots, a_n), \vec{c}) = p(f(a_1, a_2, \dots, a_n), \vec{d}) \\ \text{sse} \quad & p(f(b_1, a_2, \dots, a_n), \vec{c}) = p(f(b_1, a_2, \dots, a_n), \vec{d}) \\ & \vdots \\ \text{sse} \quad & p(f(b_1, \dots, b_{n-1}, a_n), \vec{c}) = p(f(b_1, \dots, b_{n-1}, a_n), \vec{d}) \\ \text{sse} \quad & p(f(b_1, \dots, b_n), \vec{c}) = p(f(b_1, \dots, b_n), \vec{d}); \end{aligned}$$

dunque

$$p(f(\vec{a}), \vec{c}) = p(f(\vec{a}), \vec{d}) \quad \text{sse} \quad p(f(\vec{b}), \vec{c}) = p(f(\vec{b}), \vec{d}),$$

e pertanto

$$(f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in Z(\mathbf{A}).$$

Allora $Z(\mathbf{A})$ è effettivamente una congruenza. □

ESEMPLI.

Gruppi. Sia $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ un gruppo. Se $(a, b) \in Z(\mathbf{G})$ allora, con il termine $p(x, y_1, y_2) = y_1 \cdot x \cdot y_2$ e $c \in G$, si ha

$$p(a, a^{-1}, c) = p(a, c, a^{-1});$$

ne segue

$$p(b, a^{-1}, c) = p(b, c, a^{-1}),$$

cioè

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

Posto $c = 1$ segue che

$$a^{-1} \cdot b = b \cdot a^{-1};$$

e quindi, per ogni $c \in G$,

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

Allora (a, b) è nella congruenza associata al sottogruppo normale \mathbf{N} di \mathbf{G} che è il centro inteso secondo la definizione data in teoria dei gruppi, cioè, $N = \{g \in G : h \cdot g = g \cdot h, \forall h \in G\}$.

Reciprocamente, sia \mathbf{N} il centro di \mathbf{G} inteso secondo la definizione di teoria dei gruppi. Allora per ogni termine $p(x, y_1, \dots, y_n)$ e degli elementi $a, b, c_1, \dots, c_n, d_1, \dots, d_n \in G$, se $a \cdot b^{-1} \in N$ e

$$p(a, \vec{c}) = p(a, \vec{d}),$$

allora

$$p((a \cdot b^{-1}) \cdot b, \vec{c}) = p((a \cdot b^{-1}) \cdot b, \vec{d}),$$

e quindi

$$p(b, \vec{c}) = p(b, \vec{d})$$

poiché $a \cdot b^{-1}$ è centrale. Allora, per simmetria, se $a \cdot b^{-1} \in N$,

$$p(a, \vec{c}) = p(a, \vec{d}) \quad \text{sse} \quad p(b, \vec{c}) = p(b, \vec{d}),$$

pertanto $(a, b) \in Z(\mathbf{G})$.

Ne risulta che

$$Z(\mathbf{G}) = \{(a, b) \in G^2 : (a \cdot b^{-1}) \cdot c = c \cdot (a \cdot b^{-1}), \forall c \in G\}.$$

Anelli. Sia $\mathbf{R} = (R, +, \cdot, -, 0)$ un anello. Se $(r, s) \in Z(\mathbf{R})$ allora, per $t \in R$,

$$(r - \underline{r}) \cdot t = (r - \underline{r}) \cdot 0;$$

da cui, rimpiazzando \underline{r} con s , si ha

$$(r - s) \cdot t = 0.$$

Analogamente

$$t \cdot (r - s) = 0,$$

quindi $r - s \in \text{Ann}(\mathbf{R})$, l'annullatore di \mathbf{R} . Viceversa, se $r - s \in \text{Ann}(\mathbf{R})$ e $p(x, y_1, \dots, y_n)$ è un termine e $c_1, \dots, c_n, d_1, \dots, d_n \in R$ allora da

$$p(r, \vec{c}) = p(r, \vec{d})$$

segue che

$$p((r - s) + s, \vec{c}) = p((r - s) + s, \vec{d}),$$

e quindi

$$p(s, \vec{c}) = p(s, \vec{d}).$$

Per simmetria abbiamo

$$Z(\mathbf{R}) = \{(r, s) : r - s \in \text{Ann}(\mathbf{R})\}.$$

Definizione 13.3. Sia \mathbf{A} un'algebra di tipo \mathcal{F} . Aggiungiamo ad \mathcal{F}_0 i simboli a per ogni $a \in A$. Chiamiamo \mathcal{F}_A il nuovo linguaggio ed indichiamo con \mathbf{A}_A l'algebra di tipo \mathcal{F}_A che si ottiene aggiungendo ad \mathbf{A} le costanti a , per ogni elemento $a \in A$. I termini di tipo \mathcal{F}_A si chiamano i *polinomi* di \mathbf{A} . Scriveremo $p^{\mathbf{A}}$ in luogo di $p^{\mathbf{A}_A}$. Due algebre $\mathbf{A}_1 = (A, F_1)$ ed $\mathbf{A}_2 = (A, F_2)$, eventualmente di tipi diversi, sullo stesso universo si dicono *polinomialmente equivalenti* se hanno lo stesso insieme di funzioni polinomiali, cioè se per ogni polinomio $p(x_1, \dots, x_n)$ di \mathbf{A}_1 , esiste un polinomio $q(x_1, \dots, x_n)$ di \mathbf{A}_2 tale che $p^{\mathbf{A}_1} = q^{\mathbf{A}_2}$, e viceversa.

Teorema 13.4. (Gumm, Hagemann, Herrmann). *Sia \mathbf{A} un'algebra tale che $V(\mathbf{A})$ è congruenze-permutabile. Allora le seguenti condizioni sono equivalenti:*

- (a) \mathbf{A} è polinomialmente equivalente ad un \mathbf{R} -modulo sinistro, per qualche anello \mathbf{R} .
- (b) $Z(\mathbf{A}) = \nabla_A$.
- (c) $\{(a, a) : a \in A\}$ è un laterale di una congruenza su $\mathbf{A} \times \mathbf{A}$.

14 Logica Equazionale e Congruenze Pienamente Invarianti.

In questo paragrafo studieremo le connessioni tra le identità soddisfatte da classi di algebre e le congruenze pienamente invarianti sull'algebra dei termini. In questo modo saremo in grado di fornire un insieme di regole per la deduzione di identità da identità.

Definizione 14.1. Una congruenza θ su un'algebra \mathbf{A} è *pienamente invariante* se, per ogni endomorfismo α su \mathbf{A} ,

$$(a, b) \in \theta \Rightarrow (\alpha a, \alpha b) \in \theta.$$

Indicheremo con $\text{Con}_{\text{FI}}(\mathbf{A})$ l'insieme delle congruenze su \mathbf{A} pienamente invarianti.

Lemma 14.2. $\text{Con}_{\text{FI}}(\mathbf{A})$ è chiuso rispetto ad intersezioni arbitrarie.

Definizione 14.3. Data un'algebra \mathbf{A} ed un sottoinsieme $S \subseteq A \times A$, sia $\Theta_{\text{FI}}(S)$ la minima congruenza su \mathbf{A} pienamente invariante e contenente S . La congruenza $\Theta_{\text{FI}}(S)$ è detta la *congruenza pienamente invariante generata da S* .

Lemma 14.4. *Sia \mathbf{A} un'algebra di tipo \mathcal{F} . Allora Θ_{FI} è un'operatore (binario) di chiusura algebrica su $A \times A$.*

Dimostrazione. Innanzitutto costruiamo $\mathbf{A} \times \mathbf{A}$, ed aggiungiamo alle sue operazioni fondamentali le seguenti:

$$\begin{aligned} & (a, a) && \text{per } a \in A \\ s((a, b)) &= (b, a) \\ t((a, b), (c, d)) &= \begin{cases} (a, d) & \text{se } b = c \\ (a, b) & \text{altrimenti} \end{cases} \\ e_\sigma((a, b)) &= (\sigma a, \sigma b) && \text{se } \sigma \text{ è un endomorfismo di } \mathbf{A}. \end{aligned}$$

Allora è semplice verificare che θ è una congruenza su \mathbf{A} pienamente invariante se e solo se θ è un sottouniverso dell'algebra che abbiamo appena costruito. Pertanto Θ_{FI} è un operatore di chiusura algebrica.

Per provare che Θ_{FI} è binario, definiamo una nuova algebra \mathbf{A}^* sostituendo ogni operazione fondamentale n -aria f di \mathbf{A} con l'insieme di tutte le operazioni unarie della forma

$$f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$$

dove $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$ sono elementi di A .

Proviamo che $\text{Con } \mathbf{A} = \text{Con } \mathbf{A}^*$. Chiaramente, se $\theta \in \text{Con } \mathbf{A}$, allora $\theta \in \mathbf{A}^*$ e quindi $\text{Con } \mathbf{A} \subseteq \text{Con } \mathbf{A}^*$. Per l'inclusione opposta, siano $\theta \in \text{Con } \mathbf{A}^*$ e $f \in \mathcal{F}_n$. Allora per $(a_i, b_i) \in \theta$, $1 \leq i \leq n$, si ha

$$\begin{aligned} & (f(a_1, \dots, a_{n-1}, a_n), f(a_1, \dots, a_{n-1}, b_n)) \in \theta \\ & (f(a_1, \dots, a_{n-1}, a_n), f(a_1, \dots, a_{n-2}, b_{n-1}, b_n)) \in \theta \\ & \quad \vdots \\ & (f(a_1, b_2, \dots, b_2), f(b_1, \dots, b_n)) \in \theta; \end{aligned}$$

per cui

$$(f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta.$$

Pertanto

$$\theta \in \text{Con } \mathbf{A}.$$

Se ora torniamo all'inizio della dimostrazione ed usiamo \mathbf{A}^* invece di \mathbf{A} , pur lasciando inalterate le e_σ , abbiamo che Θ_{FI} è l'operatore di chiusura Sg di un'algebra le cui operazioni sono tutte di arità al più 2. Allora, per il Lemma 4.2, Θ_{FI} è un operatore di chiusura binario. \square

Definizione 14.5. Dato un insieme di variabili X ed un linguaggio \mathcal{F} , sia

$$\tau : \text{Id}(X) \rightarrow T(X) \times T(X)$$

la biezione definita da

$$\tau(p \approx q) = (p, q).$$

Lemma 14.6. *Siano K una classe di algebre di tipo \mathcal{F} ed X un insieme di variabili. Allora $\tau(\text{Id}(X))$ è una congruenza pienamente invariante su $\mathbf{T}(X)$.*

Dimostrazione. Poiché

$$\begin{aligned} p \approx p \in \text{Id}_K(x) & \quad \text{per } p \in T(X), \\ p \approx q \in \text{Id}_K(X) & \Rightarrow q \approx p \in \text{Id}_K(X), \\ p \approx q, q \approx r \in \text{Id}_K(X) & \Rightarrow p \approx r \in \text{Id}_K(X), \end{aligned}$$

si ha che $\tau(\text{Id}_K(X))$ è una relazione d'equivalenza su $T(X)$. Ora se

$$p_i \approx q_i \in \text{Id}_K(X) \quad \text{per } 1 \leq i \leq n$$

e se $f \in \mathcal{F}_n$, allora si vede facilmente che

$$f(p_1, \dots, p_n) \approx f(q_1, \dots, q_n) \in \text{Id}_K(X),$$

e quindi $\tau(\text{Id}_K(X))$ è una congruenza su $\mathbf{T}(X)$. Ora, se α è un endomorfismo di $\mathbf{T}(X)$ e

$$p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n) \in \text{Id}_K(X),$$

si verifica immediatamente che

$$p(\alpha x_1, \dots, \alpha x_n) \approx q(\alpha x_1, \dots, \alpha x_n) \in \text{Id}_K(X);$$

pertanto $\tau(\text{Id}_K(X))$ è pienamente invariante. □

Lemma 14.7. *Dato un insieme di variabili X ed una congruenza pienamente invariante θ su $\mathbf{T}(X)$, per $p \approx q \in \text{Id}(X)$, si ha*

$$\mathbf{T}(X)/\theta \models p \approx q \Leftrightarrow (p, q) \in \theta.$$

Allora $\mathbf{T}(X)/\theta$ è libera in $V(\mathbf{T}(X)/\theta)$.

Dimostrazione. (\Rightarrow) Se

$$\begin{aligned} p &= p(x_1, \dots, x_n) \\ q &= q(x_1, \dots, x_n), \end{aligned}$$

allora

$$\begin{aligned}
& \mathbf{T}/\theta \models p(x, \dots, x_n) \approx q(x, \dots, x_n) \\
& \Rightarrow p(x_1/\theta, \dots, x_n/\theta) \approx q(x_1/\theta, \dots, x_n/\theta) \\
& \Rightarrow p(x_1, \dots, x_n)/\theta = q(x_1, \dots, x_n)/\theta \\
& \Rightarrow (p(x_1, \dots, x_n), q(x_1, \dots, x_n)) \in \theta \\
& \Rightarrow (p, q) \in \theta.
\end{aligned}$$

(\Leftarrow) Dati r_1, \dots, r_n in $T(X)$ possiamo trovare un endomorfismo ε di $\mathbf{T}(X)$ tale che

$$\varepsilon(x_i) = r_i, \quad 1 \leq i \leq n;$$

dunque

$$\begin{aligned}
& (p(x_1, \dots, x_n), q(x_1, \dots, x_n)) \in \theta \\
& \Rightarrow (\varepsilon p(x_1, \dots, x_n), \varepsilon q(x_1, \dots, x_n)) \in \theta \\
& \Rightarrow (p(r_1, \dots, r_n), q(r_1, \dots, r_n)) \in \theta \\
& \Rightarrow p(r_1/\theta, \dots, r_n/\theta) = q(r_1/\theta, \dots, r_n/\theta).
\end{aligned}$$

Quindi

$$\mathbf{T}(X)/\theta \models p \approx q.$$

Infine, dati $p \approx q \in \text{Id}(X)$, per il Lemma 11.3 si ha

$$\begin{aligned}
(p, q) \in \theta & \Leftrightarrow \mathbf{T}(X)/\theta \models p \approx q \\
& \Leftrightarrow V(\mathbf{T}(X)/\theta) \models p \approx q,
\end{aligned}$$

allora $\mathbf{T}(X)/\theta$ è libera in $V(\mathbf{T}(X)/\theta)$ per il Teorema 11.4. □

Teorema 14.8. *Dato un sottoinsieme Σ di $\text{Id}(X)$, si può trovare una classe K tale che*

$$\Sigma = \text{Id}_K(X)$$

se e solo se $\tau(\Sigma)$ è una congruenza pienamente invariante su $\mathbf{T}(X)$.

Dimostrazione. (\Rightarrow) Cfr. Lemma 14.6.

(\Leftarrow) Supponiamo che $\tau(\Sigma)$ sia una congruenza θ pienamente invariante. Sia $K = \{\mathbf{T}(X)/\theta\}$. Allora, per il Lemma 14.7,

$$\begin{aligned}
K \models p \approx q & \Leftrightarrow (p, q) \in \theta \\
& \Leftrightarrow p \approx q \in \Sigma.
\end{aligned}$$

Allora $\Sigma = \text{Id}_K(X)$. □

Definizione 14.9. Un sottoinsieme Σ di $\text{Id}(X)$ si dice una *teoria equazionale* su X se esiste una classe K di algebre tale che

$$\Sigma = \text{Id}_K(X).$$

Corollario 14.10. *Le teorie equazionali (di tipo \mathcal{F}) su X costituiscono un reticolo algebrico che è isomorfo al reticolo delle congruenze pienamente invarianti su $\mathbf{T}(X)$.*

Dimostrazione. Segue dal Lemma 14.4 e dal Teorema 14.8. \square

Definizione 14.11. Siano X un insieme di variabili e Σ un insieme di identità di tipo \mathcal{F} a variabili in X . Per $p, q \in T(X)$, diremo che Σ *fornisce* $p \approx q$ e scriveremo

$$\Sigma \vDash p \approx q$$

se, data un'algebra \mathbf{A} ,

$$\mathbf{A} \vDash \Sigma \quad \text{implica} \quad \mathbf{A} \vDash p \approx q.$$

Teorema 14.12. *Se Σ è un insieme di identità su X e $p \approx q$ è un'identità su X , allora*

$$\Sigma \vDash p \approx q \Leftrightarrow (p, q) \in \Theta_{\text{FI}}(\tau\Sigma).$$

Dimostrazione. Supponiamo

$$\mathbf{A} \vDash \Sigma.$$

Allora, poiché $\tau(\text{Id}_{\mathbf{A}}(X))$ è una congruenza pienamente invariante su $\mathbf{T}(X)$, per il Lemma 14.6 abbiamo

$$\Theta_{\text{FI}}(\tau\Sigma) \subseteq \tau \text{Id}_{\mathbf{A}}(X);$$

da cui

$$(p, q) \in \Theta_{\text{FI}}(\tau\Sigma) \Rightarrow \mathbf{A} \vDash p \approx q,$$

e quindi

$$(p, q) \in \Theta_{\text{FI}}(\tau\Sigma) \Rightarrow \Sigma \vDash p \approx q.$$

Reciprocamente, per il Lemma 14.7,

$$\mathbf{T}(X)/\Theta_{\text{FI}}(\tau\Sigma) \vDash \Sigma.$$

Dunque, se

$$\Sigma \vDash p \approx q,$$

allora

$$\mathbf{T}(X)/\Theta_{\text{FI}}(\tau\Sigma) \vDash p \approx q.$$

Pertanto, ancora per il Lemma 14.7,

$$(p, q) \in \Theta_{\text{FI}}(\tau\Sigma).$$

□

Nella dimostrazione del Lemma 14.4 abbiamo dato una descrizione esplicita delle operazioni necessarie alla costruzione della chiusura pienamente invariante $\Theta_{\text{FI}}(S)$ di un insieme S di coppie ordinate di elementi di un'algebra. Ciò ci porterà ad un elegante sistema di assiomi e regole d'inferenza da applicare alle identità.

Definizione 14.13. Dato un termine p , i *sottotermini* di p sono definiti da:

- (1) il termine p è un sottotermine di p ;
- (2) se $f(p_1, \dots, p_n)$ è un sottotermine di p e $f \in \mathcal{F}_n$, allora ogni p_i è un sottotermine di p .

Definizione 14.14. Sia Σ un insieme di identità su X , siano $p \approx q \in \Sigma$ e $r \in T(X)$ arbitrari, e supponiamo che p occorra come sottotermine di r . Detto s il termine che si ottiene sostituendo p con q in r , se $r \approx s \in \Sigma$ diremo che Σ è *chiuso per rimpiazzamento*.

Definizione 14.15. Sia Σ un insieme di identità su X , e siano $p \approx q \in \Sigma$ e $r_i \in T(X), i \in I$ arbitrari. Se l'identità che si ottiene da $p \approx q$ sostituendo contemporaneamente tutte le occorrenze di ciascuna variabile x_i con r_i è ancora in Σ , diremo che Σ è *chiuso per sostituzioni*.

Definizione 14.16. Se Σ è un insieme di identità su X , la *chiusura deduttiva* $D(\Sigma)$ di Σ è il più piccolo sottoinsieme di $\text{Id}(X)$ contenente Σ tale che

- $p \approx p \in D(\Sigma)$ per $p \in T(X)$;
- $p \approx q \in D(\Sigma) \Rightarrow q \approx p \in D(\Sigma)$;
- $p \approx q, q \approx r \in D(\Sigma) \Rightarrow p \approx r \in D(\Sigma)$;
- $D(\Sigma)$ è chiuso per rimpiazzamento;
- $D(\Sigma)$ è chiuso per sostituzioni.

Teorema 14.17. *Siano $\Sigma \subseteq \text{Id}(X)$ e $p \approx q \in \text{Id}(X)$. Allora*

$$\Sigma \vDash p \approx q \Leftrightarrow p \approx q \in D(\Sigma).$$

Dimostrazione. Le prime tre proprietà di chiusura rendono $\tau D(\Sigma)$ una relazione d'equivalenza contenente $\tau\Sigma$, la quarta assicura che tale relazione è una congruenza, e l'ultima proprietà di chiusura ci dice che $\tau D(\Sigma)$ è una congruenza pienamente invariante. Pertanto

$$\tau D(\Sigma) \supseteq \Theta_{\text{FI}}(\tau\Sigma).$$

In ogni caso $\tau^{-1}\Theta_{\text{FI}}(\tau\Sigma)$ ha tutte e cinque le proprietà di chiusura e contiene Σ ; ne segue che

$$\tau D(\Sigma) = \Theta_{\text{FI}}(\tau\Sigma).$$

Allora

$$\begin{aligned} \Sigma \vDash p \approx q &\Leftrightarrow (p, q) \in \Theta_{\text{FI}}(\tau\Sigma) \\ &\Leftrightarrow p \approx q \in D(\Sigma) \quad \text{per il Teorema 14.12} \end{aligned}$$

□

Definizione 14.18. Sia Σ un insieme di identità su X . Per $p \approx q \in \text{Id}(X)$ diremo che Σ *prova* $p \approx q$, e scriveremo

$$\Sigma \vdash p \approx q,$$

se esiste una sequenza di identità

$$p_1 \approx q_1, \dots, p_n \approx q_n$$

in $\text{Id}(X)$ tale che - per ogni i - $p_i \approx q_i$ appartiene a Σ , oppure è della forma $p \approx p$, o è il risultato di applicazioni delle ultime quattro regole di chiusura della *Definizione 14.16* a qualcuna delle precedenti identità della sequenza, e l'ultima identità $p_n \approx q_n$ è proprio $p \approx q$.

La sequenza $p_1 \approx q_1, \dots, p_n \approx q_n$ si chiama una *deduzione formale* di $p \approx q$, e n è la *lunghezza* della deduzione.

Teorema 14.19. (Teorema di Completezza di Birkhoff per la Logica Equazionale). *Siano $\Sigma \subseteq \text{Id}(X)$ e $p \approx q \in \text{Id}(X)$. Allora*

$$\Sigma \vDash p \approx q \quad \Leftrightarrow \quad \Sigma \vdash p \approx q.$$

Dimostrazione. Certamente

$$\Sigma \vdash p \approx q \quad \Rightarrow \quad p \approx q \in D(\Sigma)$$

perché nella Definizione 14.18 abbiamo usato solo proprietà rispetto alle quali $D(\Sigma)$ è chiuso.

Per provare l'implicazione opposta, osserviamo innanzitutto che si ha ovviamente

$$\Sigma \vdash p \approx q \quad \text{se} \quad p \approx q \in \Sigma$$

e

$$\Sigma \vdash p \approx p \quad \text{per ogni} \quad p \in T(X).$$

Se $\Sigma \vdash p \approx q$ allora esiste una deduzione formale

$$p_1 \approx q_1, \dots, p_n \approx q_n$$

di $p \approx q$. Ma allora

$$p_1 \approx q_1, \dots, p_n \approx q_n, q_n \approx p_n$$

è una deduzione formale di $q \approx p$.

Se $\Sigma \vdash p \approx q$ e $\Sigma \vdash q \approx r$, siano

$$p_1 \approx q_1, \dots, p_n \approx q_n \quad \text{e} \quad \bar{p}_1 \approx \bar{q}_1, \dots, \bar{p}_k \approx \bar{q}_k$$

deduzioni formali di $p \approx q$ e $q \approx r$ rispettivamente. Allora

$$p_1 \approx q_1, \dots, p_n \approx q_n, \bar{p}_1 \approx \bar{q}_1, \dots, \bar{p}_k \approx \bar{q}_k, p_n \approx \bar{q}_k$$

è una deduzione formale di $p \approx r$.

Se $\Sigma \vdash p \approx q$, siano $p_1 \approx q_1, \dots, p_n \approx q_n$ una deduzione formale di $p \approx q$ e

$$r(\dots, p, \dots)$$

un qualunque termine con una specifica occorrenza del sottotermine p . Allora

$$p_1 \approx q_1, \dots, p_n \approx q_n, r(\dots, p_n, \dots) \approx r(\dots, q_n, \dots)$$

è una deduzione formale di $r(\dots, p, \dots) \approx r(\dots, q, \dots)$.

Infine, se $\Sigma \vdash p_i \approx q_i, 1 \leq i \leq n$, e $f \in \mathcal{F}_n$, scrivendo in successione le deduzioni formali di ogni $p_i \approx q_i$ ed aggiungendo alcuni passi di rimpiazzamento, si ottiene una deduzione formale di $f(p_1, \dots, p_n) \approx f(q_1, \dots, q_n)$; cioè

$$\dots, p_1 \approx q_1, \dots, p_2 \approx q_2, \dots, \quad \dots, \quad p_n \approx q_n, \\ f(p_1, \dots, p_n) \approx f(p_1, \dots, p_{n-1}, q_n), \dots$$

Ne segue che $D(\Sigma) \subseteq \{p \approx q : \Sigma \vdash p \approx q\}$, e quindi

$$D(\Sigma) = \{p \approx q : \Sigma \vdash p \approx q\}.$$

Dal Teorema 14.17 segue allora l'asserto. □

Grazie al teorema di completezza abbiamo due diverse possibilità per studiare le conseguenze di un insieme di identità. Usando la nozione di soddisfacimento, osserviamo tutte le algebre che soddisfano un dato insieme di identità mentre, lavorando con \vdash , possiamo applicare il principio d'induzione alla lunghezza di una deduzione formale.

ESEMPLI.

- (1) Un'identità $p \approx q$ è *bilanciata* se ogni variabile occorre lo stesso numero di volte sia in p che in q . Se Σ è un insieme di identità bilanciate, ragionando per induzione sulla lunghezza di una deduzione formale possiamo dimostrare che, se $\Sigma \vdash p \approx q$, allora $p \approx q$ è bilanciata. Questo fatto non è per nulla evidente se ragioniamo soltanto con \models .
- (2) Un famoso teorema di Jacobson in teoria degli anelli afferma che, dato un numero naturale $n \geq 2$, se Σ è il sistema di assiomi della teoria degli anelli più l'identità $x^n \approx x$, allora $\Sigma \models x \cdot y \approx y \cdot x$. Ciononostante non si conosce alcuna procedura per scrivere una deduzione formale, dato n , di $x \cdot y \approx y \cdot x$ (tranne che per pochi casi speciali come $n = 2$ o 3).

Un'altra applicazione delle congruenze pienamente invarianti allo studio delle identità consiste nel mostrare l'esistenza di sottovarietà minimali.

Definizione 14.20. Una varietà V si dice *banale* se tutte le algebre in essa contenute sono banali. Una sottoclasse W di una varietà V che sia essa stessa una varietà si dice una *sottovarietà* di V . V si dice una varietà *minimale* (o *equazionalmente completa*) se V è non banale e l'unica sua sottovarietà propria (cioè diversa da V) è quella banale.

Teorema 14.21. *Sia V una varietà non banale. Allora V contiene una sottovarietà minimale.*

Dimostrazione. Sia $V = M(\Sigma)$, $\Sigma \subseteq \text{Id}(X)$ con X infinito (cfr. Lemma 11.8). Allora $\text{Id}_V(X)$ definisce V e, essendo V non banale, segue dal Lemma 14.6 che $\tau(\text{Id}_V(X))$ è una congruenza su $\mathbf{T}(X)$ pienamente invariante e diversa da ∇ . Poiché

$$\nabla = \Theta_{\text{FI}}((x, y))$$

qualunque siano gli elementi distinti $x, y \in X$, si ha che ∇ è finitamente generata (come congruenza pienamente invariante). Questo ci permette di applicare il Lemma di Zorn per estendere $\tau(\text{Id}_V(X))$ ad una congruenza pienamente invariante massimale su $\mathbf{T}(X)$, che chiameremo θ . Allora, per il Teorema 14.8, $\tau^{-1}\theta$ dovrà definire una varietà minimale, che è una sottovarietà di V . \square

ESEMPIO. La varietà dei reticoli ha un'unica sottovarietà minimale, la varietà generata da una catena a due elementi. Siano, infatti, V una sottovarietà minimale di reticoli e \mathbf{L} un reticolo non banale in V ; poiché \mathbf{L} contiene un sottoreticolo a due elementi, possiamo assumere che \mathbf{L} sia un reticolo a due elementi. Allora $V(\mathbf{L})$ è non banale ed è inclusa in V . Ne segue che $V(\mathbf{L}) = V$.

Definizione 14.22. Siano V una varietà e X un insieme di variabili. Definiamo

$$\text{IrB}(\text{Id}_V(X)) = \{|\Sigma| : \Sigma \text{ è un insieme finito} \\ \text{minimale di identità su } X, \text{ che definisce } V\}.$$

Teorema 14.23. (Tarski). *Siano V una varietà ed X un insieme di variabili. Allora $\text{IrB}(\text{Id}_V(X))$ è un insieme convesso.*

Dimostrazione. Per $\Sigma \subseteq \text{Id}_V(X)$, $\Sigma \models \text{Id}_V(X)$ implica

$$\Theta_{\text{FI}}(\tau\Sigma) = \tau \text{Id}_V(X).$$

Poiché Θ_{FI} è un operatore binario per il Lemma 14.4, l'asserto segue dal Teorema 4.4. \square

Indice

1	Definizioni ed esempi di algebre.	1
2	Algebre isomorfe. Sottoalgebre.	7
3	Reticoli algebrici e sottouniversi.	9
4	Il Teorema della base irridondante.	11
5	Congruenze ed algebre quozienti.	14
6	Omomorfismi ed isomorfismi.	18
7	Prodotti diretti, congruenze-fattore, algebre direttamente indecomponibili.	24
8	Prodotti sottodiretti, algebre sottodirettamente irriducibili, algebre semplici.	30
9	Operatori di classe e varietà.	33
10	Termini ed algebre di termini. Algebre libere.	35
11	Identità, algebre libere, il Teorema di Birkhoff.	43
12	Condizioni di Mal'cev.	50
13	Il Centro di un'algebra.	56
14	Logica Equazionale e Congruenze Pienamente Invarianti.	59