

CAPITOLO 3

[indice](#)

ALCUNE NOZIONI DI NATURA UNIVERSALE

1. Sistemi di chiusura ed operatori di chiusura

Moltissime nozioni matematiche possono essere introdotte in termini di sistemi di chiusura ed operatori di chiusura.

Definizione 1. Sia S un insieme non vuoto e denotiamo con $\Pi(S)$ l'insieme delle sua parti, allora chiameremo *sistema di chiusura* una classe C di sottoinsiemi di S tale che

- i) $S \in C$
- ii) C è chiusa rispetto alle intersezioni

La condizione ii) significa che l'intersezione di una qualunque famiglia di elementi di C appartiene ancora a C .

Definizione 2. Dato un sistema di chiusura C in S ed un sottoinsieme X di S poniamo

$$\langle X \rangle = \bigcap \{ Y \in C : Y \supseteq X \}$$

è diciamo che $\langle X \rangle$ è l'elemento di C generato da X .

Esempio di carattere topologico. Ad esempio se C è la classe degli insiemi chiusi di R allora C è un sistema di chiusura in quanto l'intersezione di una famiglia di insiemi chiusi è ancora un insieme chiuso. Se X è un sottoinsieme di R allora $\langle X \rangle = \overline{X}$ cioè $\langle X \rangle$ è la chiusura dell'insieme X .

Esempio di carattere algebrico. Sia C la classe di tutti i sottogruppi di un dato gruppo G . Allora C è un sistema di chiusura e, per ogni sottoinsieme X di G , $\langle X \rangle$ è il sottogruppo generato da X .

Esempio di carattere geometrico. Sia C la classe di tutti gli insiemi convessi del piano euclideo. Allora C è un sistema di chiusura. Per ogni insieme X di punti, $\langle X \rangle$ è la *chiusura convessa* di X .

Il seguente teorema permette di ottenere diversi interessanti esempi di reticoli completi.

Teorema 3. Ogni sistema di chiusura C è un reticolo completo. Più precisamente se $(X_i)_{i \in I}$ è una famiglia di elementi di C allora

$$\text{Inf}_{i \in I} X_i = \langle \bigcap_{i \in I} X_i \rangle, \quad \text{Sup}_{i \in I} X_i = \langle \bigcup_{i \in I} X_i \rangle.$$

Ad esempio la famiglia degli insiemi chiusi del piano euclideo è un reticolo completo in cui l'estremo superiore di una famiglia di insiemi chiusi è la chiusura dell'unione. L'insieme dei sottogruppi di un dato gruppo è un reticolo completo in cui l'estremo superiore di una famiglia di sottogruppi è il sottogruppo generato dall'unione.

Proposizione 4. L'intersezione di una qualunque famiglia di sistemi di chiusura è ancora un sistema di chiusura.

Dim. Consideriamo per semplicità espositiva solo il caso di due sistemi di chiusura C_1 e C_2 e poniamo $C = C_1 \cap C_2$. Allora poiché $S \in C_1$ e $S \in C_2$, risulta che $S \in C$. Inoltre se $(X_i)_{i \in I}$ è una famiglia di elementi di C allora $(X_i)_{i \in I}$ è sia una famiglia di elementi di C_1 che una famiglia di elementi di C_2 . Ne segue che $\bigcap_{i \in I} X_i$ appartiene sia a C_1 che a C_2 e quindi appartiene a C .

La nozione di sistema di chiusura è strettamente legata alla nozione di operatore di chiusura.

Definizione 5. Chiamiamo *operatore di chiusura* una funzione $T : \Pi(S) \rightarrow \Pi(S)$ tale che:

- a) $T(X) \supseteq X$ (proprietà di inclusione)

- b) $X \subseteq Y \Rightarrow T(X) \subseteq T(Y)$ (crescenza o monotonia)
 c) $T(T(X)) = T(X)$. (idempotenza).

Esempio di carattere topologico. Sia X un sottoinsieme di R ed indichiamo con $T(X)$ la chiusura \overline{X} dell'insieme X . Allora T è un operatore di chiusura.

Esempio di carattere algebrico. In uno spazio vettoriale per ogni insieme X di vettori indichiamo con $T(X)$ l'insieme dei vettori linearmente dipendenti da X . Allora T è un operatore di chiusura.

Definizione 6. Dato un operatore T , si chiama *punto fisso* o *punto unito* di T un insieme X tale che $T(X) = X$.

Si osservi che la proprietà di idempotenza $T(T(X)) = T(X)$ equivale a dire che $T(X)$ è un punto fisso di T . Questo significa che se T è un operatore di chiusura allora tutti gli elementi del condominio di T sono punti fissi.

La seguente proposizione mostra che gli operatori di chiusura sono strettamente collegati ai sistemi di chiusura.

Teorema 7. Sia $T : \Pi(S) \rightarrow \Pi(S)$ un operatore che verifica la proprietà di inclusione e quella di crescenza. Allora l'insieme

$$C_T = \{X \in \Pi(S) : T(X) = X\}$$

dei punti uniti di T è un sistema di chiusura.

Dim. Sia $(X_i)_{i \in I}$ una famiglia di punti uniti, allora, essendo $\cup_{i \in I} X_i \subseteq X_j$ per ogni $j \in I$, per la crescenza di T , risulta $T(\cup_{i \in I} X_i) \subseteq T(X_j)$. Ne segue che, essendo X_j punto unito per T , $T(\cup_{i \in I} X_i) \subseteq X_j$ per ogni $j \in I$. In definitiva $T(\cup_{i \in I} X_i) \subseteq \cup_{j \in I} X_j$ e ciò, per la proprietà di inclusione, prova che $\cup_{i \in I} X_i$ è un punto unito. \square

Proposizione 8. Supponiamo che T verifichi le proprietà di inclusione e di monotonia e poniamo

$$D(X) = \cup \{Y : Y \supseteq X \text{ e } Y = T(Y)\}, \quad (3)$$

Allora $D(X)$ è il minimo punto fisso contenente X .

Dim. Dal teorema 7 segue che $D(X)$ è un punto fisso. E' immediato che $D(X)$ contiene X . Infine se Y è un punto fisso che contiene X allora appartiene all'insieme $\{Y : Y \supseteq X \text{ e } Y = T(Y)\}$ e quindi contiene all'intersezione degli elementi di tale insieme.

Teorema 9. Se T è un operatore di chiusura allora l'insieme C_T dei suoi punti fissi è un sistema di chiusura. Viceversa, sia C un sistema di chiusura e definiamo l'operatore $T_C : \Pi(S) \rightarrow \Pi(S)$ ponendo

$$J_C(X) = \langle X \rangle = \langle X \rangle = \cap \{Y \in C : Y \supseteq X\}.$$

Allora T_C è un operatore di chiusura.

Dim. La prima parte del teorema segue dalla proposizione precedente in quanto un operatore di chiusura verifica la proprietà di inclusione ed è monotono. La seconda parte è evidente. Infatti è immediato che J_C verifica le proprietà di inclusione e di monotonia. D'altra parte, se si osserva che

$$Y \supseteq J_C(X) \Leftrightarrow Y \supseteq X,$$

risulta anche

$$J_C(J_C(X)) = \cap \{Y \in C : Y \supseteq J_C(X)\} = \cap \{Y \in C : Y \supseteq X\}.$$

Abbiamo visto che l'intersezione di due sistemi di chiusura è ancora un sistema di chiusura. Si pone il problema se la composizione di due operatori di chiusura sia ancora un operatore di chiusura. Questo avviene solo se i due operatori commutano.

Proposizione 10. Siano T_1 e T_2 due operatori di chiusura tali che $T_1 \circ T_2 = T_2 \circ T_1$. Allora la loro composizione è ancora un operatore di chiusura. Inoltre

X è un punto unito di $T_1 \circ T_2 \Leftrightarrow X$ è un punto unito sia di T_1 che di T_2 .

Dim. E' evidente che $T_1 \circ T_2$ verifica la proprietà di inclusione e la monotonia. Inoltre, posto $T = T_1 \circ T_2$, risulta

$$T \circ T = (T_1 \circ T_2) \circ (T_1 \circ T_2) = T_1 \circ (T_2 \circ T_1) \circ T_2 = T_1 \circ (T_1 \circ T_2) \circ T_2 = (T_1 \circ T_1) \circ (T_2 \circ T_2) = T_1 \circ T_2 = T.$$

Ne segue che T è un operatore di chiusura.

Supponiamo che X sia un punto unito di $T_1 \circ T_2$, allora essendo $T_1(T_2(X)) = X$, X appartiene al condominio di T_1 ed è quindi un punto fisso di T_1 . D'altra parte, poiché è anche $T_2(T_1(X)) = X$, X appartiene al condominio di T_2 ed è quindi un punto fisso di T_2 . Viceversa, sia X un punto unito sia di T_1 che di T_2 allora $T_1(T_2(X)) = T_1(X) = X$ e quindi X è un punto unito di $T_1 \circ T_2$.

2. Teoremi di punto fisso per operatori algebrici

La ricerca dei punti fissi di un operatore è abbastanza semplice per la seguente classe di operatori.

Definizione 1. Chiamiamo *operatore algebrico su S* ogni funzione $T : \Pi(S) \rightarrow \Pi(S)$ tale che:

- $T(X) \supseteq X$ (proprietà di inclusione)
- $X \subseteq Y \Rightarrow T(X) \subseteq T(Y)$ (crescenza o monotonia)
- $x \in T(X) \Rightarrow \exists F \subseteq X, F$ finito, $x \in T(F)$ (proprietà di compattezza o finitezza).

Diremo che T è di *tipo k* se la cardinalità dell'insieme F di cui è detto in c) è sempre minore di k .

La teoria degli operatori algebrici deve essere vista come un modo astratto di considerare un processo con cui si costruiscono nuovi oggetti a partire da un dato insieme X di oggetti. Allora a) significa che tra le cose che posso costruire con X ci sono gli elementi di X ,

b) significa che se una cosa può essere costruita a partire da X allora (a maggior ragione) può essere costruita a partire da un insieme che contiene X ,

c) afferma che dire che una cosa è costruibile a partire da X significa in realtà che è costruibile a partire da un numero finito di elementi di X . In altre parole, significa che il processo di costruzione è finitario.

Da notare che le condizioni b) e c) equivalgono a dire che

$$T(X) = \cup \{T(F) : F \subseteq X \text{ e } F \text{ finito}\}$$

cioè equivalgono a dire che il calcolo di $T(X)$ si può effettuare riferendosi solo alla parti finite di T .

Se T è un *operatore di chiusura algebrico*, cioè se oltre alle condizioni a), b) e c) verifica anche la condizione di chiusura

$$d) D(D(X)) = D(X),$$

allora tale condizione si può interpretare dicendo che:

- se un oggetto x è costruito con materiale in $D(X)$ che a sua volta è stato costruito con materiale in X allora tale oggetto è, di fatto, costruito con materiale in X .

In altre parole a partire dagli oggetti in $D(X)$ non è possibile costruire niente che non sia già in $D(X)$.

Problema. Sia S un insieme e Z un suo sottoinsieme. Dire quali proprietà verifica l'operatore T definito ponendo, per ogni sottoinsieme X di S

$$T(X) = X \cup Z.$$

Problema. Sia T l'operatore che associa ad ogni insieme X di numeri interi l'insieme $T(X)$ dei divisori degli elementi di X . Ad esempio $T(\{3,14,15\}) = \{1,3,2,7,5,14,15\}$. Dire che tipo di operatore è.

Se T è un operatore algebrico allora X è un punto fisso se e solo se $T(X) \subseteq X$ essendo l'inclusione $T(X) \supseteq X$ sempre verificata. Allora i punti fissi sono gli insiemi "saturi" rispetto al processo di costruzione T , cioè insiemi da cui non è possibile ottenere nuovo materiale utilizzando T . Se T è un operatore di chiusura allora, essendo $T(T(X)) = T(X)$, ogni $T(X)$ risulta essere un punto fisso.

Per caratterizzare gli operatori algebrici è utile il seguente lemma.

Lemma 2. Sia $(X_n)_{n \in \mathbb{N}}$ una successione di sottoinsiemi di S crescente rispetto alla inclusione ed F un sottoinsieme finito di S , allora

$$F \subseteq \bigcap_{n \in \mathbb{N}} X_n \Rightarrow \exists j \in \mathbb{N} \text{ tale che } F \subseteq X_j. \quad (1)$$

Dim. Procederemo per induzione sulla cardinalità $n = |F|$ di F . Per $n = 1$ la (1.1) è conseguenza immediata della definizione di unione. Supponiamo che (1.2) sia vera per un insieme di n elementi, sia F un insieme di $n+1$ elementi e supponiamo che $F \subseteq \bigcap_{n \in \mathbb{N}} X_n$. Allora sarà $F = F' \cup \{a\}$ con a opportuno elemento e $|F'| = n$. Pertanto, per ipotesi di induzione, essendo $F' \subseteq F \subseteq \bigcap_{n \in \mathbb{N}} X_n$ possiamo ricavare l'esistenza di un intero h tale che $F' \subseteq X_h$. Sia k tale che $a \in X_k$ e sia $j = \text{Max}\{h, k\}$, allora dalla crescita di $(X_n)_{n \in \mathbb{N}}$ si ricava che $F \subseteq X_h \cup X_k = X_j$. \square

Problema. Mostrare che il lemma ora enunciato non vale senza l'ipotesi di crescita per $(X_n)_{n \in \mathbb{N}}$ e che non vale senza l'ipotesi di finitezza per F .

Nel seguito scriveremo $T^n(X)$ per indicare il risultato della applicazione dell'operatore T n volte; più precisamente definiamo $T^n(X)$ per ricorsione su n tramite le equazioni

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

Lemma 3. Se un operatore T è algebrico allora per ogni successione crescente $(X_n)_{n \in \mathbb{N}}$ di sottoinsiemi di S risulta che

$$T(\bigcap_{n \in \mathbb{N}} X_n) = \bigcap_{n \in \mathbb{N}} T(X_n). \quad (2)$$

Dim. Supponiamo che T sia un operatore algebrico allora è evidente che, essendo $X_n \subseteq \bigcap_{n \in \mathbb{N}} X_n$ per la monotonia $T(X_n) \subseteq T(\bigcap_{n \in \mathbb{N}} X_n)$ e quindi $\bigcap_{n \in \mathbb{N}} T(X_n) \subseteq T(\bigcap_{n \in \mathbb{N}} X_n)$. Per provare che $T(\bigcap_{n \in \mathbb{N}} X_n) \subseteq \bigcap_{n \in \mathbb{N}} T(X_n)$, sia $x \in T(\bigcap_{n \in \mathbb{N}} X_n)$, allora esiste un sottoinsieme finito F di $\bigcap_{n \in \mathbb{N}} X_n$ tale che $x \in T(F)$. Detto j un intero tale che $F \subseteq X_j$ risulta anche che $x \in T(X_j)$ e quindi che $x \in \bigcap_{n \in \mathbb{N}} T(X_n)$. Ciò prova la proprietà (2).

Il seguente teorema mostra che ogni operatore compatto e monotono ammette un punto unito.

Teorema 4. Sia $T : \Pi(S) \rightarrow \Pi(S)$ un operatore compatto e monotono e sia X un insieme tale che $T(X) \supseteq X$, allora $\bigcap_{n \in \mathbb{N}} T^n(X)$ è il minimo punto unito di T contenente X . In particolare, $\bigcap_{n \in \mathbb{N}} T^n(\emptyset)$ è il minimo punto unito di T .

Dim. Cominciamo con il provare che $T(\bigcap_{n \in \mathbb{N}} T^n(X)) \subseteq \bigcap_{n \in \mathbb{N}} T^n(X)$. Ora da $T(X) \supseteq X$, applicando n volte l'operatore T , segue che $T^{n+1}(X) \supseteq T^n(X)$. Ciò prova che $T^n(X)$ è una successione crescente. Sia x un elemento di $T(\bigcap_{n \in \mathbb{N}} T^n(X))$, allora essendo T algebrico risulterà che $x \in T(F)$ per F opportuno sottoinsieme finito di $\bigcap_{n \in \mathbb{N}} T^n(X)$. Per la finitezza di F e la crescita di $T^n(X)$ esisterà $p \in \mathbb{N}$ tale che F è contenuto in $T^p(X)$. Ne segue che

$$x \in T(F) \subseteq T(T^p(X)) = T^{p+1}(X) \subseteq \bigcap_{n \in \mathbb{N}} T^n(X).$$

Ciò prova che $T(\bigcap_{n \in \mathbb{N}} T^n(X))$ è contenuto in $\bigcap_{n \in \mathbb{N}} T^n(X)$. D'altra parte sappiamo che $\bigcap_{n \in \mathbb{N}} T^n(X) \supseteq T^m(X)$ per ogni m e quindi, per la monotonia di T , che $T(\bigcap_{n \in \mathbb{N}} T^n(X)) \supseteq T^{m+1}(X)$. Ne segue che $T(\bigcap_{n \in \mathbb{N}} T^n(X)) \supseteq \bigcap_{m \in \mathbb{N}} T^{m+1}(X) = \bigcap_{n \in \mathbb{N}} T^n(X)$ e quindi che $\bigcap_{n \in \mathbb{N}} T^n(X)$ è un punto fisso di T . Per provare che $\bigcap_{n \in \mathbb{N}} T^n(X)$ è il minimo punto unito contenente X , sia M un qualsiasi punto unito contenente X , allora è immediato che $T^n(M) = M$. D'altra parte, per la monotonia di T , applicando n volte T alla disuguaglianza $M \supseteq X$, otteniamo che $T^n(M) \supseteq T^n(X)$ e quindi che $M \supseteq T^n(X)$. In definitiva $M \supseteq \bigcap_{n \in \mathbb{N}} T^n(X)$ e quindi $\bigcap_{n \in \mathbb{N}} T^n(X)$ è il minimo punto unito contenente X .

Corollario 5. Sia $T : \Pi(S) \rightarrow \Pi(S)$ un operatore algebrico, allora

$$D(X) = \bigcap_{n \in \mathbb{N}} T^n(X). \quad (3)$$

In altre parole $\bigcap_{n \in \mathbb{N}} T^n(X)$ è il minimo punto unito contenente X .

Dim. Basta osservare che se T è un operatore algebrico allora $T(X) \supseteq X$ per ogni insieme X .

Esempio. Sia A un alfabeto e definiamo l'operatore $T : \Pi(A^*) \rightarrow \Pi(A^*)$ ponendo:

$$T(X) = \{p \in A^* : \exists p' \in X \text{ tale che } p \text{ è ottenuta scambiando due lettere di } p'\} \cup X.$$

E' immediato che T è un operatore algebrico ma che non è di chiusura. Ad esempio se $A = \{a,b,c\}$ allora

$$T(\{abc,cb\}) = \{abc,cb, acb,cba,bac,bc\}.$$

$$T^2(\{abc,cb\}) = T(\{abc,cb, acb,cba,bac,bc\}) = \{abc,cb,acb,cba,bac,bc,cab\} \neq T(\{abc,cb\}).$$

Problema. Sia T uno degli operatori descritti nei problemi precedenti che sia un operatore algebrico. Trovare il minimo punto fisso di X utilizzando la proposizione precedente.

Esercizio. Sia R l'insieme dei numeri reali e $T : \Pi(R) \rightarrow \Pi(R)$ l'operatore definito ponendo

$$T(X) = X \cup \{3x+x' \mid x \in X, x' \in X\}.$$

Provare che T è un operatore algebrico e trovare il minimo punto fisso contenente $\{2,5\}$.

Esercizio. Sia $T : \Pi(R) \rightarrow \Pi(R)$ l'operatore definito ponendo

$$T(X) = X \text{ se } X \text{ è finito}$$

$$T(X) = R \text{ se } X \text{ è infinito.}$$

Dire di quali proprietà gode questo operatore e quali sono i suoi punti fissi.

Proposizione 6. Sia $T : \Pi(S) \rightarrow \Pi(S)$ un operatore algebrico e sia $D : \Pi(S) \rightarrow \Pi(S)$ definito tramite (3). Allora D è un operatore di chiusura algebrico i cui punti fissi coincidono con i punti fissi di T , cioè

$$T(X) = X \Leftrightarrow D(X) = X.$$

Dim. Poiché $D(X)$ è l'intersezione dei punti fissi contenenti X , è evidente che a), b) e d) sono verificate. Per provare c), proviamo prima per induzione su n che

c') $x \in T^n(X)$ implica che esiste $F \subseteq X$, F finito tale che $x \in T^n(F)$.

Ora per $n = 1$ c') coincide con l'ipotesi di algebricità per T . Supponiamo c') vera per n e che $x \in T^{n+1}(X) = T(T^n(X))$. Allora, essendo T algebrico, esiste un sottoinsieme finito $F = \{x_1, \dots, x_h\}$ di $T^n(X)$ tale che $x \in T(F)$. Per ipotesi di induzione esisteranno F_1, \dots, F_h sottoinsiemi finiti di X tali che $x_i \in T^n(F_i)$, pertanto posto $F' = F_1 \cup \dots \cup F_h$, sarà $x_i \in T^n(F')$ per $i = 1, \dots, h$ e quindi $F \subseteq T^n(F')$. In conclusione $x \in T(F) \subseteq T^{n+1}(F')$ e ciò prova c') nel caso $n+1$.

Sia x un elemento di $D(X)$, allora poiché $D(X) = \bigcap_{n \in \mathbb{N}} T^n(X)$, esisterà $j \in \mathbb{N}$ tale che $x \in T^j(X)$. Per la c') allora esisterà $F \subseteq X$ finito tale che $x \in T^j(F)$ e quindi, essendo $\bigcap_{n \in \mathbb{N}} T^n(F) \supseteq T^j(F)$, $x \in \bigcap_{n \in \mathbb{N}} T^n(F) = D(F)$ con F finito. Ciò prova che D è algebrico.

Supponiamo ora che $T(X) = X$ allora è chiaro che il minimo punto fisso contenente X è proprio X e cioè che $X = D(X)$. Supponiamo viceversa che $X = D(X)$, allora poiché per definizione $D(X)$ è un punto fisso di T , X è un punto fisso di T . □

Esempio: Sia S uno spazio Euclideo e sia T l'operatore definito ponendo

$$T(X) = \{x \in S \mid \exists p, \exists q \in X, x \in \underline{pq}\}$$

avendo indicato con \underline{pq} il segmento chiuso di estremi p e q . In altre parole $T(X)$ è l'insieme dei punti che si trovano su di un segmento i cui estremi appartengono a X . Sono punti uniti di T tutti e soli i sottoinsiemi convessi di S . T è un operatore algebrico di tipo due. Infatti $x \in T(X)$ implica che $x \in \underline{pq}$ con $p \in X$ e $q \in X$, e quindi $x \in T(\{p, q\})$. Ne segue che:

- l'intersezione di una famiglia di insiemi convessi è ancora un insieme convesso;
- dato un insieme X esiste il più piccolo insieme convesso $D(X)$ contenente X e lo si può ottenere come unione della catena $T^1(X), T^2(X), \dots$

3. Sottostruttura di una struttura algebrica generata da un dato insieme

In questo paragrafo faremo alcuni esempi di operatori algebrici e di applicazioni del teorema di punto fisso. Cominciamo con le strutture algebriche. Se X_1, \dots, X_n sono sottoinsiemi di una struttura algebrica con dominio D ed h è una operazione n -aria, allora chiamiamo *immagine di X_1, \dots, X_n tramite h* l'insieme

$$h(X_1, \dots, X_n) = \{h(x_1, \dots, x_n) : x_1 \in X_1, \dots, x_n \in X_n\}.$$

Ad esempio se consideriamo la somma nell'insieme R dei numeri reali, ed $X_1 = \{1, 3, 7\}$ e $X_2 = \{1, 3\}$, allora $X_1 + X_2 = \{1+1, 1+3, 3+1, 3+3, 7+1, 7+3\} = \{2, 4, 6, 8, 10\}$. Una parte D' di D si dice *stabile rispetto ad una operazione h* se

$$d_1, \dots, d_n \in D' \Rightarrow h(d_1, \dots, d_n) \in D',$$

o, equivalentemente, se $h(D', \dots, D') \subseteq D'$. Pertanto se D' è stabile la restrizione di h a D' è una operazione in D' che indichiamo con h/D' .

Proposizione 1. Siano h_1, \dots, h_r operazioni in un insieme D e consideriamo l'operatore $T : \Pi(D) \rightarrow \Pi(D)$ definito ponendo, per ogni $X \subseteq D$

$$T(X) = X \cup h_1(X, \dots, X) \cup \dots \cup h_r(X, \dots, X).$$

Allora T è un operatore algebrico ed i punti fissi di T sono le parti stabili di D . Ne segue che l'intersezione di una famiglia di parti stabili di D è una parte stabile di D e che, se indichiamo con $\langle X \rangle$ la parte stabile generata da X , allora

$$\langle X \rangle = \bigcap_{n \in \mathbb{N}} T^n(X).$$

Dim. E' immediato che T è monotono e che verifica la proprietà di inclusione. Che T sia compatto si prova osservando che se $x \in T(X)$ allora :

- se $x \in X$ allora $F = \{x\}$ è un sottoinsieme finito di X tale che $x \in T(F)$,
- se $x = I(h)(d_1, \dots, d_r)$ con $d_1 \in X, \dots, d_r \in X$ ed h operazione n -aria, allora $F = \{d_1, \dots, d_r\}$ è un sottoinsieme finito di X tale che $x \in T(F)$,
- se $x = I(c)$ allora $x \in T(\emptyset)$.

La rimanente parte della proposizione è evidente. □

Esempio. Dato un gruppo $G = (D, \cdot, ^{-1}, 1)$ ed i sottoinsiemi X_1 e X_2 , X di G poniamo

$$X_1 \cdot X_2 = \{x_1 \cdot x_2 \mid x_1 \in X_1 \text{ e } x_2 \in X_2\} \quad ; \quad X^{-1} = \{x^{-1} \mid x \in X\}.$$

Pertanto $X_1 \cdot X_2$ è l'insieme di tutti gli elementi che si possono ottenere come prodotto di un elemento di X_1 ed un elemento di X_2 e X^{-1} è l'insieme di tutti gli inversi di elementi di X . Allora

$$T(X) = X \cup (X \cdot X) \cup X^{-1} \cup \{1\}.$$

In altri termini $T(X)$ è l'insieme che si ottiene aggiungendo ad X tutti i prodotti di due elementi di X , gli inversi degli elementi di X e l'unità. T è un operatore algebrico, di tipo due ma non è un operatore di chiusura. I punti fissi di T sono tutti e soli i sottogruppi e quindi la classe dei sottogruppi costituisce un sistema di chiusura. Inoltre il sottogruppo generato da un sottoinsieme X di G si può ottenere iterando l'operatore T .

Problema. Consideriamo la struttura algebrica (N, mcd) dove $mcd(n, m)$ è il massimo comun divisore tra n ed m . Dire quale è la parte stabile generata da $\{15, 25, 8, 4\}$.

4. Relazioni di equivalenza e congruenze generate da una data relazione

La nozione di operatore di chiusura permette di costruire relazioni binarie con proprietà che si ritengono opportune. Cominciamo con le relazioni riflessive.

Proposizione 1. Sia D un insieme non vuoto, sia P una relazione binaria in D e poniamo

$$Rifl(P) = P \cup Diag(D).$$

Allora $Rifl : \Pi(D^2) \rightarrow \Pi(D^2)$ è un operatore di chiusura i cui punti fissi sono le relazioni riflessive.

Pertanto, $Rifl(P)$ è la più piccola relazione riflessiva contenente P . Ad esempio se $<$ è l'usuale relazione di ordine stretto in N allora $Rifl(<)$ è la relazione \leq .

Proposizione 2. Sia D un insieme non vuoto, sia P una relazione binaria in D e poniamo

$$Simm(P) = P \cup P^{-1}.$$

Allora $Simm : \Pi(D^2) \rightarrow \Pi(D^2)$ è un operatore di chiusura i cui punti fissi sono le relazioni simmetriche.

Pertanto $Simm(P)$ è la più piccola relazione simmetrica contenente P .

Proposizione 3. Poniamo

$$Tr(P) = (P \circ P) \cup P$$

Allora $Tr : \Pi(D^2) \rightarrow \Pi(D^2)$ è un operatore algebrico i cui punti fissi sono le relazioni transitive.

Ne segue che l'operatore $Trans : \Pi(D^2) \rightarrow \Pi(D^2)$ definito ponendo

$$Trans(P) = \bigcap Tr^n(P),$$

è un operatore di chiusura algebrico i cui punti fissi sono le relazioni transitive e $Trans(P)$ è la più piccola relazione transitiva contenente P . Un modo più esplicito per ottenere la chiusura transitiva di una relazione è il seguente.

Proposizione 4. Sia P una relazione binaria e chiamiamo *percorso* una successione x_1, \dots, x_n tale che $x_i P x_{i+1}$ per $i = 1, \dots, n-1$. Allora

$$Trans(P) = \{(x,y) \mid \text{esiste un percorso } x_1, \dots, x_n \text{ tale che } x_1 = x, x_n = y\}.$$

Proposizione 5. Poniamo

$$Ord(P) = Trans(Rifl(P)).$$

Allora $Ord : \Pi(D^2) \rightarrow \Pi(D^2)$ è un operatore di chiusura algebrico i cui punti fissi sono le relazioni di pre-ordine. Inoltre $Ord(P)$ è la più piccola relazione di preordine contenente P .

Dim. Abbiamo che $Trans$ e $Rifl$ commutano e quindi i punti fissi di Ord sono le relazioni che sono sia punto fisso di $Trans$ che punto fisso di $Rifl$.

Allo stesso modo si dimostrano le seguente proposizioni

Proposizione 6. Poniamo

$$SR(P) = Simm(Rifl(P)).$$

Allora $SR : \Pi(D^2) \rightarrow \Pi(D^2)$ è un operatore di chiusura algebrico i cui punti fissi sono le relazioni che sono riflessive e simmetriche.

Dim. Abbiamo che $Simm$ e $Rifl$ commutano e quindi i punti fissi di SR sono le relazioni che sono sia punto fisso di $Simm$ che punto fisso di $Rifl$.

Proposizione 7. Poniamo

$$Eq(P) = Trans(SR(P)).$$

Allora $Eq : \Pi(D^2) \rightarrow \Pi(D^2)$ è un operatore di chiusura algebrico i cui punti fissi sono le relazioni di equivalenza. Ne segue che $Eq(P)$ è la più piccola relazione di equivalenza contenente P . Inoltre la classe delle relazioni di equivalenza in un dato insieme costituisce un sistema di chiusura e quindi un reticolo completo.

Abbiamo visto come a partire da una qualunque relazione binaria sia possibile generare una relazione di equivalenza. Se tale relazione binaria è definita in una struttura algebrica possiamo generare anche una relazione di congruenza.

Teorema 8. Sia D il dominio di una struttura A e definiamo l'operatore $Con : \Pi(D^2) \rightarrow \Pi(D^2)$ ponendo, per ogni relazione P ,

$$Con(P) = P \cup \{(h(d_1, \dots, d_n), h(\underline{d}_1, \dots, \underline{d}_n)) : h \text{ operazione } n\text{-aria } d_1 P \underline{d}_1, \dots, d_n P \underline{d}_n\}.$$

Allora l'operatore $Cong : \Pi(D^2) \rightarrow \Pi(D^2)$ definito ponendo

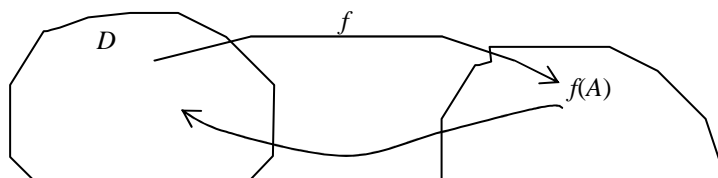
$$Cong(P) = Con(Eq(P))$$

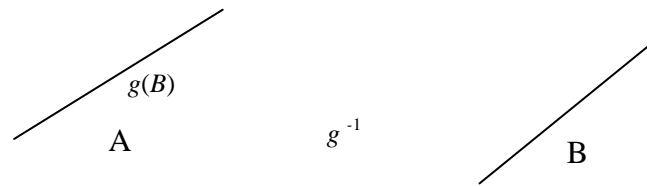
è un operatore algebrico i cui punti fissi sono le congruenze di A . Ne segue che la classe delle congruenze di A costituisce un sistema di chiusura e quindi un reticolo completo.

5*. Punti fissi e Teorema di Cantor-Bernstein

Diamo ora un esempio di applicazione della teoria degli operatori algebrici. Ricordiamo che il teorema di Cantor Bernstein afferma che:

Dati due insiemi A e B supponiamo che A abbia potenza minore o uguale B e che B abbia potenza minore o uguale ad A , allora A e B sono equipotenti.





Per tentare di trovare una dimostrazione di tale teorema dobbiamo partire dal fatto che esistono due funzioni iniettive $f: A \rightarrow B$ e $g: B \rightarrow A$ e dobbiamo trovare una funzione biettiva h di A in B . Se f fosse suriettiva potremmo porre semplicemente $h = f$. Se g fosse suriettiva potremmo invertire g e porre $h = g^{-1}$. In entrambi i casi il problema sarebbe risolto. Supponiamo pertanto che f e g non siano suriettive. L'idea che potremmo allora utilizzare per costruire una funzione biettiva $h: A \rightarrow B$ è quella di:

- fare operare in alcuni casi la funzione $f: A \rightarrow B$ (che è iniettiva ma non suriettiva)
 - in altri casi fare operare la funzione $g^{-1}: A' \rightarrow B$, dove $A' = g(B)$, (che è suriettiva in A' ma non è ovunque definita).

In altri termini l'idea è che sia possibile trovare un sottoinsieme $D \subseteq A$ in modo che la funzione

$$h(x) = \begin{cases} f(x) & \text{se } x \in D \\ g^{-1}(x) & \text{se } x \notin D \end{cases}$$

sia la funzione cercata. Si tratta ora di capire come dovrebbe essere un tale insieme perché il tutto funzioni e, naturalmente, cercare di dimostrare che tale insieme esiste.

1. Per prima cosa, perché la definizione abbia senso ogni elemento $x \notin D$ deve avere una anti-immagine $g^{-1}(x)$ e questo si ottiene solo se risulta

$$-D \subseteq g(B).$$

2. Inoltre, perché la funzione h sia iniettiva è sufficiente supporre che:

$$f(D) \cap g^{-1}(-D) = \emptyset.$$

Infatti, essendo sia f che g^{-1} iniettive in D e $-D$, rispettivamente, la non iniettività di h si potrebbe realizzare solo se esistessero $x \in D$ ed $y \in -D$ tali che $h(x) = f(x) = g^{-1}(y) = h(y)$ e ciò comporterebbe che $h(x) \in f(D) \cap g^{-1}(-D)$.

3. Infine perché g sia suriettiva deve accadere che

$$h(A) = f(D) \cup g^{-1}(-D) = B.$$

Riassumendo, dobbiamo trovare un sottoinsieme D di A tale che:

$$1) \quad -D \subseteq g(B) \quad 2) \quad f(D) \cap g^{-1}(-D) = \emptyset \quad 3) \quad f(D) \cup g^{-1}(-D) = B$$

cioè tale che

$$1. \quad D \supseteq -g(B) \quad ; \quad 2. \quad g^{-1}(-D) = -f(D)$$

Dalla prima inclusione si ricava che $-g(B) \supseteq -D$ e quindi $g(g^{-1}(-D)) = -D \cap g(B) = -D$. Pertanto, poiché dalla seconda equazione $g(g^{-1}(-D)) = g(-f(D))$ e passando al complemento, si ricava che

$$D = -g(-f(D)). \quad (1)$$

Viceversa, da (1) segue subito che $D \supseteq -g(B)$ e che $g^{-1}(-D) = g^{-1}(g(-f(D))) = -f(D)$ e quindi le due condizioni che vogliamo imporre a D equivalgono all'unica condizione (1). In definitiva, indicando con $T: P(A) \rightarrow P(A)$ l'operatore definito ponendo

$$T(X) = -g(-f(X)), \quad (2)$$

¹ Se f è una funzione di S in T ed X è un sottoinsieme di S allora $f^{-1}(f(X)) = X$. Invece se Y un sottoinsieme di T allora

$f(f^{-1}(Y))$ non coincide con Y . Infatti se y è un elemento di Y di cui non è possibile fare l'anti-immagine in quanto non appartiene ad $f(T)$, allora y "scompare" quando si calcola $f(f^{-1}(Y))$. In realtà vale l'equazione $f(f^{-1}(Y)) = Y \cap f(S)$.

dobbiamo provare che esiste un insieme D tale che

$$D = T(D).$$

Siamo allora giunti al seguente punto :

la dimostrazione del teorema di Cantor-Bernstein si riconduce alla dimostrazione che l'equazione

$$T(X) = X \tag{3}$$

ammette soluzione o, equivalentemente che T abbia un punto fisso.

Allo scopo di applicare il teorema 4 del paragrafo 3, osserviamo che T è monotono. Infatti al crescere di X :

- $f(X)$ cresce
- quindi $-f(X)$ decresce
- quindi $g(-f(X))$ decresce
- quindi $-g(-f(X))$ cresce.

Per verificare che T è compatto supponiamo che $x \in T(X)$. Allora se fosse $x \in H(\emptyset)$ la finitezza sarebbe dimostrata. Supponiamo che $x \notin T(\emptyset)$ e quindi, essendo $H(\emptyset) = -g(B)$, che $x \in g(B)$. Detto allora $b \in B$ tale che $x = g(b)$. Poiché $x \in T(X) = -g(-f(X))$, non può essere $b \notin f(X)$. Sia allora $a \in X$ tale che $b = f(a)$ e quindi tale che $x = g(f(a))$. Proviamo che $x \in T(\{a\})$. Infatti

$$T(\{a\}) = -g(B - \{f(a)\}) = -(g(B) - g(f(a))) = A - g(B) \cup \{g(f(a))\}.$$

In conclusione T è compatto e quindi, per il citato teorema, ammette un punto fisso. Volendo calcolare tale punto fisso dobbiamo considerare l'insieme $D = \bigcup_{n \in \mathbb{N}} T^n(\emptyset)$. Questo significa che dobbiamo calcolare due successioni A_0, A_1, A_2, \dots e B_0, B_1, B_2, \dots al modo seguente:

$$\begin{array}{ll} A_1 = T(\emptyset) = -g(B) & ; \quad B_1 = -f(A_1) \\ A_2 = T(T(\emptyset)) = -g(B_1) & ; \quad B_2 = -f(A_2) \\ \dots & \\ A_n = T^{n+1}(\emptyset) = -g(B_n) & ; \quad B_n = -f(A_n) \\ \dots & \end{array}$$

e poi porre $D = \bigcup_{n \in \mathbb{N}} A_n$.

6. Relazioni, giochi e labirinti

In questo paragrafo introdurremo strutture matematiche che permettono di rappresentare le più svariate situazioni in cui si debba risolvere un problema. Cominciamo con l'osservare che spesso

risolvere un problema consiste nel fare una serie di "azioni" che facciano passare da uno stato iniziale ad uno stato che si possa considerare soluzione del problema.

Naturalmente non tutte le azioni sono possibili e questo perché alcune o sono vietate oppure non sono "fisicamente" possibili. Allora nell'insieme S degli stati è definita una relazione binaria R il cui significato è che $(x,y) \in R$ se e solo se è possibile passare dallo stato x allo stato y . Consideriamo ad esempio un qualunque solitario di carte in cui si dispongono in qualche modo le carte sul tavolo. Chiamiamo *stato* una qualunque possibile distribuzione di carte sul tavolo ed indichiamo con S l'insieme degli stati. Si risolve il solitario se si raggiunge una configurazione c che viene considerata vincente (ad esempio disporre le carte in ordine crescente in quattro gruppi dello stesso colore). Le regole del solitario si possono rappresentare da una relazione binaria $R \subseteq S \times S$ in modo che sRs' che esiste una mossa (corretta in base al regolamento del gioco) che permette di passare dallo stato s allo stato s' . Risolvere il solitario significa trovare una successione s_1, s_2, \dots, s_n di stati tali che

- i) s_1 sia lo stato iniziale (in generale scelto in modo casuale cioè dopo aver mescolato le carte)
- ii) $(s_i, s_{i+1}) \in R$ cioè è lecito passare da s_i a s_{i+1} per ogni $i = 1, \dots, n-1$
- iii) s_n appartenga all'insieme delle configurazioni considerate vincenti.

Spesso la relazione R viene rappresentata tramite una freccia \rightarrow e si scrive $x \rightarrow y$ per indicare che è possibile passare da x ad y . In definitiva abbiamo la seguente definizione:

Definizione 1. Chiamiamo *sistema di riduzione* o *sistema di trasformazioni* una coppia (S, \rightarrow) con S insieme non vuoto e \rightarrow relazione binaria su S . Gli elementi di S vengono chiamati *stati*. Chiameremo *solitario* o *gioco ad una persona* una struttura $(S, \rightarrow, GOAL)$ dove (S, \rightarrow) è un sistema di trasformazioni e $GOAL$ è un insieme di stati chiamati *stati vincenti*.

Essendo un sistema di riduzione una relazione binaria, possiamo sempre rappresentarlo tramite un grafo. Un gioco sarà allora un grafo tale che alcuni dei suoi punti sono segnati come vincenti. Se la coppia x e y di elementi di S è nella relazione \rightarrow allora diremo che y è un *ridotto diretto* di x e scriveremo $x \rightarrow y$. Indichiamo con \rightarrow^* la chiusura transitiva di \rightarrow e se $x \rightarrow^* y$ diremo che y è un *ridotto* di x . Per quanto abbiamo provato sulla chiusura transitiva di una relazione, y è un ridotto di x se esiste un percorso a_1, \dots, a_n tale che $a_1 = x$ e $a_n = y$. Indicheremo con $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_{n-1} \rightarrow a_n$ un tale percorso. Un percorso a valte viene chiamato anche una successione di riduzioni.

Definizione 2. Dato un gioco $(S, \rightarrow, GOAL)$ chiamiamo *soluzione di stato iniziale* a un percorso $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_{n-1} \rightarrow a_n$ tale che $a_1 = a$ ed $a_n \in GOAL$. Chiamiamo *strategia* una funzione $f : S \rightarrow S$ che associa ad ogni stato $x \in S$ un nuovo stato $f(x)$ tale che $x \rightarrow f(x)$ se $\{y \in S : x \rightarrow y\}$ è non vuoto, $f(x) = x$ altrimenti. Una strategia si dice *vincente* se per ogni x esiste $n \in \mathbb{N}$ tale che $x \rightarrow f(x) \rightarrow f^2(x) \rightarrow \dots \rightarrow f^n(x)$ è una soluzione di stato iniziale x .

Pertanto una strategia vincente permette, dato un qualunque stato di partenza x , di arrivare ad uno stato vincente $f^n(x)$ dopo un numero finito n di “mosse”.



Un labirinto

Per mostrare come un tale formalismo permetta di rappresentare le situazioni più diverse, consideriamo uno dei problemi più antichi, quello dei labirinti. Un labirinto è un percorso in cui di tanto in tanto si deve scegliere tra più strade quale strada seguire. Lo scopo del gioco è quello di uscire dal labirinto. Un modo equivalente di rappresentare un labirinto è quello di considerare un insieme S di “stanze” più una relazione \rightarrow definita ponendo $x \rightarrow y$ se esiste un collegamento (una porta) tra una stanza e l'altra. Alcune stanze sono considerate “vincenti” (ad esempio le stanze che comunicando con l'esterno e che permettono quindi di uscire, oppure stanze in cui esiste un “tesoro”). Risolvere il gioco del labirinto a partire da una data stanza s_1 significa trovare una successione

s_1, s_2, \dots, s_n di stanze tale che:

- i) per ogni $i = 1, \dots, n-1$ sia possibile passare da s_i a s_{i+1}
- iii) s_n sia una delle stanze in cui esiste una porta di uscita.



Il gioco del quindici

Un altro famoso gioco è il gioco del quindici. Si tratta di un quadrato di plastica su cui sono inserite 15 tessere quadrate numerate mentre un quadrato rimane vuoto. Le mosse consentite sono solo spostare una delle tessere nello spazio vuoto (liberando in questo modo un altro spazio vuoto). Si vince se si riesce, partendo da una configurazione iniziale scelta a caso, a raggiungere una configurazione che si ritiene vincente. Ad esempio può essere considerata vincente la configurazione in cui tutti i numeri sono messi successivamente come nella figura affianco.

7. Parole e linguaggi come oggetti matematici: le grammatiche.

Chiamiamo *alfabeto* un qualunque insieme A di elementi, chiamiamo *parola* di lunghezza n sull'alfabeto A un qualunque elemento di A^n , cioè una qualunque n -pla di elementi di A . Nel seguito indicheremo con A^+ l'insieme delle parole sull'alfabeto A , pertanto risulterà $A^+ = \bigcup_{n \in \mathbb{N}} A^n$. Inoltre, invece di usare la notazione insiemistica (a_1, \dots, a_n) per indicare una parola, scriveremo semplicemente $a_1 \dots a_n$. Ad esempio se A è l'alfabeto $\{a, c, d\}$ allora scriveremo ad, aac, caa per denotare le parole (a, d) , (a, a, c) e (c, a, a) rispettivamente. D'altra parte sarebbe ragionevole considerare la nozione di parola come nozione primitiva invece di ricorrere a quella meno intuitiva di n -pla che è di natura insiemistica. Spesso l'insieme A^+ viene visto come una struttura algebrica quando si consideri la semplice operazione di "mettere una parola dopo l'altra". Ricordiamo che in algebra prende il nome di *semigrutto* ogni struttura (D, \cdot) con una operazione binaria che sia associativa. Prende il nome di *monoide* ogni semigrutto che ammette un elemento neutro, cioè un elemento ϕ tale che $x \cdot \phi = \phi x = x$.

Definizione 1 Chiamiamo *semi-grutto libero sull'alfabeto* A la struttura (A^+, \cdot) dove \cdot è l'operazione che associa a due parole p e q la parola pq che si ottiene ponendo le parole p e q una di seguito all'altra. In termini di n -ple l'operazione è definita dalla equazione

$$(x_1, \dots, x_n)(y_1, \dots, y_p) = (x_1, \dots, x_n, y_1, \dots, y_p).$$

Sia ϕ un qualunque simbolo non appartenente ad A e poniamo $A^* = A^+ \cup \{\phi\}$. Chiamiamo *monoide libero sull'alfabeto* l'estensione di (A^+, \cdot) ottenuta ponendo $x \cdot \phi = \phi x = x$ per ogni $x \in A^*$.

A volte il simbolo ϕ prende il nome di *parola vuota*.

Proposizione 2. (A^+, \cdot) è un semigrutto non commutativo che ammette l'insieme A come sistema di generatori. Analogamente (A^*, \cdot, ϕ) è un monoide non commutativo con A come sistema di generatori. In tale monoide nessun elemento diverso da ϕ ammette simmetrico.

In generale dato un alfabeto non tutte le parole sono accettate in un linguaggio. Ad esempio, con riferimento al linguaggio dei polinomi, se $A = \{x, y, +, \cdot, (,)\}$ allora sono parole su A le sequenze (i polinomi) $x \cdot x$, $x \cdot y$, $(x+y) \cdot x$ ma sono parole anche espressioni insensate come $x(yy+ ((, e ()))$. Il concetto di "linguaggio" si ottiene appunto quando sia stato indicato qualche modo per distinguere le parole "sensate" da quelle "non sensate" (quelle scritte "secondo le regole" da quelle "scritte male") quindi, estensionalmente, quando si sia definito un sottoinsieme di A^+ .

Definizione 3. Chiamiamo *linguaggio formale* sull'alfabeto A ogni sottoinsieme Λ di A^+ .

Un linguaggio Λ può essere dato, nel caso sia finito, mediante un elenco delle parole che lo compongono, ma in genere un linguaggio Λ viene dato tramite un insieme di regole capaci di produrre i suoi elementi e pertanto può essere anche infinito. Ad esempio, è possibile costruire gli elementi di un linguaggio "dal basso" indicando esplicitamente alcune parole-base di Λ ed alcuni procedimenti per costruire nuovi elementi di Λ a partire da dati elementi di Λ .

Esempio. Con riferimento all'alfabeto A dato sopra, potremmo avere le seguenti regole che definiscono il linguaggio dei polinomi nelle variabili x ed y :

i) x ed y sono elementi di Λ

ii) se α e β sono elementi di Λ allora anche $(\alpha)(\beta)$, e $(\alpha)+(\beta)$ sono elementi di Λ .

Il linguaggio dei polinomi viene definito come il più piccolo sottoinsieme di A^* contenente x ed y e chiuso rispetto la regola ii).

Uno dei modi principali per generare un linguaggio è tramite le grammatiche.

Definizione 4. Una *grammatica* è una quadrupla $G = (V, A, P, s)$ con:

- V (insieme delle *variabili ausiliari*) ed A (insieme dei *simboli terminali*) insiemi finiti disgiunti;

- s elemento prefissato di V detto *start-simbolo*;

- P insieme finito di espressioni del tipo $\alpha \rightarrow \beta$ (dette *produzioni*) con α e β parole nell'alfabeto $C = V \cup A$.

Ogni produzione $\alpha \rightarrow \beta$ va intesa come possibilità di sostituire in una parola alcune occorrenze di α con β . Se la parola y si ottiene dalla parola x tramite una tale sostituzione allora si dice che y deriva direttamente da x . Più precisamente, se $\alpha \rightarrow \beta$ è un elemento di P ed δ e γ sono elementi di C^+ allora diremo che $\gamma\beta\delta$ deriva direttamente da $\gamma\alpha\delta$ che $\beta\delta$ deriva direttamente da $\alpha\delta$ e che $\gamma\beta$ deriva direttamente da $\gamma\alpha$. Chiameremo *derivazione* una catena finita x_1, \dots, x_n di elementi di C^+ tali che x_{i+1} deriva direttamente da x_i per $i = 1, \dots, n-1$; in tale caso, se $\alpha = x_1$ e $\beta = x_n$, scriveremo $\alpha \mid \rightarrow \beta$. In altri termini β deriva da α nella grammatica G se è possibile ottenere β da α mediante una ripetuta sostituzione di sottoparole in accordo con quanto consentito dalle regole di produzione elencate in P .

Definizione 5. Diremo che un linguaggio Λ nell'alfabeto A è *producibile* dalla grammatica G se gli elementi di Λ si possono caratterizzare come le parole nell'alfabeto terminale A che si possono derivare dallo start simbolo s cioè se $\Lambda = \{x \in A^+ : s \mid \rightarrow x\}$. Chiamiamo *complessità* di un elemento x di Λ la minima lunghezza delle derivazioni che consentono di ottenere x .

Il concetto di complessità è fondamentale perchè, come vedremo, la maggior parte delle definizioni e delle dimostrazioni relative alle parole di un linguaggio avvengono per induzione sulla complessità. Nel seguente esempio gli alfabeti V ed A sono a loro volta insiemi di parole in un altro alfabeto.

Esempio. Vediamo come sia possibile costruire, tramite una opportuna grammatica, una piccolissima fetta della lingua italiana. Poniamo:

$V = \{\text{asserzione, articolo, soggetto, predicato}\}$

$A = \{\text{il, cane, gatto, abbaia, corre}\}$

e supponiamo che le produzioni siano:

asserzione \rightarrow *articolo soggetto predicato*;

articolo \rightarrow *il* ;

articolo \rightarrow *un* ;

soggetto \rightarrow *cane* ;

soggetto \rightarrow *gatto* ;

predicato \rightarrow *corre* ;

predicato \rightarrow *abbaia* .

Assunto come start-simbolo la variabile "*asserzione*", il linguaggio della grammatica definita in questo modo consentirà di produrre frasi del tipo

"*il cane abbaia*", "*il gatto abbaia*", "*il cane corre*", "*il gatto corre*".

Ad esempio, abbiamo la derivazione

asserzione, articolo cane predicato, il cane predicato, il cane abbaia

che si ottiene utilizzando le produzioni

asserzione \rightarrow *articolo soggetto predicato, soggetto* \rightarrow *cane, articolo* \rightarrow *il, predicato* \rightarrow *abbaia*.

Non deve stupire il fatto che sia producibile una frase del tipo "*il gatto abbaia*" in quanto una grammatica non garantisce che le frasi costruite siano vere ma solo che siano scritte correttamente.

Aumentando il numero di possibili soggetti (compatibili con l'articolo "il") e predicati (in terza persona singolare) è possibile ottenere un maggior numero di frasi della lingua italiana scritte correttamente. La costruzione di una grammatica capace di produrre (e controllare) l'intera lingua italiana è ovviamente una cosa complicatissima e non ancora completamente realizzata. Una realizzazione di un metodo di controllo permetterebbe, ad esempio, di programmare un sistema di scrittura che corregga automaticamente gli errori di grammatica.

Nota 1. L'esempio precedente fornisce un tipo di grammatica capace di produrre solo un numero finito di frasi. Ciò è dovuto al fatto che non ci sono "produzioni che chiamano se stesse". Possiamo modificare tale esempio aggiungendo una produzione del tipo

$$\text{discorso} \rightarrow \text{asserzione e discorso} \quad ; \quad \text{discorso} \rightarrow \text{asserzione}$$

dopo aver aggiunto "discorso" a V e la lettera "e" ad A . In tale caso si deve considerare come start-simbolo "discorso". È evidente che, per la seconda di tali produzioni, sarà possibile produrre tutte le frasi della grammatica precedente ma che per la prima di tali produzioni sarà possibile scrivere frasi di lunghezza non determinata.

Esempio. Sia G una grammatica in cui $A = \{a,b\}$, $V = \{v\}$, $P = \{v \rightarrow ava, v \rightarrow b\}$ e v è lo start-simbolo. Allora una derivazione è costituita dalla successione

$$v, \text{ava}, \text{aavaa}, \text{aabaa}.$$

Pertanto la parola *aabaa* appartiene al linguaggio generato da G .

Esercizio. Dire quali delle parole *abb*, *ava*, *aaabaaa*, *aba*, appartiene al linguaggio generato dalla grammatica G ora definita e trovarne la relativa complessità. Scrivere una parola del relativo linguaggio di lunghezza maggiore di 5.

Esercizio. Trovare una grammatica capace di generare l'insieme delle parole del tipo $(ab)^n$.

Nota 2. La nozione di grammatica non è nata nell'ambito informatico. Essa è stata proposta per la prima volta dal linguista americano Noam Chomsky nel 1957. La questione affrontata da Chomsky è quella di capire l'origine della straordinaria capacità dei bambini di scoprire le "regole" che stanno alla base del linguaggio. E questo a partire da un numero limitatissimo di emissioni verbali dei genitori e delle persone che li circondano. Questa capacità è tanto più sorprendente quanto si consideri che da un numero finito di casi i bambini apprendono il modo di produrre un numero potenzialmente infinito di frasi. La nozione di grammatica fornisce in un certo senso una risposta a questioni di tale tipo, essendo una grammatica un "oggetto finito" capace di produrre, a partire da un numero finito di oggetti (le parole apprese dall'ambiente) un numero potenzialmente infinito di frasi.

8. I sistemi di riscrittura.

Una categoria di giochi che sono molto collegati con la matematica sono i *sistemi di riscrittura* che sono giochi i cui gli stati sono parole di un linguaggio. Ad esempio consideriamo il problema di risolvere le equazioni di primo grado in una incognita. Chiamiamo con S l'insieme di tutte le possibili equazioni di primo grado, ad esempio

$$3x+5 = x-3x, \quad x = x-3(x+1), \quad \dots$$

Poniamo $GOAL$ uguale all'insieme delle equazioni del tipo $x = k$. Se chiamiamo equivalenti due equazioni che abbiano le stesse soluzioni, il problema che si pone è, data una equazione, di arrivare ad una equazione equivalente appartenente a $Goal$. Ciò deve essere fatto "rispettando le regole", cioè tramite una serie di operazioni che facciano passare da una equazione ad una equazione equivalente, cioè che abbia le stesse soluzioni.

Le operazioni che usualmente si utilizzano sono le seguenti:

1. passare una quantità che si somma da un lato all'altro di una equazione facendola diventare una quantità che si sottrae
2. passare una quantità che si sottrae da un lato all'altro di una equazione facendola diventare una quantità che si somma
3. passare una quantità che si moltiplica da un lato all'altro facendola diventare una quantità che divide
4. passare una quantità che si divide da un lato all'altro facendola diventare una quantità che moltiplica
5. applicare tutte le leggi dell'aritmetica (proprietà distributiva, proprietà commutativa, ...)

6. effettuare tutti i calcoli che si possono fare.

Ad esempio, partendo da $3x+5=x-3x+1$ e saltando qualche passaggio, otteniamo

$$3x+5=x-3x+1 \text{ (punto di partenza)}$$

$$3x+5 = -2x+1 \text{ (per la regola 6)}$$

$$3x+5+2x = +1 \text{ (per la regola 2)}$$

$$5x +5= +1 \text{ (per la regola 6)}$$

$$5x = -5+1 \text{ (per la regola 1)}$$

$$5x = -4 \text{ (per la regola 6)}$$

$$x = -4/5 \text{ (per la regola 3)}$$

In questo esempio una strategia consiste nello scegliere ad ogni passo nell'ordine:

“di fare i calcoli che si possono fare”

“di spostare tutte le variabili al primo membro dell'equazione”

“di spostare tutte le costanti al secondo membro dell'equazione”

Definizione 1. Un *sistema di riscrittura* è un gioco $(S, \rightarrow, GOAL)$ in cui S è l'insieme delle parole in un linguaggio L . Un sistema di *riduzione a forma normale* è un sistema di riscrittura in cui $GOAL$ è l'insieme delle foglie di \rightarrow . In tale caso diciamo che un elemento in $GOAL$ è in *forma normale*.

Da notare che nell'esempio delle equazioni abbiamo specificato anche la regola adottata in ogni passo. Questo significa che il gioco è stato descritto fornendo più regole ed una soluzione del gioco consiste anche nello specificare quale regola si è applicata. Quando si procede in questo modo è più utile la seguente definizione.

Definizione 2. Chiamiamo *sistema di riscrittura a più regole* una struttura $(S, (\rightarrow_i)_{i \in I}, GOAL)$ dove S è un linguaggio su di un dato alfabeto e $(\rightarrow_i)_{i \in I}$ è una famiglia di relazioni binarie dette *regole di riscrittura*.

Come viene fatto di solito per le relazioni binarie useremo la notazione infissa scrivendo $x \rightarrow_i y$ per indicare che $(x, y) \in \rightarrow_i$ cioè che x è nella relazione \rightarrow_i con y . In tale caso diremo anche che la parola x si può *riscrivere nella parola y in accordo con la regola di indice i* .

Proposizione 3. Dato un sistema di riscrittura a più regole $(S, (\rightarrow_i)_{i \in I}, GOAL)$, viene definito un sistema di riscrittura ad una regola $(S, \rightarrow, GOAL)$, ponendo \rightarrow uguale alla relazione che si ottiene come unione delle relazioni \rightarrow_i .

In altri termini poniamo $x \rightarrow y$ se esiste $i \in I$ tale che $x \rightarrow_i y$. Ci riferiamo a \rightarrow quando non interessa sapere quale regola è stata utilizzata per passare dallo stato x allo stato y ma solo che è consentito passare da x ad y .

Esempio, espressioni aritmetiche. Sia L l'insieme delle espressioni che si possono scrivere coinvolgendo i numeri interi, la somma, il prodotto e la divisione. Ad esempio avremo in L espressioni del tipo

$$(3+5) \cdot 37 + 1, (1/3 + 1)/2, (2/3) \cdot (3/4 + 1), \dots$$

Possiamo allora chiamare *forma normale* ogni espressione del tipo n/m con n ed m rappresentazioni decimali di due interi primi tra loro. Allora quando si esegue una operazione, ad esempio il prodotto, il problema consiste nel passare dalla forma normale di due numeri x ed y alla forma normale di $x \cdot y$. Ad esempio, la somma di $3/5$ più $2/3$ seguirà la procedura di riscrittura

$$(3/5) + (1/3) \text{ (punto di partenza)}$$

$$(3 \cdot 3 + 5 \cdot 1) / (5 \cdot 3) \text{ (per la regola della somma per cui } n/m + p/q \text{ si può riscrivere in } (n \cdot q + m \cdot p) / (m \cdot q))$$

$$(19 + 10) / 15 \text{ (per le regole di calcolo del prodotto di due interi)}$$

$$29 / 15 \text{ (per le regole di calcolo della somma di due interi)}$$

Il prodotto di $3/5$ per $2/3$ avviene secondo le seguenti riscrittura

$$(3/5) \cdot (1/3) \text{ (punto di partenza)}$$

$(3 \cdot 1)/(5 \cdot 3)$ (per la regola per cui $n/m \cdot p/q$ si può riscrivere in $(n \cdot p)/(m \cdot q)$)

$3/15$ (per le regole di calcolo del prodotto)

$1/5$ (per le regole che permettono la riduzione di una frazione a numeratore e denominatore primi tra loro)

In generale si presenta la seguente situazione. Dato un linguaggio L si considera una relazione di equivalenza in L che, detto in termini intuitivi, corrisponde all'idea che due espressioni in L "rappresentano la stessa cosa". Ad esempio:

- in aritmetica consideriamo equivalenti due espressioni che denotano lo stesso numero
- in algebra chiamiamo equivalenti due equazioni che hanno le stesse soluzioni
- nel calcolo proposizionale, come vedremo, sono *logicamente equivalenti* due formule che danno luogo alla stessa tavola di verità.

Appare allora naturale porsi il problema di come si possa trasformare una espressione di L in una più semplice che sia equivalente. Questo viene fatto appunto tramite opportune "regole di riscrittura" in cui possiamo interpretare $x \rightarrow y$ dicendo che y è equivalente ad x ma è "più semplice" di x . Pertanto una parola in forma normale è una parola che non può essere ulteriormente semplificata. Il gioco consiste allora nel partire da una parola x e trasformarla in parole equivalenti fino a giungere ad una parola che non può essere più semplificata cioè che sia in forma normale.

Per indicare una tale successione scriveremo anche $a_1 \rightarrow a_2 \dots \rightarrow a_{n-1} \rightarrow a_n$. Analogamente, x è convertibile in y se e solo $x = y$ oppure se esiste una successione a_1, \dots, a_n tale che $a_1 \leftrightarrow a_2, a_2 \leftrightarrow a_3, \dots, a_{n-1} \leftrightarrow a_n$.

Definizione 4. Dato un sistema di riscrittura $(S, \rightarrow, GOAL)$, indichiamo con \equiv la relazione di equivalenza generata da \rightarrow . Se $x \equiv y$ diremo anche che x ed y sono *convertibili*.

Problema. Un problema di notevole importanza è il seguente:

Dato un insieme S ed una relazione di equivalenza \equiv trovare un sistema di riduzione la cui relazione di equivalenza associata \rightarrow coincida con \equiv ed inoltre tale che ogni elemento può essere ridotto a forma normale unica.

L'importanza di questo problema è che se si riesce a risolverlo allora in ogni classe di equivalenza è possibile trovare un particolare elemento rappresentativo ed inoltre è possibile lavorare sugli elementi rappresentativi invece che sulle classi.