article

ISSN 2421-7247

Semigroups, monoids and free groups

Panagiote Ligouras

Abstract. *The purpose of this paper is to present the experience with mathematics teachers and students of 21 years of age concerning some abstract algebraic structures and to observe how these concepts have been perceived.*

Key words. *Free Semigroups, free monoids, free groups, word problem, conjugacy problem.*

Sommario. (Semigruppi, monoidi e gruppi liberi). *Lo scopo di questo articolo è quello di presentare l'esperienza svolta con docenti di matematica e studenti di 21 anni di età inerente alcune strutture algebriche astratte e osservare come questi concetti siano stati percepiti.*

Parole chiave. *Semigruppi liberi, monoidi liberi, gruppi liberi*, problema della parola, problema del coniugio.

Introduzione

Molto spesso in matematica il problema cruciale consiste nell'individuare e scoprire quali siano i concetti rilevanti. Ciò fatto, metà del lavoro può considerarsi compiuto.

In questo senso è molto utile poter presentare i gruppi con l'aiuto di *generatori* e *relazioni*. Questa modalità ci consente non solo di definire i gruppi in modo conciso, ma anche di studiarne le proprietà e di costruire nuovi gruppi con le proprietà desiderate.

Più di cento anni fa ed esattamente nel 1911 Dehn [5] formulò le seguenti tre decisioni fondamentali di problemi relativi alle presentazioni di un gruppo.

Sia G un gruppo, definito per mezzo di una presentazione.

1) Il *problema della parola*: per ogni parola u nei generatori considerati, decidere se u definisce l'elemento di identità di G oppure no.
2) Il *problema della coniugazione*: per ogni due parole u, v nei generatori, decidere se u e v sono coniugate o meno, cioè se esiste una parola x nei generatori dati tale che $x^{-1}ux$ definisce lo stesso elemento di v.
3) Il *problema dell'isomorfismo*: dato un gruppo F, definito per mezzo di un'altra presentazione, decidere se G è isomorfo a F o meno.

Nelle pagine che seguono presenteremo concetti e tecniche che sono fondamentali sia per poter dare già alcune risposte ai tre problemi di Dehn che ad utilizzarle per costruire

ulteriori risposte a questioni specifiche della matematica e di altri settori del sapere.

Il materiale che segue è stato presentato in un seminario di un gruppo di 11 docenti di matematica che prestavano servizio in corsi con studenti di 17, 18 e 19 anni di età e a 5 studenti che frequentavano in quel periodo il secondo anno di corso universitario in matematica.

Semigruppi liberi

Definizione. Un insieme finito o infinito A di simboli prende il nome di *alfabeto*. Ogni elemento a dell' alfabeto A si chiama *lettera* di A o *lettera*. Ogni sequenza finita di lettere u si chiama *parola* di A o *stringa* di A o *parola*. Una parola u su A formata dalle lettere $a_1, a_2, \ldots, a_n \in A$, si scrive

$$u := a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

Nota. Anche una singola lettera dell'alfabeto si può considerare parola.

Per la formazione della parola sono ammesse ripetizioni della stessa lettera.

Definizione. Sia A un alfabeto. L'insieme A^+ formato da tutte le parole su A prende il nome *insieme delle parole* di A:

$$A^+ = \{u \mid u \text{ è una parola nell'alfabeto } A\}.$$

Definizione. Siano A un alfabeto e le parole $u, v \in A^+$. Si dice che le parole u e v sono uguali se sono identiche lettera per lettera. Due *parole uguali* si indicano

$$u \equiv v.$$

Definizione. Siano A un alfabeto e le parole $u, v \in A^+$, $u = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, $v := b_1 \cdot b_2 \cdot \ldots \cdot b_m$. Si considera l'operazione binaria chiamata *operazione di giustapposizione*

$$\bullet : A^+ \times A^+ \to A^+$$

tale che

$$u \bullet v = (a_1 \cdot a_2 \cdot \ldots \cdot a_n) \bullet (b_1 \cdot b_2 \cdot \ldots \cdot b_m) = a_1 \cdot a_2 \cdot \ldots \cdot a_n \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_m$$

o

$$u\, v = (a_1 \cdot a_2 \cdot \ldots \cdot a_n)(b_1 \cdot b_2 \cdot \ldots \cdot b_m) = a_1 \cdot a_2 \cdot \ldots \cdot a_n \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_m.$$

Proposizione. L'operazione di giustapposizione è associativa.

Nota. Con la notazione $a_1 \cdot a_2$ indichiamo la parola formata dalle lettere a_1 e a_2, mentre con la notazione $a_1 \bullet a_2$ oppure $a_1\, a_2$ indicheremo il prodotto delle lettere a_1 e a_2.

Definizione. Se $u \in A^+$, $u = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ è una parola, il numero n si chiama *lunghezza di u* e si indica con $\ell(u)$. Cioè, $\ell(u) = n$.

Nota. Alcuni autori per indicare la lunghezza di una parola usano il simbolo $|u|$ mentre altri [20, 7] usano $L(u)$.

Definizione. Siano $u \in A^+$, $u = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ una parola ed $1 \le i \le j \le n$. Si chiama *sub-parola di u*, la parola

$$u_{i\ldots j} = a_i \cdot \ldots \cdot a_j .$$

Osservazione. Le lettere da a_i ad a_j della sub-parola $u_{i\ldots j}$ devono essere le stesse della parola u e scritte nello stesso ordine.

Se $i = 1$ e $1 \leq j < n$, si chiama *prefisso di u* la sub-parola

$$pre_j(u) = a_1 \cdot \ldots \cdot a_j .$$

Se $j = n$ e $1 < i \leq n$, si chiama *suffisso di u* la sub-parola

$$suff_i(u) = a_i \cdot \ldots \cdot a_n .$$

Convenzione. In alcune situazioni per indicare che una parola v è un prefisso della parola u si usa la notazione

$$v \lhd u.$$

Osservazione. La parola vuota è una sub-parola (*subword*).

Definizione. L'insieme A^+ fornito dell'operazione binaria di giustapposizione forma un semigruppo chiamato *semigruppo delle parole*.

Definizione. Prende il nome *parola vuota* di A o *parola vuota* una parola senza nessuna lettera e si indica con il simbolo 1.

Esempio. La lunghezza della parola vuota 1 è zero: $\ell(1) = 0$.

Convenzione. La parola vuota si userà in seguito come elemento neutro della *giustapposizione*.

Definizione. Siano A un alfabeto, l'insieme A^+ delle parole su A e la parola vuota 1 di A^+. Si indica con A^* l'insieme

$$A^* = A^+ \cup \{1\}.$$

Definizione. L'insieme A^* fornito dell'operazione binaria di giustapposizione e della parola vuota forma un monoide chiamato *monoide delle parole* e si indica $(A^*, \bullet)$ o semplicemente A^*.

Nota. È da sottolineare che per ogni $u \in A^*$ si ha $1 \bullet u = u = u \bullet 1$.

Osservazione. Il monoide delle parole $(A^*, \bullet)$ non è un gruppo. Infatti, fino a questo punto non abbiamo definito cosa sono gli inversi delle parole.

Convenzione. Per alleggerire la scrittura delle parole dagli eccesivi simboli abitualmente si omette il segno di moltiplicazione tra le lettere.
Questo vuol dire che le scritture $u = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ e $u = a_1 a_2 \ldots a_n$ rappresentano la stessa parola.

Gruppi liberi

Come abbiamo viste nella sezione semigruppi liberi il monoide delle parole $(A^*, \bullet)$ non è un gruppo perché non soddisfa la proprietà dell'elemento inverso. Per poter arrivare ad avere la struttura di gruppo nell'insieme delle parole abbiamo bisogno di arricchire con nuovi elementi l'alfabeto A.

Definizione. Sia l'alfabeto A. Si definisce l'insieme dei simboli A^{-1} come segue

$$A^{-1} = \{x^{-1} \mid \text{per ogni } x \in A\}.$$

Osservazioni. È importante notare che non stiamo assumendo che x^{-1} sia l'inverso di x. Al momento questa affermazione non ha alcun significato.
Esiste un'applicazione biunivoca $\varepsilon : A \to A^{-1}$ tale che $\varepsilon(x) = x^{-1}$ per ogni $x \in A$.

Lemma. Valgono le seguenti

1) $A \cap A^{-1} = \{\ \}$.

2) $|A| = |A^{-1}|$

Definizione. Si indica con $\bar{A}$ l'insieme

$$\bar{A} = A \cup A^{-1}.$$

Definizione. L'insieme $\bar{A}$ di simboli prende il nome di *alfabeto*.
Ogni elemento a del alfabeto $\bar{A}$ si chiama *lettera* di $\bar{A}$ o *lettera*.
Ogni sequenza finita di lettere u si chiama *parola* di $\bar{A}$ o *stringa* di $\bar{A}$ o *parola*.
Una parola u di $\bar{A}$ formata da n lettere, si scrive

$$u = a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n}$$

dove $a_i \in \bar{A}$, $\varepsilon_i = \pm 1$ per ogni $0 \le i \le n$ e l'intero $n \ge 0$ che dipende dalla parola u.

Nota. Anche una singola lettera dell'alfabeto si può considerare parola.
Per la formazione della parola sono ammesse ripetizioni della stessa lettera.

Definizione [10]. Si dice che una parola u è una *parola positiva* se le lettere $a_1, a_2, \ldots, a_n$ che la formano hanno tutte gli esponenti $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ positivi. Una parola u è una *parola negativa* se le lettere $a_1, a_2, \ldots, a_n$ che la formano hanno tutte gli esponenti $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ negativi.

Esempio. La parola $u = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ è una parola positiva mentre la $v = a_1^{-1} \cdot a_2^{-1} \cdot \ldots \cdot a_k^{-1}$ è una parola negativa.

Definizione. Sia l'alfabeto $\bar{A}$. L'insieme $\bar{A}^+$ formato da tutte le parole di $\bar{A}$ prende il nome *insieme delle parole* di $\bar{A}$:

$$\bar{A}^+ = \{u \mid u \text{ è una parola nell'alfabeto } \bar{A}\}.$$

Definizione. Siano $\bar{A}$ un alfabeto e le parole $u, v \in \bar{A}^+$. Si dice che le parole u e v sono uguali se sono identiche lettera per lettera ed esponente per esponente. Due *parole uguali* si indicano

$$u \equiv v.$$

Definizione. Siano $\bar{A}$ un alfabeto, $\bar{A}^+$ l'insieme delle parole su $\bar{A}$ e le parole $u, v \in \bar{A}^+$, $u = a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n}$, $v = b_1^{\delta_1} \cdot b_2^{\delta_2} \cdot \ldots \cdot b_m^{\delta_m}$. Si considera l'operazione binaria chiamata *operazione di giustapposizione* su $\bar{A}^+$

$$\bullet : \bar{A}^+ \times \bar{A}^+ \to \bar{A}^+$$

tale che

$$u \bullet v = (a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n}) \bullet (b_1^{\delta_1} \cdot b_2^{\delta_2} \cdot \ldots \cdot b_m^{\delta_m}) = a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n} \cdot b_1^{\delta_1} \cdot b_2^{\delta_2} \cdot \ldots \cdot b_m^{\delta_m}$$

o

$$u\, v = (a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n})\, (b_1^{\delta_1} \cdot b_2^{\delta_2} \cdot \ldots \cdot b_m^{\delta_m}) = a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n} \cdot b_1^{\delta_1} \cdot b_2^{\delta_2} \cdot \ldots \cdot b_m^{\delta_m}.$$

Proposizione. L'operazione di giustapposizione su $\bar{A}^+$ è associativa.

Definizione. Prende il nome *parola vuota* di $\bar{A}$ o *parola vuota* una parola senza nessuna lettera e si indica con il simbolo 1.

Nota. La parola vuota si userà in seguito come elemento neutro della *giustapposizione*.

Definizione. Siano $\bar{A}$ un alfabeto, l'insieme $\bar{A}^+$ delle parole di $\bar{A}$ e la parola vuota 1 di $\bar{A}$. Si indica

con $\bar{A}^*$ l'insieme

$$\bar{A}^* = \bar{A}^+ \cup \{1\}.$$

Nota. È da sottolineare che per ogni $u \in \bar{A}^*$ si ha $1 \bullet u = u = u \bullet 1$.

Definizione ([86]). Se $u = a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n}$ è una parola si chiama *parola inversa* di u la parola

$$u^{-1} = a_1^{-\varepsilon_1} \cdot a_2^{-\varepsilon_2} \cdot \ldots \cdot a_n^{-\varepsilon_n}.$$

Proposizione. L'insieme delle parole $\bar{A}^*$ munito dell'operazione di giustapposizione $\bullet$ e della parola vuota 1 è un gruppo.

Definizione. Il gruppo dell'insieme $\bar{A}^*$ fornito dell'operazione di giustapposizione e della parola vuota si chiama *gruppo delle parole* su $\bar{A}$ e si indica $(\bar{A}^*, \bullet, 1)$ o semplicemente $\bar{A}^*$.

Definizione. Sugli elementi $u \in \bar{A}^*$ definiamo i seguenti due tipi di operazione:

1) *inserimento* in u di una coppia di termini consecutivi $x^{-1}x$ oppure xx^{-1}, con $x \in A$;
2) *cancellazione* in u di una coppia di termini consecutivi $x^{-1}x$ oppure xx^{-1}, con $x \in A$.

Se una parola $u \in \bar{A}^*$ è della forma $u \equiv \ldots abcxx^{-1}def \ldots$ oppure $u \equiv \ldots abcx^{-1}xdef \ldots$ per qualche $x \in \bar{A}$, possiamo convenire di ridurre la sua lunghezza cancellando le coppie $x^{-1}x$ e xx^{-1}. Operando così la parola si trasforma in $u_1 \equiv \ldots abcdef \ldots$.

Una parola u si dice *ridotta* se non è possibile operare tali cancellazioni. Cioè, se non contiene coppie di simboli successivi della forma $x^{-1}x$ o xx^{-1} con $x \in A$.

Osservazione. Nell'insieme delle parole, per le parole si può introdurre la nozione della *potenza* come segue:

$$a^n := \underbrace{a\ a\ a\ \ldots\ a}_{n \text{ volte}} \cdot$$

Esempio. La parola ridotta $u = abbc^{-1}dddea^{-1}$ con l'utilizzo del concetto della potenza si può raggruppare ulteriormente e si scrive $u = ab^2c^{-1}d^3ea^{-1}$.

Definizione. Siano $(\bar{A}^*, \bullet, 1)$ il gruppo delle parole su $\bar{A}$ e due parole $u, v \in \bar{A}^*$. Si dice che le parole u e v sono *liberamente uguali* e si indica

$$u \approx v$$

se la parola u dopo aver effettuare un numero finito di cancellazioni e inserimenti si trasforma alla parola v.

Esempio. Le parole $abbcc^{-1}$ e ab^2 sono liberamente uguali.

Definizione. Sia $(\bar{A}^*, \bullet, 1)$ il gruppo delle parole su $\bar{A}$. A partire da una parola $u \in \bar{A}^*$ possiamo effettuare un numero finito di cancellazioni e inserimenti, ottenendo infine una parola ridotta u_0 che prende il nome di *forma ridotta* di u.

Osservazione. Quindi, per arrivare da u a u_0 si effettua un numero finito di passaggi intermedi del tipo

$$u \to u_1 \to u_2 \to \ldots \to u_r = u_0$$

Tale sequenza di passaggi sarà chiamata *sequenza che collega* le parole u e u_0.

Proposizione. Siano $(\bar{A}^*, \bullet, 1)$ il gruppo delle parole su $\bar{A}$ e una qualsiasi parola $u \in \bar{A}^*$. Allora esiste un'unica forma ridotta u_0 della parola u.

Lemma ([19]). La parola inversa u^{-1} di una parola ridotta u risulta ridotta.

Esempio. La parola vuota è ridotta.

Definizione. Una parola $u = x_1^{\varepsilon 1} x_2^{\varepsilon 2} \dots x_n^{\varepsilon n}$, $u \in \bar{A}^*$ dopo l'operazione di cancellazione delle coppie di simboli successivi della forma $x^{-1}x$ o xx^{-1} e l'operazione di raggruppamento delle lettere utilizzando il concetto di potenza si scrive in un unico modo nella forma

$$u = x_1^{v1} x_2^{v2} \dots x_m^{vm} \quad \text{con } m \leq n,\ x_i \neq x_{i+1},\ x_i \in A \quad \text{e} \quad v_i \in \mathbb{Z} - \{0\}.$$

Tale scrittura prende il nome *forma normale di u*.

Esempio. Sia una parola $u \in \bar{A}^*$ in forma normale $u = x_1^{v1} x_2^{v2} \dots x_m^{vm}$. Allora la *lunghezza* di u è

$$\ell(u) = \sum_{i=1}^{m} |v_i| \ .$$

Osservazione. La parola vuota 1 di $u \in \bar{A}^*$ ha lunghezza zero: $\ell(1) = 0$.

Definizione. Siano $(\bar{A}^*, \bullet, 1)$ il gruppo delle parole su $\bar{A}$ e le parole $u, v \in \bar{A}^*$. Le parole u e v si dicono *parole equivalenti*, e si scrive $u \sim v$, se hanno la stessa forma ridotta: $u_0 \equiv v_0$.

Esempio. Due parole liberamente uguali sono equivalenti.

Esempio ([15]). Ogni parola è equivalente a una parola ridotta.

Esempio. Sia una parola u e una parola ridotta u_0. Se u e u_0 sono equivalenti, $u \sim u_0$, allora

$$\ell(u) = \ell(u_0).$$

Proposizione. La relazione $\sim$ è una relazione di equivalenza sull'insieme delle parole $\bar{A}^*$.

Proposizione. Siano $(\bar{A}^*, \bullet, 1)$ il gruppo delle parole su $\bar{A}$. Alla relazione $\sim$ di equivalenza su $\bar{A}^*$, per ogni $u \in \bar{A}^*$, vengono associate le classi di equivalenza $[u]_\sim$ definite come segue:

$$[u]_\sim = \{v \in \bar{A}^* \mid v \sim u\}.$$

L'insieme $\bar{A}^*/\sim$ delle classi di equivalenza così definite

$$\bar{A}^*/\sim = \{[u]_\sim \mid \text{per ogni } u \in \bar{A}^*\},$$

che prende il nome *insieme quoziente dell'insieme delle parole* su $\bar{A}$, risulta una partizione di $\bar{A}^*$:

$$\bar{A}^* = \bigcup_{u \in \bar{A}^*} [u]_\sim \quad \text{e} \quad [u]_\sim \cap [v]_\sim = \{\ \} \quad \text{per ogni } u \neq v.$$

Convenzione. La classe di equivalenza della parola vuota 1 dell'insieme $\bar{A}^*$, grazie alle proprietà corrispondenti in $\bar{A}^*$, risulta essere un'identità nell'insieme quoziente delle parole $\bar{A}^*/\sim$ e la indicheremo con il simbolo $[1]_\sim$.

Lemma ([3]). Ogni $[u]_{\sim}$, classe di equivalenza in $\bar{A}^*/\sim$, contiene una ed una sola parola ridotta.

Proposizione. Siano ($\bar{A}^*$, •, 1) il gruppo delle parole su $\bar{A}$ e le parole u, v, u_1, $v_1 \in \bar{A}^*$. Allora i prodotti per giustapposizione di parole equivalenti sono equivalenti:

$$\text{se } u \sim u_1 \text{ e } v \sim v_1, \text{ allora } uv \sim u_1 v_1.$$

Una importante diretta conseguenza di questo risultato è il seguente:

Teorema. Sia $\bar{A}^*/\sim$ l'insieme quoziente dell'insieme delle parole $\bar{A}^*$ con la relazione di equivalenza appena introdotta ~. Allora $\bar{A}^*/\sim$ è un gruppo rispetto alla legge di composizione indotta da $\bar{A}^*$:

$$[u]_{\sim}[v]_{\sim} \overset{def}{=} [uv]_{\sim}.$$

Osservazione. La definizione della legge di composizione fatta in questo modo è una buona definizione perché si fonda sulla definizione di ~.

Nota. Per indicare l'operazione binaria su $\bar{A}^*/\sim$ utilizzeremo lo stesso simbolo • usato per l'operazione binaria di giustapposizione:

$$[u]_{\sim} \bullet [v]_{\sim} = [u]_{\sim}[v]_{\sim} \overset{def}{=} [uv]_{\sim} = [u \cdot v]_{\sim}.$$

Si mette in evidenza che se la parola in forma ridotta $u = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdot \ldots a_k^{\varepsilon_k}$ è il rappresentante della classe di equivalenza $[u]_{\sim}$, la parola $u^{-1} = a_k^{-\varepsilon_k} a_{k-1}^{-\varepsilon_{k-1}} \ldots a_1^{-\varepsilon_1}$ è il rappresentante della classe di *equivalenza inversa* di $[u]_{\sim}$ che si indica $[u^{-1}]_{\sim}$.

Convenzione. In seguito, per indicare

- il gruppo delle classi di equivalenza delle parole sull'alfabeto A si userà la scrittura $F(A)$ piuttosto che $\bar{A}^*/\sim$:

$$F(A) := \bar{A}^*/\sim.$$

- le classi di equivalenza di una parola u di dell'alfabeto A si userà la scrittura $[u]$ piuttosto che $[u]_{\sim}$:

$$[u] := [u]_{\sim}.$$

Definizione. Il gruppo $F(A)$ delle classi di equivalenza delle parole sull'alfabeto A si chiama *gruppo libero sull'insieme A* o semplicemente *gruppo libero*.

Convenzione. In seguito, per indicare

- un gruppo libero sull'insieme A si useranno le notazioni ($F(A)$, •, [1]), ($F(A)$, •), $F(A)$ o semplicemente F.
- un gruppo libero di rango n si userà la notazione F_n.

Osservazione. La classe di equivalenza $[u]$ contiene la parola u.

Esempio. Per ogni parola u risulta

1) $[u] \bullet [1] = [u] = [1] \bullet [u]$;

2) $[u]^{-1} \bullet [u] = [1] = [u] \bullet [u]^{-1}$.

Esempio. Per ogni parola scritta in forma ridotta $u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$ si verifica che

$$[u] = [x_1]^{\varepsilon_1} [x_2]^{\varepsilon_2} \dots [x_k]^{\varepsilon_k} \in F(A).$$

È una conseguenza immediata della definizione del gruppo libero e della regola degli indici che ogni parola ridotta $u \in F(A)$ ha una rappresentazione unica della forma

$$u = x_1^{v_1} x_2^{v_2} \dots x_m^{v_m} \quad \text{con } m \geq 0,\ x_i \neq x_{i+1},\ x_i \in X \quad \text{e} \quad v_i \in \mathbb{Z} - \{0\},$$

ovvero vale la seguente

Proposizione. Ogni elemento $[u]$ del gruppo libero $F(A)$ corrisponde ad un'unica parola ridotta u dell'insieme delle parole $\bar{A}^*$.

Esempio. Per moltiplicare due parole ridotte $u \equiv aabc^{-1}d$ e $v \equiv d^{-1}ce$ è sufficiente unire le due parole e cancellare:

$$uv \equiv (aabc^{-1}d)(d^{-1}ce) = aabc^{-1}d\,d^{-1}ce = aabc^{-1}ce = aabe.$$

Definizione. Siano A un insieme di simboli e $(F(A), \bullet, [1])$ il gruppo libero su A. L'applicazione

$$i_A : A \to F(A) \quad \text{tale che per ogni } x \in A \text{ risulta } \quad i_A(x) = [x]$$

prende il nome di *inclusione*.

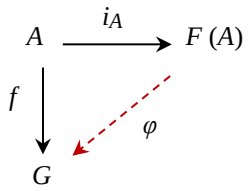
Osservazione. L'applicazione inclusione i_A mette in relazione ogni lettera dell'alfabeto A con la classe di equivalenza che la contiene dell'insieme $F(A)$.

È opportuno annunciare la seguente

Proposizione. L'insieme dell'alfabeto A è un insieme libero di generatori per l'insieme $F(A)$ delle classi di equivalenza delle parole.

Teorema (*Proprietà di tipo universale*). Siano A un insieme di simboli, $(F(A), \bullet, [1])$ il gruppo libero su A, $(G, \bullet, e)$ un gruppo, l'applicazione di inclusione $i_A : A \to F(A)$ e una qualsiasi applicazione $f : A \to G$. Allora esiste ed è unico un omomorfismo di gruppi $\varphi : F(A) \to G$ tale che $\varphi \circ i_A = f$.

In altre parole, esiste un unico omomorfismo di gruppi φ che rende commutativo il diagramma:



Convenzione. Quindi, la terminologia "*rende commutativo il diagramma*" è intesa a significare che se uno inizia dall'insieme A e procede intorno al triangolo verso G in entrambe le direzioni, componendo le funzioni, le funzioni ottenute sono identiche.

Osservazione. Si può affermare che il gruppo $F(A)$ è generato dall'insieme Im (i_A).

A questo punto è dovuto precisare che si può dimostrare che F_n, il gruppo libero su n generatori e indicati con $x_1, x_2, \dots, x_n$, è unico a meno di isomorfismi. Di conseguenza per indicarlo è comodo utilizzare la notazione

$$F_n = \langle x_1, x_2, \ldots, x_n \rangle.$$

Teorema ([59]). Siano $(F, \bullet, 1_F)$ un gruppo e X un suo sottoinsieme non vuoto: $X \subseteq F$. Se ogni elemento $u \in F$ può essere scritto in un unico modo nella forma

$$u = x_1^{v_1} x_2^{v_2} \ldots x_m^{v_m} \quad \text{con} \quad m \geq 0,\ x_i \neq x_{i+1},\ x_i \in X \ \text{ e } \ v_i \in \mathbb{Z} - \{0\},$$

allora F è libero su X.

Proposizione ([3]). Se due alfabeti A e B generano lo stesso gruppo libero $F(A)$, allora $|A| = |B|$.

Osservazione. La proposizione afferma che la cardinalità $|A|$ di ogni alfabeto A che genera il gruppo libero $\tilde{A}$ dipende solo dalle caratteristiche del gruppo stesso.

Proposizione ([3, 18, 15]). Siano S e T gruppi liberi, rispettivamente, sugli insiemi X e Y. Le cardinalità X e Y coincidono se e solo se S e T sono isomorfi:

$$|X| = |Y| \quad \Leftrightarrow \quad S \cong T.$$

Proposizione ([18]). Sia F un gruppo libero su un insieme A. Risulta che

1) ogni u elemento non banale di F ha un ordine infinito;
2) Se $|X| > 1$, allora $Z(F) = 1$.

Proposizione ([13]). Ogni gruppo libero F finitamente generato è Hopfian.

Definizioni. Sia $F(A)$ un gruppo libero su un insieme A. Chiameremo *rango del gruppo libero F* o *rango di F* la cardinalità $|A|$. Il rango di F può essere finito o infinito e si indica $rk(F)$:

$$rk(F) := |A|.$$

Un *gruppo libero di rango n* si indica con la notazione F_n.

Il *gruppo degli automorfismi di un gruppo libero di rango n* si indica con $Aut(F_n)$ o $Aut\, F_n$.

Osservazione. La proposizione XXX può essere formulata anche come segue:

Due gruppi liberi S e T sono isomorfi se e solo se i loro ranghi coincidono.

Proposizione ([3]). Siano S e T gruppi liberi, rispettivamente, sugli insiemi X e Y. Se un'applicazione $\psi : S \to T$ è un epimorfismo, allora

$$rk(S) \geq rk(T) \quad \Leftrightarrow \quad |X| \geq |Y|.$$

Osservazione. Siano A un insieme di simboli e $(F(A), \bullet, [1])$ il gruppo libero su A.

Se $|A| = n < \infty$, allora il gruppo $F(A)$ è libero di rango n.

Definizione. Siano G un gruppo qualsiasi, $\{X_i\}_{i \in I}$ la famiglia degli insiemi finiti e infiniti che generano G. e k la dimensione minima degli insiemi X_i. Si chiama *rango di G* il numero cardinale k e si indica $rk(G)$.

Dimostriamo che questo minimo si ottiene da un insieme che genera G. Questo è evidente se almeno un insieme che genera G è finito. Se tutti i gruppi che generano G sono infiniti, le loro cardinalità coincidono con la cardinalità del gruppo G e questo minimo è uguale al numero cardinale $|G|$ di G. Infatti, sia X un insieme infinito che genera G. Allora ogni elemento di G è il prodotto di un numero finito di elementi dell'insieme $X \cup X^{-1}$. Poiché X è infinito, la cardinalità dell'insieme che raccoglie tutte le sequenze finite di elementi di X è uguale a $|X|$. Questo significa che $|G| = |X|$.

Proposizione ([13]). L'unione $\bigcup F_i$ di una catena ascendente di gruppi liberi $F_1 \subseteq F_2 \subseteq \ldots$ di gradi finiti è Hopfian.

Lemma ([9]). Il centro $Z(F)$ di ogni gruppo libero non ciclico F è banale.

Definizione. Un elemento di un gruppo libero F è chiamato *elemento primitivo* se è elemento di qualche base di F.

Sottogruppi di gruppi liberi

Si annuncia il seguente importante risultato

Teorema. (*Nielsen–Schreier*). I sottogruppi di un gruppo libero sono anch'essi liberi.

L'importante risultato che segue ottenuto da Schreier è quantitativamente più accurato rispetto al precedente teorema.

Proposizione (*Formula di Schreier*). Sia F un gruppo libero di rango finito n, e sia $H \leq F$ sottogruppo di indice finito $(F : H) = m$. Allora, H è un gruppo libero ed il suo rango è finito e uguale a $nm - m + 1$.

Il rango desiderato si può presentare anche come segue: $rk(H) = m(rk(F) - 1) + 1$ oppure

$$(F : H) = \frac{rk(H) - 1}{rk(F) - 1} .$$

Proposizione ([13]). Ogni gruppo libero F di rango maggiore di 1 contiene un sottogruppo di rango infinito.

Lemma. Sia F un gruppo libero. Allora, il sottogruppo derivato $[F, F]$ di F ha rango infinito.

Proposizione ([11, 12]). Siano F_1 un gruppo libero ed $F_1 \supseteq F_2 \supseteq \ldots$ tale che ogni F_{i+1} risulta sottogruppo caratteristico proprio di F_i. Allora, $\bigcap F_i = \{1\}$.

Proposizione ([8]). Sia F un gruppo libero. Se un sottogruppo H di F è finitamente generato e ha come sottoinsieme un sottogruppo normale e non banale di F, allora H ha un indice finito in F.

Corollario. Sia F un gruppo libero. Se un sottogruppo non banale H di F è normale e finitamente generato, allora $(H : F)$ l'indice di H in F è finito.

Proposizione ([13]). Sia F un gruppo libero. Se un sottogruppo H di F è finitamente generato e non è contenuto in nessun sottogruppo di rango infinito di F, allora $(H : F)$ l'indice di H in F è finito.

Il seguente risultato è in un determinato modo una inversione della precedente proposizione.

Proposizione. Sia F un gruppo libero di rango maggiore di 1. Se H è un sottogruppo di F finitamente generato e $(H : F)$ l'indice di H in F è finito, allora H è contenuto in un sottogruppo G di F che non ha un rango maggiore del rango di H: $rk(G) \leq rk(H)$.

Proposizione ([9]). Un gruppo libero F di rango finito $rk(F) = k$ non può essere generato da meno di k elementi.

Proposizione. Se un gruppo libero F di rango finito $rk(F) = k$ è generato da un insieme X formato da k elementi, allora X è una base per F.

Proposizione ([9]). Se F è un gruppo libero finitamente generato, allora il gruppo degli automorfismi $Aut\,(F)$ risulta finitamente generato.

Proposizione ([6]). Il gruppo libero F_n è residualmente finito.

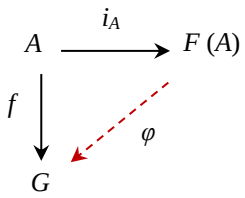
Proposizione. Il gruppo $Aut\,(F_n)$ è residualmente finito.

Presentazioni di gruppi con generatori e relazioni

In questa sezione illustreremo come presentare i gruppi con l'aiuto di *generatori* e *relazioni*. Questa modalità ci consente non solo di definire i gruppi in modo conciso, ma anche di studiarne le proprietà e di costruire gruppi con le proprietà desiderate. Tali presentazioni si fondano naturalmente nella teoria e nella topologia dei gruppi.
Una conseguenza del teorema delle proprietà di tipo universale è il seguente

Teorema. Siano A un insieme di simboli, $(F\,(A), \bullet, [1])$ il gruppo libero su A, $(G, \bullet, e)$ un gruppo, l'applicazione di inclusione $i_A : A \to F\,(A)$ e un'applicazione $f : A \to G$. Se A è un sistema di generatoti di G ed f è l'immersione di A in G, allora

1) esiste ed è unico un omomorfismo suriettivo di gruppi $\varphi : F\,(A) \to G$ tale che $\varphi \circ i_A = f$
2) $G \cong F\,(A) / \ker\,(\varphi)$.



Quindi, questo teorema afferma che:

ogni gruppo è immagine omomorfa di un gruppo libero.

Osservazione. Il precedente teorema può essere annunciato anche così [18], [19]:

ogni gruppo G è quoziente di un gruppo libero.

Definizione. Un isomorfismo del tipo

$$G \cong F\,(A) / \ker\,(\varphi)$$

si chiama *presentazione del gruppo G* e gli elementi di $\ker\,(\varphi)$ si chiamano *relazioni della presentazione* o *relatori di definizione* (*defining relators*).

Definizione. Se l'insieme dei generatori $\{g_i\}_{i \in S}$ di una presentazione di un gruppo G è un insieme finito, si dice che si tratta di una *presentazione finitamente generata*.

Definizione. Se l'insieme delle relazioni $\{r_i\}_{i \in T}$ di una presentazione di un gruppo G è un insieme finito, si dice che si tratta di una *presentazione finitamente relazionata*.

Definizione. Se gli insiemi dei generatori $\{g_i\}_{i \in S}$ e delle relazioni $\{r_i\}_{i \in T}$ di una presentazione di un gruppo G sono insiemi finiti, si dice che si tratta di una *presentazione finita del gruppo G* o che il gruppo G è *finitamente presentato*.

Definizione. Siano F un gruppo, un insiemi di generatori $G = \{g_i\}_{i \in S}$ e un insieme di relazioni R

$= \{r_i\}_{i\in T}$ di una sua presentazione. La presentazione così definita si denota:

$$F = \langle \{g_i\}_{i\in S} \mid \{r_i\}_{i\in T} \rangle \quad \text{o} \quad F = \langle G \mid R \rangle.$$

Convenzione. In letteratura per denotare la presentazione di un gruppo F in forma generica si usa abitualmente il simbolo $F = \langle G \mid R \rangle$ dove G, che si posiziona a sinistra del simbolo " | ", rappresenta i generatori ed R , che si posiziona a destra del simbolo " | ", le relazioni della presentazione.

Osservazione. A volte si indicano le relazioni anche con $r_i = 1$.

Qualche volta si usa la scrittura "$u = v$", con $u, v \in F$, per indicare una relazione di una presentazione del gruppo F. In questi casi tale scrittura corrisponde alla relazione della presentazione uv^{-1}.

Esempio ([15]). Risulta che $\langle X \mid - \rangle$ è una presentazione del gruppo libero su X di rango $|X|$:

$$F(X) \cong \langle X \mid - \rangle.$$

Esempio. Una presentazione per il gruppo $\mathbb{Z}$ dei numeri interi è data da un solo generatore x e nessuna relazione:

$$\mathbb{Z} \cong \langle x \rangle.$$

Esempio. Una presentazione per il gruppo $\mathbb{Z}$ dei numeri interi è data da tre generatori x, y, z e da tre relazioni x, y^{-1}, zx^{-1}:

$$\mathbb{Z} \cong \langle x, y, z \mid x, y^{-1}, zx^{-1} \rangle.$$

Esempio. Risulta che

$$\mathbb{Z}_n \cong \langle x \mid x^n \rangle \quad \text{per ogni } n \in \mathbb{N},\ n > 0.$$

Esempio. Siano un numero intero $n > 0$ e un gruppo ciclico $(G, \bullet, 1)$ di ordine n. Allora, G ha una presentazione come segue

$$G \cong \langle x \mid x^n \rangle.$$

Esempio. Sia D_4 il gruppo diedrale che corrisponde alle simmetrie del quadrato,

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

ed una sua presentazione

$$D_4 \cong \langle a, b \mid a^4 = 1, b^2 = 1, ab = ba^3 \rangle.$$

Considerando che ogni relazione si può scrivere uguale a 1, la precedente presentazione si può riscrivere ommettendo la parte "= 1" come segue:

$$D_4 \cong \langle a, b \mid a^4, b^2, abab \rangle.$$

Le relazioni di una presentazione $a^4 = 1, b^2 = 1, ab = ba^3$ scritte nel modo $a^4, b^2, abab$ si chiamano *relatori* (*relators*) o *relatori della presentazione*.

Sia $F = \langle a, b \rangle$ il gruppo generato dagli elementi a e b e $D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$ il gruppo diedrale delle simmetrie del quadrato.

Si definisce l'omomorfismo $\omega : F \to D_4$ tale che $\omega\left(a_{n_1} b_{n_2} \ldots a_{n_{k-1}} b_{n_k}\right) = x_{n_1} y_{n_2} \ldots x_{n_{k-1}} y_{n_k}$, con $n_i \in \mathbb{Z}$, $k \in \mathbb{Z}$, $k \geq 0$ per ogni i.

Sia $N = \langle a^4, b^2, abab \rangle$ il sottogruppo generato da a^4, b^2 e $abab$.

Ricordando che un requisito per la normalità è che $N = zNz^{-1}$, per tutte le parole $z \in F$, N deve essere il sottogruppo generato dalle parole $za^4z^{-1}, zb^2z^{-1}, zababz^{-1}$, per ogni $z \in F$.

Si osserva che ker (ω) = N e Im (ω) = D_4, poiché chiaramente $D_4 \subseteq Im$ (ω) e Im (ω) $\subseteq D_4$. Quindi, dal primo teorema di isomorfismo, F / N = F / ker (ω) $\cong Im$ (ω) = D_4.

In questo modo si è ottenuto il gruppo D_4 dal gruppo libero $F = \langle a, b \rangle$.

Proposizione. Ogni gruppo ha una presentazione.

Osservazione. Un gruppo G in generale ha molte presentazioni diverse tra di loro.

Proposizione ([2, 14, 16]). Esistono gruppi finitamente generati che non hanno una presentazione finita.

Proposizione ([18]). Ogni gruppo finito G ha una presentazione finita.

Infatti, gli elementi del gruppo G possono essere considerati generatori e la tabella di moltiplicazione fornisce le relazioni della presentazione.

Esempio ([15]). Sia [a, b] il commutatore di a e b. Allora, il gruppo

$$G = \langle x, y \mid [x, y^{-k} xy^k] \text{ per ogni intero } k \geq 1 \rangle$$

è finitamente generato ma non è finitamente presentato.

Due degli ultimi esempi e una delle ultime proposizioni esposte ha affermato che ogni gruppo G ha almeno una presentazione che dipendono dalle scelte delle famiglie dei generatori e delle relazioni fatte. Questo è uno dei motivi per cui è difficile estrarre informazioni profonde sulla struttura di un gruppo da una determinata presentazione. Per esempio, non è sempre facile riconoscere, a partire da una presentazione arbitraria, il gruppo che essa rappresenta. Il problema di stabilire in un numero finito di passi, a partire da una presentazione per un gruppo G, se una presentazione arbitraria H è isomorfa o meno a quella di partenza si chiama *problema dell'isomorfismo*. Tale problema, è decisamente più difficile di quello della parola e del coniugio ed è noto non essere risolvibile algoritmicamente.

In generale è difficile dimostrare che due di queste presentazioni sono isomorfe. In effetti, dati due gruppi finiti, sarà in generale impossibile decidere se sono isomorfi o meno.

Inoltre, sempre in generale, non è facile provare o confutare che due parole date u e v nell'alfabeto $X \cup X^{-1}$ rappresentano lo stesso elemento del gruppo G. Questo problema, chiamato *problema della parola* (*word problem*), è algoritmicamente indecidibile anche nella classe dei gruppi finitamente presentati [4], [17].

Una conseguenza di queste difficoltà presenti è che dovremo sfruttare le caratteristiche speciali di ogni possibile presentazione di gruppo sperando di poter ricavarne volta per volta nuove preziose informazioni sulla struttura del gruppo.

Tuttavia, se il gruppo è presentato in maniera finita ed è residualmente finito, allora il problema della parola è decidibile.

Nel contesto di gruppi di trecce e monoidi di trecce, il problema della parola può essere formulato come segue:

> Date due sequenze $u_1, u_2, \ldots, u_s$ e $v_1, v_2, \ldots, v_t$ di generatori del gruppo (o del monoide) di trecce, gli elementi $u = u_1 u_2 \ldots u_s$ e $v = v_1 v_2 \ldots v_t$ sono uguali tra loro?

È estremamente importante progettare algoritmi più efficienti dagli esistenti per risolvere il problema della parola.

Il problema della parola in B_n è stato posto per la prima volta da Artin [1].

La soluzione del problema della parola da lui proposta è basata sulla conoscenza della struttura

del *kernel*, ker (φ), dell'applicazione $\varphi : B_n \to S_n$ che collega il generatore σ_i con la trasposizione $s_i = (i, i + 1)$. Cioè, $\varphi(\sigma_i) = s_i$.
Ha usato le proprietà teoriche di gruppo riguardanti il ker (φ) per mettere una treccia in una forma normale chiamata "*treccia pettinata*" (*combed braid*).

Presentazioni di monoidi

Le considerazioni fatte per i gruppi liberi e per le presentazioni di gruppi sono generalmente valide anche per i monoidi liberi e le presentazioni di monoidi.

Definizione. Siano M monoide, $G = \{g_i\}_{i\in S}$ insiemi di generatori e $R = \{r_i\}_{i\in T}$ insieme di relazioni di una sua presentazione. La presentazione così definita si denota:

$$M = \langle \{g_i\}_{i\in S} \mid \{r_i\}_{i\in T} \rangle \quad \text{o} \quad M = \langle G \mid R \rangle.$$

Definizione. Se gli insiemi dei generatori $\{g_i\}_{i\in S}$ e delle relazioni $\{r_i\}_{i\in T}$ di una presentazione di un monoide M sono insiemi finiti, si dice che si tratta di una *presentazione finita del monoide M*.

Definizione. Una presentazione $M = \langle \{g_i\}_{i\in S} \mid \{r_i\}_{i\in T} \rangle$ si dice *ponderata* o *pesata* se esiste un omomorfismo $\ell : M \to \mathbb{N}$ tale che per ogni $g_k \in \{g_i\}_{i\in S}$ risulta $\ell(g_k) \geq 1$.

L'omomorfismo ℓ si chiama *peso*.

Discussione e conclusioni

L'esperienza ha avuto una durata di 10 ore e l'adesione dei corsisti è stata su base volontaria. Durante gli incontri sono state proposte poche dimostrazioni delle proposizioni ma sono stati presentati e svolti molti esempi di difficoltà non elevata in modo chiaro. I corsisti in modalità collaborativa sia durante gli incontri ma anche tra un incontro e l'altro hanno svolto alcuni esercizi semplici.
I docenti più giovani laureati in matematica e gli studenti dopo, le difficoltà dell'impatto iniziale con l'argomento nuovo, sono riusciti a seguire le attività con una discreta autonomia. Ma essendo il numero dei partecipanti ristretto non si possono dedurre affermazioni generalizzate.
L'esperienza sta proseguendo con nuovi incontri, con gli stessi partecipanti e con un argomento che si presta bene come oggetto per sperimentazioni didattiche a scuola preferibilmente in orario extra-scolastico con alunni di 17-19 anni di età. Il nuovo argomento che si sta esplorando sono le trecce.

Dichiarazione di conflitti di interesse

L'autore dichiara di non avere conflitti di interesse rispetto la paternità o la pubblicazione di questo articolo.

Bibliografia

[1] E. Artin, (1925). *Theorie der Zöpfe*, Abhandlungen aus dem Mathematischen, Abh. Math. Sem. Univ. Hamburg 4, 47-72, 2

[2] G. Baumslag, (1976). *Multiplicators and metabelian groups*, J. Austral. Math. Soc. Ser. A 22, 305–312, 32

[3] O. Bogopolski, (2008). *Introduction to Group Theory*, European Mathematical Society Publishing House, Zürich, 31

[4] W.W. Boone, (1959). *The word problem*. Ann. of Math. (2) 70, 207–265, 35

[5] M. Dehn. (1911). *Über unendliche diskontinuierliche Gruppen*, Math. Ann., 71(1), 116–144, 54

[6] S. Dey, K. Gongopadhyay, 2018. *Commutator subgroups of welded braid groups*, Topology Appl., 237: 7–20, 128

[7] F.A. Garside, (1969). *The braid group and other groups*, Quart. J. Math. Oxford Ser. 20, 235–254, 45

[8] L. Greenberg, (1960). *Discrete groups of motions*, Canad. J. Math. 12, 414-425, 63

[9] D.L. Johnson, (1997). *Presentations of groups*, Cambridge University Press, United Kingdom, 85

[10] E.-K. Lee, (2010). *A positive presentation for the pure braid group*, Journal of the Chungcheong Mathematical Society, Vol. 23, No. 3, pp. 555-561, 47

[11] F.W. Levi, (1930). *Über die Untergruppen der freien Gruppen I*, Math. Z. 32, 315-318, 61

[12] F.W. Levi, (1933). *Über die Untergruppen der freien Gruppen II*, Math. Z. 37, 90-97, 62

[13] R.C. Lyndon, P.E. Schupp, (1977). *Combinatorial group theory*, Springer-Verlag, Berlin, Heidelberg, New York, 60

[14] W. Magnus, A. Karrass, D. Solitar, (1976). *Combinatorial group theory*, Dover Publ. Inc., NewYork, 33

[15] S. Moran, (1983). *The Mathematical Theory of Knots and Braids*, North–Holland Mathematics Studies, vol. 82, Elsevier, Amsterdam, 82

[16] B.H. Neumann, (1937). *Some remarks on infinite groups*. J. London Math. Soc. 12, 120–127, 34

[17] P.S. Novikov, (1958). *On the algorithmic insolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov. 44 (1955), 3–143; English transl. Amer. Math. Soc. Transl. (2) 9, Amer. Math. Soc., Providence, RI, 1–122, 36

[18] D.J.S. Robinson, (2003). *An introduction to abstract algebra*, Walter de Gruyter, Berlin, 59

[19] J.J. Rotman, (1995). *An introduction to the theory of groups*, 4th ed., Springer-Verlag New York, Ine, 86

[20] V. Vershinin, (2010). *On the singular braid monoid*, St. Petersburg Math. J., Vol. 21, No. 5, pp. 693-704, 44

L'Autore

Panagiote Ligouras
I.I.S. "Leonardo da Vinci – Galileo Galilei" - Noci (BA)
Via Col di Lana, 33, 70011 Alberobello (BA)
ligouras@alice.it
Italy

Teacher of mathematics and computer science. Passionate about mathematical problem-solving, ICT, didactic communication and online and Blended educational activities. It also deals with learning and evaluation processes in various training and system contexts.

Collaborates for years with the Italian Ministry of Education, University and Research (MIUR), with the INDIRE (National Institute of Documentation, Innovation and Educational Research, Italy), with INVALSI (National Institute for the Evaluation of the Educational System of Education and training, Italy) and with the USR Puglia (Regional School Office, Italy).

Trainer accredited in "Evaluation of learning and system" - SNV.

He is the author of numerous scientific papers.

Received April 14, 2019; *revised* July 22, 2019; *accepted* November 8, 2019; *published online* December 23, 2019