Elementi di ALGEBRA d.p.d.v.s.

SCHEDE INTEGRATIVE

Cap. 1 – DAI MONOIDI AI GRUPPI

A partire da monoidi $(M,\cdot,1_M)$ si possono costruire gruppi con varie tecniche. Ora ne vediamo alcune.

1.1. - *Il gruppo delle unità di un monoide*. Gli elementi di un monoide M che hanno l'inverso rispetto alla moltiplicazione · si dicono *elementi unitari* e costituiscono il gruppo M^*, detto *gruppo delle unità* del monoide.

Infatti, $1_M \in M^*$. Inoltre, $\forall a,b \in M^*$, $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1} \Rightarrow a\cdot b \in M^*$, e l'operazione resta ovviamente associativa anche in M^*. Infine, $\left(a^{-1}\right)^{-1} = a \Rightarrow a^{-1} \in M^*$.

Esempio 1.1.1. Nel caso del monoide X^X delle funzioni da X ad X il gruppo delle unità è precisamente il *gruppo simmetrico* S_X, i cui elementi sono le biiezioni da X in sé e che si chiamano *permutazioni di X*.

Se $X = \{1,2,\ldots,n\}$, il suo gruppo simmetrico si denota con S_n. Dal calcolo combinatorio sappiamo che S_n possiede n! elementi. Dal corso di Algebra I sono note le nozioni di

- ciclo e sua lunghezza
- cicli disgiunti e loro permutabilità
- fattorizzazione sostanzialmente unica di una permutazione in cicli disgiunti e suo ordine come mcm delle lunghezze dei fattori
- trasposizioni e permutazioni pari e dispari
- il gruppo alterno A_n delle permutazioni pari ed il suo ordine $\frac{n!}{2}$.

1.2. – *Simmetrizzazione di un monoide regolare*. Sia $(M,*,1_M)$ un monoide commutativo regolare, allora esiste un gruppo abeliano G, contenente un sottomonoide M' *isomorfo* ad M e tale che per ogni g∈G esistono a,b∈M' tali che $g = a * b^{-1}$.

Dimostrazione. Si consideri il prodotto cartesiano M×M, i cui elementi sono le coppie ordinate (a, b), con a, b∈M. Si definisca in M×M la seguente operazione:

(a, b)*(c, d) = (a*c, b*d).

Non è difficile provare che essa possiede la proprietà associativa ed ha elemento neutro (1_M, 1_M). Si ha così il monoide ($M\times M$, *, (1_M, 1_M)), che è a sua volta commutativo e regolare.

Si definisca ora in $M\times M$ la seguente relazione: (a, b) ~ (a', b') se a*b' = b*a'.

Non è difficile provare che ~ è una relazione d'equivalenza in $M\times M$, ossia che possiede le proprietà riflessiva, simmetrica e transitiva.

Si denoti con [a, b] la *classe d'equivalenza* di (a, b), costituita da tutte le coppie equivalenti ad (a, b). Si tenga presente che se (a, b) ~ (a', b') allora [a, b] = [a', b']; inoltre, due classi distinte hanno sempre intersezione vuota.

A titolo di esempio, una coppia (c, d) è equivalente alla la coppia (1_M, 1_M) se e solo se $c * 1_M = d * 1_M$, ossia se e solo se c = d. Pertanto [1_M, 1_M] = {(a, a) | a∈M} = [a, a] per ogni a∈M.

Denotiamo con G l'insieme $M\times M/\sim$ delle classi, ossia l'*insieme quoziente*.

La proprietà da sottolineare è la seguente: la relazione ~ è *compatibile* con *:

(a, b) ~ (a', b') e (c, d) ~ (c', d') ⇒ (a*c, b*d) ~ (a'*c', b'*d').

E' allora possibile definire tra le classi la seguente operazione:

[a, b] * [c, d] = [a*c, b*d],

sicuri che il risultato non dipende dalle particolari coppie prescelte per rappresentare le classi d'equivalenza, ma solo dalle classi stesse. Si verifica facilmente che questa operazione in G è associativa, commutativa ed ha elemento neutro [1_M, 1_M]. Inoltre, ogni classe [a, b] possiede l'inversa: è la classe [b, a], infatti,

[a, b] * [b, a] = [a*b, b*a] = [a*b, a*b] = [1_M, 1_M] = 1_G.

Pertanto, (G, *) è un gruppo *abeliano* (ossia con la proprietà commutativa)

Si verifica poi che il sottoinsieme M' costituito dalle classi del tipo [a, 1_M] è un *sottomonoide* del gruppo G e che è isomorfo ad M: l'isomorfismo è la funzione $a \mapsto [a, 1_M]$. Gli elementi di M' si possono identificare allora con quelli di M, cioè per ogni a∈M si pone a = [a, 1_M].

Si osservi che ora per ogni g = [a, b]∈G, si ha [a, b] = [a, 1_M]*[b, 1_M]$^{-1}$, ma allora si può scrivere, in G, [a, b] = a*b^{-1} (o anche = a:b). Ossia, ogni elemento di G è *quoto* di due elementi di M.

Esempio 1.2.1. Nel caso di (N, +, 0) la relazione ~ diventa: (a,b) ~ (c,d) se a+d = b+c. L'operazione tra le coppie è: (a,b)+(c,d) = (a+c, b+d). Il suo elemento neutro è la coppia (0, 0). Poiché si sta parlando in termini di addizione, si parla di *opposto* e non di inverso, e anziché [a, b]$^{-1}$ si scrive -[a, b] = [b, a]. Identifichiamo N con il sottoinsieme {[x,0] | x∈N}. Allora si ha la seguente proprietà:

ogni elemento [a, b] o appartiene ad N o è l'opposto di un elemento di N. (*)

Infatti, se a ≥ b si ha [a, b] = [a-b, 0], risultando a+0 = b+(a-b).

Se invece a < b, essendo a+(b-a) = b+0, si ha [a, b] = [0, b-a] = -[b-a, 0].

Pertanto la classe [a,b] può essere denotata con il numero naturale a-b quando a ≥ b, e con -(b-a) quando a < b. Per esempio, [7, 3] = 4, [6, 8] = -2.

Si ha così che il gruppo quoziente è sostanzialmente il gruppo additivo (Z, +) dei numeri interi relativi. In questo gruppo si ha $a + x = b \Leftrightarrow x = b + (-a)$

NOTA. Questa costruzione di **Z**, pur così astratta, presenta alcuni vantaggi: le definizioni e le dimostrazioni sono dirette e generali e non è necessario esaminare sottocasi. Essa consentirebbe di definire in **Z** anche la moltiplicazione e l'ordinamento, a partire da quelli di **N**, ma non in modo abbastanza elementare. Si otterrebbe l'anello **Z** e, da questo, con un procedimento generale derivato dalla simmetrizzazione dei monoidi regolari, al campo razionale **Q**. Questa è la via seguita nei corsi universitari. Nei corsi d'Algebra della scuola secondaria non viene però mai seguita.

Esempio 1.2.2. Nel caso del monoide $\left(\mathbf{N}^+, \cdot, 1\right)$, le coppie (a, b) di elementi di $\mathbf{N}^+$ sono dette *frazioni* e sono scritte nella forma $\frac{a}{b}$. La relazione ~ è in questo caso: $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c$. L'operazione tra le frazioni è: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$. L'elemento neutro è la frazione $\frac{1}{1}$. Il gruppo quoziente è il gruppo moltiplicativo Q^+ dei "numeri razionali assoluti" (non nulli). L'inverso di $\left[\frac{a}{b}\right]$ è $\left[\frac{b}{a}\right]$. Il sottomonoide corrispondente ad $\mathbf{N}^+$ è $\left\{\left[\frac{a}{1}\right] \,\middle|\, a \in \mathbf{N}^+\right\}$. Identificando a con $\left[\frac{a}{1}\right]$, si ha $\left[\frac{a}{b}\right] = a \cdot b^{-1}$, quindi ogni elemento di Q^+ è *quoto* di due elementi di N. Gli elementi di Q^+ si denotano comunque con $\frac{a}{b}$ anziché con $\left[\frac{a}{b}\right]$ o con ab^{-1}.

Non vale in Q^+ una proprietà analoga a (*). Infatti per esempio $\frac{2}{3}$ non è un numero naturale e neppure il reciproco di un numero naturale, perché 2 non divide 3 e 3 non divide 2. I due gruppi $\left(\mathbf{Z}, +\right)$ e $\left(\mathbf{Q}^+, \cdot\right)$ sono assai diversi e non sono isomorfi, dato che il primo è ciclico, generato da 1, mentre il secondo non lo è, anzi, nessun sottoinsieme finito lo genera, dato che ci sono infiniti numeri primi.

NOTA. Questa costruzione di $\mathbf{Q}^+$ consente di definire agevolmente anche l'addizione, dapprima tra le frazioni ponendo $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ e, poiché anche questa operazione risulta compatibile con la relazione d'equivalenza ~, in seguito anche tra le classi di frazioni, cioè tra numeri razionali assoluti. Considerando anche le frazioni $\frac{0}{b}$, $b \neq 0$, il quoziente $\mathbf{N} \times \mathbf{N}^+ / \sim$ con l'addizione quoziente è un monoide commutativo regolare. La simmetrizzazione di tale monoide è il gruppo additivo (**Q**, +) dei numeri razionali. Esso diviene infine un *campo* estendendo convenientemente anche la moltiplicazione. Questa via è sostanzialmente seguita nei corsi di Aritmetica della scuola secondaria. E' astratta come la precedente, le dimostrazioni non sono facilissime (ma quasi sempre

sono omesse), tuttavia la scrittura $\frac{a}{b}$, cui si è abituati fin dalle scuole elementari, la rende abbastanza accessibile.

1.3. *Presentazione di un gruppo*. Partiamo ora dal monoide libero delle parole su un alfabeto A, che sappiamo possedere la legge di cancellazione. Per sottolineare che qui le lettere non sono variabili, ma puri simboli, ed anche per mdare a questa teoria l'aspetto di gioco, al posto delle lettere ci serviremo di *stuzzicadenti*, normali o colorati. Partiamo da un alfabeto costituito da un solo simbolo, un normale stuzzicadenti, di cui supponiamo di avere infinite copie.
Che cosa si può fare? Fra le tante attività, la più elementare è quella di mettere gli stuzzicadenti in fila uno dietro l'altro per formare delle *stringhe* e contarli:

Ø	I	II	III	IIII	IIIII	IIIIII	IIIIIII	IIIIIIII	IIIIIIIII	…
0	1	2	3	4	5	6	7	8	9	…

Il simbolo del vuoto rappresenta qui la "stringa vuota" di stuzzicadenti. Osserviamo che i numeri in basso esprimono la lunghezza della stringa di stuzzicadenti sovrastante. Questo primo passo ricorda un poco le tacche che i nostri antenati cavernicoli incidevano su ossa o bastoni per contare. Ed ora, date due stringhe di stuzzicadenti, possiamo ottenerne una nuova collocando la seconda stringa dietro la prima. Chiamiamo *concatenazione* questo procedimento. Per rappresentarlo sulla carta ci serve un simbolo, per esempio la "e commerciale" &:

IIIIII & IIIIIIII = IIIIIIIIIIIII

La lunghezza della stringa ottenuta è naturalmente la somma delle lunghezze delle due stringhe di partenza. Tutto qui? Sì, perché senza altre regole quasi solo questo si può fare…
Osserviamo solo che se una stringa viene concatenata con la stringa vuota non cambia.

Nota. L'operazione di concatenazione nell'insieme delle stringhe di stuzzicadenti è automaticamente commutativa, associativa ed ha come elemento neutro la stringa vuota. Inoltre, la lunghezza della somma è la somma delle lunghezze. Si tratta infatti di un modo primitivo di rappresentare l'insieme dei numeri naturali e l'operazione di addizione, ossia il monoide (**N**,+,0). Questo monoide è quindi ***libero*** da regole: la manipolazione degli stuzzicadenti sopra descritta non ha infatti altre regole oltre al modo di costruire la concatenata di due stringhe. Tutto il resto, ossia le proprietà della concatenazione, sono automatiche.

Come trasformare tutto ciò in un gioco un po' più interessante? Proviamo ad inventare regole per complicare il gioco di partenza: al semplice concatenare stringhe di stuzzicadenti, potremmo per esempio aggiungere la regola seguente:

1.3.a) Fissato un numero n > 0, "mangiare" ogni stringa di n stuzzicadenti, ossia sostituirla con la stringa vuota. In simboli, $\underbrace{\text{I}\text{I}\text{I}\ldots\text{I}}_{n} = \varnothing$

Esempio 1.3.1. Fissiamo n = 5. Allora avremo il 4 come lunghezza massima, e le stringhe a disposizione saranno solo cinque: **ø** **I** **II** **III** **IIII**

Che cosa succede quando le concateniamo? Ogni volta che abbiamo 5 stuzzicadenti in una stringa, li "mangiamo", come nella dama, ossia li togliamo dalla stringa. In definitiva, una stringa di cinque stuzzicadenti equivale alla stringa vuota.

Avremo così per esempio:

$$\text{III} \,\&\, \text{IIII} = \underbrace{\text{IIIII}}_{5\to\varnothing}\ \text{II} = \text{II}.$$

Possiamo anche riassumere in una tabella i 25 risultati possibili. Notiamo che in ogni riga e colonna i risultati sono tutti diversi:

&	∅	I	II	III	IIII
∅	∅	I	II	III	IIII
I	I	II	III	IIII	∅
II	II	III	IIII	∅	I
III	III	IIII	∅	I	II
IIII	IIII	∅	I	II	III

Nota. Quel che si ottiene, per ogni "tetto" prefissato n > 0, è un gruppo con n elementi, detto *gruppo ciclico d'ordine n*. Questo è un altro modo di rappresentare il gruppo delle rotazioni del piano di ampiezza $\frac{2\pi k}{n}$, $0 \le k \le n-1$ intorno ad un centro O fissato.

1.3.b) Fissati m, n > 0, sostituire ad ogni stringa di n stuzzicadenti una stringa di m stuzzicadenti. In simboli, $\underbrace{\text{I}\text{I}\text{I}\ldots\text{I}}_{n} \to \underbrace{\text{I}\text{I}\text{I}\ldots\text{I}}_{m}$ (regola *monodirezionale*).

Se m = n non succede niente. Se n < m, che cosa accade?

Esempio 1.3.2. Prendiamo n = 4 ed m = 5. La stringa vuota e quelle con uno, due o tre stuzzicadenti non cambiano, ma a partire da quella con quattro, si può aumentarne la lunghezza all'infinito, collocando 5 stuzzicadenti al posto di 4 in tutti i modi possibili. Gli informatici scriverebbero "overflow" oppure "out of memory", ma noi possiamo dominare questa situazione col simbolo ∞. In definitiva, abbiamo solo cinque stringhe:

ø **I** **II** **III** **∞**

Possiamo riassumere in una tabella le 25 possibili concatenazioni. Notiamo che la stringa infinita "assorbe" le altre.

&	∅	I	II	III	∞
∅	∅	I	II	III	∞
I	I	II	III	∞	∞
II	II	III	∞	∞	∞
III	III	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞

Nota. Pare che il nostro occhio sappia distinguere, senza contarli, solo fino a 3 oggetti, e dopo ci sia solo una moltitudine indistinguibile. Somiglia un po' a questo nostro gioco. Il monoide ottenuto è commutativo, ha ø come elemento neutro e ∞ come elemento assorbente.

Resta il caso di n > m. Qui abbiamo un limite massimo alle lunghezze delle parole, uguale ad n-1, perché ogni volta che si arriva ad n, il numero scende ad m < n. In questo caso di ottengono monoidi commutativi non regolari, ma privi di elemento assorbente.

Esistono giochi *banali*? Che cosa può significare questa banalità? Potremmo dire che un gioco è banale se fa scomparire tutti gli stuzzicadenti, lasciando solo la stringa vuota. In un certo senso, potremmo dire che in tal caso le regole stabilite sono contraddittorie. Per esempio, le regole **III = ø, II = ø** implicano **I = ø.**

1.3.c. Ci procuriamo ora due confezioni di stuzzicadenti e coloriamo in modo diverso il contenuto delle due scatole. Nelle figure sottostanti si useranno i colori nero e rosso, che nella stampa in bianco e nero diventeranno nero e grigio.

Il gioco di base, libero da regole, è come quello del caso precedente, ma proprio l'assenza di regole crea subito qualche complicazione, dato che non è lecito per esempio permutare stuzzicadenti di colori diversi:

ø	I	I	II	II	II	II	III	III	III	III	III	III	III	III	…
0	1		2				3								

Le stringhe distinte di data lunghezza n ≥ 0 sono 2^n. La concatenazione di due stringhe di stuzzicadenti colorati è tale che la stringa risultante ha come lunghezza la somma delle lunghezze delle due stringhe date. La stringa vuota non produce variazioni nella sua concatenazione con altre stringhe. Lo scambio dei due termini nella concatenazione in generale produce risultati diversi:

III & II = IIIII II & III = IIIII

Nota. L'operazione di concatenazione nell'insieme delle stringhe di stuzzicadenti bicolori è automaticamente associativa ed ha come elemento neutro la stringa vuota. Inoltre, la lunghezza della somma è la somma delle lunghezze, e vale la legge di cancellazione. Si ottiene il *monoide libero* $\left(\mathcal{F}_2, \&, \varnothing\right)$ *su due generatori*. Discorsi analoghi si potrebbero ripetere con tre o più colori.

Ora introduciamo man mano delle regole.

1.3.c.1). Commutatività: **IǀI = IǀI**

Possiamo scambiare di posto in una stringa ogni stuzzicadente con ogni altro. In questo caso, per ogni n ≥ 0 ci sono solo n+1 stringhe distinte di lunghezza n. Aggiungiamo la convenzione di collocare sempre prima gli stuzzicadenti neri e poi i rossi. Allora abbiamo un modo "canonico" di mettere in una stringa gli stuzzicadenti:

ø	I	I	II	II	II	III	III	III	III	…
0	1		2			3				

Abbiamo in particolare un modo "canonico" di scrivere il risultato di una concatenazione:

III & IIIII = IIIIIII = IIIIIIII

Nota. In questo caso si ottiene un monoide commutativo regolare. Si tratta di un altro modo di rappresentare la *somma diretta* del monoide additivo (**N**, +, 0) con se stesso o il monoide moltiplicativo dei *monomi monici in due indeterminate*.

1.3.c.2) Commutatività e opposti: **IǀI = IǀI, IǀI = ø**

Essa implica solo stringhe monocromatiche, una per ciascuna lunghezza possibile. Potremmo disporre le stringhe di stuzzicadenti come segue:

…	IIIII	IIII	III	II	I	ø	I	II	III	IIII	IIIII	…
…	-5	-4	-5	-2	-1	0	1	2	3	4	5	…

La concatenazione di due stringhe dello stesso colore ne fa sommare le lunghezze, mentre in caso di colore diverso le lunghezze si sottraggono e resta una stringa del colore prevalente. Due stringhe della stessa lunghezza, ma di colore diverso, si distruggono a vicenda lasciando la stringa vuota. E' evidente la somiglianza, o meglio l'*isomorfismo*, con il gruppo (**Z**, +) dei numeri interi relativi: basta sostituire per esempio ad ogni stringa nera il numero positivo che ne esprime la lunghezza, mentre ad ogni stringa rossa si sostituisce l'opposto della sua lunghezza. Questa è una costruzione di (**Z**, +) più simile a quella della scuola media, nella quale si prendono due copie di **N**, si muniscono di segni + e -, si identificano i loro zeri (+0 = -0) e si definisce la somma come abbiamo fatto con i nostri stuzzicadenti colorati.

NOTA. Il fatto che le stringhe siano monocromatiche e che la stringa rossa e la nera di uguale lunghezza siano opposte, fa dire in definitiva che, *come gruppo*, il generatore è unico.

Imponiamo ora che la massima lunghezza di una stringa rossa o di una stringa nera siano limitate. Per esempio, stabiliamo di "mangiare" tre stuzzicadenti neri o due rossi consecutivi. Allora abbiamo la seguente situazione:

ø	I	I	II	II	II	III	III	III	III	…
0	1		2			3				

Sono possibili quindi stringhe del tipo IIIIIIIIIIIII, senza mai due rossi o tre neri consecutivi. Si ottiene un insieme infinito di stringhe che, rispetto alla concatenazione, forma un gruppo non commutativo numerabile. Per esempio,

$$\left(\text{IIIIIIIIIIII} \right)^{-1} = \text{IIIIIIIIIIIII}.$$

Nota. Tale gruppo è chiamato *prodotto libero* dei due gruppi ciclici di ordini 2 e 3. Ovviamente si può ripetere lo stesso discorso con due gruppi ciclici finiti di ordine qualsiasi.

Aggiungiamo regole per potere in qualche modo scambiare gli stuzzicadenti neri con i rossi. Vediamo alcuni esempi interessanti.

Esempio 1.3. 3). Commutatività e limitatezza: **II = II, II = ø, III = ø**.

Non è difficile dedurne che si hanno a disposizione solo sei stringhe di stuzzicadenti:

ø I I II II III

Ed ecco la tavola dei risultati delle 36 concatenazioni: si osservi che ogni stringa ha l'*inversa*: **I & II = III = ø; II & III = IIIII = ø**, ecc. Si ha così un gruppo.

La tavola è stata manipolata con un programma di disegno, per poter mostrare i colori.

&	∅	I	II	I	II	III
∅	∅	I	II	I	II	III
I	I	II	∅	II	III	I
II	II	∅	I	III	I	II
I	I	II	III	∅	I	II
II	II	III	I	I	II	∅
III	III	I	II	II	∅	I

Nota. L'operazione di concatenazione nell'insieme delle stringhe di stuzzicadenti bicolori è come sempre associativa ed ha come elemento neutro la stringa vuota. In questo caso è anche commutativa, ed ogni elemento ha l'inverso, perché la stringa vuota compare in ogni riga e colonna. Si ottiene così un gruppo abeliano d'ordine 6, *prodotto diretto* dei due gruppi ciclici d'ordine 3 (gli stuzzicadenti neri) e 2 (i rossi), quindi *isomorfo* al gruppo ciclico d'ordine 6.

La regola si generalizza variando le lunghezze massime delle stringhe nere o rosse. Per ogni m, n interi positivi, si ottiene un insieme di m·n stringhe. In definitiva, si ottiene sempre un gruppo abeliano d'ordine m·n, *prodotto diretto* dei due gruppi ciclici d'ordine m ed n.

Esempio 1.3.4) Inversione e limitatezza: **|| = |||, || = ø, ||| = ø**.

In questo caso è un po' più difficile dedurre che si hanno a disposizione solo sei stringhe di stuzzicadenti:

ø | | || || |||

Infatti, la regola **|| = |||** consente di scambiare rosso-nero con nero-nero-rosso, aumentando la lunghezza. Però, intanto consente di separare sempre gli stuzzicadenti neri dai rossi, quindi le altre due regole provvedono a limitare la lunghezza. Mostriamo un esempio, mettendo un po' di spazio tra gli stuzzicadenti per evidenziare le parti da manipolare:

||| = || | = ||| | = || || = || ||| = ||| || = ø ||= ||

Ne viene la possibilità di ottenere la tavola di concatenazione: come nel caso precedente, ogni stringa ha l'inversa, quindi si ha un gruppo di ordine 6, ma non c'è la proprietà commutativa:

&	∅	|	||	|	||	|||
∅	∅	|	||	|	||	|||
|	|	||	∅	||	|||	|
||	||	∅	|	|||	|	||
|	|	|||	||	∅	||	|
||	||	|	|||	|	∅	||
|||	|||	||	|	||	|	∅

La regola **|| = |||** è detta *di inversione* perché la stringa **||** è inversa della stringa **|** : lo scambio del rosso e del nero sostituisce al nero la sua stringa inversa.

NOTA. In questo caso si ottiene un gruppo non abeliano d'ordine 6, detto *gruppo diedrale* D_3 ed è solo un altro modo di rappresentare il gruppo delle simmetrie di un triangolo equilatero. Se la lunghezza della stringa nera che viene mangiata è m > 2, e nella regola d'inversione la sequenza rosso-nero diventa la sequenza di m-1 neri ed un rosso, si ottengono gruppi non abeliani d'ordine 2m, detti *gruppi diedrali* D_m. Se m = 2 si ottiene invece un gruppo abeliano d'ordine 4 non ciclico.

La regola precedente si generalizza variando le lunghezze massime delle stringhe nere o rosse e la regola d'inversione, ma non in modo arbitrario, per evitare giochi banali, o in cui resta un solo colore. Ma quali di questi insiemi di regole producono giochi banali? Questo è un problema incredibilmente difficile, così come è altrettanto difficile sapere se alla fine avremo un numero finito o infinito di stringhe di stuzzicadenti.

DALLE TACCHE ALLE LETTERE. L'uso di lineette verticali per raffigurare gli stuzzicadenti alla fine risulta pesante e rende difficile la lettura di ciò che si sta facendo, oltre alla difficoltà di usare i colori nelle formule e nella stampa. Torniamo pertanto ad usare delle lettere Ossia, in luogo di **|||||||||||** scriviamo bbbaabaaabbb, sostituendo allo stuzzicadenti nero la lettera a e al posto del rosso la b. Questo oggetto è una *parola* (o *stringa*) nell'alfabeto $\{a, b\}$. Per migliorarne la leggibilità, si possono anche usare gli esponenti e scrivere $b^3a^2ba^3b^3$, ottenendo una *parola normalizzata*. A causa della somiglianza con i monomi, il solo pericolo è introdurre istintivamente la commutatività

delle lettere e trasformare erroneamente $b^3a^2ba^3b^3$ in a^5b^7. Se si vuole farlo, occorre postulare esplicitamente la commutatività delle lettere.

La parola vuota si esprime di solito con il simbolo 1. Le regole via via introdotte diventano quindi uguaglianze di parole, dette anche *relazioni*.

Il modo che si usa in Teoria dei Gruppi in questi casi è il seguente: entro due specie di parentesi a punta si collocano l'insieme A delle lettere da usare, dette *generatori*, e, dopo una barra verticale, l'insieme R delle regole del gioco, dette *relazioni*: $G = \langle A \mid R \rangle$.

Nelle relazioni, trattandosi di gruppi, sono permesse potenze ad esponente negativo, con la clausola tacita che, denotando con x una lettera qualunque, sia sempre $xx^{-1} = x^{-1}x = 1 = x^0$. Quindi nel caso che un elemento a abbia ordine infinito, non compaiono due lettere che, se accostate, si annichilano a vicenda, ma una sola senza relazioni. Pertanto, con questa convenzione, la scrittura $\langle a \mid \varnothing \rangle$ individua il *gruppo libero con un solo generatore di periodo infinito*, isomorfo a $(\mathbf{Z}, +)$.

ESEMPI 1.3.5.

- Il gruppo *ciclico* di ordine n: $C_n = \langle a \mid a^n = 1 \rangle \cong \mathbf{Z}_n$
- Il gruppo *diedrale* numerabile: $D_\infty = \langle a, b \mid b^2 = 1,\ ba = a^{-1}b \rangle$
- Il gruppo diedrale di ordine 2n: $D_n = \langle a, b \mid a^n = 1 = b^2, ba = a^{-1}b \rangle$
- Il gruppo *abeliano libero* con due generatori: $\langle a, b \mid ab = ba \rangle \cong \mathbf{Z} \times \mathbf{Z}$
- Il prodotto diretto di due gruppi ciclici: $\langle a, b \mid ab = ba,\ a^m = 1 = b^n \rangle \cong \mathbf{Z}_m \times \mathbf{Z}_n$

Nota. Quel che abbiamo visto è un caso particolare di *presentazione* di un gruppo, ossia del modo usato dagli esperti per descrivere un gruppo astratto come insieme di parole nell'alfabeto costituito dai generatori, manipolate mediante le regole date dalle relazioni.

Un teorema di Von Dick afferma che se le relazioni di un gruppo G sono un sottoinsieme delle relazioni di un gruppo H con gli stessi generatori, allora c'è un epimorfismo tra G ed H.

Ritroviamo così il fatto ben noto che i gruppi ciclici $C_n = \langle a \mid a^n = 1 \rangle$ sono quozienti del gruppo libero $\mathbf{Z} \cong \langle a \mid \varnothing \rangle$. Analogamente, i gruppi diedrali finiti sono quozienti del gruppo D_∞, e i prodotti diretti di due gruppi ciclici sono quozienti di $\mathbf{Z}\times\mathbf{Z}$.

Tuttavia, uno stesso gruppo si può presentare in modi assai diversi, e non è sempre possibile stabilire se si tratti o no dello stesso gruppo. Per esempio, $D_\infty \cong \left\langle x, b \,\middle|\, x^2 = b^2 = 1 \right\rangle$, cioè è isomorfo al prodotto libero di due gruppi ciclici di ordine 2.

Con il pretesto del gioco con gli stuzzicadenti, colorati o no, abbiamo visto esempi di monoidi e gruppi anche assai generali. Ovviamente, aumentando i colori, ossia le lettere, aumenta la complessità delle costruzioni.

NOTA. Ripeto che in questo contesto, il ruolo delle lettere non è quello di variabili su un insieme, ma di *indeterminate*, ossia di oggetti astratti, estranei agli insiemi numerici, manipolati con regole del gioco stabilite di volta in volta. Per evitare questa confusione tra indeterminate e variabili si sono usati inizialmente gli stuzzicadenti colorati al posto delle più comuni lettere dell'alfabeto.

ESEMPIO 1.3.6. Sia $G = \left\langle a, b \,\middle|\, a^4 = 1,\ b^2 = a^2,\ ba = a^3 b \right\rangle$. Questo è un gruppo con 8 elementi, il più sfuggente di tutti. È denotato con Q_8 ed è detto *gruppo dei quaternioni*. Per costruirlo seguiamo la convenzione che ogni elemento sia scritto in modo che la potenza di a preceda quella di b. Non basta, perché ogni elemento può essere scritto in più modi: $a^3 = a \cdot a^2 = a \cdot b^2$. Inoltre,

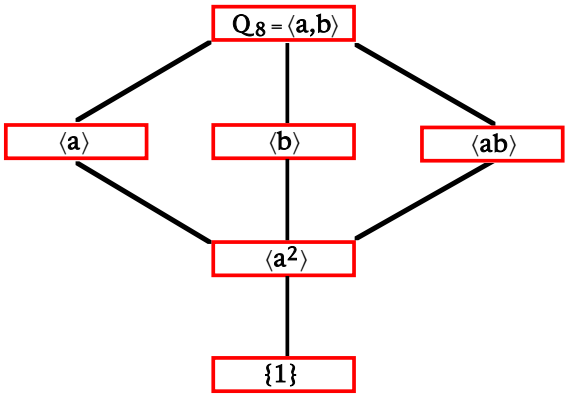
$$b^4 = \left(b^2\right)^2 = \left(a^2\right)^2 = a^4 = 1,\ (ab)^2 = abab = a\left(a^3 b\right)b = a^4 b^2 = b^2$$

Ne segue che i sei elementi $a,\ a^3,\ b,\ b^3,\ ab,\ a^3 b = ab^3 = (ab)^3$ hanno periodo 4.

Infine, l'elemento $x = a^2 = b^2 = (ab)^2$ commuta con tutti gli altri ed è il quadrato dei sei precedenti. Allora,

$$Q_8 = \left\{id,\ a,\ a^2,\ a^3,\ b,\ b^3,\ ab,\ a^3 b\right\}.$$

Qui accanto c'è il diagramma di Hasse dei sei sottogruppi di Q_8, ordinati per inclusione.



Osserviamo che pur non essendo abeliano, i suoi sottogruppi sono tutti normali: quelli d'ordine 4 perché hanno ciascuno indice 2; il sottogruppo $\left\langle a^2 \right\rangle$, d'ordine 2, è la loro intersezione, ed è il *centro* del gruppo. Il nome deriva dal fatto che è un sottogruppo importante del gruppo moltiplicativo del corpo dei Quaternioni.

Riassumiamo qui i gruppi di ordine 8: a meno d'isomorfismi sono solo cinque, di cui tre abeliani:

- il gruppo ciclico $C_8 = \left\langle a \,\middle|\, a^8 = 1 \right\rangle \cong \left(\mathbf{Z}_8, +\right)$;

- il prodotto diretto $\mathbf{Z}_4 \times \mathbf{Z}_2 \cong \left\langle a, b \;\middle|\; ab = ba,\ a^4 = 1 = b^2 \right\rangle$;
- il gruppo del quadrato $D_4 = \left\langle a, b \;\middle|\; a^4 = 1 = b^2, ba = a^{-1}b \right\rangle$;
- il gruppo dei quaternioni $Q_8 = \left\langle a, b \;\middle|\; a^4 = 1,\ b^2 = a^2,\ ba = a^3 b \right\rangle$
- il *2-gruppo abeliano elementare* 3-generato:

$$\left(\mathbf{Z}_2\right)^3 \cong \left\langle a, b, c \;\middle|\; a^2 = b^2 = c^2 = 1,\ ab = ba,\ ac = ca,\ cb = bc \right\rangle.$$

Ci sono solo questi: sia infatti G un gruppo d'ordine 8. Se ha un elemento a d'ordine 8, è ciclico, $G \cong \mathbf{Z}_8$.

Se, esclusa l'unità, G ha tutti gli elementi d'ordine 2, è necessariamente abeliano ed è dunque il 2-gruppo abeliano elementare $\left(\mathbf{Z}_2\right)^3$.

Negli altri casi G ha almeno un elemento a d'ordine 4. Allora il sottogruppo $A = \langle a \rangle$ è normale in G. Sia $b \in G \setminus A$. Allora bA = Ab, quindi $\exists k \in \mathbf{N}$, $1 \le k \le 3$, tale che $ba = a^k b$. Inoltre, posto $B = \langle b \rangle$, si ha $G = AB = \langle \{a, b\} \rangle$. Osserviamo subito che se k = 2 si ha:

$$ba = a^2 b \Rightarrow bab = a^2 \Rightarrow (ba)^2 = (bab)a = a^3 = a^{-1}$$

di ordine 4, e poiché $ba \notin A$, segue $|ba| = 8$, **assurdo**.

Ciò posto, vediamo dapprima il caso in cui esista $b \in G \setminus A$ di ordine 2. Allora:

- Se k = 1 si ha ba = ab, quindi G è abeliano, anche B è normale in G e $A \cap B = \{1\}$, dunque $G \cong A \times B \cong \mathbf{Z}_4 \times \mathbf{Z}_2$.
- Se k = 3, allora $ba = a^3 b = a^{-1} b$, quindi otteniamo il gruppo D_4.

Vediamo infine il caso in cui ogni $b \in G \setminus A$ abbia ordine 4. Allora anche $B = \langle b \rangle$ è normale in G. Se $|A \cap B| = 1$ allora $G \cong A \times B \cong \mathbf{Z}_4 \times \mathbf{Z}_4$ avrebbe 16 elementi, assurdo. Dunque $|A \cap B| = 2$. Allora necessariamente $b^2 = a^2$. Vediamo ora i due casi di k:

- Se k = 1 si ha ba = ab, quindi G è abeliano, ma si ha subito $ab \notin A$, $(ab)^2 = 1$, **assurdo**.
- Se k = 3, allora $ba = a^3 b = a^{-1} b$, quindi otteniamo il gruppo Q_8.

Cap. 2 – IL GRUPPO DI SIMMETRIA DI UNA FIGURA PIANA

Questo capitolo prosegue quello sul gruppo delle isometrie piane presente nelle schede integrative del modulo di Elementi di Geometria 2014/15

Il gruppo Γ delle isometrie piane è un gruppo di permutazioni sui punti del piano. Esso agisce quindi anche sull'insieme delle *figure piane*, cioè sull'insieme dei sottoinsiemi del piano.

Chiamiamo *gruppo di isometrie* di una figura $\Im$ lo *stabilizzatore* $\Gamma_{\Im}$ di $\Im$ in Γ, costituito da tutte le isometrie di Γ che trasformano l'insieme $\Im$ in se stesso. Descriviamo ora tale gruppo per una classe importante di figure.

Una figura $\Im$ si dice *limitata* se è contenuta in un cerchio. Il teorema seguente descrive gli elementi di una figura limitata.

TEOREMA 2.1. Sia $\Im$ una figura limitata e sia $\Gamma_{\Im}$ il suo gruppo d'isometrie. Allora si ha:

a) $\Gamma_{\Im}$ non contiene né traslazioni (a parte l'identità) né antitraslazioni.

b) Tutte le rotazioni appartenenti a $\Gamma_{\Im}$ hanno lo stesso centro, per il quale passano tutti gli assi delle (eventuali) simmetrie appartenenti a $\Gamma_{\Im}$.

Dimostrazione. a) Per assurdo sia τ una traslazione $\neq$ id appartenente a $\Gamma_{\Im}$ e sia δ il modulo del vettore associato $v(\tau)$. Siano poi d il diametro di un cerchio contenente $\Im$ e P un punto di $\Im$. Per ogni $n \in \mathbf{N}$, posto $P_n = \tau^n(P)$, la lunghezza del segmento PP_n è $n\delta$. Per la proprietà archimedea dei segmenti, esiste n tale che $n\delta > d$. Dunque, si ha $PP_n > d$, quindi P_n non appartiene al cerchio che copre $\Im$ e pertanto neppure ad $\Im$, nonostante $P \in \Im$ e $\tau^n \in \Gamma_{\Im}$, assurdo.

Di conseguenza, poiché il quadrato di un'antitraslazione è una traslazione, $\Gamma_{\Im}$ non può contenere neppure antitraslazioni.

b) Siano per assurdo ρ_1, ρ_2 due rotazioni appartenenti a $\Gamma_{\Im}$ e con centri diversi. Allora $\rho_1 \circ \rho_2$ e $\rho_2 \circ \rho_1$ appartengono a $\Gamma_{\Im}$ e, per a), non possono essere traslazioni, per cui sono rotazioni con la stessa ampiezza α e centri diversi.

Essendo però $\alpha+(-\alpha) = 0$, l'isometria $\left(\rho_2 \circ \rho_1\right) \circ \left(\rho_1 \circ \rho_2\right)^{-1}$, che appartiene a $\Gamma_{\Im}$, è una traslazione, assurdo.

Infine vi siano per assurdo in $\Gamma_{\mathfrak{I}}$ una rotazione ρ di centro O ed una simmetria σ di asse s non passante per O. Il prodotto $\rho \circ \sigma$ è un'isometria inversa, prodotto di tre simmetrie i cui assi non passano per uno stesso punto né sono tutti paralleli, quindi è un'antitraslazione, assurdo.

Proposizione 2.2. Sia H un sottogruppo finito di Γ. Allora i suoi elementi sono o tutte rotazioni con lo stesso centro, quindi H è ciclico, oppure metà dei suoi elementi sono rotazioni e metà sono simmetrie assiali i cui assi passano per il centro di rotazione, ed H è diedrale.

Dimostrazione. Poiché traslazioni non banali ed antitraslazioni hanno periodi infiniti, allora H non ne contiene. Come nella dimostrazione del teorema precedente, se H contenesse rotazioni con centri diversi o una rotazione ed una simmetria con asse non passante per i centro della rotazione, allora H conterrebbe anche una traslazione non banale, assurdo. Perciò gli elementi di H sono come detto nell'enunciato. Sia ora ρ la rotazione non banale di ampiezza minima α e sia n il suo periodo; allora si ha $\alpha = \frac{2\pi}{n}$, e le altre rotazioni sono necessariamente sue potenze. Infatti, se un'altra rotazione θ ha ampiezza $\beta > \alpha$, posto $q = \mathrm{int}\left(\frac{\beta}{\alpha}\right)$ e $\gamma = \beta - q\alpha$, allora la rotazione $\theta \circ \left(\rho^q\right)^{-1} \in H$ ha ampiezza $0 \le \gamma = \beta - q\alpha < \alpha$, assurdo se $\gamma \neq 0$. Perciò $\gamma = 0$, $\theta = \rho^q$. Allora il sottogruppo di H costituito dalle rotazioni è ciclico, generato da r, quindi d'ordine n.

Se non esaurisce H, c'è almeno una simmetria assiale s. Allora per ogni k, 0 ≤ k ≤ n-1, il prodotto $\rho^k \circ \sigma$ non è una rotazione, ma una simmetria assiale, quindi di periodo 2. Inversamente, se $\theta \in H$ e non è una rotazione, allora $\theta \circ \sigma$ è una isometria diretta, ossia una rotazione ρ^k. Perciò $\theta = \rho^k \circ \sigma$. Ne segue che H ha 2n elementi e si ha:

$$\left(\rho^k \circ \sigma\right)^2 = \mathrm{id} \;\Rightarrow\; \rho^k \circ \sigma \circ \rho^k \circ \sigma = \mathrm{id} \;\Rightarrow\; \rho^k \circ \sigma = \sigma \circ \left(\rho^k\right)^{-1}$$

Pertanto, H è il gruppo diedrale d'ordine 2n.

ESEMPI 2.3.

1. *Il gruppo di un poligono regolare con n lati*. Il gruppo di un (qualsiasi) poligono regolare con n lati (che è una figura limitata) contiene 2n elementi, cioè le rotazioni r_k di ampiezze $2\pi k/n$, $0 \le k < n$, con il centro nel centro O del poligono, e le n simmetrie rispetto alle rette congiungenti O con i vertici o con i punti medi dei lati. Si tratta quindi del gruppo diedrale con 2n elementi.

2. *Il gruppo del cerchio*. Sia dato un cerchio e sia O il suo centro. Le isometrie che trasformano il cerchio in sé sono tutte e sole quelle che hanno O come punto unito, pertanto il gruppo del cerchio coincide con lo stabilizzatore Γ_O del suo centro, ed è costituito dalle rotazioni di centro O e dalle simmetrie il cui asse passa per O.

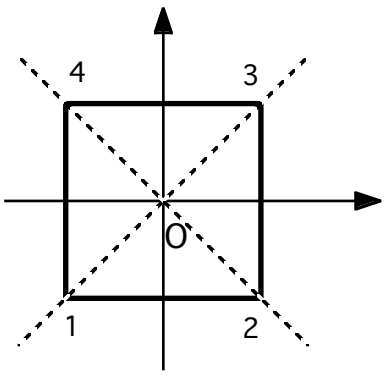
3. *Il gruppo della retta*. Sia r una retta e sia Γ_r il suo gruppo: poiché r non è una figura limitata, non è applicabile il teorema 2.1. Possiamo però determinare gli elementi di Γ_r mediante lo studio delle rette unite delle varie isometrie. Si ottiene così che Γ_r contiene:

- le traslazioni il cui vettore è parallelo ad r;
- le rotazioni di ampiezza un angolo piatto (simmetrie centrali) il cui centro è su r;
- la simmetria di asse r
- le simmetrie di asse perpendicolare ad r;
- le antitraslazioni di asse r.

Esercizio 2.4. a) Si determinino i gruppi d'isometrie di un rombo e di un rettangolo (che non siano quadrati): sono isomorfi?
b) Per ogni $n \geq 2$ si determini una figura piana il cui gruppo d'isometrie sia ciclico d'ordine n.

IL GRUPPO DEL QUADRATO. Numeriamo i vertici di un quadrato con 1, 2, 3, 4, in senso antiorario. Sia poi O il suo centro, cioè il punto d'incontro delle diagonali e degli assi dei lati. Sappiamo che ogni isometria del piano che trasforma in sé il nostro quadrato è determinata completamente dalla permutazione che essa induce sui vertici (ne basterebbero tre) e che, di conseguenza, le permutazioni così ottenute costituiscono un gruppo isomorfo al gruppo D_4 delle simmetrie del quadrato. Siano ρ la rotazione di $\pi/2$ in senso antiorario intorno ad O, e σ la simmetria rispetto all'asse dei lati 1 4 e 2 3. Le due permutazioni ρ e σ generano D_4:

$$D_4 = \left\{ id,\ \rho,\ \rho^2,\ \rho^3,\ \sigma,\ \rho\circ\sigma,\ \rho^2\sigma,\ \rho^3\sigma \right\}$$

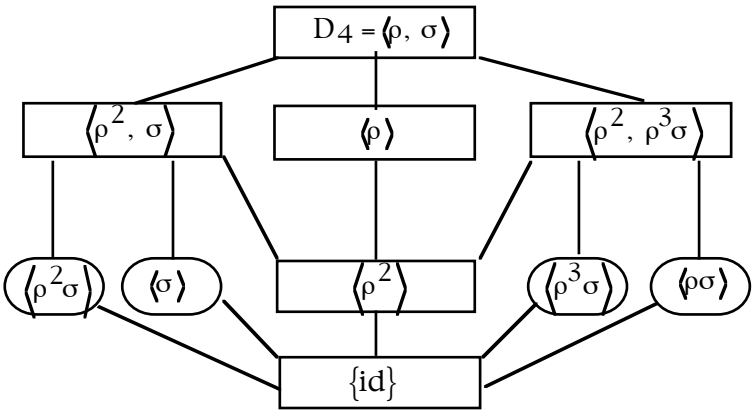


Permutaz.	isometria che la induce sui vertici
id	identità
(1 2 3 4)	rotazione di $\pi/2$ in senso ant. intorno ad O
(1 3)(2 4)	simmetria rispetto ad O
(1 4 3 2)	rot. di $3\pi/2$ in senso antior. intorno ad O
(1 4)(2 3)	simmetria rispetto all'asse dei lati 1 4 e 2 3
(1 3)	simmetria rispetto alla diagonale 2 4
(1 2)(3 4)	simmetria rispetto all'asse dei lati 1 2 e 3 4
(2 4)	simmetria rispetto alla diagonale 1 3

La tavola di moltiplicazione di D_4 è calcolata con un software applicando un programma apposito. I numeri 1, ... , 8 sostituiscono gli elementi di D_4 secondo l'ordine sopra riportato. Il quadrato in alto a sinistra è la tavola del sottogruppo $\langle\rho\rangle$ costituito dalle rotazioni.

∘	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	6	7	8	5
3	3	4	1	2	7	8	5	6
4	4	1	2	3	8	5	6	7
5	5	8	7	6	1	4	3	2
6	6	5	8	7	2	1	4	3
7	7	6	5	8	3	2	1	4
8	8	7	6	5	4	3	2	1

Ed ecco il diagramma dei sottogruppi, ordinati per inclusione:

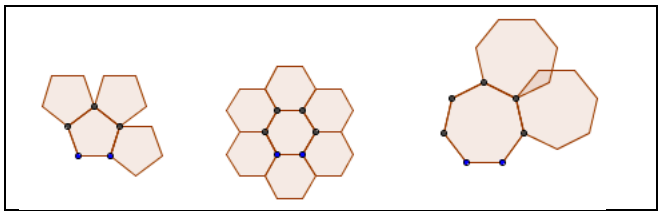


NOTE. A) La simmetria centrale ρ^2 commuta con tutte le altre.

B) Oltre a $\langle\rho\rangle$ ci sono altri due sottogruppi d'ordine 4, non ciclici, derivanti dal fatto che il quadrato è anche un rettangolo ed un rombo.

IL GRUPPO DI UNA TASSELLAZIONE DEL PIANO. Il piano si può ricoprire in molti modi mediante figure geometriche. Per esempio, si può rivestire mediante piastrelle quadrate uguali fra loro, o con piastrelle a forma di triangolo equilatero o di esagono regolare uguali fra loro.

Nessun altro tipo di poligono regolare può servire come forma per piastrelle, a causa degli angoli interni troppo grandi o non divisori interi di 360°, come per i pentagoni.



Ogni tipo di tassellazione possiede un proprio gruppo di simmetria, che contiene normalmente traslazioni non banali. In questo caso, i gruppi possibili sono stranamente in numero finito, solo 17, detti anche *gruppi delle carte da parati*.

L'ESPRESSIONE ANALITICA DI UNA ISOMETRIA PIANA. Troviamo ora la forma analitica delle isometrie, incominciando dalle simmetrie assiali. Introduciamo nel piano un sistema di assi cartesiani ortogonali. Allora una retta s ha equazione $ax+by+c = 0$, con $(a, b) \neq (0, 0)$. Dividendo eventualmente i tre coefficienti per a^2+b^2, possiamo supporre $a^2+b^2 = 1$.

Sia ora P(x, h) un punto e sia P'(x', h') il suo simmetrico rispetto alla retta s.

La retta PP' è perpendicolare ad s, per cui si ha:

$$b(h - h') - a(x - x') = 0.$$

Inoltre, il punto medio di PP' appartiene ad s, quindi si ha:

$$a \cdot \frac{x + x'}{2} + b \cdot \frac{y + y}{2} + c = 0.$$

Si ottiene così il sistema lineare $\begin{cases} bx' - ah' = bx - ah \\ ax' + bh' = -ax - bh - 2c \end{cases}$.

La sua matrice dei coefficienti ha determinante $-a^2-b^2 = -1$, per cui il sistema è determinato. Si ottiene, eseguendo i calcoli:

$$(*) \quad \begin{cases} x' = \left(b^2 - a^2\right)x - 2abh - 2ac \\ h' = -2abx - \left(b^2 - a^2\right)h - 2bc \end{cases}.$$

Siano $X' = \begin{bmatrix} x' \\ h' \end{bmatrix}$, $X = \begin{bmatrix} x \\ h \end{bmatrix}$, $A = \begin{bmatrix} b^2 - a^2 & -2ab \\ -2ab & a^2 - b^2 \end{bmatrix}$, $B = \begin{bmatrix} -2ac \\ -2bc \end{bmatrix}$.

Allora le equazioni (*) della simmetria σ diventano, in forma matriciale:

$$X' = A \times X + B.$$

Detta A^t la trasposta di A, si vede subito che $A^t = A^{-1}$, cioè A è *ortogonale*.

Data ora un'altra simmetria assiale σ_1, essa si potrà rappresentare con la equazione matriciale $X' = A_1X + B_1$, dove anche A_1 è una matrice ortogonale con determinante -1. Allora la composta $\sigma_1 \circ \sigma$ avrà equazione matriciale:

$$X' = A_1 \times (A \times X + B) + B_1 = (A_1 \times A) \times X + (A_1 \times B + B_1)$$

dove la matrice $A_1 \times A$ è ancora ortogonale (come si verifica facilmente), ma con determinante 1. Pertanto un movimento ha equazione $X' = M \times X + C$, dove $M = A \times A_1$ è ortogonale con determinante 1 e $C = (A_1 \times B + B_1)$ è un vettore-colonna.

Poiché la matrice di σ dipende solo dai coefficienti a e b della retta e non dal termine noto c, simmetrie con assi paralleli hanno la stessa matrice A. Sappiamo che, essendo gli assi paralleli, allora $\sigma_1 \circ \sigma$ è una traslazione, ed essendo $A_1 = A$, allora $M = A^2 = I_2$, denotando

con I_2 la matrice unità. Pertanto, l'equazione di una traslazione è X' = X + C, dove C è il corrispondente dell'origine O = (0, 0) nella traslazione stessa.

Infine, componendo una simmetria con un movimento si riottiene un'equazione matriciale dello stesso tipo, ma con il determinante -1.
Pertanto:

TEOREMA 2.6. Per ogni isometria f esistono una matrice ortogonale A ed un vettore-colonna B tali che f ha equazione (in forma matriciale) X' = A×X + B. Si ha inoltre: $f \in M \Leftrightarrow \det(A) = 1$, ed $f \in T \Leftrightarrow A = I_2$.

Osservazioni. 1. Si può anche dimostrare che, inversamente, per ogni matrice ortogonale A e per ogni vettore-colonna B la trasformazione f di equazione X' = A×X + B è un'isometria.
2. Data l'isometria f di equazione X' = A×X+B, come classificarla? Abbiamo visto già che è una traslazione se e solo se $A = I_2$ ed è un movimento se e solo se det(A) = 1, per cui se $A \neq I_2$ e det(A) = 1 allora f è una rotazione, e viceversa.

Sia det(A) = -1: f è una simmetria assiale se e solo se ha periodo 2, quindi se e solo se $f^2 = id$, cioè se e solo se A×B+B = O (vettore nullo). Se ciò non accade, f^2 è una traslazione non identica e quindi f è un'antitraslazione.

RISOLUBILITÀ DEL GRUPPO DELLE ISOMETRIE PIANE. Una proprietà importante per un gruppo G è la sua *risolubilità*. Il nome deriva dalla Teoria di Galois sulla risolubilità per radicali di una equazione algebrica.

Una sequenza finita di sottogruppi come la seguente:

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

è detta *serie subnormale*. I sottogruppi $G_0, \ldots, G_n$ sono detti *termini*; ciascuno di essi è normale nel successivo (ma non necessariamente in G). I quozienti G_{i+1}/G_i sono detti *fattori* della serie. Il gruppo G si dice *risolubile* se possiede una serie subnormale *abeliana*, ossia tale che i fattori G_{i+1}/G_i siano tutti abeliani.
I gruppi abeliani sono banalmente risolubili. Invece, per esempio, da un teorema di Galois segue che per $n \geq 5$ il gruppo simmetrico S_n non è risolubile, mentre lo è per $n \leq 4$.

Mostriamo che il gruppo Γ è risolubile. Sappiamo che è un gruppo infinito, contenente il sottogruppo T delle traslazioni che è isomorfo al gruppo $(\mathbf{R}^2, +)$ dei vettori del piano, per cui Γ non è numerabile. Sappiamo anche che non è abeliano. Si ha poi:

LEMMA 2.7. Il sottogruppo M dei movimenti ha indice 2 in Γ ed è pertanto un sottogruppo normale.

Dimostrazione. Sia σ una simmetria assiale fissata e sia f un'isometria inversa. Il prodotto $f\circ\sigma$ è un movimento, cioè esiste $\varphi\in M$, tale che $f\circ\sigma = \varphi$. Ma allora $f = \varphi\circ\sigma$, cioè f appartiene al laterale destro $M\sigma$. Ne segue $\Gamma \setminus M = M\sigma$, pertanto gli unici laterali destri di M in Γ sono M stesso ed $M\sigma$, quindi M ha indice 2. Ovviamente si ha anche $\sigma M = \Gamma \setminus M = M\sigma$, quindi M è normale in Γ.

Dati in un gruppo G due sottogruppi H e K, con $K \triangleleft G$, tali che $H\cap K = \{1_G\}$, se $HK = G$ (ossia ogni $g\in G$ è prodotto di un $h\in H$ per un $k\in K$), allora G è detto *prodotto semidiretto* di H per K. Si ha allora anche $KH = G$.
Una formulazione equivalente è che ogni $g\in G$ appartiene ad un laterale kH, con $k\in K$, o anche che ogni $g\in G$ appartiene ad un laterale hK, con $h\in H$.
Se G è prodotto semidiretto di H per $K\triangleleft G$, allora G/K è isomorfo ad H.
Ciò posto:

PROPOSIZIONE 2.8. Siano T il sottogruppo delle traslazioni, O un punto del piano e Γ_O il suo stabilizzatore. Si ha:
a) Il sottogruppo T è normale in Γ.
b) Si ha $\Gamma = T\Gamma_O$, $T\cap\Gamma_O = \{id\}$, ossia Γ è prodotto semidiretto di T per Γ_O.
c) M è prodotto semidiretto di T per $(M\cap\Gamma_O)$.

Dimostrazione. a) Proviamo che T è normale in Γ. Poiché le simmetrie assiali generano Γ, basta provare che per ogni simmetria σ e per ogni traslazione τ, anche $\sigma^{-1}\circ\tau\circ\sigma = \sigma\circ\tau\circ\sigma$ è una traslazione. Sia s l'asse di σ e sia $\tau = \sigma_2\circ\sigma_1$, con σ_i simmetria di asse s_i, ed s_1 parallelo ad s_2.
Se anche s è parallelo ad s_1 si ha $\sigma^{-1}\circ\tau\circ\sigma = (\sigma\circ\sigma_2)\circ(\sigma_1\circ\sigma)$ prodotto di due traslazioni, quindi è una traslazione.
Se invece s non è parallela alle altre due rette, essa forma con esse angoli coniugati interni supplementari, per cui le due rotazioni $\sigma\circ\sigma_2$ e $\sigma_1\circ\sigma$ hanno ampiezze opposte. Pertanto, $\sigma\circ\tau\circ\sigma = (\sigma\circ\sigma_2)\circ(\sigma_1\circ\sigma)$ è una traslazione.

b) Sia f un'isometria e siano $O' = f(O)$, τ la traslazione associata al vettore $\vec{OO'}$. Allora $\tau^{-1}\circ f(O) = O$, cioè $\tau^{-1}\circ f\in\Gamma_O$. Ne segue $f \in \tau\Gamma_O$, quindi $\Gamma = T\Gamma_O$.

Poiché l'unica traslazione che abbia punti uniti è l'identità, si ha $T \cap \Gamma_O = \{id\}$.

c) T è ovviamente normale anche in M. Sia μ un movimento e siano $O' = \mu(O)$ e τ la traslazione associata al vettore $\vec{OO'}$. Allora $\tau^{-1} \circ \mu(O) = O$, cioè $\tau^{-1} \circ \mu \in (M \cap \Gamma_O)$. Ne segue $\mu \in \tau(M \cap \Gamma_O)$, quindi $M = T(M \cap \Gamma_O)$.

PROPOSIZIONE 2.9. Il gruppo Γ è risolubile.

Dimostrazione. La serie $1 = \{id\} \lhd T \lhd M \lhd \Gamma$ è una serie normale e si ha:

- $T/1 \cong T \cong \left(\mathbf{R}^2, +\right)$, abeliano;
- $M/T \cong (M \cap \Gamma_O)$ = gruppo delle rotazioni di centro O, isomorfo al gruppo $\left(\mathbf{R}/2\pi\mathbf{Z}, +\right)$ degli angoli, che è abeliano;
- Γ /M è abeliano perché ha ordine 2.

Pertanto la serie data è abeliana e Γ è risolubile.

Osservazione. Anche il gruppo Σ delle similitudini del piano è risolubile, perché il sottogruppo Γ delle isometrie è normale in Σ e Σ/Γ è isomorfo al gruppo moltiplicativo di $\mathbf{R}$, che è abeliano. Dunque, Σ ha la serie abeliana $1 = \{id\} \lhd T \lhd M \lhd \Gamma \lhd \Sigma$.

Invece, il gruppo delle affinità del piano non è risolubile.