Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

UN'INTRODUZIONE A QUASIGRUPPI E LOOPS

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
MONICA IDÀ

Presentata da:
MATTEO ALLEGRO

Correlatore:
Chiar.mo Prof.
LIBERO VERARDI

II Sessione
Anno Accademico 2011/2012

A tutti quelli che hanno preparato con me almeno un appello
(vale anche se ci hanno segato).

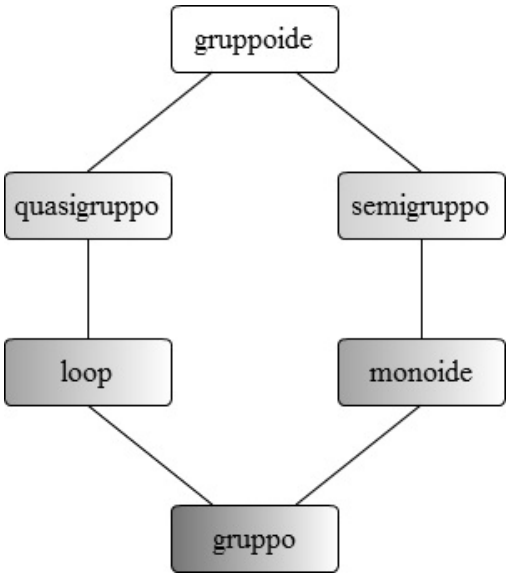
Ai Miei e a Frency.

Indice

Introduzione

Obiettivo di questa tesi è presentare, insieme al maggior numero possibile di esempi, alcuni tra i principali risultati introduttivi alla teoria dei quasigruppi e dei loops, strutture algebriche che hanno una sola operazione binaria, non associativa.
Nata quindi dal desiderio di approfondire almeno un pò la conoscenza di queste due strutture, quasigruppo e loop, questa tesi ha portato a considerare nel testo oltre trenta tipi di semigruppoidi non associativi, buona parte dei quali è illustrata nelle due tavole fuori testo (p. 1 e p. 24).

Quando si introduce la struttura di gruppo si richiede, in genere ordinatamente, che l'operazione sia interna e associativa (semigruppo), l'esistenza e unicità dell'elemento neutro (monoide) e infine dell'inverso di ogni elemento. Inoltre si può richiedere a qualsiasi livello che la struttura sia commutativa e si presentano spesso i semigruppi commutativi a fianco dei semigruppi e i monoidi commutativi insieme ai monoidi.



Nel primo capitolo si cominciano a studiare i semigruppoidi con varie proprietà aggiuntive, ad esempio la cancellazione sinistra e la cancellazione destra ((1.1) e (1.2)), la divisione a sinistra e la divisione a destra ((1.3) e (1.4)), per arrivare a studiare i quasigruppi combinatori ed equazionali, arrivando a far vedere l'equivalenza delle due definizioni (teorema 1.3). Si parla inoltre delle parastrofi di un quasigruppo (vedi 1.4), dei sistemi tripli di Steiner che danno luogo ad esempi di quasigruppi, e per finire si illustra come da un quasigruppo con opportune proprietà si possa costruire un gruppo; questo viene fatto in 1.5.2 sotto particolari ipotesi per via puramente algebrica, mentre in 1.6 si illustra una costruzione classica, cioè la legge di gruppo su una cubica piana, che non è altro che la costruzione geometrica di un quasigruppo e del gruppo associato. Nel capitolo 2 si studiano i loops, cioè i quasigruppi con elemento neutro. In particolare si parla di inversi destri e sinistri (definizione 2.10) e di proprietà dell'inverso destro e proprietà dell'inverso sinistro (definizione 2.9), cercando di vedere quando questi inversi coincidono. Si prosegue studiando svariate proprietà più deboli dell'associativa (quali sono le identità di Bol-Moufang) o restrizioni della stessa (per esempio le proprietà alternative) che possono valere in ambienti propriamente non associativi. In particolare si studiano i Moufang loops e i Bol loops.

Con $(A\,,\,*)$ verrà denotata una qualsiasi struttura algebrica con un'operazione binaria $*$ interna sull'insieme A. Tale insieme sarà sempre non vuoto.
Ovunque nel testo si farà a essa riferimento, si intenderà per *proprietà associativa* dell'operazione binaria $*$ sull'insieme A la:

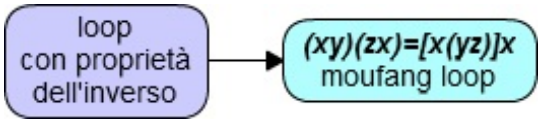
$$(a * b) * c = a * (b * c)\ \forall\, a, b, c \in A.$$

Si cercherà sempre di non confondere la struttura $(A\,,\,*)$ con l'insieme A a essa sottogiacente e si userà la notazione A in luogo della $(A\,,\,*)$ solo se preferibile per snellire il testo e dove questo non generi ambiguità, per esempio ove non ci sia altrimenti esigenza di menzionare l'operazione esplicitamente. In questi casi si avrà sempre A accompagnato da un'apposizione: 'il gruppoide A', oppure 'un quasigruppo A', ecc.
Nel capitolo 1, e più frequentemente nel capitolo 2, l'operazione di quasigruppo, sempre preferibilmente in notazione moltiplicativa, verrà denotata con la giustapposizione. L'operazione di gruppo su una cubica piana, oggetto della sezione 1.6, sarà invece espressa in notazione additiva secondo la tradizione.

Sia $A = \{a_1, \ldots, a_n\}$; si chiamerà *tavola di moltiplicazione* o *tavola di Cayley*[1] di una struttura $(A\,, *)$ la matrice quadrata di ordine n con $a_i * a_j$ elemento di posto (i, j). Tale matrice verrà rappresentata nella notazione di tabella bordata, con gli elementi $a_i \in A$ a etichettarne le righe e $a_j \in A$ a etichettarne le colonne.
In analogia con la teoria dei gruppi, già nel primo capitolo si chiamerà *ordine* della struttura $(A\,, *)$ la cardinalità dell'insieme A.
Quanto alla composizione di applicazioni $fg(x)$ indicherà $f(g(x))$, mentre la funzione identità sull'insieme A sarà denotata con Id_A. Per i vettori si è preferita la notazione $\mathbf{v}$ alla $\vec{v}$.
Le notazioni usate derivano da quelle adottate da un certo numero di autori diversi, non solo tra quelli elencati in bibliografia, e così pure alcuni tratti dell'esposizione; in entrambi i casi ogni scelta è stata fatta in un'ottica di chiarezza e di sintesi e organicità della trattazione.

Si è volutamente trascurata, per ovvie ragioni di spazio, la trattazione dei sistemi di generatori dei gruppoidi e della teoria dei quasigruppi liberi e si è ridotta a pochi accenni la trattazione dell'omomorfismo e dell'isotopia. Questo in favore della descrizione di un maggior numero di fatti di natura più puramente aritmetica. Vi sono nondimeno risultati interessantissimi in merito, alcuni dei quali risultano praticamente invariati rispetto alla teoria dei gruppi, mentre altri subiscono modifiche sostanziali. Ad esempio, contrariamente a quanto accade per i gruppi (teorema di Lagrange), esiste un sotto-loop di ordine 2 di un loop di ordine 5.
Nel tentativo di esporre le nozioni nella massima generalità verrà adottato, laddove non comune agli altri autori, il punto di vista di Bruck in [2].

Le due tavole fuori testo (p. 1 e p. 24) sono state preparate online su cacoo.com, [10]. Nella seconda di queste, la freccia



indica per esempio che ogni Moufang loop è un loop con la proprietà dell'inverso o, meglio, che aggiungendo un'ulteriore proprietà o identità a un loop con la proprietà

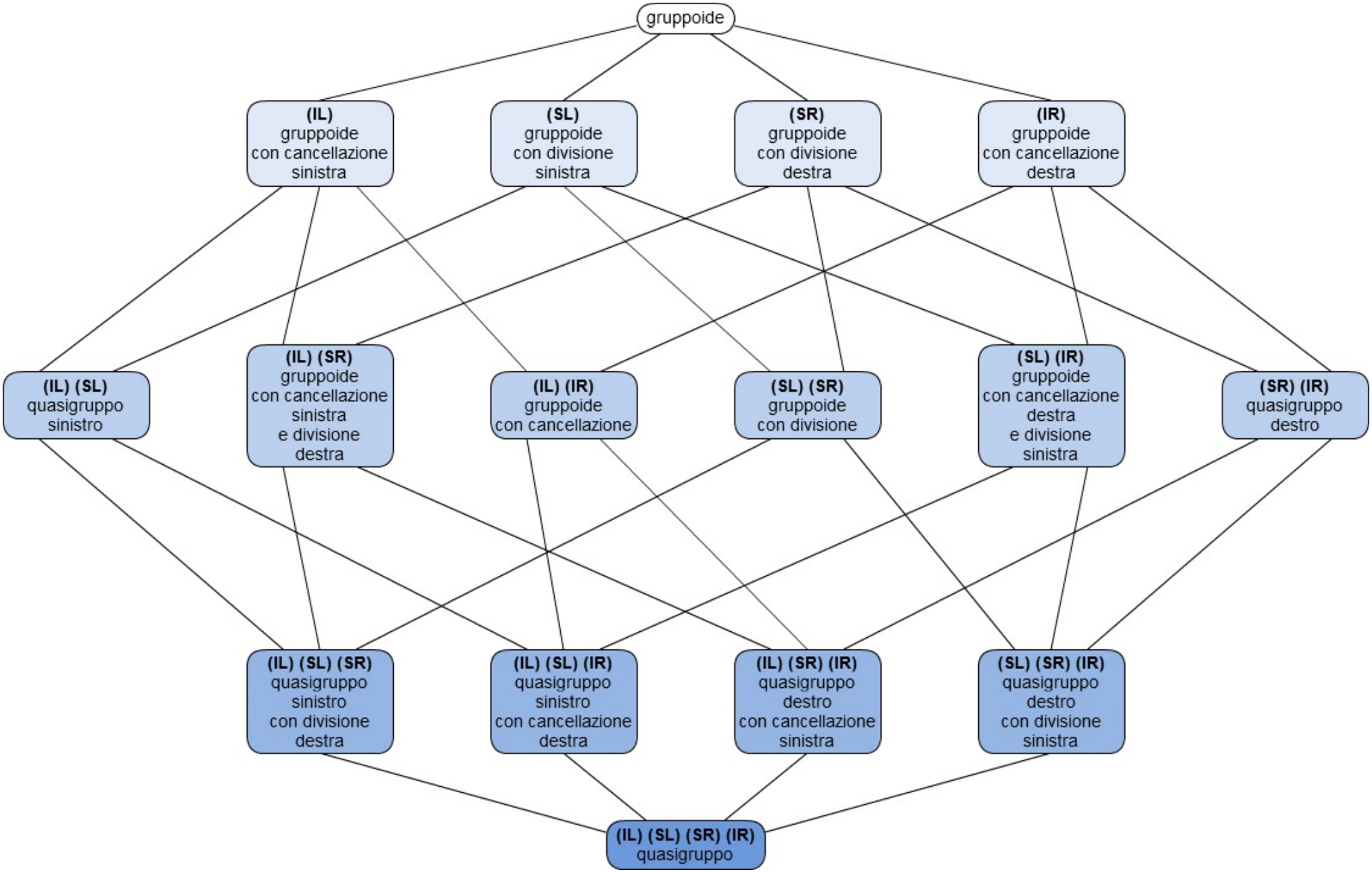
[1] Arthur Cayley (1821–1895), cui deve il proprio nome anche l'algebra degli ottonioni.

dell'inverso, si ottiene un Moufang loop. Tale identità è riportata in grassetto corsivo sopra il nome della nuova struttura.

Lungo tutta la tesi vengono sempre dati numerosi esempi. Tra gli esempi e applicazioni che non sono stati considerati per ragioni di tempo, due meritano a mio parere un attimo di attenzione.
Una pagina di Wikipedia in lingua italiana[2], pur sprovvista dei minimi riferimenti bibliografici, descrive un procedimento per ottenere un left-loop o un loop dalla 'sezione' di un gruppo.
Per quanto riguarda le applicazioni dei quasigruppi in crittografia, rimandiamo allo stesso autore di [14] e [16]: l'articolo [15] di Victor Shcherbacov fornisce una ampia panoramica sull'argomento, oltre a una bibliografia che metterebbe a dura prova anche il lettore più paziente.

Per quanto riguarda i legami con la geometria, si ha che come la nozione di gruppo è collegata alla risolubilità delle equazioni algebriche e alla estensione della teoria di Galois alle equazioni differenziali, così la nozione di quasigruppo e di loop sono legate alla coordinatizzazione di un piano proiettivo astratto. Secondo il metodo di M. Hall (o quello di D. Hughes), ad ogni piano proiettivo è possibile associare una struttura algebrica $(R\,,\,*)$ dove $*$ è una operazione ternaria, ed R è l'insieme dei punti di una retta fissata (meno uno, fissato, detto ∞). In particolari situazioni, sono definite due operazioni binarie $+$ e $\cdot$ in modo tale che $y = *(x, a, b)$ se e solo se $y = a \cdot x + b$ (che diventa l'equazione della retta generica) e queste due operazioni binarie formano dei loops $(R\,,\,+\,,\,0)$ e $(R\backslash\{0\}\,,\,\cdot\,,\,1)$ e $\cdot$ è distributiva (a destra o a sinistra) rispetto a $+$. Se poi il gruppo delle proiettività è particolarmente ricco (o se, equivalentemente, sono presenti nel piano proiettivo opportune configurazioni geometriche) $(R\,,\,+\,,\,0)$ diventa un gruppo, $(R\backslash\{0\}\,,\,\cdot\,,\,1)$ è un Moufang loop o un gruppo e possono valere entrambe le proprietà distributive. Ciò rende più interessante lo studio dei quasigruppi e dei loops, perché lo collega ad altre teorie matematiche, come la geometria proiettiva, o anche le geometrie non euclidee.

[2] `http://it.wikipedia.org/wiki/Left_loop#Sezione_di_un_gruppo`, consultata il 19 settembre 2012.


gruppoide
(IL) gruppoide con cancellazione sinistra
(SL) gruppoide con divisione sinistra
(SR) gruppoide con divisione destra
(IR) gruppoide con cancellazione destra
(IL) (SL) quasigruppo sinistro
(IL) (SR) gruppoide con cancellazione sinistra e divisione destra
(IL) (IR) gruppoide con cancellazione
(SL) (SR) gruppoide con divisione
(SL) (IR) gruppoide con cancellazione destra e divisione sinistra
(SR) (IR) quasigruppo destro
(IL) (SL) (SR) quasigruppo sinistro con divisione destra
(IL) (SL) (IR) quasigruppo sinistro con cancellazione destra
(IL) (SR) (IR) quasigruppo destro con cancellazione sinistra
(SL) (SR) (IR) quasigruppo destro con divisione sinistra
(IL) (SL) (SR) (IR) quasigruppo

Capitolo 1

Quasigruppi

1.1 Definizioni preliminari

Definizione 1.1. Sia A un insieme non vuoto, sia $A \times A$ il prodotto cartesiano di A per se stesso e sia $R \subseteq A \times A$. Si chiama *operazione binaria interna* su A una qualsiasi funzione $* : R \to A$.

Il sottoinsieme R di $A \times A$ si dice *range* dell'operazione $*$ in A e verrà denotato con $R(A\,,\,*)$ o semplicemente con $R(*)$.
Se $(a, b) \in R(*)$, si preferisce usare per l'elemento $*(a, b)$ di A la notazione relazionale $a * b$. Se $R(*) \subsetneq A \times A$, certi autori chiamano $*$ 'semioperazione'[1]. La scrittura $a * b$ nel seguito sottintende che $(a, b) \in R(*)$.

Definizione 1.2. Si chiama *semigruppoide*[2] una struttura $(G\,,\,*)$ costituita da un insieme non vuoto G con un'operazione binaria $*$ interna a G.

Esempio 1.1. Sia G l'insieme $\mathbb{N}$ dei numeri naturali e sia $*$ l'usuale operazione di sottrazione, denotata con $-$. La coppia $(\mathbb{N}\,,\,-)$ è un semigruppoide con range:

$$R(\mathbb{N}\,,\,-) = \left\{(a, b) \in \mathbb{N}^2 \mid b \leq a\right\}.$$

Definizione 1.3. Sia $(G\,,\,*)$ un semigruppoide e sia H un sottoinsieme non vuoto di G. Si dice che $(H\,,\,\circ)$ è un *sottosemigruppoide* di $(G\,,\,*)$ se $(H\,,\,\circ)$ è un semigruppoide tale che $a * b = c$ in G per ogni a, b tali che $a \circ b = c$ in H.

[1] *Halfoperation*.
[2] *Halfgroupoid* in [2].

Esempio 1.2. Si osservino le due tavole di moltiplicazione seguenti[3]:

G :

$*$	l	m	n
l	l		
m		n	
n		l	

H :

$\circ$	l	m
l	l	
m		

si ha immediatamente che H è un sottosemigruppoide di G.

Definizione 1.4. Si chiama *gruppoide* o *magma* un semigruppoide $(G\,,\,*)$ tale che

$$R(G\,,\,*) = G \times G.$$

Esempio 1.3. L'insieme $\mathbb{R}^+$ dei numeri reali positivi con l'operazione di elevamento a potenza a^b costituisce una struttura di gruppoide.

Definizione 1.5. Sia $(G\,,\,*)$ un gruppoide, si dice *ordine* di $(G\,,\,*)$ la cardinalità dell'insieme sostegno G.

Definizione 1.6 (sottosemigruppoide chiuso)**.** Sia $(G\,,\,*)$ un semigruppoide e sia $(H\,,\,\circ)$ un sottosemigruppoide di $(G\,,\,*)$. Si dice che H è *chiuso* in G se per ogni $a, b \in H$ si ha che $(a, b) \in R(G\,,\,*)$ implica $(a, b) \in R(H\,,\,\circ)$, cioè $(H \times H) \cap R(G\,,\,*) = R(H\,,\,\circ)$.

Esempio 1.4. Siano G e H come nell'esempio 1.2: H non è chiuso in G.

Esempio 1.5. La coppia $(\mathbb{N}\,,\,-)$ è un sottosemigruppoide di $(\mathbb{Z}\,,\,-)$, non chiuso.

Definizione 1.7. Sia $(G\,,\,*)$ un semigruppoide, si dice che H è un *sottogruppoide* di G se $(H\,,\,*)$ è un gruppoide ed è un sottosemigruppoide di $(G\,,\,*)$.

Esempio 1.6. Sia G come nell'esempio 1.2 e sia K un sottosemigruppoide di G come sotto: K è chiuso in G ed è un sottogruppoide di G.

K :

$*$	l
l	l

Definizione 1.8. Un *omomorfismo* θ da un semigruppoide $(H\,,\,*)$ in un semigruppoide $(K\,,\,\bullet)$ è una funzione $\theta : H \to K$ tale che $a * b = c$ in H implica $\theta(a) \bullet \theta(b) = \theta(c)$ in K.

[3] Come in [1, p. 127].

Definizione 1.9. Un elemento x di un gruppoide $(G\,,\,*)$ si dice *idempotente* se $x*x=x$; un gruppoide si dice *gruppoide idempotente* se ogni suo elemento è idempotente.

Esempio 1.7. Sia A un insieme non vuoto e sia $\mathcal{P}(A)$ l'insieme delle parti di A, siano $\cup$ e $\cap$ le usuali operazioni di unione e intersezione. Si ha che $(\mathcal{P}(A)\,,\,\cup)$ e $(\mathcal{P}(A)\,,\,\cap)$ sono gruppoidi idempotenti.

Esempio 1.8. Si considerino le strutture moltiplicative su $\mathbb{Z}_2$ e $\mathbb{Z}_3$. Come si può vedere per esempio costruendone le tavole di Cayley, $(\mathbb{Z}_2\,,\,\cdot)$ è idempotente mentre in $(\mathbb{Z}_3\,,\,\cdot)$ sono idempotenti solo gli elementi $[\,0\,]_3$ e $[\,1\,]_3$. Risulta infatti che $0^2 \equiv_3 0$ e $1^2 \equiv_3 1$, mentre $2^2 \equiv_3 1$.

Definizione 1.10 (gruppoide unipotente)**.** Un gruppoide $(G\,,\,*)$ si dice *unipotente* se verifica l'identità $x*x=y*y$ per ogni $x,y\in G$.

Esempio 1.9. Al termine della dimostrazione della proposizione 2.2, nel capitolo 2, vengono mostrati un gruppoide idempotente $(Q\,,\,\cdot)$ di ordine 4 e un gruppoide unipotente $(Q'\,,\,\bullet)$ di ordine 5.

Definizione 1.11. Un gruppoide $(G\,,\,*)$ si dice *totalmente simmetrico* se $a*b=c$ implica $\widetilde{a}*\widetilde{b}=\widetilde{c}$, ove $(\widetilde{a},\widetilde{b},\widetilde{c})$ sia una qualsiasi permutazione di (a,b,c).

Esempio 1.10. Si considerino i seguenti tre gruppoidi su $G=\{a,b,c\}$: solo il secondo è totalmente simmetrico. Infatti si ha: $c*b=b$, $b*b=a$ e: $c\circ c=b$, $c\circ b=a$.

$*$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

$\bullet$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Osservazione 1.1. Una struttura totalmente simmetrica è necessariamente anche commutativa, come si vede prendendo $(\widetilde{a},\widetilde{b},\widetilde{c})=(b,a,c)$. Non è vero invece il viceversa, come è mostrato nell'esempio 1.10.

Esempio 1.11. Il semigruppoide $(\mathbb{Z}\,,\,-)$ è un gruppoide ma non è totalmente simmetrico.

Definizione 1.12. Un gruppoide $(G\,,\,*)$ si dice *entropico* se verifica l'identità

$$(x*y)*(z*t)=(x*z)*(y*t)$$

per ogni $x,y,z,t\in G$.

Definizione 1.13. Sia $(G\,,\,*)$ un gruppoide e sia $a \in G$. Si dicono *traslazione sinistra* la funzione $L_a : G \to G$, $L_a(x) = a * x$ e *traslazione destra* la funzione $R_a : G \to G$, $R_a(x) = x * a$.

Osservazione 1.2. Sia $(G\,,\,*)$ un gruppoide di ordine finito. Allora ciascuna delle due traslazioni su G, L_a ed R_a, è iniettiva se e solo se è suriettiva, per ogni $a \in G$.

1.2 Leggi di cancellazione

Le due implicazioni seguenti possono valere oppure no in un arbitrario semigruppoide $(G\,,\,*)$ e si dicono *legge di cancellazione sinistra* e *legge di cancellazione destra* rispettivamente.

$$\forall\, a, b, c \in G \;\; (a * b = a * c \;\Rightarrow\; b = c) \tag{1.1}$$

$$\forall\, a, b, c \in G \;\; (b * a = c * a \;\Rightarrow\; b = c) \tag{1.2}$$

Esempio 1.12. Il gruppoide su $\mathbb{R}^+$ nell'esempio 1.3 ha la cancellazione sinistra e anche destra; i due gruppoidi in esempio 1.7 nessuna delle due.

Come vedremo, le (1.1) e (1.2) ricoprono un ruolo fondamentale nella definizione dei quasigruppi. Si osservi che la (1.1) si può riformulare come segue:

$$\text{se } a, d \in G, \text{ esiste al più un } x \text{ tale che } a * x = d \text{ in } G.$$

Definizione 1.14. Se $(G\,,\,*)$ è un semigruppoide con cancellazione sinistra, cioè verificante (1.1), si può definire un'operazione di *divisione a sinistra* $\backslash$ su G come segue:

$$a \backslash c = b \quad \Leftrightarrow \quad a * b = c \tag{1.3}$$

Analogamente, se $(G\,,\,*)$ è un semigruppoide con cancellazione destra, cioè verificante (1.2), si può definire un'operazione di *divisione a destra* $/$ su G come segue:

$$c / b = a \quad \Leftrightarrow \quad a * b = c \tag{1.4}$$

Osservazione 1.3. Sia $(G\,,\,*)$ un semigruppoide con cancellazione sinistra, allora lo è anche $(G\,,\,\backslash)$. Inoltre se $\backslash$ è l'operazione di divisione a sinistra in $(G\,,\,*)$, $*$ è l'operazione di divisione a sinistra in $(G\,,\,\backslash)$: le operazioni $\backslash$ e $*$ si possono scambiare nella doppia implicazione (1.3).

Definizione 1.15. Si dice *semiquasigruppo*[4] o *semigruppoide con cancellazione*[5] un semigruppoide $(G\,,\,*)$ che verifichi entrambe le proprietà di cancellazione (1.1) e (1.2).

In un semiquasigruppo $(G\,,\,*)$ *divisione a sinistra* $\backslash$ e *divisione a destra* $/$ vengono quindi definite ponendo che siano equivalenti le:

$$a * b = c \qquad\qquad a\backslash c = b \qquad\qquad c/b = a \tag{1.5}$$

esse valgono tutte oppure non vale nessuna delle tre.
Le strutture $(G\,,\,*\,,\,\backslash)$ e $(G\,,\,*\,,\,\backslash\,,\,/)$, rappresentative rispettivamente del semigruppoide con cancellazione sinistra (1.3) e del semiquasigruppo (1.5), vengono talvolta menzionate con il nome di 'semialgebra'[6].

Definizione 1.16. Sia $(G\,,\,*)$ un semiquasigruppo, si dice che H è un *sottosemiquasigruppo* di G se $(H\,,\,*)$ è un semiquasigruppo ed è un sottosemigruppoide di $(G\,,\,*)$ e quindi anche sottosemigruppoide di $(G\,,\,\backslash)$ e di $(G\,,\,/)$.

Definizione 1.17 (sottosemiquasigruppo chiuso)**.** Siano G e H come nella definizione 1.16. Un tale H si dice *chiuso* in G se è chiuso come sottosemigruppoide rispetto a ciascuna operazione. Ciò significa che, se $a * b = c$ in G e se due tra a, b, c sono elementi di H, il terzo è in H e $a * b = c$ in H.

Definizione 1.18. Si chiama *quasigruppo sinistro* (rispettivamente *destro*) un gruppoide $(G\,,\,*)$ tale che, per ogni coppia ordinata $(a, b) \in G \times G$, esista uno e un solo $x \in G$ tale che $a * x = b$ (rispettivamente uno e un solo $y \in G$ tale che $y * a = b$).

Definizione 1.19. Si chiama *quasigruppo*, o anche *quasigruppo combinatorio*, un gruppoide che sia contemporaneamente un quasigruppo sinistro e destro.

Dunque un quasigruppo è una coppia $(Q\,,\,\cdot)$ dove Q è un insieme non vuoto e $\cdot$ è un'operazione binaria su Q tale che valgano i seguenti assiomi:

$$\forall\, a, b \in Q\ \exists!\, c \in Q\ :\ a \cdot b = c \tag{1.6}$$

$$\forall\, a, b \in Q\ \exists!\, x \in Q\ :\ a \cdot x = b \tag{1.7}$$

$$\forall\, a, b \in Q\ \exists!\, y \in Q\ :\ y \cdot a = b \tag{1.8}$$

[4] *Halfquasigroup* in [2].
[5] *Cancellation halfgroupoid* in [2].
[6] Rispettivamente *special halfalgebra* e *halfalgebra* in [2].

Esempio 1.13. Si consideri il gruppoide $(G\,,\,*)$ ove G è l'insieme $\mathbb{R}^+ \cup \{0\}$ dei numeri reali non negativi e $a * b = |a - b|$. Esso è commutativo ma non è un quasigruppo[7]: l'equazione $5 * x = 2$ ha due distinte soluzioni in G, 3 e 7.

Osservazione 1.4. Sia G un gruppoide; allora G è un quasigruppo se e solo se la traslazione destra R_q e la traslazione sinistra L_q sono biettive su G, cioè sono permutazioni di G, per ogni $q \in G$.

Definizione 1.20. Un *quadrato latino* di ordine n è una matrice quadrata di ordine n i cui n^2 elementi sono esattamente n oggetti distinti e con la proprietà che ogni riga e ogni colonna contiene ciascuno degli n oggetti esattamente una volta.

Esempio 1.14. Nella tabella seguente vi sono tre quadrati latini di ordine 4.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

3	2	1	4
2	1	4	3
1	4	3	2
4	3	2	1

4	2	3	1
3	1	4	2
2	4	1	3
1	3	2	4

Osservazione 1.5. Un gruppoide $(Q\,,\,\cdot)$ di ordine finito n verifica la (1.7) se e solo se, comunque fissato $a \in Q$, la traslazione sinistra L_a è una biezione di Q o, equivalentemente, se ogni riga della tavola di moltiplicazione contiene ciascun elemento di Q esattamente una volta. Analogamente, Q verifica la (1.8) se e solo se ogni colonna della tavola di moltiplicazione contiene ogni elemento di Q esattamente una volta; riguardo ciò in particolare si veda ancora l'osservazione 1.4. Dunque condizione necessaria e sufficiente affinchè un gruppoide di ordine finito sia un quasigruppo è che la (una qualsiasi) sua tavola di moltiplicazione sia un quadrato latino.

1.3 Quasigruppo combinatorio ed equazionale

Gli assiomi di quasigruppo per $(Q\,,\,\cdot)$, (1.6), (1.7) e (1.8), si possono sintetizzare in uno come segue:

> se due qualsiasi tra x, y, z sono elementi di Q fissati, l'equazione $x \cdot y = z$ determina univocamente il terzo come elemento di Q.

[7] Tale struttura figura con il nome di *division system* tra gli esempi in [3], e come *gruppoide con divisione* nella prima tavola fuori testo.

Definizione 1.21. Si chiama *quasigruppo equazionale* e si denota con $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$ una struttura costituita da un insieme non vuoto Q con tre operazioni binarie interne tali che $(Q\,,\,\cdot)$, $(Q\,,\,\backslash)$ e $(Q\,,\,/)$ siano gruppoidi, e che verifichino le identità:

$$y \cdot (y\backslash x) = x \tag{SL}$$

$$(x/y) \cdot y = x \tag{SR}$$

$$y\backslash(y \cdot x) = x \tag{IL}$$

$$(x \cdot y)/y = x \tag{IR}$$

Teorema 1.1. *Una struttura $(Q\,,\,\cdot\,,\,\backslash)$ costituita da un insieme $Q \neq \emptyset$ e da due operazioni binarie interne tali che $(Q\,,\,\cdot)$ e $(Q\,,\,\backslash)$ siano gruppoidi, è un quasigruppo sinistro se e solo se $\backslash$ coincide con la divisione a sinistra di $(Q\,,\,\cdot)$ e valgono* (SL) *e* (IL).

Dimostrazione. Proviamo che una tale struttura è un quasigruppo sinistro, cioè che per ogni a, b esiste unico x tale che $a \cdot x = b$.
Siano quindi a e b dati; per la (SL), $a\backslash b$ è soluzione della $a \cdot x = b$. D'altra parte se x' è un'altra soluzione si ha, per (IL):

$$x = a\backslash b = a\backslash(a \cdot x') = x'$$

da cui la soluzione è unica.
Quindi (SL) garantisce l'esistenza di una soluzione e (IL) l'unicità per l'equazione $a \cdot x = b$.
Viceversa, sia $(Q\,,\,\cdot)$ un quasigruppo sinistro; se $\backslash$ indica la divisione a sinistra in $(Q\,,\,\cdot)$, sappiamo che $(Q\,,\,\backslash)$ è un gruppoide e si ha per definizione:

$$a\backslash c = b \quad \Leftrightarrow \quad a \cdot b = c$$

quindi

$$a \cdot (a\backslash c) = c \tag{SL}$$

$$a\backslash(a \cdot b) = b \tag{IL}$$

□

Teorema 1.2. *Una struttura $(Q\,,\,\cdot\,,\,/)$ costituita da un insieme $Q \neq \emptyset$ e da due operazioni binarie interne tali che $(Q\,,\,\cdot)$ e $(Q\,,\,/)$ siano gruppoidi, è un quasigruppo destro se e solo se $/$ coincide con la divisione a destra di $(Q\,,\,\cdot)$ e valgono* (SR) *e* (IR).

Dimostrazione. Analoga a quella del teorema 1.1. □

Teorema 1.3. *Si ha che* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$ *è un quasigruppo equazionale se e solo se* $(Q\,,\,\cdot)$ *è un quasigruppo combinatorio, e le operazioni* $\backslash$ *e* $/$ *coincidono rispettivamente con la divisione a sinistra e a destra di* $(Q\,,\,\cdot)$.

Dimostrazione. Segue dal teorema 1.1 e dal teorema 1.2. □

Osservazione 1.6. Si è visto nell'osservazione 1.4 che in un quasigruppo combinatorio le traslazioni destra R_q e sinistra L_q sono biettive. Le (SL) e (SR) esprimono la suriettività e le (IL) e (IR) l'iniettività di L_q ed R_q rispettivamente.

Lemma 1.1. *In un quasigruppo equazionale* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$ *valgono le:*

$$y/(x\backslash y) = x \tag{1.9}$$

$$(y/x)\backslash y = x \tag{1.10}$$

Dimostrazione. Sostituendo $x\backslash y$ ad y si può riscrivere (IR) come $(x \cdot (x\backslash y))/(x\backslash y) = x$; da questa, per (SL) a meno della permutazione delle due variabili, si ottiene $y/(x\backslash y) = x$, (1.9).
Allo stesso modo, sostituendo y/x ad y si può riscrivere (IL) come $(y/x)\backslash((y/x) \cdot x) = x$ e da questa, per (SR), si ottiene $(y/x)\backslash y = x$, cioè (1.10). □

Lemma 1.2. *In un quasigruppo equazionale* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$,

- *dalle identità* (SR) *e* (1.9) *segue la* (SL)*;*
- *dalle identità* (IL) *e* (1.9) *segue la* (IR).

Dimostrazione. Si può riscrivere (SR) come $(x/(y\backslash x))\cdot(y\backslash x) = x$; da questa, per la (1.9), si ottiene $y \cdot (y\backslash x) = x$, cioè (SL).
Allo stesso modo si può riscrivere la (1.9) come $(x \cdot y)/(x\backslash(x \cdot y)) = x$ e da questa, per (IL), si ottiene $(x \cdot y)/y = x$, cioè (IR). □

Lemma 1.3. *In un quasigruppo equazionale* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$,

- *dalle identità* (SL) *e* (1.10) *segue la* (SR)*;*
- *dalle identità* (IR) *e* (1.10) *segue la* (IL).

Dimostrazione. Si può riscrivere (SL) come $(x/y) \cdot ((x/y)\backslash x) = x$ e da questa, per la (1.10), si ottiene $(x/y) \cdot y = x$, cioè (SR).
Allo stesso modo si può riscrivere la (1.10) come $((y \cdot x)/x)\backslash(y \cdot x) = x$; da questa, per (IR), si ottiene $y\backslash(y \cdot x) = x$, cioè (IL). □

Teorema 1.4. *Una struttura* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$ *costituita da un insieme non vuoto* Q *e da tre operazioni binarie interne tali che* $(Q\,,\,\cdot)$, $(Q\,,\,\backslash)$ *e* $(Q\,,\,/)$ *siano gruppoidi, con le identità* (SR), (IL) *e* (1.9) *è un quasigruppo.*

Dimostrazione. Segue dal lemma 1.2. □

Teorema 1.5. *Una struttura* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$ *costituita da un insieme non vuoto* Q *e da tre operazioni binarie interne tali che* $(Q\,,\,\cdot)$, $(Q\,,\,\backslash)$ *e* $(Q\,,\,/)$ *siano gruppoidi, con le identità* (SL), (IR) *e* (1.10) *è un quasigruppo.*

Dimostrazione. Segue dal lemma 1.3. □

Corollario 1.5.1 (Shcherbacov)**.** *Una struttura* $(Q\,,\,\cdot\,,\,\backslash\,,\,/)$ *costituita da un insieme non vuoto* Q *e da tre operazioni binarie interne tali che* $(Q\,,\,\cdot)$, $(Q\,,\,\backslash)$ *e* $(Q\,,\,/)$ *siano gruppoidi, è un quasigruppo equazionale, posto che verifichi una qualsiasi delle seguenti quaterne di equazioni:* (SL), (SR), (IL), (1.9)*;* (SR), (IL), (IR), (1.9)*;* (SL), (SR), (IR), (1.10)*;* (SL), (IL), (IR), (1.10) *oppure:* (SL), (IL), (1.9), (1.10)*;* (SL), (IR), (1.9), (1.10)*;* (SR), (IL), (1.9), (1.10)*;* (SR), (IR), (1.9), (1.10).

Dimostrazione. Segue dai lemmi 1.2 e 1.3 e dai teoremi 1.4 e 1.5. □

Esempio 1.15. Siano $(\mathbb{Z}\,,\,+\,,\,\cdot)$ l'anello degli interi, $/$ la divisione in $\mathbb{Z}$ e $[a]$ la parte intera di a. Sia $x \circ y = [x/2] - y$, allora il gruppoide $(\mathbb{Z}\,,\,\circ)$ è un *quasigruppo sinistro con divisione a destra*, in quanto verifica (SL), (IL) e anche (SR) ma non (IR).

Un quasigruppo sinistro con divisione a destra si può allora in generale caratterizzare, tenuto conto dell'osservazione 1.6 come un gruppoide ove la traslazione sinistra sia biettiva e la traslazione destra soltanto suriettiva. In virtù dell'osservazione 1.2, una tale struttura non può avere ordine finito.

1.4 Quasigruppi coniugati

Sia $(Q\,,\,\circ)$ un quasigruppo e siano $\backslash$ e $/$ la sua divisione sinistra e la sua divisione destra; allora è facile vedere che anche $(Q\,,\,\backslash)$ e $(Q\,,\,/)$ sono quasigruppi.
Definiamo ora l'operazione $\bullet$ su Q, *opposta* a $\circ$, mediante l'identità:

$$a \bullet b = b \circ a \tag{1.11}$$

Anche $(Q\,,\,\bullet)$ è un quasigruppo, le cui operazioni di divisione sinistra e destra[8] si possono denotare rispettivamente con $\backslash\backslash$ e $//$. Essendo equivalenti le:

$$\begin{array}{ll} a \circ b = c & b \bullet a = c \\ a\backslash c = b & c//a = b \\ c/b = a & b\backslash\backslash c = a \end{array} \tag{1.12}$$

si hanno allora da $(Q\,,\,\circ)$ cinque ulteriori quasigruppi: $(Q\,,\,\backslash)$, $(Q\,,\,/)$, $(Q\,,\,\bullet)$, $(Q\,,\,\backslash\backslash)$ e $(Q\,,\,//)$. Ciascuno di questi si dice[9] *quasigruppo coniugato* o *parastrofe* di $(Q\,,\,\circ)$.
Dunque ogni quasigruppo determina un insieme di sei quasigruppi, in generale tutti distinti. Un quasigruppo totalmente simmetrico si può caratterizzare come coincidente con tutte le sue parastrofi. Se $(Q\,,\,\circ)$ è un gruppoide, $(Q\,,\,\bullet)$ è un gruppoide mentre le altre quattro parastrofi non sono in generale definite; se $(Q\,,\,\circ)$ è un gruppoide commutativo, $(Q\,,\,\bullet)$ coincide con $(Q\,,\,\circ)$. Se $(Q\,,\,\circ)$ è un loop (si veda il capitolo 2), $(Q\,,\,\bullet)$ è a sua volta un loop mentre, tra le altre quattro parastrofi, $(Q\,,\,\backslash)$ e $(Q\,,\,\backslash\backslash)$ sono left-loops e $(Q\,,\,/)$ e $(Q\,,\,//)$ sono right-loops.

Osservazione 1.7. Se $(Q\,,\,\circ)$ è un quasigruppo sinistro (destro), $(Q\,,\,\bullet)$ è un quasigruppo destro (sinistro).

Una parastrofe di un gruppo abeliano verrà discussa in maggior dettaglio nella sezione 1.5.2.

Infine, un accenno alle parastrofi nel contesto dei quasigruppi equazionali. Si consideri, in $(Q\,,\,\circ)$, la $a \circ b = c$: applicando alla terna di elementi di Q le 6 permutazioni del gruppo simmetrico su tre lettere $\mathcal{S}_3$, si ottengono le (1.12). Siano $(Q\,,\,\circ)$, $(Q\,,\,\backslash)$, $(Q\,,\,/)$, $(Q\,,\,\bullet)$, $(Q\,,\,\backslash\backslash)$ e $(Q\,,\,//)$ le sei parastrofi di un quasigruppo in notazione combinatoria: i corrispondenti quasigruppi equazionali risultano essere rispettivamente $(Q\,,\,\circ\,,\,/\,,\,\backslash)$,

[8] *Opposite divisions* in [17].
[9] In lingua inglese *conjugate*, *adjugate* o *parastrophe*.

$(Q\,,\,\backslash\,,\,//\,,\,\circ)$, $(Q\,,\,/\,,\,\circ\,,\,\backslash\backslash)$, $(Q\,,\,\bullet\,,\,\backslash\backslash\,,\,//)$, $(Q\,,\,\backslash\backslash\,,\,\bullet\,,\,/)$ e $(Q\,,\,//\,,\,\backslash\,,\,\bullet)$. Tale insieme di quasigruppi equazionali permette un'ulteriore immediata verifica dell'osservazione 1.3.

1.5 Esempi

Vengono ora mostrati due modi di costruire quasigruppi, nel primo caso (in 1.5.1) di ordine finito, nel secondo (in 1.5.2) di ordine finito oppure no.

1.5.1 Sistemi tripli di Steiner

Sia X un insieme di cardinalità $n \geq 3$, sia $\mathcal{P}(X)$ l'insieme delle parti di X. Un *n-sistema triplo di Steiner* di X, T_n, è definito così: $T_n \subseteq \mathcal{P}(X)$, $|T| = 3$ per ogni $T \in T_n$ e:

$$a, b \in X\,,\; a \neq b \;\Rightarrow\; \exists\,!\, c \in X \;:\; \{a, b, c\} \in T_n.$$

Se chiamiamo 'terzina' un sottoinsieme di X con tre elementi (dunque necessariamente distinti), un n-sistema triplo di Steiner è quindi un insieme di terzine di X, tali che ogni coppia non ordinata di elementi di X appare in una e una sola terzina. Ad esempio, se $n = 5$ non possiamo costruire un 5-sistema triplo di Steiner, perché le coppie $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{1, 5\}$ devono comparire in una qualche terzina e quindi avremo per esempio $\{1, 2, 3\}$ e $\{1, 4, 5\}$; ma allora la coppia $\{2, 4\}$ non può apparire in nessuna terzina, perché non si può aggiungere 1 altrimenti si ha che $\{1, 2\}$ compare in $\{1, 2, 3\}$ e in $\{2, 4, 1\}$, e così via.
Esistono n-sistemi tripli di Steiner se e solo se $n > 1$ ed $n \equiv_6 1$ oppure $n \equiv_6 3$: la dimostrazione di questo fatto non è banale [3, p. 64]. Dunque i primi termini della successione degli n per cui esistono n-sistemi tripli di Steiner sono: $3, 7, 9, 13, 15, 19, 21, 25, 27, 31, \ldots$
Ogni elemento di X è contenuto in esattamente k terzine di T_n e il numero delle terzine T di T_n è t, cioè $|T_n| = t$, essendo $n = 2k + 1$ ed $nk = 3t$, da cui anche $n^2 - n = 6t$. Si tratta di una costruzione combinatoria: le terzine sono combinazioni semplici di 3 tra n elementi.
Esempi di n-sistemi tripli di Steiner per n piccolo sono (qui abc denota $\{a, b, c\}$):

$$n = 3 \quad : \quad \{\,123\,\}$$

$$n = 7 \quad : \quad \{\,123\,,\,145\,,\,167\,,\,246\,,\,257\,,\,347\,,\,356\,\}$$

$$n = 7 \quad : \quad \{\, 124\,,\, 135\,,\, 167\,,\, 236\,,\, 257\,,\, 347\,,\, 456\,\}$$

$$n = 7 \quad : \quad \{\, 124\,,\, 137\,,\, 156\,,\, 235\,,\, 267\,,\, 346\,,\, 457\,\}$$

$$n = 7 \quad : \quad \{\, 125\,,\, 134\,,\, 167\,,\, 236\,,\, 247\,,\, 357\,,\, 456\,\}$$

$$n = 7 \quad : \quad \{\, 127\,,\, 136\,,\, 145\,,\, 235\,,\, 246\,,\, 347\,,\, 567\,\}$$

$$n = 9 \quad : \quad \{\, 123\,,\, 147\,,\, 159\,,\, 168\,,\, 249\,,\, 258\,,\, 267\,,\, 348\,,\, 357\,,\, 369\,,\, 456\,,\, 789\,\}$$

Si vuole ora mostrare come i sistemi tripli di Steiner siano correlati con i quasigruppi di una certa classe, che non sono loops (si veda il capitolo 2). Essi sono anche correlati con una classe di loops[10] come verrà mostrato nell'esempio 2.3. Sia T_n un n-sistema triplo di Steiner, si può associare a T_n un quasigruppo totalmente simmetrico e idempotente (un tale quasigruppo si dice *quasigruppo di Steiner* o *squag*) di ordine n definendo come segue un'operazione $\circ$ su $\{1, 2, \ldots, n\}$:

$$a \circ b := \begin{cases} a & , \quad b = a \\ c \ : \ \{a, b, c\} \in T_n & , \quad b \neq a \end{cases} \tag{1.13}$$

Al contrario, ad ogni quasigruppo di Steiner di ordine $n \geq 3$ finito, $n \equiv_6 1$ oppure $n \equiv_6 3$, si può associare un sistema triplo di Steiner T_n, utilizzando la (1.13) per definire le terzine.

Le seguenti sono le tavole di moltiplicazione rispettivamente del primo e dell'ultimo tra i cinque 7-sistemi tripli di Steiner mostrati in questa sezione.

X :

$\circ$	1	2	3	4	5	6	7
1	1	3	2	5	4	7	6
2	3	2	1	6	7	4	5
3	2	1	3	7	6	5	4
4	5	6	7	4	1	2	3
5	4	7	6	1	5	3	2
6	7	4	5	2	3	6	1
7	6	5	4	3	2	1	7

X :

$\circ$	1	2	3	4	5	6	7
1	1	7	6	5	4	3	2
2	7	2	5	6	3	4	1
3	6	5	3	7	2	1	4
4	5	6	7	4	1	2	3
5	4	3	2	1	5	7	6
6	3	4	1	2	7	6	5
7	2	1	4	3	6	5	7

Osservazione 1.8. È immediato vedere che un gruppoide G totalmente simmetrico è un quasigruppo; in effetti, dato che l'operazione è definita su $G \times G$, la soluzione, unica, dell'equazione $ax = b$ è $x = ab$ e analogamente per $xa = b$.

[10] *Steiner loops* o *sloops*.

1.5.2 Quasigruppi associati ai gruppi

Si vuole ora mostrare come a ogni gruppo G si possa accostare, con un'opportuna costruzione, un quasigruppo Q, detto quasigruppo associato a G.
Risulta che quasigruppi associati a gruppi distinti sono distinti e si ricava un criterio per costruire, dato Q, il gruppo di cui Q è l'associato. Segue infine che la legge che a G associa Q induce una biezione tra i sottogruppi di G e i sottoquasigruppi di Q.
Il quasigruppo Q è uno delle cinque parastrofi[11] di G il quale, essendo un gruppo, è a sua volta un quasigruppo. Dunque il quasigruppo Q associato al gruppo G ha lo stesso insieme sostegno di G.
La costruzione è la seguente. Sia $(G\,,\,\cdot)$ un gruppo, e consideriamo la sua parastrofe (vedi sezione 1.4) $(G\,,\,/)$; si ha:

$$a/b = a \cdot b^{-1},$$

infatti $x \cdot b = a$ se e solo se $x = a \cdot b^{-1}$.
Nel seguito denoteremo l'operazione / su G con un simbolo più comodo; poniamo dunque:

$$\forall\, a, b \in G,\ a * b := a \cdot b^{-1} \tag{1.14}$$

È immediato verificare che $(G\,,\,*)$ verifica gli assiomi (1.6), (1.7) e (1.8). Non vale però in generale la proprietà associativa:

$$(a * b) * c = (a \cdot b^{-1}) * c = a \cdot b^{-1} \cdot c^{-1}$$

mentre, dato che in un gruppo vale la $(xy)^{-1} = y^{-1}x^{-1}$:

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

Un tale $(G\,,\,*)$ si dice *quasigruppo associato* al gruppo $(G\,,\,\cdot)$.

Teorema 1.6. *Condizione necessaria e sufficiente affinché un quasigruppo $(G\,,\,*)$ sia l'associato di un gruppo con sostegno sull'insieme G è che:*

1. *esista un elemento $e \in G$ tale che si abbia $a * b = e$ se e solo se $b = a$;*

2. *G verifichi l'identità*[12] $(a * c) * (b * c) = a * b$.

[11] Definite nella sezione 1.4.
[12] *Law of right transitivity.*

Dimostrazione. Se $(G\,,\,\cdot)$ è un gruppo con quasigruppo associato $(G\,,\,*)$, cioè se $*$ è definita dalla (1.14), la condizione 2 è soddisfatta in quanto $(a\cdot c^{-1})\cdot(b\cdot c^{-1})^{-1}=a\cdot b^{-1}$ ed esiste inoltre in G un elemento che verifica la condizione 1, precisamente l'elemento neutro. Questo prova la necessità.

Sia ora $(G\,,\,*)$ un quasigruppo verificante le condizioni 1 e 2. Sullo stesso insieme sostegno si consideri la struttura data dall'operazione $\cdot$ definita da:

$$a\cdot b:=a*(e*b) \tag{1.15}$$

Verifichiamo che la struttura $(G\,,\,\cdot)$ data dalla (1.15) è effettivamente un gruppo. Inanzitutto G è sicuramente chiuso rispetto all'operazione $\cdot$ definita in (1.15).
Occorre allora dimostrare che:

a) per ogni $a\in G$ esiste $b\in G$ tale che $a\cdot b=e=b\cdot a$;

b) per ogni $a\in G$ vale $a\cdot e=a=e\cdot a$;

c) per ogni $a,b,c\in G$ vale $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

Proviamo a. Per la (1.15) si ha che $a\cdot b=e$ se e solo se $a*(e*b)=e$ mentre, per la condizione 1, quest'ultima è equivalente alla $a=e*b$. Questa ha soluzione unica in b, da cui esiste ed è unico l'inverso destro b di a. Analogamente $\widetilde{b}\cdot a=e$ se e solo se $\widetilde{b}*(e*a)=e$, se e solo se $\widetilde{b}=e*a$, da cui esiste ed è unico l'inverso sinistro $e*a$ di a. Sostituendo $c=a$ nella condizione 2 si ottiene $(a*a)*(b*a)=a*b$ da cui, per la 1:

$$e*(b*a)=a*b\quad\forall\,a,b\in G \tag{1.16}$$

Risulta $\widetilde{b}=b$ se e solo se $\widetilde{b}*b=e$. Sostituendo qui le espressioni trovate per gli inversi, si ha $(e*a)*b=e$, poi $(e*(e*b))*b=e$. Per la (1.16) questa si può scrivere come $(b*e)*b=e$, vera perché è vera la:

$$b*e=b\quad\forall\,b\in G \tag{1.17}$$

La (1.17) si ottiene sostituendo $c=b$ nella condizione 2: $(a*b)*(b*b)=a*b$. Per la condizione 1 $(a*b)*e=a*b$, cioè $d*e=d$ per ogni $d\in G$ (in quanto ogni $d\in G$ si può scrivere, in molti modi, come $a*b$). Abbiamo quindi provato:

$$a^{-1}=e*a \tag{1.18}$$

Proviamo b. Dalla 1 e dalla (1.17) si ha:

$$a \cdot e := a * (e * e) = a * e = a.$$

Dalla (1.16) si ha:

$$e \cdot a := e * (e * a) = a * e = a.$$

Dunque l'elemento e di G è neutro in $(G\,,\,\cdot)$.
Proviamo c. Vale:

$$(a \cdot b) \cdot c = (a * (e * b)) * (e * c),$$

e:

$$a \cdot (b \cdot c) = a * (e * (b * (e * c))).$$

Sostituendo nella seconda la (1.16) e usando la condizione 2 si ottiene:

$$\begin{aligned} a \cdot (b \cdot c) &= a * ((e * c) * b) = \\ &= (a * (e * b)) * (((e * c) * b) * (e * b)) = \\ &= (a * (e * b)) * ((e * c) * e) = \\ &= (a * (e * b)) * (e * c) = \\ &= (a \cdot b) \cdot c. \end{aligned}$$

Il quasigruppo associato al gruppo $(G\,,\,\cdot)$ è proprio il quasigruppo da cui siamo partiti, cioè $(G\,,\,*)$. Infatti per la (1.18), la (1.16) e la (1.17):

$$\begin{aligned} a \cdot b^{-1} &= a * (e * b) = \\ &= a * (e * (e * b)) = \\ &= a * (b * e) = \\ &= a * b. \end{aligned}$$

Questo completa la dimostrazione. □

Conseguenza di questo teorema è che gli assiomi di gruppo per $(G\,,\,\cdot)$ si possono riformulare in termini dell'operazione $*$.
La biezione tra i sottogruppi di $(G\,,\,\cdot)$ e i sottoquasigruppi di $(G\,,\,*)$ segue immediatamente e a ogni sottogruppo fa corrispondere il quasigruppo a esso associato: ogni sottoquasigruppo H di $(G\,,\,*)$ è, in $(G\,,\,\cdot)$, un sottogruppo. Infatti, se $a, b \in H$, vale $a * b = a \cdot b^{-1} \in H$ (H è chiuso rispetto all'operazione di quasigruppo) e questa è condizione necessaria e sufficiente affinchè H sia un sottogruppo di $(G\,,\,\cdot)$.

Osservazione 1.9. Se G ha ordine finito, per quanto appena detto, l'ordine di ogni sottoquasigruppo di $(G\,,\,*)$ divide l'ordine di $(G\,,\,*)$, cosa questa non vera in generale per i sottoquasigruppi di ogni quasigruppo.

Esempio 1.16. Sia $(\mathbb{Z}\,,\,+)$ il gruppo abeliano additivo degli interi, il quasigruppo a esso associato è $(\mathbb{Z}\,,\,-)$, non associativo, non totalmente simmetrico e non commutativo.

Esempio 1.17. Sia $(\mathbb{Z}_n\,,\,+)$ il gruppo abeliano additivo delle classi di equivalenza degli interi modulo n, il quasigruppo a esso associato è $(\mathbb{Z}_n\,,\,-)$ ove $[\,a\,]_n - [\,b\,]_n := [\,a+n-b\,]_n$.

Esempio 1.18. Sia $(\mathbb{Q}\setminus\{0\}\,,\,\cdot)$ il gruppo abeliano moltiplicativo dei razionali, il quasigruppo a esso associato è $(\mathbb{Q}\setminus\{0\}\,,\,/)$, non associativo e non commutativo.

1.6 Quasigruppi, gruppi e curve cubiche piane

Strutture di quasigruppo totalmente simmetrico si incontrano, insieme a strutture di gruppo, nello studio della geometria delle curve cubiche piane. Le proprietà di tali quasigruppi si possono interpretare come risultati sulle cubiche mentre non è invece vero che ogni tale quasigruppo si possa interpretare come l'insieme dei punti di una cubica piana.
L'idea è questa: se $\mathcal{C}$ è una cubica piana proiettiva su un campo algebricamente chiuso, per esempio $\mathbb{C}$, ogni retta del piano la incontra in tre punti, contati con molteplicità; quindi se a e b sono punti di $\mathcal{C}$, la retta per a e b incontra $\mathcal{C}$ in un terzo punto c e questo permette di definire un'operazione binaria interna su $\mathcal{C}$ che denoteremo con $\bullet$, nel modo seguente: $a \bullet b = c$.
Con l'operazione $\bullet$ così definita, la totalità dei punti di $\mathcal{C}$ o un qualsiasi sottoinsieme di $\mathcal{C}$ finito o no, chiuso rispetto alla moltiplicazione, costituisce un quasigruppo totalmente simmetrico, in quanto è chiaro che se σ è una qualsiasi permutazione su $\{a, b, c\}$, risulta $\sigma(a) \bullet \sigma(b) = \sigma(c)$. Le strutture di gruppo associate a questo quasigruppo sono un argomento classico di geometria algebrica e di teoria dei numeri, trattato in molti testi. Qui rimandiamo a [4] e a [8].
Si osservi che la costruzione della legge di gruppo sulla cubica $\mathcal{C}$, ottenuta dal quasigruppo $(\mathcal{C}\,,\,\bullet)$ come verrà spiegato nei paragrafi seguenti, presenta analogie con il teorema 1.6 ma non è la stessa costruzione (si veda l'osservazione 1.10).

1.6.1 Alcuni richiami sul proiettivo

Richiamiamo ora brevemente quanto segue. Il *piano proiettivo complesso*, denotato $\mathbb{P}^2(\mathbb{C})$, è il quoziente di $\mathbb{C}^3\setminus\{\mathbf{0}\}$ con la relazione di equivalenza $\sim$, dove:

$$\forall\, \mathbf{v},\mathbf{w}\in\mathbb{C}^3\setminus\{\mathbf{0}\}\ ,\ \mathbf{v}\sim\mathbf{w}\ \Leftrightarrow\ \exists\, k\in\mathbb{C}\setminus\{0\}\ :\ \mathbf{v}=k\mathbf{w}.$$

La classe di equivalenza $[(x_0,x_1,x_2)]$ del vettore $(x_0,x_1,x_2)\in\mathbb{C}^3\setminus\{\mathbf{0}\}$ si scriverà qui $[x_0,x_1,x_2]$; x_0,x_1,x_2 sono dette *coordinate omogenee* su $\mathbb{P}^2(\mathbb{C})$ e sono quindi definite a meno di un fattore di proporzionalità; una classe $[a_0,a_1,a_2]$ è un punto di $\mathbb{P}^2(\mathbb{C})$.
Il piano proiettivo $\mathbb{P}^2(\mathbb{C})$ si può identificare con l'unione del piano affine $\mathbb{A}^2$ e della *retta impropria*, infatti si ha:

$$\mathbb{P}^2(\mathbb{C})=\{\,[1,a,b]\mid a,b\in\mathbb{C}\,\}\cup\{\,[0,a,b]\mid a,b\in\mathbb{C}\,\}$$

e vi è una identificazione naturale tra i punti del tipo $[1,a,b]$ di $\mathbb{P}^2(\mathbb{C})$ e i punti $(a,b)\in\mathbb{A}^2$: tale biezione è data dal passaggio da coordinate proiettive a coordinate affini (qui $x_0\neq 0$):

$$x=\frac{x_1}{x_0}\qquad\qquad y=\frac{x_2}{x_0}\tag{1.19}$$

Il punto $[0,a,b]$ è invece un punto improprio, cioè la direzione della retta $r\ :\ bx-ay=0$ in $\mathbb{A}^2$ e di tutte le sue parallele. La retta affine generica parallela a r è $bx-ay+c=0$, la cui chiusura proiettiva è la retta proiettiva: $bx_1-ax_2+cx_0=0$. Sostituendo qui $[x_0,x_1,x_2]=[0,a,b]$ si ottiene $ba-ab+0c=0$, cioè $[0,a,b]$ è l'unico punto che abbiamo aggiunto alla retta affine $bx-ay+c=0$ per ottenere la retta proiettiva $bx_1-ax_2+cx_0=0$.

Una *(curva) cubica* $\mathcal{C}$ in $\mathbb{P}^2(\mathbb{C})$ è il luogo degli zeri un polinomio omogeneo di terzo grado in x_0, x_1, x_2 a coefficienti complessi, cioè l'insieme dei punti $[x_0,x_1,x_2]$ di $\mathbb{P}^2(\mathbb{C})$ che soddisfano un'equazione del tipo:

$$A\,{x_0}^3+B\,{x_1}^3+C\,{x_2}^3+D\,{x_0}^2x_1+E\,{x_0}^2x_2+F\,{x_1}^2x_2+G\,x_0\,{x_1}^2+H\,x_0\,{x_2}^2+I\,x_1\,{x_2}^2+L\,x_0\,x_1\,x_2=0.$$

Se ci mettiamo nella carta affine

$$U_0:=\left\{\,[x_0,x_1,x_2]\in\mathbb{P}^2(\mathbb{C})\mid x_0\neq 0\,\right\}$$

possiamo dividere per ${x_0}^3$ ottenendo:

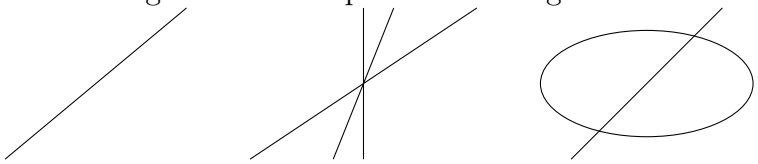
$$A+B\left(\frac{x_1}{x_0}\right)^3+C\left(\frac{x_2}{x_0}\right)^3+D\,\frac{x_1}{x_0}+E\,\frac{x_2}{x_0}+F\,\frac{{x_1}^2x_2}{{x_0}^3}+G\left(\frac{x_1}{x_0}\right)^2+H\left(\frac{x_2}{x_0}\right)^2+I\,\frac{x_1{x_2}^2}{{x_0}^3}+L\,\frac{x_1\,x_2}{{x_0}^2}=0$$

e, sostituendo le coordinate affini (1.19) e riordinando:

$$B\,x^3 + C\,y^3 + F\,x^2y + I\,x\,y^2 + G\,x^2 + H\,y^2 + L\,x\,y + D\,x + E\,y + A = 0.$$

In casi molto speciali, ad esempio partendo da un'equazione omogenea quale ${x_0}^3 = 0$ oppure ${x_0}^2x_1 + {x_0}^3 = 0$, il polinomio a primo membro può diventare il polinomio nullo o abbassarsi di grado, ma in generale sarà un polinomio non omogeneo di grado 3 che definisce una curva cubica affine.
Sia $\mathcal{C}$ una curva cubica in $\mathbb{P}^2(\mathbb{C})$, diremo che $\mathcal{C}$ è *liscia* se ha esattamente una tangente in ogni punto. Non è difficile dimostrare che le cubiche non liscie sono le cubiche degeneri (unione di tre rette contate con molteplicità oppure unione di una conica liscia e di una retta) e le cubiche irriducibili con un punto doppio, che può essere una cuspide o un nodo.

Figura 1.1: esempi di cubica degenere.



Sia ora $\mathcal{C}$ una cubica liscia di $\mathbb{P}^2(\mathbb{C})$; se r è una retta proiettiva, l'intersezione di $\mathcal{C}$ con r è costituita da tre punti, contati con molteplicità. Infatti se $\mathcal{C}$ ha equazione $F(x_0, x_1, x_2) = 0$, ed r ha equazioni parametriche:

$$x_0 = a_0s + b_0t \qquad x_1 = a_1s + b_1t \qquad x_2 = a_2s + b_2t,$$

l'equazione risolvente è:

$$F(a_0s + b_0t, a_1s + b_1t, a_2s + b_2t) = 0$$

che risulta essere un'equazione omogenea di terzo grado in due incognite. Considerando a parte le eventuali soluzioni con $t = 0$, e risolvendo poi in $\frac{s}{t}$, si vede subito che così come un'equazione di terzo grado in un'incognita su $\mathbb{C}$ ha tre soluzioni contate con molteplicità, questa ha, identificando soluzioni proporzionali tra loro, tre soluzioni contate con molteplicità, che a loro volta danno tre punti di $\mathbb{P}^2(\mathbb{C})$ contati con molteplicità.
Vi sono dunque tre casi: tre intersezioni distinte, due coincidenti in un punto a (tangenza di r a $\mathcal{C}$ in a), tre coincidenti in un punto a (in questo caso a è un punto di flesso ed r è la *tangente inflessionale* in a).

1.6.2 Legge di gruppo su una cubica

Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ una curva cubica liscia. Per ogni $a, b \in \mathcal{C}$, sia $a \bullet b$ la terza intersezione della retta r per a e b con $\mathcal{C}$; se $a = b$, come retta r prendiamo la tangente a $\mathcal{C}$ in a. Abbiamo così definito, grazie al fatto che $\mathcal{C}$ è liscia e quindi la tangente è unica in ogni punto, un'operazione binaria interna sui punti di $\mathcal{C}$:

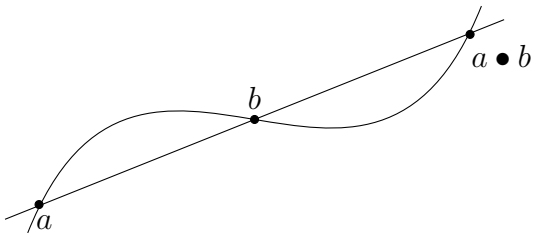
$$\begin{aligned} \mathcal{C} \times \mathcal{C} &\to \mathcal{C} \\ (a, b) &\mapsto a \bullet b \end{aligned}$$

Si avrà:

- $a \bullet b = a$ quando la retta r è tangente in a a $\mathcal{C}$,
- $a \bullet b = b$ quando la retta r è tangente in b a $\mathcal{C}$,
- $a = b = a \bullet b$ quando a è un punto di flesso ed r è quindi la tangente inflessionale in a.

Quindi $(\mathcal{C}, \bullet)$ è un quasigruppo totalmente simmetrico; questo dipende dal fatto che la proprietà che tre punti di $\mathcal{C}$ siano le tre intersezioni di $\mathcal{C}$ con una retta non dipende dall'ordine con cui si considerano i punti.

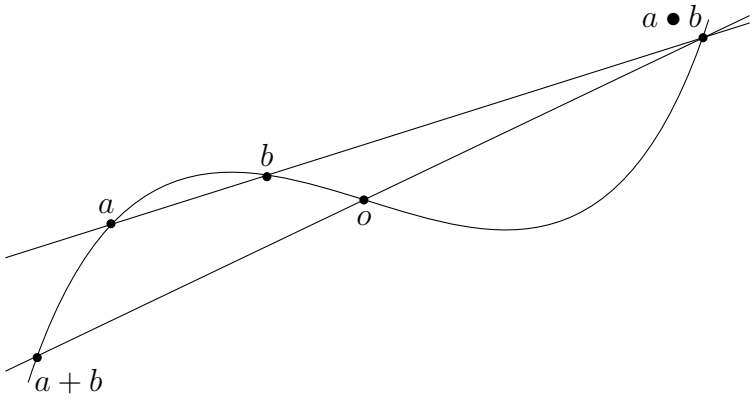
Figura 1.2: totale simmetria di $\bullet$.



È possibile definire una nuova operazione su $\mathcal{C}$ utilizzando $\bullet$: precisamente, fissiamo un punto o qualsiasi di $\mathcal{C}$; per ogni $a, b \in \mathcal{C}$ si definisce la somma:

$$a + b := (a \bullet b) \bullet o$$

Figura 1.3: operazione + di gruppo.

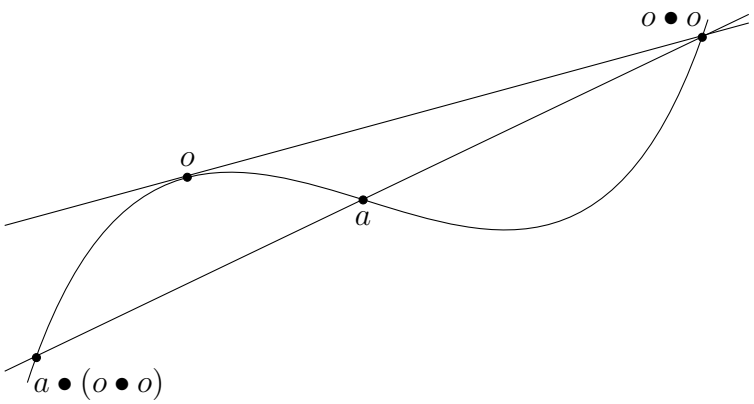


Teorema 1.7. *La coppia* $(\mathcal{C}, +)$ *è un gruppo abeliano con elemento neutro* o*.*

Dimostrazione. La dimostrazione della proprietà associativa non è immediata e rimandiamo, per questa parte, a [8, pp. 11 segg.].
L'operazione + è ben definita perché lo è $\bullet$, inoltre è commutativa essendo $\bullet$ totalmente simmetrica.
Il punto o è elemento neutro: $a + o = (a \bullet o) \bullet o = a$ ed esiste l'opposto $-a = a \bullet (o \bullet o)$, infatti $-a + a = ((a \bullet (o \bullet o)) \bullet a) \bullet o = o$. □

Osservazione 1.10. La costruzione ora vista non è la stessa data dal teorema 1.6. Infatti il quasigruppo $(\mathcal{C}, \bullet)$, formato dai punti di una cubica con l'operazione $\bullet$ della terza intersezione, non verifica le proprietà richieste nel teorema 1.6, ad esempio la 1 del teorema 1.6 sarebbe nel nostro caso l'affermazione che la tangente in un qualsiasi punto $a \in \mathcal{C}$ passa per o, e viceversa che se la retta per due punti $a, b \in \mathcal{C}$ passa per o allora è la tangente in a, entrambe chiaramente false.
D'altra parte, anche l'operazione di gruppo è definita a partire dall'operazione di quasigruppo in modo diverso.

Figura 1.4: elemento neutro o di $+$.



In [8] si da la seguente definizione:

> Un quasigruppo totalmente simmetrico $(E\,,\,\bullet)$ è detto *abeliano* se per ogni $u \in E$ la legge di composizione
>
> $$xy = (x \bullet y) \bullet u$$
>
> lo rende un gruppo abeliano.

Dunque, una cubica piana proiettiva lisica $\mathcal{C}$ è, con l'operazione $\bullet$ sopra definita, un quasigruppo abeliano.

1.6.3 Legge di gruppo in un caso particolare

Sia $\mathcal{C}$ la curva $y^2 = x(x-1)(x-\lambda)$ in coordinate affini, con $\lambda \in \mathbb{C}\setminus\{0,1\}$ fissato. Il punto rappresentato da $(0,0,1)$ in coordinate proiettive è per tale curva un flesso con tangente inflessionale di equazione $x_0 = 0$. L'equazione di $\mathcal{C}$ si può scrivere $y^2 = x^3-(\lambda+1)x^2+\lambda x$, cioè

$$y^2 = x^3 + \mu x^2 + \lambda x,$$

avendo sostituito $\mu = -(\lambda + 1)$.
Scegliamo $o = (0, 0, 1)$ e usiamo coordinate affini per descrivere la legge di gruppo su $\overline{\mathcal{C}} = \mathcal{C} \cup \{o\}$. Sia $p = (p_0, p_1)$, allora la retta per o e per p ha equazione $x = p_0$. Le intersezioni della retta op con $\mathcal{C}$ sono le coppie (x, y) che sono soluzioni del sistema:

$$\begin{cases} x = p_0 \\ y^2 = {p_0}^3 + \mu\, {p_0}^2 + \lambda\, p_0 \end{cases}$$

ma, poiché una delle due radici ha ordinata p_1, l'altra ha ordinata $-p_1$:

$$\begin{cases} x = p_0 \\ y = \pm p_1 \end{cases}$$

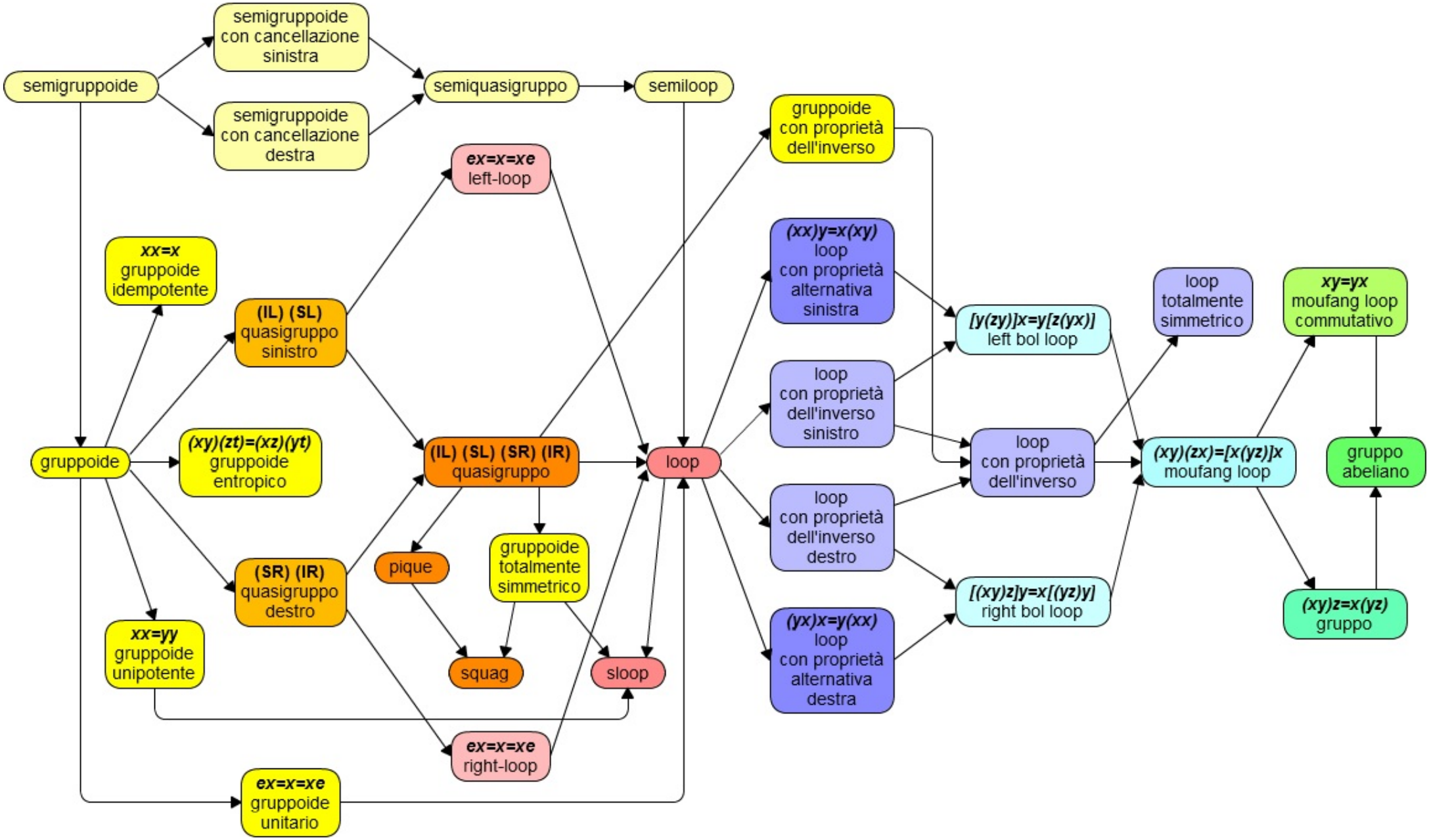
quindi $p \bullet o$ è il simmetrico di p rispetto all'asse x. Poiché o è un flesso per $\mathcal{C}$, $o \bullet o = o$ quindi $a = a \bullet (o \bullet o) = a \bullet o$, simmetrico di a rispetto all'asse x. In particolare:

$$a + b = (a \bullet b) \bullet o = -a \bullet b,$$

cioè $a + b + a \bullet b = 0$. Abbiamo provato il seguente:

Teorema 1.8. *Se $\mathcal{C}$ è la curva cubica liscia $y^2 = x(x-1)(x-\lambda)$, esiste una unica legge di gruppo su $\mathcal{C}$ tale che il punto improprio $o = (0, 0, 1)$ sia l'elemento neutro; l'opposto è dato da $-(p_0, p_1) = (p_0, -p_1)$ e, per ogni $a, b, c \in \mathcal{C}$, vale $a + b + c = 0$ se e solo se a, b e c giacciono sulla stessa retta.*

Dimostrazione. L'operazione $a + b$ di gruppo esiste per quanto visto sopra; essa è unica perché $a + b := -c$, dove $c = a \bullet b$. □


semigruppoide
semigruppoide con cancellazione sinistra
semigruppoide con cancellazione destra
semiquasigruppo
semiloop
ex=x=xe left-loop
xx=x gruppoide idempotente
(IL) (SL) quasigruppo sinistro
gruppoide
(xy)(zt)=(xz)(yt) gruppoide entropico
(IL) (SL) (SR) (IR) quasigruppo
loop
(SR) (IR) quasigruppo destro
pique
gruppoide totalmente simmetrico
xx=yy gruppoide unipotente
squag
sloop
ex=x=xe right-loop
ex=x=xe gruppoide unitario
gruppoide con proprietà dell'inverso
(xx)y=x(xy) loop con proprietà alternativa sinistra
loop con proprietà dell'inverso sinistro
loop con proprietà dell'inverso destro
(yx)x=y(xx) loop con proprietà alternativa destra
[y(zy)]x=y[z(yx)] left bol loop
loop con proprietà dell'inverso
[(xy)z]y=x[(yz)y] right bol loop
loop totalmente simmetrico
(xy)(zx)=[x(yz)]x moufang loop
xy=yx moufang loop commutativo
gruppo abeliano
(xy)z=x(yz) gruppo

Capitolo 2

Loops

2.1 Elemento neutro

Definizione 2.1. Sia $(G\,,\,\cdot)$ un gruppoide. L'elemento e di G è un *elemento neutro sinistro* di $(G\,,\,\cdot)$ se $e\cdot x = x$ per ogni $x \in G$. Analogamente, $f \in G$ è un *elemento neutro destro* di $(G\,,\,\cdot)$ se $x \cdot f = x$ per ogni $x \in G$.

Osservazione 2.1. Un elemento e di un gruppoide G è un elemento neutro sinistro (destro) se e solo se la traslazione sinistra L_e (destra R_e) è l'identità su G.

Definizione 2.2. Si dice che $e \in G$ è un *elemento neutro* del gruppoide $(G\,,\,\cdot)$ se:

$$e \cdot x = x = x \cdot e \quad \forall\, x \in G.$$

Un elemento neutro di un gruppoide $(G\,,\,\cdot)$ si può pensare anche come operazione nullaria su G, per questo motivo un gruppoide con elemento neutro e viene indicato da certi autori con notazioni quali ad esempio $(G\,,\,\cdot\,,\,e)$. Inoltre l'elemento neutro è spesso denotato con 0 o 1 in notazione additiva e moltiplicativa rispettivamente.

Osservazione 2.2. Un gruppoide può avere più di un elemento neutro sinistro (destro).

Esempio 2.1. Nel gruppoide $(G\,,\,\cdot)$ sotto, 1 e 2 sono elementi neutri sinistri mentre tutti gli elementi di H sono elementi neutri destri in $(H\,,\,\bullet)$ (risulta: $x \bullet y = x\ \forall\, x, y \in H$).

G :

$\cdot$	1	2	3
1	1	2	3
2	1	2	3
3	3	3	3

H :

$\bullet$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

Osservazione 2.3. Sia $(H\,,\,\bullet)$ un gruppoide come nell'esempio 2.1: poiché ogni elemento di H è neutro destro, esso è un quasigruppo destro. Infatti per ogni $(a,b) \in H \times H$ esiste ed è unico $x \in H$ tale che $x \bullet a = b$, e precisamente $x = b$. L'implicazione non si può però invertire, come mostra la tavola di moltiplicazione per $(H\,,\,\circ)$:

H :

$\circ$	a	b	c
a	b	a	a
b	a	b	b
c	c	c	c

Si è definito elemento neutro di un gruppoide G un $e \in G$ che sia contemporaneamente elemento neutro sinistro e destro e si è visto che uno stesso gruppoide può avere più di un elemento neutro sinistro oppure destro. Ma se e ed f sono rispettivamente un elemento neutro sinistro e destro di un gruppoide $(G\,,\,\cdot)$, si ha $f = e \cdot f = e$. Dunque un gruppoide può avere al massimo un elemento neutro. Di più, se un gruppoide G ha (unico) elemento neutro e, non può esistere $f \in G$, $f \neq e$, che sia anche soltanto elemento neutro destro oppure sinistro.

Se G è un gruppoide di ordine n finito e con elemento neutro e, gli elementi di G si possono ordinare come $a_1, \ldots, a_n$ in modo tale che sia $a_j = e$. Allora nella j-esima riga e nella j-esima colonna della tavola di moltiplicazione appaiono gli elementi di G nello stesso ordine $a_1, \ldots, a_n$.
Un gruppoide con elemento neutro si dice anche *gruppoide unitario*.

Definizione 2.3. Si dice *semiloop*[1] un semiquasigruppo con elemento neutro.

Definizione 2.4. Si dice *left-loop* (*right-loop*) un quasigruppo sinistro (destro) con elemento neutro.

Definizione 2.5. Si dice *loop* o *cappio* un quasigruppo con elemento neutro.

Per la definizione 2.2 di elemento neutro, un loop L è un quasigruppo ove vale l'identità:

$$x \backslash x = y / y \quad \forall\, x, y \in L$$

dunque un loop (semiloop) $(G\,,\,\cdot)$ è un quasigruppo (semiquasigruppo) ove esiste un $e \in G$ tale che:

$$x \cdot e = e \cdot x = x \qquad x \backslash x = x / x = e \qquad e \backslash x = x / e = x \tag{2.1}$$

[1] *Halfloop* in [2].

per ogni $x \in G$. Qui e è elemento neutro in $(G\,,\,\cdot)$, elemento neutro sinistro in $(G\,,\,\backslash)$, destro in $(G\,,\,/)$.

Osservazione 2.4. In un quasigruppo G con elemento neutro e la $xy = e$ ha un'unica soluzione sia in x che in y; ciò significa che in un loop G con elemento neutro e esistono, unici per ogni x e in generale distinti, x_l e x_r tali che $x_l\, x = e = x\, x_r$.

Osservazione 2.5. Poiché le (1.6), (1.7) e (1.8) insieme con la proprietà associativa implicano l'esistenza di un $e \in G$ che verifichi la (2.1), si ha che 'quasigruppo associativo' è sinonimo di 'gruppo' così come 'loop associativo', [3, p. 63].

Definizione 2.6. Sia $(L\,,\,\cdot)$ un loop, K si dice *sottoloop* di L se $K \subseteq L$ e se $(K\,,\,\cdot)$ è esso stesso un loop.

Osservazione 2.6. Per le proprietà di cancellazione (1.1) e (1.2), un sottoloop (sotto-semiloop) di un loop (semiloop) L ha lo stesso elemento neutro di L.

In certi contesti può essere utile la seguente generalizzazione di loop.

Definizione 2.7. Si chiama *pique*[2] un quasigruppo con un elemento idempotente.

Dunque ogni quasigruppo idempotente è banalmente un pique ma anche ogni loop è un pique: se un gruppoide ha elemento neutro, esso è certamente idempotente.

Definizione 2.8 (loop unipotente)**.** Un elemento x di un loop $(L\,,\,\cdot)$ si dice *unipotente* se $x \cdot x = e$; un loop si dice *unipotente* se ogni suo elemento è unipotente[3].

Esempio 2.2. Il gruppoide $(L\,,\,\circ)$ sotto è un loop di ordine 6, con elemento neutro e, evidentemente unipotente e non commutativo. Esso non è un gruppo: $(1\circ 2)\circ 3 \neq 1\circ(2\circ 3)$.

L :

$\circ$	e	1	2	3	4	5
e	e	1	2	3	4	5
1	1	e	3	5	2	4
2	2	5	e	4	1	3
3	3	4	1	e	5	2
4	4	3	5	2	e	1
5	5	2	4	1	3	e

[2] *Pointed idempotent quasigroup.*

[3] Si confronti questa con la definizione 1.10.

L'elemento neutro di un loop è banalmente unipotente, mentre un elemento unipotente di G distinto da e ha quadrato e.

2.1.1 Alcune proposizioni

Una caratterizzazione dei loops tra i quasigruppi è la seguente. L'operazione del quasigruppo Q verrà qui denotata con la giustapposizione.

Proposizione 2.1. *Un quasigruppo Q è un loop se e solo se verifica l'identità*[4]*:*

$$[\, x\,(y/y)\,]\, z = x\,[\,(y/y)\, z\,] \tag{2.2}$$

Dimostrazione. Se Q è un loop con elemento neutro e allora, per la (2.1), $y/y = e$ per ogni $y \in Q$ e la (2.2) segue.
Al contrario, se nel quasigruppo Q vale la (2.2), ponendo $z = y$ si ottiene $[\, x\,(y/y)\,]\, y = xy$ dalla (SR), dunque $x\,(y/y) = x$. Dividendo a sinistra per x si ha $y/y = x\backslash x$. □

Un quasigruppo idempotente $(Q\,,\,\cdot)$ con almeno due elementi non può essere un loop. Infatti si ha $x \cdot x = x$ e $y \cdot y = y$ per ogni $x, y \in Q$, per cui se $x \neq y$ è $x\backslash x \neq y/y$. Però è possibile immergerlo in in loop unipotente aggiungendo un elemento, che sarà l'elemento neutro:

Proposizione 2.2. *Dato un quasigruppo idempotente $(Q\,,\,\cdot)$, la:*

$$x \bullet y = \begin{cases} e & ,\quad y = x \\ x \cdot y & ,\quad y \neq x \end{cases} \tag{2.3}$$

insieme con l'identità di elemento neutro $e \bullet x = x = x \bullet e$, definisce una struttura di loop $(Q'\,,\,\bullet)$, unipotente, sull'unione disgiunta Q' di Q ed $\{e\}$.

Dimostrazione. Poiché $(Q\,,\,\cdot)$ è un quasigruppo, ogni elemento di Q appare esattamente una volta in ogni riga ed esattamente una volta in ogni colonna nella tavola di moltiplicazione. Inoltre, per idempotenza, l'elemento x di Q appare, nella riga etichettata da x, esattamente nella colonna x, cioè sulla diagonale.
Si consideri ora la nuova tavola di moltiplicazione ottenuta dalla precedente aggiungendo, come prima riga, una riga etichettata da e e, come prima colonna, una colonna etichettata da e. Come da (2.3) si sostituiscano gli elementi di Q, ordinatamente sulla diagonale,

[4] *Slightly associative identity* in [17, Proposizione 1.3].

con e (questo conferisce l'unipotenza alla nuova struttura) e si scrivano tali elementi sia nelle caselle di posto 1 all'interno della stessa riga che in quelle di posto 1 all'interno della stessa colonna della nuova tavola di moltiplicazione, cioè nella colonna e nella riga etichettate da e (da cui e elemento neutro). Lasciando invariata la posizione degli altri elementi si ottiene una tavola per Q' come da tesi: in questo modo infatti Q' è ancora un quasigruppo. □

Sia $e = 0$. Un esempio di tavole per tali Q e Q' è mostrato nella tabella 2.1 seguente.

Tabella 2.1: quasigruppo idempotente $(Q\,,\,\cdot)$ e loop unipotente $(Q'\,,\,\bullet)$ come in proposizione 2.2.

Q :

$\cdot$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Q' :

$\bullet$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

Proposizione 2.3. *Un loop $(L\,,\,\cdot)$ totalmente simmetrico è unipotente.*

Dimostrazione. Sia e l'elemento neutro di L, dalla $e \cdot x = x$ si ottiene subito $x \cdot x = e$. □

Esempio 2.3 (Steiner loop)**.** Sia $(Q\,,\,\circ)$ un quasigruppo di Steiner, cioè un quasigruppo idempotente e totalmente simmetrico. Con il procedimento illustrato dalla proposizione 2.2 si può associare a $(Q\,,\,\circ)$ un loop $(Q'\,,\,\bullet)$, unipotente e totalmente simmetrico. Un tale loop si dice *Steiner loop* o *sloop*. Per la proposizione 2.3, 'loop totalmente simmetrico' e 'Steiner loop' indicano la stessa struttura.

2.2 Proprietà dell'inverso

In strutture associative, il concetto di elemento inverso è dato normalmente legandolo all'esistenza di un elemento neutro. In un gruppoide qualsiasi la proprietà dell'inverso si può definire in assenza di elemento neutro.

Definizione 2.9. Un quasigruppo G verifica la *proprietà dell'inverso sinistro* se:

$$\forall\, x \in G \quad \exists\, z \in G \,:\, z\,(xy) = y \;\forall\, y \in G \tag{2.4}$$

e verifica la *proprietà dell'inverso destro* se:

$$\forall\, x \in G \quad \exists\, t \in G \,:\, (yx)\,t = y \;\forall\, y \in G \tag{2.5}$$

Si dice che un loop, o un quasigruppo qualsiasi, verifica la *proprietà dell'inverso* se verifica entrambe le (2.4) e (2.5).

Se esiste z come in (2.4), tale z è unico (perché, fissati x e y, esiste unico z tale che $z(xy) = y$) e qunidi lo denoteremo con x_l^{-1}. Analogamente se esiste t come in (2.5) verrà denotato con x_r^{-1}.

Definizione 2.10. Sia G un loop con elemento neutro e. Per ogni $a \in G$ esiste ed è unico $\widetilde{a}$ tale che $a\widetilde{a} = e$ ed esiste ed è unico a' tale che $a'a = e$, perché un loop è un quasigruppo e quindi ogni equazione lineare ha una e una sola soluzione. Chiamiamo a' *inverso sinistro* e $\widetilde{a}$ *inverso destro* di a e li denotiamo rispettivamente a_l e a_r.

Si osserva che la sola esistenza di tali inversi (in assenza di proprietà associativa) non implica la validità delle (2.4) e (2.5). Dunque non tutti i loop hanno la proprietà dell'inverso. In un loop G vale sempre la:

$$\forall\, y \in G \quad (y_l)_r = y = (y_r)_l.$$

Esempio 2.4. Si consideri il loop $(L\,,\,\cdot)$ come nella tabella 2.2 alla pagina seguente: ha elemento neutro 1 ed è unipotente, dunque ogni elemento di L coincide col proprio inverso sinistro e destro. Infatti l'unico x che verifica $x \cdot (3 \cdot 4) = 4$ è $x = 2$, mentre l'unico y che verifica $y \cdot (3 \cdot 5) = 5$ è $y = 4$, cioè non vale la (2.4). Infine non è totalmente simmetrico, non essendo commutativo.

Teorema 2.1. *Sia G un quasigruppo che verifica la proprietà dell'inverso, siano $J_l : G \to G$, $J_l(x) = x_l^{-1}$ e $J_r : G \to G$, $J_r(x) = x_r^{-1}$, con x_l^{-1} e x_r^{-1} come in (2.4) e (2.5) rispettivamente. Allora:*

$$(J_l)^2 = \mathrm{Id}_G = (J_r)^2 \tag{2.6}$$

Tabella 2.2: esempio 2.4.

L :

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

Dimostrazione. Se nella $x_l^{-1}(xy) = y$ si sostituiscono x con x_l^{-1} e y con xy, si ottiene $(x_l^{-1})_l^{-1}[\, x_l^{-1}(xy)\,] = xy$. Ma poiché $x_l^{-1}(xy) = y$, vale $(x_l^{-1})_l^{-1} y = xy$, da cui $(x_l^{-1})_l^{-1} = x$, cioè $(J_l)^2 = \mathrm{Id}_G$.
Allo stesso modo si ottiene $(J_r)^2 = \mathrm{Id}_G$ dalla $(yx)\, x_r^{-1} = y$. □

Osservazione 2.7. Un quasigruppo idempotente e totalmente simmetrico è un gruppoide che verifica (2.4) e (2.5) senza essere un loop.

In un gruppo valgono le proprietà dell'inverso (2.4) e (2.5) in virtù della proprietà associativa.

Osservazione 2.8. In un loop con la proprietà dell'inverso sinistro, ponendo $y = e$ nella (2.4), si ha $x_l^{-1}\, x = e$ da cui, come già osservato, x_l^{-1} è univocamente determinato per ogni x e coincide con l'inverso sinistro di x cioè, nella notazione della definizione 2.9, $x_l^{-1} = x_l$. Sempre dalla $x_l^{-1}\,(xy) = y$, con $y = x_l^{-1}$ si ha $x_l^{-1}\,(x x_l^{-1}) = x_l^{-1}$, cioè $x x_l^{-1} = e$ cioè x_l^{-1} coincide con l'inverso destro di x: $x_l^{-1} = x_r$. Dunque, in un tale loop:

$$x x_l^{-1} = e = x_l^{-1}\, x \qquad , \qquad (x_l^{-1})_l^{-1} = x \qquad , \qquad x_l^{-1} = x_l = x_r \tag{2.7}$$

Analogamente, in un loop con la proprietà dell'inverso destro (2.5) si ottengono:

$$x x_r^{-1} = e = x_r^{-1}\, x \qquad , \qquad (x_r^{-1})_r^{-1} = x \qquad , \qquad x_r^{-1} = x_l = x_r \tag{2.8}$$

In un quasigruppo con la proprietà dell'inverso, sia $xy = z$. Dalla (2.4) si ottiene $x_l^{-1} z = y$. Applicando poi la (2.5) si ottiene $y z_r^{-1} = x_l^{-1}$. Infine, applicando nuovamente la (2.4), si ha:

$$y_l^{-1} x_l^{-1} = z_r^{-1}.$$

In un loop con la proprietà dell'inverso la situazione si semplifica: le (2.4) e (2.5) e la (2.7) o la (2.8) permettono di usare la notazione x^{-1} per $x_l^{-1} = x_r^{-1} = x_l = x_r$. Possiamo quindi dare la seguente:

Definizione 2.11. Sia L un loop con la proprietà dell'inverso; per ogni $x \in L$ poniamo $x^{-1} := x_l^{-1}$ dove $x_l^{-1} = x_r^{-1} = x_l = x_r$.

In un loop con la proprietà dell'inverso possiamo perciò scrivere:

$$(xy)^{-1} = y^{-1}x^{-1} \tag{2.9}$$

Quest'ultima non va confusa con la[5]:

$$(xy)^{-1} = x^{-1}y^{-1} \tag{2.10}$$

più restrittiva della (2.9) ma più debole della proprietà commutativa.

Teorema 2.2. *Un quasigruppo Q è totalmente simmetrico se e solo se è commutativo e vale la proprietà dell'inverso sinistro* (2.4) *con $x = x_l^{-1}$ per ogni $x \in Q$.*

Dimostrazione. Se un quasigruppo è totalmente simmetrico, allora esso è commutativo come evidenziato nell'osservazione 1.1. Inoltre permutando tra loro x, y e xy nella $xy = xy$ si ottiene $x\,(xy) = y$.
Valgano invece le $xy = yx$ e $x(xy) = y$ per ogni $x, y \in Q$. Dalla $xy = z$ si ottiene, per la prima ipotesi, $yx = z$. Inoltre si ha $x(xy) = xz$ da cui, per la seconda ipotesi, $y = xz$. In modo analogo si ricavano le identità corrispondenti alle rimanenti tre permutazioni di x, y, z. □

Definizione 2.12. Si dice *omotopia* da un gruppoide $(G\,,\,\cdot)$ ad un gruppoide $(H\,,\,\circ)$ una terna ordinata (f, g, h) di applicazioni da G in H tali che $a \cdot b = c$ in G implichi $f(a) \circ g(b) = h(c)$ in H.
Un omotopia con f, g, h biezioni si dice *isotopia* e un'isotopia di $(G\,,\,\cdot)$ in sé si dice *autotopia*.
Se esiste un'isotopia tra G e G', chiamiamo G e G' *isotopi*.

[5] *Automorphic inverse property.*

L'isotopia è una relazione di equivalenza su qualsiasi classe non vuota di gruppoidi. Una tale classe si dice *chiusa rispetto all'isotopia* se contiene tutti gli isotopi dei suoi elementi. Tra i gruppoidi, i quasigruppi sono chiusi rispetto isotopia, mentre questo non vale per i loops, [11, p. 59].

2.3 Loops di Bol-Moufang

Una delle classificazioni possibili per quasigruppi e loops distingue due categorie, loops (quasigruppi) di tipo Bol-Moufang, e non.

Definizione 2.13. Sia G un quasigruppo. Si chiama *identità di Bol-Moufang* un'identità tra gli elementi di G per cui valgono le seguenti proprietà:

1. sono coinvolti gli stessi tre elementi distinti,
2. i tre elementi compaiono nello stesso ordine,
3. uno solo dei tre elementi compare due volte.

Un *quasigruppo di Bol-Moufang* è un quasigruppo dove vale un'identità di Bol-Moufang.

Nelle sezioni che seguono vengono trattati due tipi di quasigruppi di Bol-Moufang: Moufang loops[6] e Bol loops[7].

2.3.1 Moufang loops

Definizione 2.14. Le seguenti tre identità:

$$(xy)(zx) = [\,x\,(yz)\,]\,x \qquad [\,(xy)\,z\,]\,y = x\,[\,y\,(zy)\,] \qquad x\,[\,y\,(xz)\,] = [\,(xy)\,x\,]\,z \tag{2.11}$$

si dicono *identità di Moufang*[8]. Un loop che verifica una qualsiasi delle (2.11) si dice *Moufang loop*; vedremo infatti tra breve che le (2.11) sono a due a due equivalenti.

[6] Dal nome di Ruth Moufang (1905–1977) che per prima li ha introdotti nel 1935.
[7] Dal nome di Gerrit Bol (1906–1989).
[8] Rispettivamente *middle Moufang* o *Bruck-Moufang identity*, *right moufang identity*, *left Moufang identity*.

Dalla caratterizzazione delle identità di Bol-Moufang segue subito che i Moufang loops sono di Bol-Moufang.
Il più piccolo Moufang loop non associativo ha ordine 12 ed è unico a meno di isomorfismi[9].

Osservazione 2.9. A titolo di esempio, la terza delle (2.11) si può esprimere in termini di traslazione sinistra come: $L_x L_y L_x = L_{(xy)\,x}$. Oppure, equivalentemente ma con entrambe le traslazioni: $L_x R_{xz} = R_z R_x L_x$. Si noti che per la composizione di applicazioni vale la proprietà associativa, cosicchè $L_x L_y L_z$ ha un unico significato possibile.

Definizione 2.15. Sia G un gruppoide. Le identità tra elementi di G:

$$(xx)\,y = x\,(xy) \qquad (xy)\,x = x\,(yx) \qquad (yx)\,x = y\,(xx) \tag{2.12}$$

si dicono *proprietà alternative*, rispettivamente *proprietà alternativa sinistra*, *proprietà alternativa mediale*[10] e *proprietà alternativa destra*.

Definizione 2.16. Un elemento u di un loop G con la proprietà dell'inverso si dice essere un *elemento di Moufang* di G se la prima delle (2.11): $(uy)(zu) = [\,u\,(yz)\,]\,u$ vale per ogni $y, z \in G$.

Lemma 2.1. *Se un loop G verifica una delle* (2.11)*, allora le verifica tutte, verifica inoltre le tre proprietà alternative* (2.12) *e verifica le proprietà dell'inverso* (2.4) *e* (2.5)*.*

Dimostrazione. Una dimostrazione completa si trova in [2, p. 115–116]. Qui illustriamo solo alcune delle implicazioni necessarie a provare completamente il lemma.

Sia qui x^{-1} tale che $x^{-1}x = e$ e sia $J : G \to G$, $J(x) = x^{-1}$. La notazione x^{-1} è lecita in un Moufang loop G in quanto nella classe dei Bol loops (che vedremo nella prossima sezione 2.3.2 e che contiene propriamente la classe dei Moufang loops) vale $y_r = y_l$ per ogni $y \in G$, [13, Teorema 2.1]. Porremo $x^{-1} := x_l = x_r$. Quindi in un Moufang loop vale anche $(x^{-1})^{-1} = x$.

Se vale la prima delle (2.11), ponendo in questa $x = y^{-1}$ si ottiene $zy^{-1} = [\,y^{-1}(yz)\,]\,y^{-1}$, da cui $z = y^{-1}(yz)$, equivalente alla proprietà dell'inverso sinistro (2.4).

[9] La tavola di Cayley si trova su `http://www.uwyo.edu/moorhouse/pub/bol/htmlfiles12/12_9_1_1.html` al 19 settembre 2012.
[10] *Medial alternative* o *flexible* identity.

Dalla prima delle (2.11) con $y = e$, si ottiene subito $x(zx) = (xz)x$. Invece, con $z = x^{-1}$, si ottiene $xy = [\, x\,(yx^{-1})\,]\,x$ e $xy = x\,[\,(yx^{-1})\,x\,]$ per quanto appena trovato, da cui la proprietà dell'inverso destro (2.5) $y = (yx^{-1})\,x$. Quindi G verifica la proprietà dell'inverso.

Poiché $(L_x\,,\ R_x\,,\ R_xL_x)$ è un autotopia di G (infatti, se $yz = t$, la prima delle (2.11) dà $L_x(y)R_x(z) = R_xL_x(t)$), lo è anche $(JL_xJ\,,\ R_xL_x\,,\ R_x)$: omettiamo la dimostrazione di questo fatto, mostrato in [2, p. 116]. Inoltre si è appena visto che, se vale la prima delle (2.11), xzx è definito in modo non ambiguo. Allora, per ogni $x, y, z \in G$, risulta:

$$y[x(zx)] = y(xzx) = (JL_xJ(yx))(R_xL_x(z)) = R_x((yx)\,z) = [\,(yx)\,z\,]\,x.$$

Scambiando tra loro x e y si ottiene la seconda delle (2.11).

Se vale la seconda delle (2.11), ponendo in questa $z = y^{-1}$, si ha $[\,(xy)\,y^{-1}\,]\,y = xy$ da cui ancora, semplificando y, la proprietà dell'inverso destro.
Ponendo invece nella seconda delle (2.11) $x = y^{-1}$, si ha $zy = y^{-1}\,[\,y\,(zy)\,]$; sostituendo poi $z = ty^{-1}$ risulta $t = y^{-1}(yt)$, proprietà dell'inverso sinistro.

Si consideri ancora la seconda delle (2.11) $[\,(xy)\,z\,]\,y = x\,[\,y\,(zy)\,]$. Invertendo entrambi i membri si ha la $y^{-1}\,[\,z^{-1}\,(y^{-1}x^{-1})\,] = [\,(y^{-1}z^{-1})\,y^{-1}\,]\,x^{-1}$, equivalente alla terza delle (2.11). Invertendo ancora si ha l'implicazione inversa.

Dalla terza delle (2.11) con $y = e$ si ottiene immediatamente $(xx)z = x(xz)$ e, in modo analogo, le prime due (2.11) implicano le altre due (2.12). □

Proposizione 2.4. *Ciascuna delle* (2.11) *è equivalente alla:*

$$(xy)(zx) = x\,[\,(yz)\,x\,] \tag{2.13}$$

Dimostrazione. In virtù del lemma 2.1, ciascuna delle (2.11) è equivalente alle altre due e implica le tre proprietà alternative (2.12). Dunque sostituendo y con yz nella seconda delle (2.12) si può mutare la prima delle (2.11), valida per ipotesi, nella (2.13). □

Esempio 2.5. Sia $\mathbb{F}$ un campo, finito oppure no. Una *matrice di Zorn*[11] su $\mathbb{F}$ è una matrice quadrata di ordine 2:

$$A = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix}$$

[11] *Zorn vector matrix.*

dove α e β sono 'scalari' in $\mathbb{F}$, cioè $\alpha, \beta \in \mathbb{F}$, mentre $\mathbf{a}$ e $\mathbf{b}$ sono vettori di $\mathbb{F}^3$. La norma di tale matrice, *determinante di Zorn*, è definito come $\mathrm{N}(A) = \alpha\,\beta - \mathbf{a} \cdot \mathbf{b}$, dove $\cdot$ denota il prodotto scalare standard in $\mathbb{F}^3$. L'insieme di tali matrici costituisce uno spazio vettoriale di dimensione 8 sul campo $\mathbb{F}$, con somma e prodotto per scalare usuali.
Si consideri invece il prodotto:

$$\begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \times \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} = \begin{bmatrix} \alpha\,\gamma + \mathbf{a} \cdot \mathbf{d} & \alpha\mathbf{c} + \delta\mathbf{a} - \mathbf{b} \wedge \mathbf{d} \\ \gamma\mathbf{b} + \beta\mathbf{d} + \mathbf{a} \wedge \mathbf{c} & \beta\,\delta + \mathbf{b} \cdot \mathbf{c} \end{bmatrix}$$

dove $\wedge$ denota il prodotto vettoriale in $\mathbb{F}^3$. Con tale operazione, l'insieme delle matrici di Zorn con norma N unitaria costituisce un Moufang loop non commutativo e non associativo con elemento neutro:

$$e = \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{bmatrix}.$$

La dimostrazione di questo fatto si può trovare in [17, p. 15].

Osservazione 2.10. Un Moufang loop L è commutativo se e solo se vale l'identità (cfr. [11, p. 107]):

$$(xy)(zx) = x^2(yz).$$

È facile vedere che se un Moufang loop L è commutativo allora $(xy)(zx) = [\,x\,(yz)\,]\,x = [\,(yz)\,x\,]\,x$, che è $(yz)\,x^2$ per la terza delle (2.12).

Esempio 2.6 (Moufang loop commutativo di Zassenhaus[12])**.** Sia $L = {\mathbb{F}_3}^4$, spazio vettoriale di ordine 81 e dimensione 4 sul campo finito $\mathbb{F}_3$ e di elemento $x = (x_1\,,\,x_2\,,\,x_3\,,\,x_4)$, $x_i \in \mathbb{F}_3$, $1 \leq i \leq 4$. Si consideri su L l'operazione $\circ$ definita:

$$x \circ y := x + y + (0\,,\,0\,,\,0\,,\,(x_3 - y_3)(x_1y_2 - x_2y_1)).$$

Si osservi che $(x_3 - y_3)(x_1y_2 - x_2y_1)$ è funzione simmetrica di x e y: la coppia $(L\,,\,\circ)$ è il più piccolo Moufang loop commutativo che non è un gruppo, [18, p. 93].

Un ultimo risultato rilevante è il seguente (si confronti con le ultime righe della sezione 2.2).

Teorema 2.3. *La classe dei Moufang loops è chiusa rispetto isotopia.*

Per la dimostrazione si rimanda a [11, p. 102].

[12] Dal nome di Hans Julius Zassenhaus (1912–1991).

2.3.2 Bol loops

Si descrive ora una seconda classe di loops di Bol-Moufang che generalizza i Moufang loops.

Definizione 2.17. Le due identità:

$$[\,y\,(zy)\,]\,x = y\,[\,z\,(yx)\,] \qquad\qquad [\,(xy)\,z\,]\,y = x\,[\,(yz)\,y\,] \tag{2.14}$$

si dicono rispettivamente *identità di Bol sinistra* e *identità di Bol destra*. Un loop che verifica la prima delle (2.14) si dice *Bol loop sinistro* mentre uno che verifica la seconda si dice *Bol loop destro*.

Molti autori parlano in generale di Bol loops, data la dualità tra Bol loops sinistri e destri: siano $(G\,,\,\circ)$ e $(G\,,\,\bullet)$ due gruppoidi e siano le due operazioni come in (1.11) nel capitolo 1, cioè $a \bullet b = b \circ a$. Allora $(G\,,\,\circ)$ è un Bol loop sinistro se e solo se $(G\,,\,\bullet)$ è un Bol loop destro.

Proposizione 2.5. *Un Bol loop sinistro (rispettivamente destro) verifica la proprietà dell'inverso sinistro* (2.4) *(rispettivamente destro* (2.5)*) e l'alternativa sinistra (rispettivamente destra).*

Dimostrazione. Vediamo il caso di un Bol loop destro G.
Se nella $[\,(xy)\,z\,]\,y = x\,[\,(yz)\,y\,]$ si sostituisce $z = y_r$ (come sempre $y\,y_r = e = y_l\,y$) si ottiene $[\,(xy)\,y_r\,]\,y = x\,[\,(y\,y_r)\,y\,] = xy$ per ogni $x, y \in G$. Dunque $(xy)\,y_r = x$: vale la proprietà dell'inverso destro (2.5) e inoltre $x_r^{-1} = x_r$ per ogni $x \in G$.
Se nella $[\,(xy)\,z\,]\,y = x\,[\,(yz)\,y\,]$ si sostituisce $z = e$ si ottiene $[\,(xy)\,e\,]\,y = x\,[\,(y\,e)\,y\,]$ per ogni $x, y \in G$, cioè $(xy)y = x(yy)$ per ogni $x, y \in G$, alternativa destra. □

Teorema 2.4. *Sia G un Bol loop destro. Allora G è un Moufang loop se e solo se vale una qualsiasi delle seguenti:*

1. *G ha la proprietà dell'inverso sinistro* (2.4)*;*
2. *G ha la proprietà alternativa sinistra;*
3. *G è un Bol loop sinistro;*
4. *in G è vera l'identità* (2.9)*.*

Dimostrazione. Se G è un Moufang loop, allora verifica ciascuna delle quattro condizioni, [11, p. 116]. Proviamo le implicazioni inverse. Per la proposizione 2.5, G ha la proprietà dell'inverso destro, e per l'osservazione 2.8 si ha quindi $x_r^{-1} = x_r = x_l$ per ogni $x \in G$. Utilizziamo perciò la notazione $x^{-1} := x_r$ come nella dimostrazione del lemma 2.1, e J denoterà anche qui la funzione su G che associa ad ogni x il suo inverso x^{-1}.

Mostreremo ora quanto segue: a) Se G ha la proprietà dell'inverso sinistro, allora G ha la proprietà alternativa sinistra; b) Se G ha la proprietà alternativa sinistra, allora G è un Moufang loop; c) Se G è un Bol loop sinistro, allora G è di Moufang; d) Se in G è vera l'identità (2.9), allora G è di Moufang.

a) Se G è un Bol loop destro, allora verifica la proprietà dell'inverso destro (2.5). Dunque se verifica anche la (2.4), G è un loop con proprietà dell'inverso. In un tale loop $(JR_x{}^{-1}J\,,\, R_x\,,\, R_xL_x)$ è autotopia per ogni $x \in G$, come in [11, p. 116]. Inoltre, in un qualsiasi quasigruppo con proprietà dell'inverso, si ha $JR_x{}^{-1}J = L_x$ da cui $(L_x\,,\, R_x\,,\, R_xL_x)$ è un autotopia di G. Applicando questo al prodotto yz si ottiene la prima delle (2.11).

b) La proprietà alternativa sinistra $(xx)\,y = x\,(xy)$ e l'identità di Bol destra $[\,(xy)\,z\,]\,y = x\,[\,(yz)\,y\,]$ implicano, se si pone $y = x$:

$$[\,x\,(xz)\,]\,x = [\,(xx)\,z\,]\,x = x\,[\,(xz)\,x\,].$$

Ponendo ora $xz = y$ si ottiene $(xy)\,x = x\,(yx)$. Questa, insieme con una delle due identità di Bol, implica una tra le identità di Moufang.

c) Se un Bol loop destro G è un Bol loop sinistro, allora ha la proprietà dell'inverso sinistro. Dunque, per il punto a, G è di Moufang.

d) Se $(xy)^{-1} = y^{-1}x^{-1}$ per ogni $x, y \in G$ allora, invertendo entrambi i membri dell'identità alternativa destra $(xy)\,y = x\,(yy)$, si ottiene $y^{-1}(y^{-1}x^{-1}) = (y^{-1}y^{-1})\,x^{-1}$, cioè $z\,(zt) = (zz)\,t$, alternativa sinistra. Così, per il punto b, G è di Moufang.

Questo completa la dimostrazione. □

Corollario 2.4.1. *Se un loop L è un Bol loop sinistro e destro, allora L è un Moufang loop.*

Vale anche l'altra implicazione: si veda [13, p. 341]. Quindi un loop è un Moufang loop se e solo se è un Bol loop sinistro e destro.

Esempio 2.7. Sia $L = {\mathbb{F}_2}^3$, di cardinalità 8 ed elemento generico $x = (x_1\,,\, x_2\,,\, x_3)$, $x_i \in \mathbb{F}_2$, $1 \leq i \leq 3$. Si consideri su L l'operazione $\bullet$ definita:

$$x \bullet y := x + y + (0\,,\, 0\,,\, x_2y_1y_2).$$

La coppia $(L\,,\, \bullet)$ è un Bol loop destro, non commutativo: si ha subito che, se $x = (0, 1, 0)$ e $y = (1, 1, 0)$, allora $x \bullet y = (1, 0, 1)$ mentre $y \bullet x = (1, 0, 0)$. Inoltre esso non è di Moufang, come tra poco verificheremo.
Di più, 8 è il minimo ordine per un Bol loop che non sia un gruppo; vi sono sei tali Bol loops di ordine 8 distinti a meno di isotopia, nessuno commutativo, e solo due di questi hanno esattamente cinque elementi il cui quadrato è e. Considerazioni di questo tipo sono esposte in dettaglio in [9].
Identificando ora $(a\,,\, b\,,\, c) \in {\mathbb{F}_2}^3$ con $n \in \{0, \ldots, 7\}$ tale che abc sia la stringa di bits che esprime n in base 2, si ha per $(L\,,\, \bullet)$ la tavola di moltiplicazione 2.3 alla pagina seguente. Essa mostra che $(L\,,\, \bullet)$ non è di Moufang infatti, per esempio, $x = 2$, $y = 3$ e $z = 4$ non verificano la prima delle 2.11:

$$(2 \bullet 3) \bullet (4 \bullet 2) = 1 \bullet 6 = 7$$

mentre

$$[2 \bullet (3 \bullet 4)] \bullet 2 = [2 \bullet 7] \bullet 2 = 4 \bullet 2 = 6.$$

Anche la classe dei Bol loops, che contiene propriamente la classe dei Moufang loops, è chiusa rispetto isotopia.

Infine, un ulteriore risultato sui Bol loops che giustifica quanto detto nell'esempio 2.7, e cioè che 8 è il minimo ordine per un Bol loop che non sia un gruppo, dovuto ad R. P. Burn e citato in [9] e in [11]:

Proposizione 2.6. *Se p è un numero primo qualsiasi, un Bol loop di ordine p, $2p$ o p^2 è un gruppo.*

Tabella 2.3: esempio 2.7.

L :

•	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	5	4
3	3	2	1	0	7	6	4	5
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	1	0
7	7	6	5	4	3	2	0	1

2.4 Potenza associativa

Sia $(G\,,\,\cdot)$ una struttura associativa, per esempio un semigruppo (moltiplicativo). Allora, per ogni $x \in G$, $x^1 = x$, $x^2 = x \cdot x$ ed, in generale, x^n è il prodotto di n copie di x, univocamente determinato e non ambiguo. Per contro, se $(G\,,\,\cdot)$ è un gruppoide non associativo e non commutativo, per esempio un qualsiasi quasigruppo, x^n non è ben definito per $n \geq 3$. In una tale struttura x^3 potrebbe indicare sia $(x \cdot x) \cdot x$, sia $x \cdot (x \cdot x)$, mentre x^4 potrebbe indicare almeno cinque oggetti distinti. Se $(G\,,\,\cdot)$ è un gruppoide commutativo e non associativo, x^n è ancora non ben definito per $n \geq 4$.
In un tale contesto certi autori adottano la seguente definizione ricorsiva: x^n è x^{n-1} moltiplicato a sinistra per x. Secondo questa definizione si avrebbe per esempio $x^4 = ((x \cdot x) \cdot x) \cdot x$.

Definizione 2.18. Sia L un quasigruppo moltiplicativo, siano $x_1, \ldots, x_n \in L$ e siano $m_1, \ldots, m_n \in \mathbb{N}$. Si chiama *sottoquasigruppo generato da* $x_1, \ldots, x_n$ in L l'insieme K degli elementi di L di tipo ${x_1}^{m_1} \ldots {x_n}^{m_n}$. Si dice anche che $x_1, \ldots, x_n$ *generano* K in L e si usa la notazione:

$$K = \langle x_1, \ldots, x_n \rangle \subseteq L$$

Definizione 2.19. Un quasigruppo L si dice *associativo per potenze*[13] se ogni elemento di L genera un sottoquasigruppo associativo (cioè, per l'osservazione 2.5, un sottogruppo) di L.

[13] *Power-associative quasigroup.*

Nel caso, tale sottogruppo è abeliano.

Definizione 2.20. Un quasigruppo L si dice *quasigruppo di-associativo*[14] se ogni coppia di elementi di L genera un sottoquasigruppo associativo (sottogruppo) di L.

Un quasigruppo di-associativo è necessariamente associativo per potenze: $\langle a, b\rangle = \langle a\rangle$ se $b = a$. Non vale invece l'implicazione inversa.

Proposizione 2.7. *Ogni Bol loop è associativo per potenze.*

Dimostrazione. Un Bol loop destro verifica l'alternativa destra; ponendo $x = y$ nella terza delle (2.12) si ha $(xx)x = x(xx)$. Analogamente per un Bol loop sinistro. Quindi è facile provare induttivamente che in un Bol loop, destro o sinistro, vale la potenza associativa. □

Quindi in un Bol loop (sinistro o destro) è possibile definire il periodo di un elemento x così come si fa in un gruppo: se e è l'elemento neutro, diremo che x ha periodo finito uguale a k se esiste una potenza di x uguale a e, nel qual caso il più piccolo intero $k > 0$ tale che $x^k = e$ è detto il *periodo* di x.

Esempio 2.8. Le due tavole di moltiplicazione seguenti, tratte da [9], rappresentano i due Bol loops destri di ordine 8 (ed elemento neutro 0) con esattamente cinque elementi di periodo 2 e che non sono di Moufang.

·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	5	6	7	2	4	3
2	2	5	0	7	6	1	3	4
3	3	7	6	5	0	4	2	1
4	4	6	7	0	5	3	1	2
5	5	2	1	4	3	0	7	6
6	6	4	3	2	1	7	0	5
7	7	3	4	1	2	6	5	0

·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	6	7	5	2	4	3
2	2	5	0	6	7	3	1	4
3	3	7	5	0	6	4	2	1
4	4	6	7	5	0	1	3	2
5	5	2	3	4	1	7	0	6
6	6	4	1	2	3	0	7	5
7	7	3	4	1	2	6	5	0

Nessuno dei due è commutativo, come già detto nell'esempio 2.7, né verifica (2.10): nel primo caso (tavola a sinistra) $6 = 1 \cdot 3 = 1^{-1} \cdot 4^{-1} \neq (1 \cdot 4)^{-1} = 7^{-1} = 7$, mentre nel secondo $4 = 1 \cdot 6 = 1^{-1} \cdot 5^{-1} \neq (1 \cdot 5)^{-1} = 2^{-1} = 2$. Nel primo caso gli elementi 3 e 4

[14] *Di-associative quasigroup.*

hanno periodo 4 mentre tutti gli altri sono unipotenti, nel secondo caso gli elementi 5 e 6 hanno periodo 4 mentre tutti gli altri sono unipotenti.
Dalla tavola di moltiplicazione 2.3 di $(L\,,\,\bullet)$ emerge che esso ha a sua volta cinque elementi di periodo 2, e dunque è uno dei due mostrati in questo esempio. Quale, tra le due tavole di Cayley qui sopra, sia quella isotopa alla tavola di $(L\,,\,\bullet)$ si può stabilire nel modo seguente. In $(L\,,\,\bullet)$ gli elementi di periodo 4 (denotati con 6 e 7) non commutano con ogni altro elemento di L e ciò si nota dal fatto che, se a è uno tra tali due elementi, gli otto elementi di L compaiono in ordine differente sulla riga e sulla colonna indicizzate da a. Tra i due loops mostrati in questo esempio, solo il primo (tavola a sinistra) condivide questo comportamento, evidentemente invariante rispetto isotopia.

Segue un ultimo importante teorema, di cui omettiamo la dimostrazione.

Teorema 2.5 (Moufang)**.** *Ogni Moufang loop L è di-associativo. Di più, se a, b, c sono elementi di un Moufang loop L tali che $(ab)\,c = a\,(bc)$, allora a, b, c generano in L un sottoloop associativo (sottogruppo).*

Per la dimostrazione si veda [2, pp. 117–119].

Proposizione 2.8. *Un Bol loop è di Moufang se e solo se è di-associativo.*

Dimostrazione. Sia L un Moufang loop, allora L è di-associativo per il teorema 2.5 di Moufang.
Se L è un Bol loop di-associativo, allora verifica la seconda delle (2.12). Da questa, sostituendo yz ad y, si ottiene un'identità di Moufang. □

Un loop è un Moufang loop se e solo se è un Bol loop sinistro e destro. Inoltre i Moufang loops sono tutti e soli i loops che sono di Bol destri o sinistri e che sono di-associativi, [13, p. 341].

Bibliografia

[1] Ball, R. W. (1973) 'Free generation in halfgroupoids', *Algebra Universalis*, vol. 3, no. 1, pp. 127–128.

[2] Bruck, R. H. (1958) *A survey of binary systems*, Berlin-Göttingen-Heidelberg: Springer-Verlag.

[3] Bruck, R. H. (1963) 'What is a loop?', in Albert, A. A. (ed.) *MMA Studies in Mathematics vol. 2 Studies in modern algebra*, Englewood Cliffs: Prentice-Hall.

[4] Etherington, I. M. H. (1965) 'Quasigroups and cubic curves', *Proceedings of the Edinburgh Mathematical Society (Series 2)*, vol. 14, no. 4, pp. 273–291, DOI 10.1017/S001309150000897X.

[5] Frigerio, A. (1958) 'Sui quasigruppi associati ai gruppi', *Rendiconti del Seminario Matematico della Università di Padova*, vol. 28, pp. 107–111. Disponibile su: `http://www.numdam.org/item?id=RSMUP_1958__28__107_0` [19 settembre 2012].

[6] Ilojide, E. (2011) *An algebraic study of groupoids and quasigroups represented by linear-bivariate polynomials over the ring* $\mathbb{Z}_n$, M. Sc., Obafemi Awolowo Univeristy.

[7] Jaiyeola, T. G. (2009) *A study of new concepts in Smarandache quasigroups and loops*, ILQ. Disponibile su: `http://fs.gallup.unm.edu/SmarandacheQuasigroupsAndLoops.pdf` [19 settembre 2012].

[8] Manin, Yu. I. (1986) *Cubic forms. Algebra, geometry, arithmetic*, 2^{nd} edition, tradotto dal russo da M. Hazewinkel, Amsterdam: North-Holland.

[9] Moorhouse, G. E. (2007) *Bol loops of small order*, [online]. Disponibile su: `http://www.uwyo.edu/moorhouse/pub/bol/` [19 settembre 2012].

[10] Nulab Inc. (2012) *Cacoo*, [online]. Disponibile su `https://cacoo.com/` [19 settembre 2012].

[11] Pflugfelder, H. O. (1990) *Quasigroups and loops: Introduction*, Berlin: Heldermann.

[12] Pflugfelder, H. O. (2000) 'Historical notes on loop theory', *Comment. Math. Univ. Carolin.*, vol. 41, no. 2, pp. 359–370. Disponibile su: `http://dml.cz/dmlcz/119169` [19 settembre 2012].

[13] Robinson, D. A. (1966) 'Bol loops', *Trans. Amer. Math. Soc.*, vol. 123, no. 2, pp. 341–354. Disponibile su: `www.ams.org/journals/tran/1966-123-02/S0002-9947-1966-0194545-4/` [19 settembre 2012].

[14] Shcherbacov, V. A. (2007) 'On definitions of groupoids closely connected with quasigroups', *Bul. Acad. Ştiinte Repub. Mold. Mat.*, no. 2, pp. 43–54. Disponibile su: `http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=basm&paperid=61` [19 settembre 2012].

[15] Shcherbacov, V. A. (2009) 'Quasigroups in cryptology', *Computer Science Journal of Moldova*, vol. 17, no. 2 (50), pp. 193–228. Disponibile su: `http://www.math.md/files/csjm/v17-n2/v17-n2-(pp-193-228).pdf` [19 settembre 2012].

[16] Shcherbacov, V. A., Pushkashu, D. I. e Shcherbacov, A. V. (2010) *Equational quasigroup definitions*. Disponibile su: `http://arxiv.org/pdf/1003.3175.pdf` [19 settembre 2012].

[17] Smith, J. D. H. (2006) *An introduction to quasigroups and their representations*, Boca Raton: Chapman and Hall/CRC.

[18] Smith, J. D. H. e Romanowska, A. B. (1999) *Post-modern algebra*, New York: John Wiley & Sons.

[19] Vasantha Kandasamy, W. B. (2002) *Groupoids and Smarandache groupoids*, Rehoboth: American Research Press. Disponibile su: `http://fs.gallup.unm.edu/Vasantha-Book2.pdf` [19 settembre 2012].

[20] Weisstein, E. W. *Steiner Triple System*, [online]. Disponibile su: `http://mathworld.wolfram.com/SteinerTripleSystem.html` [19 settembre 2012].

[21] Whittaker, J. V. (1955) 'On the postulates defining a group', *The American Mathematical Monthly*, vol. 62, no. 9, pp. 636–640.

Ringraziamenti

Etichetta vuole, ed è giusto così, che cominci ringraziando la Prof.ssa Monica Idà per avermi lasciato fare sempre tutto quello che mi interessava[1]. Che continui ringraziando Mamma e Papà per avermi sempre sostenuto, economicamente e non, e Marcello per aver portato la NWOBHM[2] in casa. Poi magari Francesca, mia compagna in questi tre anni, anche quando appelli d'esame e nervi mai troppo rilassati genera(va)no fulmini e saette. Ma a tutti questi soggetti posso esprimere verbalmente la mia gratitudine e qualsivoglia commenti e impressioni nella comodità del privato.

Questa tesi, e con essa l'impegno di questi anni, è dedicata a un numero ormai importante di persone le cui storie si sono intrecciate con la mia in questo gioco di ruolo chiamato Università del dopo-Berlinguer. Molte di queste non sono arrivate a raccogliere i frutti del loro (spesso invidiabile) talento, alcuni si sono persi per strada mentre altri hanno distintamente salutato (e tra questi anche io?) prima di scegliere un'altro percorso, questa volta più spesso facendo bene o, talvolta, grandi cose davvero.
Dai giorni in cui, nell'estate del 2002, l'aver superato la maturità di un soffio azzerava una fetta importante della torta dei miei problemi, tante persone hanno collaborato con me, come sempre succede, e lasciato una traccia più o meno nitida nei miei pensieri di oggi. Tra gli amici 'di un tempo' che sento ancora e che non sento più ricordo con affetto non quantificabile quelli che hanno condiviso con me le grandi studiate e le grandi seratacce (spesso consecutive, animate entrambe dai medesimi protagonisti), le grandi gioie e le madornali stangate. Quelli che hanno preparato con me lo stesso esame cinque volte tra il 2003 e il 2006 per poi mandarmi una mail in Inghilterra nel 2008 con scritto che lo avevano superato.

[1] Non ultimo il tirocinio!
[2] *New wave of british heavy metal.*

Enrico, Ale e Betto, Cece, Cola, Davide, Giovanni e la Monica, Kabir aka Francesco, Lorenzo e (il) Bruno, Sergio e Filippo, Vito, Dario e Nick (anche se adesso facciamo così fatica a bere una birra tutti e quattro nello stesso posto e contemporaneamente), Jordan, Federico e penso anche qualcun altro hanno contribuito in modo determinante al Matteo di oggi. Da questi ragazzi ho imparato ad affrontare e superare le difficoltà con profitto e nella maniera nostra. Grazie. E anche se pochi di questi e di queste saranno con me a festeggiare questa laurea, il ricordo delle tante cose fatte bene insieme non mi abbandona mai un attimo. Senza dimenticare come uno di loro mi abbia presentato la mia attuale ragazza, che ci sarà e che ridi e scherza in queste pagine è già stata citata tre volte.

I ragazzi di Southampton, qui rappresentati dalla figura di Jack Tocci, sono già stati citati in una pagina analoga a questa, che ho scritto in inglese quattro estati fa.
Tra gli amici 'di matematica' ringrazio chi ha *tifato per me* e chi ha pensato che io quel giorno là *meritassi onore*.

Ringrazio il mio correlatore, il Prof. Libero Verardi, gentilissimo e puntualissimo.
Tra i docenti 'di una volta' ringrazio il Dott. Andrea Zucchelli perché è il migliore e gli studenti (con cui io parlo, senza discriminazione di Facoltà) se ne sono accorti.
I would like to express my gratitude and vibrant satisfaction to G. Eric Moorhouse and Jaiyeola Temitope Gbolahan for supporting this job with literature, [6], [7], [9], answers to my questions, encouragement.

Grazie a Carla per aver recuperato a Ferrara il Bruck [2] che ha dato il via ai lavori, e ai ragazzi di Black Market Tattoo di via Rialto, perché mi va.