Appunti sulla teoria elementare dei gruppi

Andrea Loi

Indice

Capitolo 1

Semigruppi, monoidi e gruppi

1.1 Semigruppi

Sia X un insieme diverso dal vuoto. Un' *operazione binaria* $\cdot$ su X è un'applicazione

$$\cdot : X \times X \to X, (x, y) \mapsto x \cdot y.$$

Diremo che un'operazione binaria $\cdot$ su un insieme X è associativa se

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in X.$$

Osservazione 1.1.1 Indicheremo con xy il prodotto $x \cdot y$ rta due elementi x, y quando l'operazione binaria $\cdot$ sarà chiara dal contesto. Inoltre se vale la proprietà associativa, dati tre elementi x, y, z potremo scrivere senza ambiguità xyz per indicare $(xy)z = x(yz)$

Definizione 1.1.2 *Un* semigruppo *è una coppia* $(S, \cdot)$, *dove* $S \neq \emptyset$ *e* $\cdot$ *è un'operazione binaria su* S *associativa.*

Dato un semigruppo $(S, \cdot)$ diremo che S è il *supporto* del semigruppo $(S, \cdot)$ e indichieremo la sua cardinalità con $|S|$. A volte chiameremo $|S|$ *l' ordine* del semigruppo $(S, \cdot)$. Diremo anche che un semigruppo è *finito* (risp. *infinito*) se il suo ordine è finito (risp. infinito).

Un'operazione binaria su un insieme $X \neq \emptyset$ è detta *commutativa* se

$$x \cdot y = y \cdot x, \forall\, x, y \in X.$$

Un semigruppo $(S, \cdot)$ nel quale l'operazione binaria $\cdot$ è commutativa verrà chiamato *semigruppo abeliano o commutativo*.

Esempio 1.1.3 Le coppie $(S,+)$ dove $S=\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, dove $+$ è la somma usuale sono semigruppi abeliani infiniti.

Esempio 1.1.4 Le coppie $(S^+,+)$ dove $S^+=\mathbb{N}^+$, $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ sono semigruppi abeliani infiniti. In quest'esempio $S^+=\{x\in S \mid x>0\}$.

Esempio 1.1.5 Le coppie $(S,\cdot)$ dove $S=\mathbb{N}, \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, dove $\cdot$ è la moltiplicazione usuale sono semigruppi abeliani infiniti.

Esempio 1.1.6 Le coppie $(S,\cdot)$ dove $S=\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ sono semigruppi abeliani infiniti. In queste note indicheremo con $S^*=S\setminus\{0\}$ se S è un insieme numerico contenente 0 (si noti che $\mathbb{N}^+=\mathbb{N}^*$).

Esempio 1.1.7 Sia P l'insieme dei numeri interi pari allora $(P,+)$, $(P^+,+)$, $(P,\cdot)$, e $(P^*,\cdot)$ sono semigruppi abeliani infiniti, dove la somma e la motiplicazione sono quelle usuali.

Esempio 1.1.8 Sia $m\geq 2$ un numero naturale allora $(\mathbb{Z}_m,+)$ e $(\mathbb{Z}_m,\cdot)$ con le operazioni definite sulle classi modulo m come

$$[x]_m+[y]_m=[x+y]_m \tag{1.1}$$

e

$$[x]_m\cdot[y]_m=[xy]_m \tag{1.2}$$

sono semigruppi abeliani di ordine m.

Esempio 1.1.9 Sia $P(X)$ l'insieme delle parti di un insieme $X\neq\emptyset$. Sia $\cup$ (risp. $\cap$) l'operazione binaria su $\mathrm{P}(X)$ che a due elementi $A,B\in \mathrm{P}(X)$ $(A,B\subset X)$ associa la loro unione (risp. intersezione) $A\cup B$ (risp. $A\cap B$). Allora $(\mathrm{P}(X),\cup)$ (risp. $(\mathrm{P}(X),\cap)$) è un semigruppo abeliano. L'ordine di $\mathrm{P}(X)$ è finito se e solo se X ha cardinalità finita.

Esempio 1.1.10 Sia X un insieme, $X\neq\emptyset$. Definiamo un'operazione binaria $\cdot$ su X come

$$x\cdot y=x, \forall x,y\in X. \tag{1.3}$$

Si verifica immediatamente che $(X,\cdot)$ è un semigruppo. non abeliano se X ha almeno due elementi. Analogamente possiamo definire su X l'operzione binaria

$$x\cdot y=y, \forall x,y\in X. \tag{1.4}$$

Esempio 1.1.11 Sia X un insieme, $X \neq \emptyset$. Consideriamo l'insieme $S = X^X$ costituito da tutte le applicazioni da X in se stesso con operazione binaria

$$f \circ g, \forall f, g \in S,$$

dove $\circ$ denota la composizione di applicazioni. Si verifica immediatamente che $(S, \circ)$ è un semigruppo. Inoltre questo semigruppo non è abeliano se X ha almeno due elementi. Infatti se $a, b \in X$, $a \neq b$ allora le applicazioni (costanti) $f, g \in S$ definite da $f(x) = a$ e $g(x) = b$, per ogni $x \in X$, sono tali che $f(g(a)) = a$ e $g(f(a)) = b$ e quindi $f \circ g \neq g \circ f$.

Sia $\cdot$ un'operazione binaria su un insieme $X \neq \emptyset$. Diremo che $x \in X$ è *cancellabile a sinistra (risp. a destra)* se

$$x \cdot y = x \cdot z \;\Rightarrow\; y = z, \; \forall y, z \in X \tag{1.5}$$

$$\text{(risp. } y \cdot x = z \cdot x \;\Rightarrow\; y = z, \; \forall y, z \in X). \tag{1.6}$$

Un'operazione binaria $\cdot$ su un insieme X soddisfa la *legge di cancellazione a sinistra (risp. a destra)* se ogni elemento di X è cancellabile a sinistra (risp. a destra), cioè

$$x \cdot y = x \cdot z \;\Rightarrow\; y = z, \; \forall x, y, z \in X \tag{1.7}$$

$$\text{(risp. } y \cdot x = z \cdot x \;\Rightarrow\; y = z, \; \forall x, y, z \in X). \tag{1.8}$$

Diremo che un'operazione binaria su $X \neq \emptyset$ soddisfa la *legge di cancellazione* se soddisfa la legge di cancellazione sia a sinistra che a destra.

Osservazione 1.1.12 Se l'operazione binaria è commutativa allora ogni $x \in X$ è cancellabile a sinistra se e solo se è cancellabile a destra e quindi vale la legge di cancellazione a sinistra se e solo se vale la legge di cancellazione a destra se e solo se vale la legge di cancellazione.

Esempi 1.1.13 Il lettore è invitato a convincerci fornendo se necessario una dimostrazione della validità delle affermazioni seguenti.

1. nei semigruppi abeliani $(S, +)$ e $(S^+, +)$ degli Esempi 1.1.3 e 1.1.4 vale la legge di cancellazione.

2. Nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.5 non vale la legge di cancellazione: infatti $0 \cdot 2 = 0 \cdot 3$ ma $2 \neq 3$. Un elemento è cancellabile se e solo se è diverso da 0.

3. nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.6 vale la legge di cancellazione.

4. nei semigruppi abeliani $(P, +)$, $(P^+, +)$ e $(P^*, \cdot)$ dell'Esempio 1.1.7 vale la legge di cancellazione. Mentre nel semigruppo abeliano $(P, \cdot)$ dello stesso esempio non vale la legge di cancellazione (un elemento è cancellabile se e solo se è diverso da 0).

5. l'operazione binaria (1.1) soddisfa la legge di cancellazione. Mentre l'operazione binaria (1.2) non la soddisfa. Infatti $[0]_m[0]_m = [0]_m[1]_m = [0]_m$ ma $[0]_m \neq [1]_m$. Lo studio degli elementi cancellabili nel semigruppo $(\mathbb{Z}_m, \cdot)$ è legato ai divisori dello zero nell'anello $(\mathbb{Z}_m, \cdot)$, argomento non trattato in queste note.

6. il semigruppo abeliano $(\mathrm{P}(X), \cup)$ (risp. $(\mathrm{P}(X), \cap)$) non soddisfa la legge di cancellazione. Per esempio se $A \subset B$ e $A \subset C$ e $B \neq C$ allora $A = A \cap B = A \cap C$ non implica $B = C$.

7. sia X un insieme con almeno due elementi. Allora l'operazione binaria (1.3) (risp. (1.4)) soddisfa la legge di cancellazione a destra (risp. sinistra) ma non a sinistra (risp. destra).

8. nel semigruppo $(S, \circ)$ dell'Esempio 1.1.11 un elemento $f \in S$ è cancellabile a sinistra (risp. a destra) se e solo se f è iniettiva (risp. suriettiva).

Sia $\cdot$ un'operzaione binaria su un insime $X \neq \emptyset$. Diremo che $b \in X$ è *idempotente* se

$$b^2 := b \cdot b = b.$$

Esempi 1.1.14 Il lettore è invitato a convincersi fornendo se necessario una dimostrazione della validità delle affermazioni seguenti.

1. nei semigruppi $(S, +)$ dell' Esempio 1.1.3 l'unico elemento idempotente è 0.

2. nei semigruppi $(S^+, +)$ dell' Esempio 1.1.4 non ci sono elementi idempotenti.

3. nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.5 ci sono due elementi idempotenti, 0 e 1.

4. nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.6 l'unico elemento idempotente è 0.

5. nei semigruppo $(P, +)$ e $(P, \cdot)$ l'unico elemento idempotente è 0. Nei semigruppo $(P^+, +)$ e $(P^*, \cdot)$ non ci sono elementi idempotenti.

6. nel semigruppo $(\mathbb{Z}_m, +)$, $[0]_m$ è l'unico elemento idempotente se m è dispari. Cosa succede se m è pari?

7. nei semigruppi degli Esempi 1.1.9 e 1.1.10 tutti gli elementi sono idempotenti.

Osservazione 1.1.15 Nel semigruppo $(S, \circ)$ dell'Esempio 1.1.11 ci possono essere tanti elementi idempotenti e la loro classificazione varia al variare dell'insieme X. Il lettore è inviato a riflettere sul caso $X = \mathbb{R}$.

Concludiamo questa sezione dimostrando l'esistenza di un elemento idempotente in un semigruppo finito.

Proposizione 1.1.16 *Sia $(S, \cdot)$ un semigruppo finito. Allora esiste almeno un elemento idempotente di S.*

Dimostrazione: Sia $x \in S$ un elemento arbitrario. Per la proprietà associativa dell'operazione binaria $\cdot$ possiamo definire

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ volte}}, \ \forall n \in \mathbb{N}^+.$$

Inoltre per induzione su $n \in \mathbb{N}^+$ si dimostra che

$$x^{n+1} = x^n x = x x^n, \ \forall n \in \mathbb{N}^+ \tag{1.9}$$

e, più in generale,

$$x^{m+n} = x^n x^m = x^m x^n, \ \forall m, n \in \mathbb{N}^+. \tag{1.10}$$

La (1.10) segue facilmente fissando $m \in \mathbb{N}_+$, usando l'induzione su n e la (1.9). Sia

$$C(x) = \{x^n \mid n \in \mathbb{N}^+\}.$$

Poichè $C(x) \subset S$ e $|S| < \infty$ anche $|C(x)| < \infty$. Consideriamo ora l'applicazione

$$f : \mathbb{N}^+ \to C(x), \ n \mapsto x^n.$$

Poiche la cardinalità di $\mathbb{N}^+$ è infinita, l'applicazione f non è iniettiva. Esisteranno quindi $i, j \in \mathbb{N}^+$, con $i > j$ tali che:

$$x^i = x^j. \tag{1.11}$$

Dalla (1.10) segue allora che

$$x^i = x^{i-j}x^j = x^j. \tag{1.12}$$

Inoltre, abbiamo che

$$x^i = x^{n(i-j)}x^j, \ \forall n \in \mathbb{N}^+. \tag{1.13}$$

La (1.13) si dimostra per induzione come segue. Per $n = 1$ è vera per la (1.12). Supponiamola vear per n, cioè supponiamo la validità di (1.13). Allora da (1.10), (1.11) e (1.12) si ottiene

$$\begin{aligned} x^{(n+1)(i-j)}x^j &= x^{n(i-j)+(i-j)}x^j = x^{n(i-j)}x^{i-j}x^j = \\ &= x^{n(i-j)}x^j x^{i-j} = x^i x^{i-j} = x^j x^{i-j} = x^i, \end{aligned}$$

che mostra la validità di (1.13) per $n + 1$.

Scegliamo ora $k \in \mathbb{N}^+$ tale che $k(i-j) > j$ e definiamo $b \in S$ come

$$b := x^{k(i-j)}.$$

Mostriamo che b è un elemento idempotente. Infatti

$$\begin{aligned} b^2 = b \cdot b = x^{k(i-j)}x^{k(i-j)} &= x^{k(i-j)}x^{k(i-j)-j}x^j = x^{k(i-j)}x^j x^{k(i-j)-j} = \\ &= x^i x^{k(i-j)-j} = x^j x^{k(i-j)-j} = x^{k(i-j)} = b. \end{aligned}$$

□

Osservazione 1.1.17 I semigruppi $(S^+, +)$ dell' Esempio 1.1.4 mostrano che l'ipotesi che S sia finito è necessaria per la validità della proposizione precedente.

1.2 Monoidi

Sia $\cdot$ un'operazione binaria su un insieme $X \neq \emptyset$. Un elemento $1 \in M$ si dice *elemento neutro a destra (risp. sinistra)* per l'operazione binaria $\cdot$, se

$$x \cdot 1 = x \text{ (risp. } 1 \cdot x = x), \ \forall x \in X.$$

Diremo che 1 é un elemento neutro per l'operazione binaria $\cdot$ se 1 é un elemento neutro sia a destra che a sinistra.

Se l'operazione binaria è chiara dal constesto, parleremo di elemento neutro (a destra oppure sinistra) senza specificare l'operazione binaria.

Osservazione 1.2.1 Se l'operazione binaria su un insieme X è commutativa allora 1 é un elemento neutro a destra se e solo se 1 é un elemento neutro a sinistra se e solo se 1 è un elemento neutro.

Osserviamo che se esiste un elemento neutro 1 per un'operazione binaria su un insieme X, allora 1 é l'unico elemento neutro, e parleremo quindi di 1 come l'elemento neutro. Infatti, se $\tilde{1} \in X$ é un altro elemento neutro allora

$$\tilde{1} = \tilde{1} \cdot 1 = 1,$$

dove nella prima uguaglianza stiamo usando il fatto che 1 é un elemento neutro a destra, mentre nella seconda che $\tilde{1}$ é un elemento neutro a sinistra.

Definizione 1.2.2 *Un semigruppo* $(M, \cdot)$ *é un* monoide *se esiste l'elemento neutro* $1 \in M$*.*

Equivalentemente, un monoide è un tripletta $(M, \cdot, 1)$, dove $(M, \cdot)$ é un semigruppo ed 1 é l'elemento neutro. Un monoide $(M, \cdot, 1)$ é detto *abeliano o commutativo* se il semigruppo $(M, \cdot)$ é abeliano.

Notazione 1.2.3 Nel caso di un monoide abeliano scriveremo l'operazione binaria con $+$ e l'elemento neutro con 0. Quindi un monoide abeliano sará indicato con $(M, +, 0)$. Un monoide arbitrario sará indicato con $(M, \cdot, 1)$.

Esempio 1.2.4 Le coppie $(S, +)$ dell' Esempio 1.1.3 sono monoidi abeliani infiniti dove l'elemento neutro é lo 0.

Esempio 1.2.5 Nessuna delle coppie $(S^+, +)$ dell'Esempio 1.1.4 é un monoide.

Esempio 1.2.6 Le coppie $(S, \cdot)$ dell'Esempio 1.1.5 sono monoidi abeliani infiniti con elemento neutro 1.

Esempio 1.2.7 Le coppie $(S, \cdot)$ dell'Esempio 1.1.6 sono semigruppi abeliani infiniti con elemento neutro 1.

Esempio 1.2.8 Sia P l'insieme dei numeri interi pari come nell'Esempio 1.1.7. Allora $(P, +, 0)$ è un monoide abeliano infinito. Mentre nessuna delle coppie $(P^+, +)$, $(P, \cdot)$ e $(P^*, \cdot)$ é un monoide.

Esempio 1.2.9 In riferimento all'Esempio 1.1.8, $(\mathbb{Z}_m, +, [0]_m)$ e $(\mathbb{Z}_m, \cdot, [1]_m)$ sono entrambi monoidi abeliani di ordine m.

Esempio 1.2.10 In riferimento all'Esempio 1.1.9 $(P(X), \cup, \emptyset)$ (risp. $(P(X), \cap, X)$) sono monoidi abeliani.

Esempio 1.2.11 In riferimento all'Esempio 1.2.11, $(X, \cdot)$ non é mai un monoide per $|X| \geq 2$.

Esempio 1.2.12 In riferimento all'Esempio 1.1.11, $(S = X^X, \circ)$ é un monoide con elemento neutro id_X ($\mathrm{id}_X(x) = x$ per ogni $x \in X$).

Dato un monoide $(M, \cdot, 1)$ allora l'elemento neutro è chiaramente un elemento idempotente ($1 \cdot 1 = 1$).

Proposizione 1.2.13 *Sia $(M, \cdot, 1)$ un monoide dove vale la legge di cancellazione a destra oppure a sinistra. Allora 1 é l'unico elemento idempotente.*

Dimostrazione: Supponiamo che $b \in M$ sia un idempotente e che valga la legge di cancellazione a destra. Allora dalla relazione

$$b \cdot b = b^2 = b = 1 \cdot b$$

si ottiene (b é cancellabile a destra) $b = 1$. Analogamente, se vale la legge di cancellazione a sinistra da

$$b \cdot b = b^2 = b = b \cdot 1$$

si ottiene (b é cancellabile a sinistra) $b = 1$. □

Senza l'ipotesi della legga di cancellazione la proposizione precedente non è valida come mostra il monoide dell'Esempio 1.2.10, dove tutti gli elementi sono idempotenti. La Proposizione 1.2.13 non si estende a semigruppi. Si pensi, per esempio, ad un insieme X con operazione binaria $x \cdot y = x$ (cf. Esempio 1.1.10). Come abbiamo osservato in quest'esempio vale la legge di cancellazione a destra ma non a sinistra e tutti gli elementi sono idempotenti.

D'altra parte la Proposizione 1.2.13 si estende a semigruppi se si richiede che valga la legge di cancellazione (sia a destra che a sinistra).

Proposizione 1.2.14 *Sia $(S, \cdot)$ un semigruppo dove vale la legge di cancellazione e sia $b \in S$ un elemento idempotente. Allora b é l'elemento neutro e quindi $(S, \cdot, b)$ é un monoide.*

Dimostrazione: Supponiamo che $b \in M$ sia un idempotente. Allora

$$b \cdot b \cdot x = b^2 x = bx, \ \forall x \in S.$$

Usando la legge di cancellazione a sinistra si ottiene quindi che $b \cdot x = x$ per ogni $x \in S$ e quindi b é un elemento neutro a sinistra. In modo analogo, dalla relazione

$$x \cdot b \cdot b = x \cdot b^2 = x \cdot b, \ \forall x \in S$$

e usando la legge di cancellazione a destra si ottiene $b \cdot x = x$ per ogni $x \in S$. Quindi b é l'elemento neutro e $(S, \cdot, b)$ é un monoide. $\square$

Combinando la Proposizione 1.1.16 con la Proposizione 1.2.14 si ottiene:

Corollario 1.2.15 *Un semigruppo finito dove vale la legge di cancellazione è un monoide.*

1.3 Gruppi

Sia $(M, \cdot, 1)$ un monoide e sia $x \in M$. Diremo che $a \in M$ é un inverso destro di x se

$$x \cdot a = 1. \tag{1.14}$$

Diremo che $a \in M$ é un inverso sinistro di x se

$$a \cdot x = 1. \tag{1.15}$$

Diremo che a è un'inverso di x se, a é sia inverso destro che inverso sinistro. Se x ha un'inverso allora diremo che x é *invertibile*.

Proposizione 1.3.1 *Sia x un elemento di un monoide $(M, \cdot, 1)$. Se x é invertibile allora il suo inverso è unico.*

Dimostrazione: Siano a e b due inversi di x. Per la proprietá associativa possiamo scrivere

$$a = a \cdot 1 = a \cdot (x \cdot b) = (a \cdot x) \cdot b = 1 \cdot b = b,$$

dove nella seconda uguaglianza abbiamo usato il fatto che b é l'inverso destro di x e nella terza che a é l'inverso sinistro di x. $\square$

In virtú della proposizione precedente dato un elemento inveritibile $x \in M$ parleremo *del* suo inverso che indicheremo (momentaneamente) con $i(x)$.

Definizione 1.3.2 *Una tripletta $(G, \cdot, 1)$ é un* gruppo *se é un monoide e tutti gli elementi di G sono invertibili.*

Quindi un gruppo é una tripletta $(G, \cdot, 1)$ dove $(G, \cdot)$ é un semigruppo (cioé l'operazione binaria $\cdot : G \times G \to G$ é associativa) tale che:

$$x \cdot 1 = x, \forall x \in G \ \ (1 \text{ è elemento neutro a destra}); \tag{1.16}$$

$$1 \cdot x = x, \forall x \in G \ \ (1 \text{ è elemento neutro a sinistra}); \tag{1.17}$$

e per ogni $x \in G$ esiste $i(x)$ tale che:

$$x \cdot i(x) = 1 \ \ (i(x) \ \text{ è inverso destro di } x); \tag{1.18}$$

$$i(x) \cdot x = 1 \ \ (i(x) \ \text{ è inverso sinistro di } x). \tag{1.19}$$

Osservazione 1.3.3 Come conseguenza dell'esistenza di un inverso per ogni elemento otteniamo che ogni equazione di primo grado in un gruppo G ha sempre un'unica soluzione: dati $a, b \in G$. esiste un unico $x \in G$ che soddisfa l'equazione.

$$ax = b. \tag{1.20}$$

Infatti moltiplicando a sinistra (risp. destra) per a^{-1} l'equazione precedente si ottiene $a^{-1} \cdot (a \cdot x) = (a^{-1} \cdot a) \cdot x = x$ (risp. $a^{-1}b$). E quindi l'unica soluzione dell'equazione (1.20) è $x = a^{-1}b$.

Notiamo che alcune delle proprietá nella definizione di gruppo sono ridondanti. Infatti, come mostra la seguente proposizione, basta richiedere la validitá del'esistenza di un elemento neutro a destra (risp. sinistra) e di un inverso destro (risp. sinistro) per ogni elemento di un semigruppo per essere sicuri che il semigruppo sia in effetti un gruppo.

Proposizione 1.3.4 *Sia $(S, \cdot)$ un semigruppo. Supponiamo che le* (1.16) *e* (1.18) *(risp.* (1.17) *e* (1.19)*) siano soddisfatte. . Allora $(S, \cdot, 1)$ é un gruppo.*

Dimostrazione: Sia $x \in S$. Per la (1.18) esiste $i(x) \in S$ tale che $x \cdot i(x) = 1$. Vogliamo mostrare che $i(x)$ é anche inverso sinistro di x. Osserviamo che

$$b := i(x) \cdot x$$

é idempotente. Infatti

$$b^2 = b \cdot b = (i(x) \cdot x) \cdot (i(x) \cdot x) = i(x) \cdot (x \cdot i(x)) \cdot x = (i(x) \cdot 1) \cdot x = i(x) \cdot x = b,$$

dove nella penultima uguaglianza abbiamo usato la (1.16). Sia ora $i(b)$ l'inverso destro di b che esiste sempre per la (1.18). Allora

$$1 = b \cdot i(b) = b^2 \cdot i(b) = b \cdot (b \cdot i(b)) = b \cdot 1 = b$$

e quindi $i(x) \cdot x = 1$ e $i(x)$ é inverso sinistro di x. Inoltre 1 è un elemento neutro a sinistra. Infatti

$$1 \cdot x = (x \cdot i(x)) \cdot x = x \cdot (i(x) \cdot x) = x \cdot 1 = x.$$

In modo analogo si dimostra che un semigruppo dove valgono le (1.17) e (1.19) é un gruppo. □

Osservazione 1.3.5 Le conclusioni della Proposizione 1.3.4 non sono valide se si richiede che valgano le (1.16) e (1.19) (risp. (1.17) e (1.18)). Per esempio sia $(X, \cdot)$ il semigruppo dato da un insieme $X \neq \emptyset$ con operazione binaria $x \cdot y = x$ per ogni $x, y \in X$ (si veda l'Esempio 1.1.10). Allora ogni elemento di X è un elemento neutro a destra e ogni elemento di X ha un inverso sinistro e come abbiamo già osservato $(X, \cdot)$ non é un monoide (si veda Esempio 1.2.11). Un altro esempio è fornito dal semigruppo $(\mathbb{R}^*, \cdot)$ con operazione binaria

$$x \cdot y = |x|\, y,$$

dove $|x|$ denota il valore assoluto di $x \in \mathbb{R}^*$. In questo caso 1 é un elemento neutro sinistro (ma non destro $|x| = x \cdot 1 \neq x$, se $x < 0$) e ogni elemento x ha inverso destro dato da $|x|^{-1}$. D'altra parte, un qualunque $y \in \mathbb{R}^*$, con $y < 0$ non ha inverso sinistro. Notiamo che in questo esempio esistono due elementi neutri a sinistra ± 1 e se si fosse scelto -1 come elemento neutro sinistro allora ogni $y \in \mathbb{R}^*$ con $y > 0$ non avrebbe avuto inverso sinistro.

Notazione 1.3.6 Nel resto di queste note indicheremo con G invece che con $(G, \cdot, 1)$ un gruppo, quando l'operazione binaria e l'elemento neutro saranno chiari dal contesto. Inoltre indicheremo con x^{-1} l'inverso di un elemento $x \in G$ ($x \cdot x^{-1} = x^{-1} \cdot x = 1$). Se il gruppo G é abeliano useremo anche la notazione $+$ per l'operazione binaria, 0 per l'elemento neutro e $-x$ per l'inverso di $x \in G$ (e scrivermo $x + (-x) = x - x = 0$).

1.3.1 Alcuni esempi di gruppi

Il lettore è invitato a convincersi che gli esempi che seguono sono effettivamente gruppi e di capire perchè alcuni dei monoidi degli Esempi 1.2.4-1.2.12 non appartengono a questa lista.

Esempio 1.3.7 Le coppie $(S, +, 0)$, dove $S = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $+$ è la somma usuale sono gruppi abeliani infiniti.

Esempio 1.3.8 Le coppie $(S, \cdot, 1)$, dove $S = \mathbb{Q}^*,\ \mathbb{R}^*,\ \mathbb{C}^*$ e $\cdot$ è la moltiplicazione usuale sono gruppi abeliani infiniti.

Esempio 1.3.9 (il cerchio unitario) L'insieme

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

è un gruppo abeliano infinito con la moltiplicazione $\cdot$ usuale tra numeri complessi. Ricordiamo che se $z = x + iy$ allora il suo modulo è definito come $|z| = \sqrt{x^2 + y^2}$. Infatti, il prodotto di due numeri complessi di modulo unitario è un numero complesso di modulo unitario, in quanto

$$|zw| = |z||w| = 1, \forall z, w \in S^1,$$

e quindi la moltiplicazione è un'operazione binaria su S^1. $(S^1, \cdot)$ è un semigruppo perchè la legge associativa vale in $\mathbb{C}^*$ e a fortiori in S^1. Inoltre $1 \in S^1$ è l'elemento neutro in $\mathbb{C}^*$ e quindi in S^1. Segue che $(S^1, \cdot, 1)$ è un monoide abeliano. Infine se $z \in S^1$ allora $z^{-1} \in S^1$. Infatti

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \bar{z} \in S^1,$$

dove $\bar{z}$ è il coniugato di z (se $z = x + iy$ allora $\bar{z} = x - iy$).

Per descrivere altri esempi di gruppi definiamo il concetto di campo. Una cinquina $\mathbb{K} = (\mathbb{K}, +, \cdot, 0, 1), 0, 1 \in \mathbb{K}, 0 \neq 1$, è un campo se $(\mathbb{K}, +, 0)$ e $(\mathbb{K}^*, \cdot, 1)$ ($K^* = \mathbb{K} \setminus \{0\}$) sono gruppi abeliani e vale la seguente proprietè distributiva del prodotto $\cdot$ rispetto alla somma $+$:

$$x \cdot (y + z) = x \cdot y + x \cdot z,\ \forall x, y, x \in \mathbb{K}.$$

Segue dagli Esempi 1.3.7 e 1.3.8 che $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con le operazioni usuali di somma e prodotto sono campi infniti. Esistono anche campi finiti. Quello a cui siamo interessati in questo corso è il campo $\mathbb{Z}_p = (\mathbb{Z}_p, +, \cdot, [0]_p, [1]_p)$ degli interi modulo p, con p numero primo, con somma e moltiplicazione definite da (1.1) e (1.2). Il fatto che $\mathbb{Z}_p$ sia un campo (con p elementi) segue dal fatto che $(\mathbb{Z}_p, +, [0]_p)$ è un gruppo abeliano (cf. l'Esempio 1.1.8), che $(\mathbb{Z}_p, +, [1]_p)$ è un monoide (cf. l'Esempio 1.2.9) e ogni $[a]_p \neq [0]_p$ è invertibile. Quest'ultimo fatto si dimostra come segue: per il teorema di Bezout essendo a coprimo con p esistono $u, v \in \mathbb{Z}$ tali che $ua + vp = 1$. Segue che

$$[ua]_p = [a]_p \cdot [u]_p = [u]_p \cdot [a]_p = [1]_p$$

e quindi $[u]_p$ è l'inverso di $[a]_p$.

Si noti che un campo ha almeno 2 elementi ($0 \neq 1$) e che $\mathbb{Z}_2$ è un campo con 2 elementi.

Esempio 1.3.10 (il gruppo lineare) Sia $n \in \mathbb{N}^+$ un intero positivo e sia $\mathbb{K}$ un campo. Definiamo $M_n(\mathbb{K})$ come l'insieme delle matrici quadrate di ordine n, ovvero $n \times n$, a coefficienti in $\mathbb{K}$. Un elemento $A \in M_n(\mathbb{K})$ può essere scritto come

$$A = (a_{ij}), \quad i, j = 1, \ldots, n,$$

dove $a_{ij} \in \mathbb{K}$ rappresenta l'elemento della i-esima riga e j-esima colonna.

Possiamo definire una somma tra due matrici: se $A = (a_{ij})$ e $B = (b_{ij})$ sono due matrici in $M_n(\mathbb{K})$, la matrice somma $C := A + B \in M_n(\mathbb{K})$ è definita come

$$C = (c_{ij}), \quad c_{ij} = a_{ij} + b_{ij}, \quad i, j = 1, \ldots, n.$$

Questa operazione è una somma componente per componente.

Inoltre, $(M_n(\mathbb{K}), +, O_n)$ è un *monoide*, dove O_n denota la *matrice nulla*, cioè la matrice $n \times n$ le cui entrate sono tutte uguali a 0, ossia:

$$O_n = (0_{ij}), \quad 0_{ij} = 0, \ \forall i, j = 1, \ldots, n.$$

Possiamo anche definire il prodotto tra due matrici: se $A = (a_{ik})$ e $B = (b_{kj})$ sono due matrici in $M_n(\mathbb{K})$, la matrice prodotto $C := A \cdot B \in M_n(\mathbb{K})$ è definita mediante il prodotto righe per colonne, ossia:

$$C = (c_{ij}), \quad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad i, j = 1, \ldots, n.$$

Anche questa è un'operazione binaria. Inoltre, $(M_n(\mathbb{K}), \cdot, I_n)$ è un *monoide* rispetto al prodotto, dove I_n denota la *matrice identità*, definita come:

$$I_n = (\delta_{ij}), \quad \delta_{ij} = \begin{cases} 1, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases}$$

La matrice identità ha 1 su tutta la diagonale principale e 0 altrove.

La dimostrazione che $(M_n(\mathbb{K}), \cdot, I_n)$ è un monoide segue gli stessi passaggi visti nei corsi di algebra lineare, con l'ipotesi che il campo $\mathbb{K}$ sia $\mathbb{R}$ o $\mathbb{C}$.

Per $n \in \mathbb{N}^+$, il *gruppo lineare generale* su un campo $\mathbb{K}$ è definito come

$$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid A \text{ è invertibile}\},$$

dove una matrice $A \in M_n(\mathbb{K})$ è detta *invertibile* se esiste una matrice $B \in M_n(\mathbb{K})$ tale che

$$AB = BA = I_n.$$

Una tale matrice B è chiamata *inversa* di A ed è anch'essa un elemento di $GL_n(\mathbb{K})$, ossia invertibile. La condizione che A sia invertibile è equivalente al fatto che il suo *determinante*, $\det(A)$, sia diverso da 0, dove $0 \in \mathbb{K}$ è l'elemento nullo del campo. Il determinante di una matrice quadrata A su un campo $\mathbb{K}$ si definisce nello stesso modo che per $\mathbb{K} = \mathbb{R}$ o $\mathbb{K} = \mathbb{C}$.

Si invitano i lettori a verificare che tutte le proprietà del determinante viste nei corsi di algebra lineare si estendono al caso generale di un campo arbitrario. Ad esempio, la formula di Binet, che afferma che

$$\det(AB) = \det(A)\det(B), \ \forall A, B \in M_n(\mathbb{K}),$$

vale in qualsiasi campo $\mathbb{K}$.

Usando la formula di Binet, si può concludere che $(GL_n(\mathbb{K}), \cdot, I_n)$ è un *gruppo*, che in generale non è abeliano per $n \geq 2$. Tuttavia, è un gruppo abeliano per $n = 1$, poiché $GL_1(\mathbb{K}) = \mathbb{K}^*$.

Concludiamo questa sezione mostrando come, a partire da un monoide, si possa costruire un gruppo considerando i suoi elementi invertibili.

Proposizione 1.3.11 *Sia $M = (M, \cdot, 1)$ un monoide. Definiamo l'insieme degli elementi invertibili di M come:*

$$U(M) = \{x \in M \mid x \text{ è invertibile}\}.$$

Allora $(U(M), \cdot, 1)$ è un gruppo.

Dimostrazione: Siano $x, y \in U(M)$, cioè x e y sono invertibili. Dimostriamo che anche il loro prodotto è invertibile. In particolare, mostriamo che l'inverso di $x \cdot y$ è dato da:

$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}. \tag{1.21}$$

Infatti:

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1,$$

e, analogamente:

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = y^{-1} \cdot (x^{-1} \cdot x) \cdot y = y^{-1} \cdot 1 \cdot y = y^{-1} \cdot y = 1.$$

Pertanto, $x \cdot y$ è invertibile e l'inverso è $y^{-1} \cdot x^{-1}$. Da ciò si deduce che la moltiplicazione definita su M induce un'operazione binaria su $U(M)$. Ora, osserviamo che $(U(M), \cdot)$ è un semigruppo, poiché la proprietà associativa vale in

M e, quindi, anche nel sottoinsieme $U(M)$. Inoltre, $(U(M), \cdot, 1)$ è un monoide, in quanto 1 è invertibile (essendo il suo stesso inverso). Infine, per costruzione, tutti gli elementi di $U(M)$ sono invertibili, il che dimostra che $(U(M), \cdot, 1)$ è un gruppo. $\square$

Osservazione 1.3.12 Segue immediatamente dalla definizione di gruppo che, se G è un gruppo, allora $U(G) = G$, poiché per definizione tutti gli elementi di un gruppo sono invertibili.

Osservazione 1.3.13 La formula (1.21) si estende facilmente a più elementi: se $x_1, \ldots, x_k$, $k \geq 2$ sono elementi di G, allora

$$(x_1 \cdots x_k)^{-1} = x_k^{-1} \cdots x_1^{-1}.$$

Non è detto che il gruppo $U(M)$ sia sempre interessante. Ad esempio, nel caso del monoide $(\mathbb{Z}, +, 0)$ (rispettivamente $(\mathbb{Z}, \cdot, 1)$), l'insieme degli elementi invertibili è costituito solo da 0 (rispettivamente 1). Un altro esempio è dato dal monoide $(\mathbb{Q}, \cdot, 1)$ (rispettivamente $(\mathbb{R}, \cdot, 1)$ e $(\mathbb{C}, \cdot, 1)$), in cui l'insieme degli elementi invertibili è $\mathbb{Q}^*$ (rispettivamente $\mathbb{R}^*$ e $\mathbb{C}^*$).

Un esempio rilevante è dato da $U(M_n(\mathbb{K}), \cdot, I_n) = GL_n(\mathbb{K})$, l'insieme delle matrici invertibili di ordine n su un campo $\mathbb{K}$.

Esempio 1.3.14 Consideriamo il monoide $(\mathbb{Z}_m, \cdot, [1]_m)$, dove $\mathbb{Z}_m$ sono gli interi modulo m e $[1]_m$ è l'elemento neutro rispetto alla moltiplicazione modulo m. L'insieme degli elementi invertibili di $(\mathbb{Z}_m, \cdot)$ è dato da:

$$U(\mathbb{Z}_m, \cdot) = \{[a]_m \in \mathbb{Z}_m \mid (a, m) = 1\}, \tag{1.22}$$

dove (a, m) indica il massimo comun divisore tra a e m. Infatti, se a è coprimo con m, esistono $u, v \in \mathbb{Z}$ tali che $ua + vm = 1$. Questo implica che:

$$[ua]_m = [a]_m \cdot [u]_m = [u]_m \cdot [a]_m = [1]_m, \tag{1.23}$$

e quindi $[u]_m$ è l'inverso di $[a]_m$.

Viceversa, se $[a]_m \in U(\mathbb{Z}_m, \cdot)$, esiste $[u]_m \in \mathbb{Z}_m$ tale che valga la relazione (1.23), il che implica che $au + km = 1$ per un intero k, e quindi $(a, m) = 1$.

Osserviamo che questo ragionamento mostra che $\mathbb{Z}_m$ è un campo se e solo se m è un numero primo.

1.3.2 La legge di cancellazione in un gruppo

Un risultato fondamentale nei gruppi è espresso dalla seguente proposizione.

Proposizione 1.3.15 *In un gruppo G vale la legge di cancellazione.*

Dimostrazione: Siano $x, y, z \in G$ tali che $xy = xz$. Moltiplicando a sinistra per x^{-1} (l'inverso di x) il primo e secondo membro di quest'equazione si ottiene $x^{-1}(xy) = x^{-1}(xz)$. Per la proprietà associativa il primo (risp. secondo) membro si scrive come $x^{-1}(xy) = (x^{\cdot -1}x)y = 1y = y$ (risp. $x^{-1}(xz) = (x^{\cdot -1}x)z = 1z = z$). Segue dunque che $y = z$, il che mostra la validità dellla legge di cancellazione a sinistra. Analogamente da $yx = zx$ si ottiene $y = z$ moltiplicando a destra per x^{-1}. □

A questo punto sorge spontanea una domanda: in un semigruppo o in un monoide in cui vale la legge di cancellazione, l'insieme è necessariamente un gruppo? Le due proposizioni seguenti esplorano questa questione.

Proposizione 1.3.16 *Sia M un monoide finito. Se vale la legge di cancellazione a destra o a sinistra, allora M è un gruppo.*

Dimostrazione: Sia $x \in M$. Dimostriamo che x è invertibile. Se vale la legge di cancellazione a sinistra consideriamo la *traslazione a sinistra* definita da:

$$L_x : M \to M,\ y \mapsto xy.$$

Questa funzione è iniettiva: se $L_x(y) = L_x(z)$ allora $xy = xz$ e, cancellando x a sinistra si ottiene $y = z$. Poichò M è finito, L_x è anche suriettiva. Quindi esiste un elemento $i(x) \in M$ tale che $= x \cdot i(x) = L_x(i(x)) = 1$, dimostrando che $i(x)$ è un inverso destro di x. Dal momento che 1 è l'elemento neutro a destra, segue dalla Proposizione 1.3.4 che $i(x)$ è anche inverso sinistro di x e quindi x è invertibile. Se invece vale la legge di cancellazione a destra, consideriamo la *traslazione a destra*:

$$R_x : M \to M,\ y \mapsto yx$$

che si dimostra essere iniettiva, e quindi suriettiva, da cui si deduce che x è invertibile. □

Osservazione 1.3.17 Il fatto che M sia finito è essenziale per la validità della proposizione precedente. Consideriamo, infatti, l'insieme infinito X e il monoide $(\mathrm{Inj}(X), \cdot, id_X)$ delle applicazioni iniettive da X in se stesso, con l'operazione di composizione. In questo monoide vale la legge di cancellazione a sinistra, ma non è un gruppo poiché esistono applicazioni iniettive non invertibili. Analoghe considerazioni valgono per il monoide $(\mathrm{Surj}(X), \cdot, id_X)$ delle applicazioni suriettive, dove vale la legge di cancellazione a destra ma non si tratta di un gruppo.

Corollario 1.3.18 *Sia S un semigruppo finito. Se vale la legge di cancellazione, allora S è un gruppo.*

Dimostrazione: Dal Corollario 1.2.15 $(S, \cdot, b)$ è un monoide, e quindi la conclusione segue dalla Proposizione 1.3.16. $\square$

Osservazione 1.3.19 Anche nel caso del Corollario 1.3.18, la finitezza di S è fondamentale. Ad esempio, $(\mathbb{N}^+, +)$ è un semigruppo con infiniti elementi in cui vale la legge di cancellazione, ma non è un monoide e tantomeno un gruppo.

Osservazione 1.3.20 Nel Corollario 1.3.18, l'ipotesi della legge di cancellazione non può essere indebolita richiedendo solo la validità della legge di cancellazione a destra (o a sinistra), anche se il semigruppo è finito. Infatti, se X è un insieme finito con almeno due elementi, l'operazione binaria (1.3) (rispettivamente, (1.4)) soddisfa la legge di cancellazione a destra (rispettivamente, a sinistra), ma $(X, \cdot)$ non è un monoide e tantomeno un gruppo.

1.3.3 Potenze, il commutatore e l'ordine di un elemento

Sia $(G, \cdot, 1)$ un gruppo, $x \in G$ e $m \in \mathbb{Z}$. Definiamo

(a) $x^0 := 1$;

(b) $x^n := \underbrace{x \cdot x \cdots x}_{n \text{ volte}}$, se $n > 0$ (definizione per induzione);

(c) $x^n := (x^{-1})^{-n}$, se $n < 0$.

Osservazione 1.3.21 La relazione (c) con $n = -1$, mostra che x alla potenza -1 è proprio x^{-1}, l'inverso di x. Inoltre la (c) vale anche se $n > 0$. Infatti, applicando la (3) si ottiene

$$(x^{-1})^{-n} = \left((x^{-1})^{-1}\right)^n = x^n,$$

dove si è usato il fatto che

$$(x^{-1})^{-1} = x.$$

La seguente proposizione descrive le proprietà delle potenze con esponente intero in un gruppo.

Proposizione 1.3.22 *Sia G un gruppo. Allora per ogni $x \in G$ e per ogni $m, n \in \mathbb{Z}$ si ha:*

(1) $x^n = x^{n-1}x = xx^{n-1}$;

(2) $x^{m+n} = x^n x^m = x^m x^n$;

(3) $(x^n)^{-1} = x^{-n}$;

(4) $x^{mn} = (x^m)^n = (x^n)^m$.

Dimostrazione: Se n è un numero naturale la formula

$$x^n = x^{n-1}x = xx^{n-1} \tag{1.24}$$

ossia la (1) per $n \geq 0$, si dimostra per induzione su n usando la proprietà associativa. Se $n < 0$:

$$x^n = (x^{-1})^{-n} = (x^{-1})^{-n} \cdot 1 = (x^{-1})^{-n} x^{-1} x = (x^{-1})^{-n+1} x = x^{n-1} x$$

dove nella penultima uguaglianza si è usato la (1.24) in quanto $-n > 0$ e nella prima e ultima uguaglianza la (c). Analogamente

$$x^n = (x^{-1})^{-n} = 1 \cdot (x^{-1})^{-n} = xx^{-1}(x^{-1})^{-n} = x(x^{-1})^{-n+1} = xx^{n-1}.$$

Per dimostare la (2) è sufficiente dimostrare la prima uguaglianza $x^m x^n = x^{m+n}$, poiché $m + n = n + m$. Fissiamo m e supponiamo innanzitutto che n sia un numero naturale. Procediamo per induzione su n. Se $n = 0$, l'uguaglianza è vera. Supponiamo che sia vera per $n - 1$, allora usando la (1), si ha:

$$x^m x^n = x^m x^{n-1} x = x^{m+n-1} x = x^{m+n-1+1} = x^{m+n} \tag{1.25}$$

ossia la (2) quando $n > 0$. Se invece $n < 0$, allora dalla (c) e dalla (1.25) ($-n > 0$) si ha:

$$x^m x^n = (x^{-1})^{-m} (x^{-1})^{-n} = (x^{-1})^{-m-n} = x^{m+n}.$$

Dalla (2) e dalla (a) si ottiene:

$$x^n x^{-n} = x^{n-n} = x^0 = 1$$

dalla quale segue la (3) per l'unicità dell'inverso. Infine, per dimostare la (4), è sufficiente dimostrare la prima uguaglianza $(x^m)^n = x^{mn}$, poiché $mn = nm$. Fissiamo m e supponiamo inizialmente che n sia un numero naturale. Procediamo per induzione su n. Se $n = 0$, l'uguaglianza è vera. Supponiamo che sia vera per $n-1$, ossia $(x^m)^{n-1} = x^{m(n-1)}$, allora, usando la (1) otteniamo:

$$(x^m)^n = (x^m)^{n-1}x^m = x^{m(n-1)}x^m = x^{mn-m+m} = x^{mn}, \tag{1.26}$$

ossia la (4) quando $n > 0$.

Se invece $n < 0$, allora:

$$(x^m)^n = ((x^m)^{-1})^{-n} = (x^{-m})^{-n} = x^{(-m)(-n)} = x^{mn},$$

dove nella prima uguaglianza si è usata la (c), nella seconda la (3) e nella terza la (1.26). □

Notazione 1.3.23 Supponiamo G abeliano e usiamo la notazione additiva $G = (G, +, 0)$. Allora le (a), (b), (c), (1), (2), (3), (4) si scrivono come segue.

- $0 \cdot x = 0$;
- $nx = \underbrace{x + \cdots + x}_{n \text{ volte}}$, se $n > 0$;
- $nx = (-n)(-x)$ se $n < 0$;
- $nx = (n-1)x + x = x + (n-1)x$;
- $(m+n)x = nx + mx = mx + nx$;
- $-(nx) = (-n)x$;
- $(mn)x = n(mx) = m(nx)$.

Definizione 1.3.24 *Sia G un gruppo. Diremo che $x, y \in G$* commutano *o sono* permutabili *se*

$$xy = yx.$$

Dati due elementi qualunque $x, y \in G$, chiameremo il commutatore *tra x e y il seguente elemento di G:*

$$[x, y] = xyx^{-1}y^{-1}.$$

Segue immediatamente che $x, y \in G$ sono permutabili se e solo se $[x, y] = 1$. Chiaramente l'elemento neutro commuta con ogni altro elemento del gruppo.

Proposizione 1.3.25 *Siano $x, y \in G$ due elementi permutabili, cioè $[x, y] = 1$. Allora, per ogni $m, n \in \mathbb{Z}$, valgono i seguenti fatti:*

(i) $[x^n, y^m] = 1$;

(ii) $(xy)^n = x^n y^n$.

Dimostrazione: La (i) per $n = -1$ e $m = 1$ e per $n = m = -1$ e cioè

$$[x^{-1}, y] = 1 \tag{1.27}$$

e

$$[x^{-1}, y^{-1}] = 1 \tag{1.28}$$

seguono facilmente da $[x, y] = 1$ e sono lasciate come semplice verifica.

Per dimostrare la (i) supponiamo prima $n \in \mathbb{N}$ e lavoriamo per induzione su n. La base dell'induzione è chiara: se $n = 0$ allora $[x^0, y^m] = [1, y^m] = 1$. Supponiamo che la (i) sia vera per tutti i naturali strettamente minori di $n \geq 1$. In particolare

$$[x^{n-1}, y^m] = 1 \tag{1.29}$$

e

$$[x, y^m] = 1 \tag{1.30}$$

Allora

$$x^n y^m = x x^{n-1} y^m = x y^m x^{n-1} = y^m x x^{n-1} = y^m x^n,$$

dove nella seconda uguaglianza si è usata la (1.29), nella terza la (1.30) e nella prima e ultima la (1) della Proposizione 1.3.22. La (i) è quindi dimostrata quando $n \in \mathbb{N}$.

Se $n < 0$ allora essendo $-n > 0$ possiamo scrivere

$$x^n y^m = (x^{-1})^{-n} y^m = y^m (x^{-1})^{-n} = y^m x^n,$$

dove nella seconda uguaglianza abbiamo usato la (1.27).

Per dimostrare la (ii), supponiamo $n \in \mathbb{N}$ e lavoriamo per induzione su n. Se $n = 0$: $(xy)^0 = 1 = 1 \cdot 1 = x^0 y^0$. Supponiamo la (ii) valga per $n - 1$ e cioè $(xy)^{n-1} = x^{n-1} y^{n-1}$. Allora

$$(xy)^n = (xy)^{n-1} xy = x^{n-1} y^{n-1} xy = x^{n-1} x y^{n-1} y = x^n y^n,$$

dove nella prima e nell'ultima uguaglianza abbiamo usato la la (1) della Proposizione 1.3.22 e nella terza uguaglianza abbiamo usato $[x, y^{n-1}] = 1$ la cui validità segue dalla (i). Se $n < 0$ allora

$$(xy)^n = ((xy)^{-1})^{-n} = (x^{-1} y^{-1})^{-n} = (x^{-1})^{-n} (y^{-1})^{-n} = x^n y^n,$$

dove nella seconda uguaglianza abbiamo usato la (1.28) e nella terza la (ii) per $-n > 0$. □

Osservazione 1.3.26 In un gruppo abeliano G le (i) e (ii) valgono per ogni coppia di elementi e in effetti si dimostra che se $x_1, \ldots, x_k$, $x_j \in G$ e $[x_l, x_m] = 1$ per ogni $l, m = 1, \ldots, k$, allora

$$(x_1 \cdots x_k)^n = x_1^n \cdots x_k^n. \tag{1.31}$$

Osservazione 1.3.27 Se in gruppo G vale che

$$(xy)^2 = x^2y^2$$

per ogni coppia di elementi $x, y \in G$. Allora il gruppo è abeliano. Infatti

$$xyxy = (xy)^2 = x^2y^2 = xxyy$$

e cancelando x a sinistra e y a destra si ottiene $xy = yx$. Essendo x e y arbitrari segue che il gruppo è abeliano. Viene spontaneo chiedersi: se in gruppo G vale

$$(xy)^3 = x^3y^3, \tag{1.32}$$

per ogni coppia di elementi $x, y \in G$. Possiamo affermare che il gruppo G è abeliano? La risposta è negativa in generale (si veda l'Esercizio 1.8).

Concludiamo questo paragrafo (e questo capitolo) definendo l'ordine di un elemento in un gruppo e le sue principali proprietà.

Sia dunque G un gruppo e sia $x \in G$.

Consideriamo l'insieme

$$A_x = \{n \in \mathbb{N}^+ \mid x^n = 1\}.$$

Se $A_x \neq \emptyset$ allora, per il principio del buon ordinamento, esiste $o(x) \in \mathbb{N}^+$ tale che $o(x)$ è il più piccolo naturale tale che

$$x^{o(x)} = 1.$$

Definizione 1.3.28 *Sia $A_x \neq \emptyset$. Chiameremo $o(x)$ l'*ordine *dell'elemento x. Se invece $A_x = \emptyset$ diremo che che l'ordine di x è infinito e scriveremo $o(x) = \infty$.*

Esempio 1.3.29 Se $G = (\mathbb{Z}, +, 0)$ e $x \in \mathbb{Z}$. Allora $o(x) = \infty$ per ogni $x \neq 0$. Mentre $o(x) = 1$ se $x = 0$.

Esempio 1.3.30 Se $G = (\mathbb{Z}_m, +, [0]_m)$. Allora $o([1]_m) = m$.

Osservazione 1.3.31 In un gruppo arbitrario $o(x) = 1$ se e solo se $x = 1$.

Osservazione 1.3.32 Se G ha ordine finito, allora $o(x) < \infty$ per ogni $x \in G$. Infatti l'applicazione

$$f : \mathbb{N}^+ \to G, d \mapsto x^d$$

non può essere iniettiva ed esistono quindi $u, v \in \mathbb{N}^+$, $u > v$ tali che $x^u = x^v$. Se $u = v + n$, $n \in \mathbb{N}^+$, possiamo scrivere $x^u = x^{v+n} = x^v$ da cui $x^n = 1$ e quindi l'insieme $A_x \neq \emptyset$.

Ricordiamo che il massimo comun divisore tre due interi a e b si denota con (a, b).

Proposizione 1.3.33 *Sia G un gruppo, $x \in G$ tale che $o(x) = m \in \mathbb{N}^+$. Allora*

(i) $x^k = 1$ *se e solo se* $m \mid k$;

(ii) $x^k = x^n$ *se e solo se* $n - k \equiv 0 \mod m$;

(iii) $o(x^k) = \frac{m}{(m,k)}$;

(iv) $o(x^{-1}) = m$.

Dimostrazione: dimostrazione della (i): se $m \mid k$ allora $k = mq$, $q \in \mathbb{Z}$. Quindi

$$x^k = x^{mk} = (x^m)^k = 1^k = 1$$

Viceversa, se supponiamo $x^k = 1$. Per la divisione euclidea possiamo scrivere

$$k = mq + r,\ 0 \leq r < m.$$

Segue che

$$x^k = x^{mq+r} = x^{mq}x^r = (x^m)^q x^r 1 \cdot x^r = x^r.$$

Essendo $m = o(x)$ il più piccolo naturale positivo tale che $x^m = 1$ si ottiene $r = 0$ e quindi $k = mq$, ossia $m \mid q$.
Dimostrazione della (ii): $x^k = x^n$ se e solo se $x^{k-n} = 1$. Quindi, per la (i), $m \mid k - n$ e quindi la tesi.
Dimostrazione della (iii): siano $s := o(x^k)$ e $d = (m, k)$. Quindi $d \mid m$ e $d \mid k$, ossia $m = dm_1$ e $k = dk_1$. Inoltre $(m_1, k_1) = 1$. La dimostrazione sarà conclusa

se mostriamo che $m_1 = s$. Sfruttando prima la condizione che $(x^k)^s = 1$ si ottiene

$$1 = (x^k)^s = x^{ks} = x^{dk_1 s}$$

Per la (i) segue che $m = dm_1 \mid dk_1 s$, cioè $m_1 \mid k_1 s$. Essendo $(m_1, k_1) = 1$ si ottiene

$$m_1 \mid s. \tag{1.33}$$

D'altra parte

$$(x^k)^{m_1} = x^{km_1} = x^{dk_1 m_1} = x^{dm_1 k_1} = x^{mk_1} = (x^m)^{k_1} = 1^{k_1} = 1.$$

Sempre dalla (i) si deduce che

$$s \mid m_1. \tag{1.34}$$

Mettendo insieme le (1.33) e la (1.34) si ottiene $s = m_1$. La (iv) segue dalla (iii) per $k = -1$. □

Esempio 1.3.34 Calcoliamo l'ordine di $[15]_{24}$ in $\mathbb{Z}_{24}$. Osserviamo che $o([1]_{24}) = 24$ e $[15]_{24} = 15[1]_{24}$. Dalla (iii) della Proposizione 1.3.25 si deduce dunque che:

$$o([15]_{24}) = \frac{24}{(15, 24)} = \frac{24}{3} = 8.$$

Esempio 1.3.35 Calcoliamo l'ordine di $[4]_9$ in $U(\mathbb{Z}_9, \cdot)$ Osserviamo

$$U(\mathbb{Z}_9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$$

$([2]_9)^2 = [4]_9$, $([2]_9)^3 = [8]_9$, $([2]_9)^4 = [7]_9$, $([2]_9)^5 = [5]_9$, $([2]_9)^6 = [1]_9$ quindi $o([2]_9) = 6$. Analogamente si verifica facilmente o con un calcolo diretto che $o([4]_9) = 3$, oppure suando la (iii) della Proposizione 1.3.25

$$o([4]_9) = o([2]_9^2) = \frac{6}{(6, 2)} = \frac{6}{2} = 3.$$

1.4 Esercizi

Esercizio 1.1 Si dica quali delle seguenti operazioni binarie sull'insieme indicato é associativa e commutativa. Si dica inoltre per quali di queste operazioni esiste un elemento neutro e quali $x \in \mathbb{R}$ sono invertibili. In particolare si identifichino i semigruppi, i monoidi e i gruppi.

1. $x \cdot y = x + y + k$, $x, y \in \mathbb{R}$ e $k \in \mathbb{R}$ una costante fissata;
2. $x \cdot y = \sqrt{x^2 + y^2}$, $x, y \in \mathbb{R}$;
3. $x \cdot y = |x + y|$, $x, y \in \mathbb{R}$;
4. $x \cdot y = x - y$, $x, y \in \mathbb{R}$;
5. $x \cdot y = \max\{x, y\}$, $x, y \in \mathbb{R}$;
6. $x \cdot y = \frac{xy}{2}$, $x, y \in \mathbb{R}^*$;
7. $x \cdot y = x + y + xy, , x \in \mathbb{R} \setminus \{-1\}$;
8. $x \cdot y = \frac{x+y}{x+y+1}$, $x \in (-1, 1) = \{x \in \mathbb{R} \mid -1 < x < 1\}$.

Esercizio 1.2 Sia G il prodotto cartesiano $\mathbb{Q} \times \mathbb{Z}^*$. Definiamo un'operazione su G nel modo seguente:

$$(q, m) \cdot (q', m') = (q + mq', mm').$$

Si provi che $(G, \cdot)$ é un monoide e si calcolino gli elementi invertibili. Si dica se G é un gruppo e se G é abeliano.

Esercizio 1.3 Sia G il prodotto cartesiano $\mathbb{Q}^* \times \mathbb{Q}$. Definiamo un'operazione su G nel modo seguente:

$$(a, b) \cdot (a', b') = (aa', ab' + \frac{a}{b'}).$$

Si provi che G é un gruppo e si dica se G é abeliano.

Esercizio 1.4 Quali delle seguenti operazioni binarie definisce un gruppo sull'insieme indicato?

1. $(a, b) \cdot (c, d) = (ad + bc, bd)$ su $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \neq 0\}$;
2. $(a, b) \cdot (c, d) = (ac, bc + d)$ su $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \neq 0\}$;

3. $(a,b)\cdot(c,d) = (ac, bc+d)$ su $\mathbb{R}\times\mathbb{R}$;

4. $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$ su $\mathbb{R}^*\times\mathbb{R}^*$;

5. $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$ su $\mathbb{R}\times\mathbb{R}$.

Esercizio 1.5 Sia $A = \{a, b\}$ un insieme con due elementi. Descrivere tutte le operazioni binarie su A. In particolare si dica quali di queste operazioni é commutativa e associativa. Si dica inoltre per quali di queste operazioni esiste un elemento neutro e quali elementi di A sono invertibili. Mostrare infine che ci sono 8 strutture di semigruppo di cui 6 non abeliane e 2 abeliane e che di queste solo 2 risultano un gruppo.

Esercizio 1.6 Sia $(M, \cdot, 1)$ un monoide e sia S un sottoinsieme di M tale che $(S, \cdot)$ risulta un semigruppo e $1 \notin S$. Si puó affermare che $(S, \cdot)$ non é un monoide?

Esercizio 1.7 Sia G un gruppo finito e sia S l'insieme degli elementi di G diversi dal proprio inverso $S = \{x \in G| \mid x \neq x^{-1}\}$. Dimostrare che:

1. S ha un numero pari di elementi;

2. $|G| \equiv |G \setminus S| \mod 2$;

3. se G ha un numero pari di elementi allora esiste $x \in G \setminus S$, $x \neq 1$ (quindi un gruppo di ordine pari ha almeno un elemento di ordine 2).

Esercizio 1.8

1. Sia G il gruppo costituito dalle matrici a entrate in $\mathbb{Z}_3$ della forma

$$\begin{bmatrix} [1]_3 & [a]_3 & [b]_3 \\ 0 & [1]_3 & [c]_3 \\ 0 & 0 & [1]_3 \end{bmatrix}$$

   Si dimostri che G è un gruppo non abeliano dove tutti gli elementi diversi dall'elemento neutro hanno ordine 3.

2. Sia G un gruppo che non ha elementi di ordine 3. Supponiamo che

$$(xy)^3 = x^3y^3, \forall x, y \in G. \tag{1.35}$$

   Dimostrare che G é abeliano.

(Suggerimento per la seconda parte: si osservi che

$$[x,y]^3 = ((xyx^{-1})y^{-1})^3 \overset{(1.35)}{=} xy^3x^{-1}y^{-3} = [x,y^3],\ \forall x,y \in G \tag{1.36}$$

e che

$$xy^3x^{-1} = (xyx^{-1})^3 = ((xy)x^{-1})^3 \overset{(1.35)}{=} (xy)^3x^{-3} \overset{(1.35)}{=} x^3y^3x^{-3},\ \forall x,y \in G$$

dalla quale segue

$$[x^2,y^3],\ \forall x,y \in G, \tag{1.37}$$

la quale ci dice che i quadrati sono permutabili con tutti i cubi. Dalla (1.8) e dalla (1.36) si ottiene dunque

$$[x^2,y],\ \forall x,y \in G, \tag{1.38}$$

la quale ci dice che i quadrati sono permutabili con ogni elemento del gruppo. Dalla (1.36) e dalla (1.37) si ottiene

$$[x,y]^3 = [x,y^3] = xy^3x^{-1}y^{-3} = xyx^{-1}y^{-1} = [x,y],\ \forall x,y \in G$$

e quindi

$$1 = [x,y]^2 = xyx^{-1}y^{-1}xyx^{-1}y^{-1} \overset{(1.37)}{=} xyxyxyx^{-3}y^{-3} = (xy)^3x^{-3}y^{-3} \overset{(1.35)}{=}$$

$$= x^3y^3x^{-3}y^{-3} \overset{(1.38)}{=} xyx^{-1}y^{-1} = [x,y]).$$

Esercizio 1.9 Sia $n \in \mathbb{N}_+$ e p un primo. Si dimostri che

$$|GL_n(\mathbb{Z}_p)| = (p^n-1)(p^n-p)(p^n-p^2)(p^n-p^{n-1}).$$

(Suggerimento: le righe di una matrice di $GL_n(\mathbb{Z}_p)$ sono linearmente indipendenti. Quindi la prima riga r_1 di una tale matrice puó essere qualsiasi cosa tranne il vettore nullo, quindi ci sono p^n-1 possibilitá per la prima riga. Per ognuna di queste possibilitá, la seconda riga r_2 puó essere qualsiasi cosa tranne un multiplo della prima riga, il che dá p^n-p possibilitá. Per qualsiasi scelta di r_1 e r_2 delle prime due righe, la terza riga puó essere qualsiasi cosa trana combinazione lineare di r_1 e r_2. Il numero di combinazioni lineari $\lambda_1r_1+\lambda_2r_2$ é p^2 cioé il numero di scelte per la coppie λ_1 e λ_2. Ne consegue che per ogni r_1 e r_2 ci sono p^n-p^2 possibilitá per la terza riga. Procedendo allo stesso modo sulle rimanenti righe si ottiene il risultato).

Esercizio 1.10 Dieci uomini vengono condannati a morte e rinchiusi nella stessa cella la notte precedente all'esecuzione. Gli viene data peró una possibilitá per salvarsi la vita. La mattina dell'esecuzione i dieci condannati verranno messi in fila indiana e verrá messo sulla testa di ognuno di essi un cappello di colore o bianco o nero. Nessuno dei condannati potrá vedere il colore del proprio cappello (quello che ha nella propria testa) ma solo, eventualmente, quello dei condannati che si trovano di fronte a lui. Per salvarsi, ognuno di loro, a turno potrá dire la parola "nero" oppure la parola "bianco". Se la parola detta da un condannato corrisponde al colore del proprio cappello allora il condannato sará graziato e quindi liberato. In caso contrario sará ucciso. Quale é la strategia che i dieci condannati dovranno escogitare la notte prima dell'esecuzione per essere sicuri che almeno 9 di loro siano graziati? Generalizzare a n condannati e k colori.