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 $x \cdot y$ quando l'operazione binaria $\cdot$ sarà chiara dal contesto.

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*.

Esempio 1.1.2 Le coppie $(S, +)$ dove $S = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $+$ è la somma usuale sono semigruppi abeliani infiniti.

Esempio 1.1.3 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 1.1.4 Le coppie $(S, \cdot)$ dove $S = \mathbb{N}, \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\cdot$ è la moltiplicazione usuale sono semigruppi abeliani infiniti.

Esempio 1.1.5 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 1.1.6 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 1.1.7 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 1.1.8 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 commutativo. L'ordine di $\mathrm{P}(X)$ è finito se e solo se X ha cardinalità finita.

Esempio 1.1.9 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 1.1.10 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 $(S, \cdot)$ 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 1.1.11 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 1.1.12 Il lettore è invitato a convincerci fornendo se necessario una dimostrazione della validità delle affernazioni seguenti.

1. nei semigruppi abeliani $(S, +)$ e $(S^+, +)$ degli Esempi 1.1.2 e 1.1.3 vale la legge di cancellazione.

2. Nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.4 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 1.1.5 vale la legge di cancellazione.

4. nei semigruppi abeliani $(P, +)$, $(P^+, +)$ e $(P^*, \cdot)$ dell'Esempio 1.1.6 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 $[0]_m[0]_m = [0]_m[1]_m = [1]_m$ 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 1.1.10 un elemento $f \in S$ è cancellabile a sinistra (risp. a destra) se e solo se f è iniettiva (risp. suriettiva).

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

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

Esempi 1.1.13 Il lettore è invitato a convincersi fornendo se necessario una dimostrazone della validità delle affernazioni seguenti.

1. nei semigruppi $(S, +)$ dell' Esempio 1.1.2 l'unico elemento idempotente è 0.

2. nei semigruppi $(S^+, +)$ dell' Esempio 1.1.3 non ci sono elementi idempotenti.

3. nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.4 ci sono due elementi idempotenti, 0 e 1.

4. nei semigruppi $(S, \cdot)$ dell'Esempio 1.1.5 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 1.1.8 e 1.1.9 tutti gli elementi sono idempotenti.

Osservazione 1.1.14 Nel semigruppo $(S, \circ)$ dell'Esempio 1.1.10 ci possono essere tanti elementi idempotenti e la loro classficazione 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 1.1.15 *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'appliczione

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

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

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

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

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

□

Osservazione 1.1.16 I semigruppi $(S^+, +)$ dell' Esempio 1.1.3 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 e 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.

Diremo che 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 1.2.2 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 1.2.3 Le coppie $(S, +)$ dell' Esempio 1.1.2 sono monoidi abeliani infiniti dove l'elemento neutro é lo 0.

Esempio 1.2.4 Nessuna delle coppie $(S^+, +)$ dell'Esempio 1.1.3 é un monoide.

Esempio 1.2.5 Le coppie $(S, \cdot)$ dell'Esempio 1.1.4 sono monoidi abeliani infiniti con elemento neutro 1.

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

Esempio 1.2.7 Sia P l'insieme dei numeri interi pari come nell'Esempio 1.1.6. Allora $(P, +, 0)$ è un monoide abeliano infinito. Mentre nessuna delle coppie $(P^+, +)$, $(P, \cdot)$ e $(P^*, \cdot)$ é un monoide.

Esempio 1.2.8 In riferimento all'Esempio 1.1.7, $(\mathbb{Z}_m, +, [0]_m)$ e $(\mathbb{Z}_m, \cdot, [1]_m)$ sono entrambi monoidi abeliani di ordine m.

Esempio 1.2.9 In riferimento all'Esempio 1.1.8 $(P(X), \cup, \emptyset)$ (risp. $(P(X), \cap, X)$) sono monoidi abeliani.

Esempio 1.2.10 In riferimento all'Esempio 1.2.10, $(X, \cdot)$ non é mai un monoide per $|X| \geq 2$.

Esempio 1.2.11 In riferimento all'Esempio 1.1.10, $(S = X^X, \circ)$ 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 1.2.12 *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 1.2.9, dove tutti gli elementi sono idempotenti. La Proposizione 1.2.12 non si estende a semigruppi. Si pensi, per esempio, ad un insieme X con operazione binaria $x \cdot y = x$ (cf. Esempio 1.1.9). 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 1.2.12 si estende a semigruppi se si richiede che valga la legge di cancellazione (sia a destra che a sinistra).

Proposizione 1.2.13 *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. □

Combinando la Proposizione 1.1.15 con la Proposizione 1.2.13 si ottiene:

Corollario 1.2.14 *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. □

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

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 1.3.2 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 rindondanti. 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 1.3.3 *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 1.3.4 Le conclusioni della Proposizione 1.3.3 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 1.1.9). 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 1.2.10). 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 1.3.5 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 1.2.3-1.2.11 non appartengono a questa lista.

Esempio 1.3.6 Le coppie $(S, +)$ dove $S = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $+$ è la somma usuale sono gruppi abeliani infiniti.

Esempio 1.3.7 Le coppie $(S, \cdot)$ $S = \mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ e $\cdot$ è la moltiplicazione usuale sono gruppi abeliani infiniti.

Esempio 1.3.8 (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 1.3.6 e 1.3.7 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 1.1.7), che $(\mathbb{Z}_p, +, [1]_p)$ è un monoide (cf. l'Esempio 1.2.8) 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 1.3.9 (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

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

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

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

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:

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

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:

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

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

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

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 $\mathrm{GL}_n(\mathbb{K})$, 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 $(\mathrm{GL}_n(\mathbb{K}), \cdot, I_n)$ è un *gruppo*, che in generale non è abeliano per $n \geq 2$. Tuttavia, è un gruppo abeliano per $n = 1$, poiché $\mathrm{GL}_1(\mathbb{K}) = \mathbb{K}^*$.

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

Proposizione 1.3.10 *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:

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

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. □

Osservazione 1.3.11 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.

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 $U(M_n(\mathbb{K}), \cdot, I_n) = \mathrm{GL}_n(\mathbb{K})$, l'insieme delle matrici invertibili di ordine n su un campo $\mathbb{K}$.

Esempio 1.3.12 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:

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

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:

$$[ua]_m = [a]_m \cdot [u]_m = [u]_m \cdot [a]_m = [1]_m, \tag{1.21}$$

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 (1.21), il che implica che $au + km = 1$ per un intero k, e quindi $(a, m) = 1$.

Osserviamo che questo ragionamento mostra $\mathbb{Z}_m$ 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 1.3.13 *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'equsazione 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 1.3.14 *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 1.3.3 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 1.3.15 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 1.3.16 *Sia S un semigruppo finito. Se vale la legge di cancellazione, allora S è un gruppo.*

Dimostrazione: Dal Corollario 1.2.14 $(S, \cdot, b)$ è un monoide, e quindi la conclusione segue dalla Proposizione 1.3.14. □

Osservazione 1.3.17 Anche nel caso del Corollario 1.3.16, 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 1.3.18 Nel Corollario 1.3.16, 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 né un monoide né 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) $^n := \underbrace{x \cdot x \cdots x}_{n \text{ volte}}$, se $n > 0$;

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

Osservazione 1.3.19 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

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

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 1.3.20 *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

$$x^n = x^{n-1}x = xx^{n-1} \tag{1.22}$$

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 (1.22) 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:

$$x^m x^n = x^m x^{n-1}x = x^{m+n-1}x = x^{m+n-1+1} = x^{m+n} \tag{1.23}$$

ossia la (2) quando $n > 0$.

Se invece $n < 0$, allora dalla (c) e dalla (1.23) ($-n > 0$) si ha:

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

La (3) si ottiene dalla (2) e dalla (a):

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

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 $n-1$, allora:

$$(x^m)^n = (x^m)^{n-1}x^m = x^{m(n-1)}x^m = x^{mn-m+m} = x^{mn} \tag{1.24}$$

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 (1.24). □

Notazione 1.3.21 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 $n < 0$;
- $nx = (n-1)x + x = x + (n-1)x$;
- $(m+n)x = nx + mx = mx + nx$;
- $-(nx) = (-n)x$;
- $(mn)x = n(mx) = m(nx)$.

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 1.3.22 *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

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

e

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

seguono facilmente da $[x, y] = 1$.

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 $[x, y^m] = 1$ e $[x^{n-1}, y^m] = 1$. Allora

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

e la (i) è 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 abbiamo usato $[x^{-1}, y] = 1$.

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 $n - 1$. 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 terza uguaglianza abbiamo usato $[x, y^{n-1}] = 1$ (cioè la (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 il fatto che $[x^{-1}, y^{-1}] = 1$ che segue da $[x, y] = 1$. □

Osservazione 1.3.23 In un gruppo abeliano G le (i) e (ii) valgono per ogni coppia di elementi e in effetti si dimostra che se G è abeliano allora se $x_1, \ldots, x_k$, $x_j \in G$, allora

$$(x_1 \cdots x_k)^n = x_1^n \cdots x_k^n. \tag{1.25}$$

Osservazione 1.3.24 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

$$(xy)^3 = x^3y^3, \tag{1.26}$$

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

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

Se tale $o(x)$ esiste (ossia se $A_x \neq \emptyset$) allora 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 1.3.25 Se $G = (\mathbb{Z}, +, 0)$ e $x \in \mathbb{Z}$. Allora $o(x) = \infty$ per ogni $x \neq 0$. Mentre l'ordine $o(x) = \infty$ se $x = 0$.

Esempio 1.3.26 Se $G = (\mathbb{Z}_m, +, [0]_m)$. Allora $o([1]_m) = m$.

Osservazione 1.3.27 In un gruppo arbitrario $o(x) = 1$ se e solo se $x = 1$.

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

Proposizione 1.3.28 *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 $m_1 = s$. Sfruttiamo 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

$$m_1 \mid s. \tag{1.27}$$

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

$$s \mid m_1. \tag{1.28}$$

Mettendo insieme le (1.27) e la (1.28) si ottiene $s = m_1$. □

Esempio 1.3.29 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 1.3.22 si deduce dunque che:

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

Esempio 1.3.30 Calcoliamo l'ordine di $[4]_9$ in $U(\mathbb{Z}_9, \cdot)$ Osserviamo

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

e che

$$([4]_9)^2 = [7]_9,\ ([4]_9)^3 = [4]_9 \cdot [7]_9 = [1]_9.$$

Segue che $0([4]_9) = 3$.

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 $x \in G\setminus S$, $x \neq 1$.

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

$$(xy)^3 = x^3y^3, \forall x,y \in G. \tag{1.29}$$

   Dimostrare che G é abeliano.

(Suggerimento per la seconda parte: si osservi che

$$[x,y]^3 = ((xyx^{-1})y^{-1})^3 \overset{(1.29)}{=} xy^3x^{-1}y^{-3} = [x,y^3],\ \forall x,y \in G \tag{1.30}$$

e che

$$xy^3x^{-1} = (xyx^{-1})^3 = ((xy)x^{-1})^3 \overset{(1.29)}{=} (xy)^3x^{-3} \overset{(1.29)}{=} x^3y^3x^{-3},\ \forall x,y \in G$$

dalla quale segue

$$[x^2,y^3],\ \forall x,y \in G, \tag{1.31}$$

la quale ci dice che i quadrati sono permutabili con tutti i cubi. Dalla (1.8) e dalla (1.30) si ottiene dunque

$$[x^2,y],\ \forall x,y \in G, \tag{1.32}$$

la quale ci dice che i quadrati sono permutabili con ogni elemento del gruppo. Dalla (1.30) e dalla (1.32) 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

$$1 = [x,y]^2 = xyx^{-1}y^{-1}xyx^{-1}y^{-1} \overset{(1.32)}{=} xyxyxyx^{-3}y^{-3} = (xy)^3x^{-3}y^{-3} \overset{(1.29)}{=}$$

$$= x^3y^3x^{-3}y^{-3} \overset{(1.32)}{=} xyx^{-1}y^{-1} = [x,y]).$$

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

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

(Suggerimento: le righe di una matrice di $\mathrm{GL}_n(\mathbb{Z}_p)$ 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 tranne una combinazione lineare di r_1 e r_2. Il numero di combinazioni lineari $\lambda_1 r_1 + \lambda_2 r_2$ 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.

Capitolo 2

Due gruppi importanti: D_n e S_n

Questo capitolo è dedicato a due gruppi di ordine finito che rivestono un ruolo importante nella teoria dei gruppi: il gruppo diedrale e il gruppo simmetrico.

2.1 Il gruppo diedrale

Sia $n \geq 3$ e sia P_n un poligono regolare di n lati in un piano euclideo $\mathcal{E}$. Consideriamo l'insieme D_n costituito dalle isometrie f di $\mathcal{E}$ che lasciano invariato P_n, cioè $f(P_n) = P_n$.

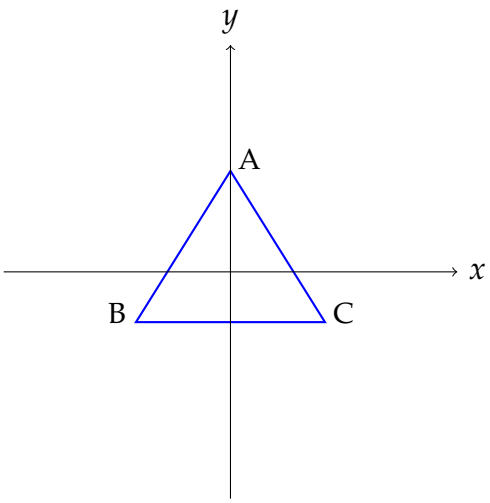
Possiamo allora definire un'operazione binaria associativa su D_n data dalla composizione ($f \circ g$, per ogni $f, g \in D_n$) che rende $D_n = (D_n, \circ, 1)$ un monoide, dove 1 denota l'applicazione identità da $\mathcal{E}$ in se stesso.

Essendo le isometrie di $\mathcal{E}$ applicazioni invertibili deduciamo anche che D_n è un gruppo, chiamato il *gruppo diedrale*. Infatti l'inverso f^{-1} di un isometria f di $\mathcal{E}$ soddisfa $f^{-1}(P_n) = P_n$.

Per capire meglio la natura del gruppo diedrale D_n, analizziamo in dettaglio i casi $n = 3$ e $n = 4$.

2.1.1 Il gruppo D_3

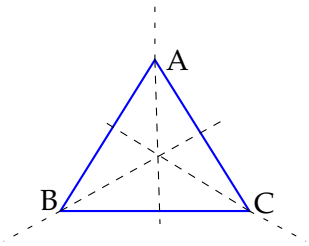
In questo caso il poligono regolare P_3 è un triangolo equilatero di vertici A, B e C che possiamo pensare centrato nell'origine degli assi di un sistema di riferimento cartesiano.



Le isometrie distinte del piano che fissano il triangolo sono 6:

- l'applicazione identica, denotata con 1;
- la rotazione $r_{\frac{2\pi}{3}}$ in senso antiorario intorno all'origine di angolo $\frac{2\pi}{3} = 120^0$;
- la rotazione $r_{\frac{4\pi}{3}}$ in senso antiorario intorno all'origine di angolo $\frac{4\pi}{3} = 240^0$;
- la riflessione s_A rispetto alla bisettrice dell'angolo A;
- la riflessione s_B rispetto alla bisettrice dell'angolo B;
- la riflessione s_C rispetto alla bisettrice dell'angolo C.

Le bisettrici sono rappresentati in figura.



Quindi D_3 è un gruppo di ordine 6.

Se indichiamo con $r = r_{\frac{2\pi}{3}}$ allora $r_{\frac{4\pi}{3}} = r^2 = r \circ r$, $r^3 = r \circ r \circ r = 1$ (osserviamo che le rotazioni in senso antiorario di angolo $\frac{\pi}{3}$ e $\frac{4\pi}{3}$ sono date rispettivamente da r^2 e r). Possiamo quindi scrivere

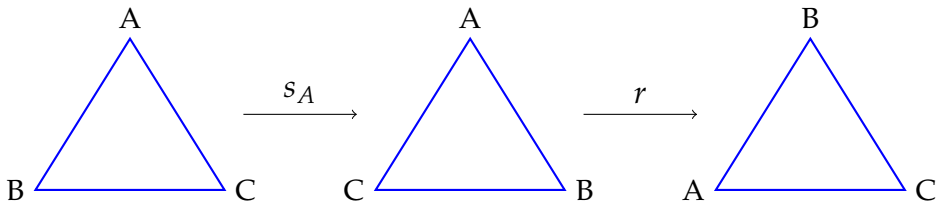
$$D_3 = \{1, r, r^2, s_A, s_B, s_C\}$$

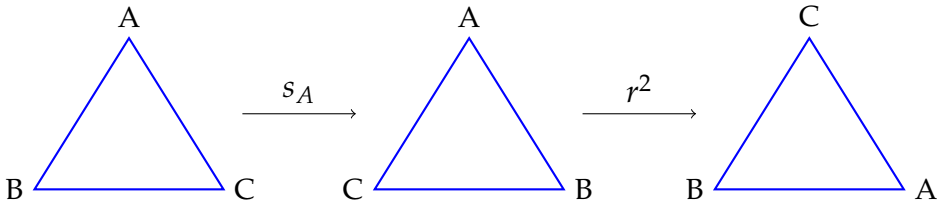
Vediamo più a fondo la strruttura di gruppo. Chiaramente

$$r^3 = s_A^2 = s_B^2 = s_C^2 = 1.$$

Quindi r ha ordine 3 e le riflessioni hanno ordine 2.

Si può facilmente verificare che che $r \circ s_A = s_C$, $r^2 \circ s_A = s_B$, come mostrato dai seguenti disegni:





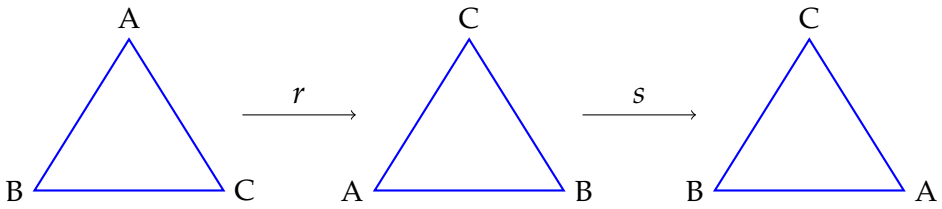
Possiamo quindi esprimene gli elementi di D_3 in funzione di r e di $s := s_A$ come

$$D_3 = \{1, r, r^2, s, r \circ s, r^2 \circ s\}$$

Osserviamo anche che la rotazione r e la riflessione s non commutano. Più precisamente

$$s \circ r = r^2 \circ s = s_B, \tag{2.1}$$

come si evince dal seguente disegno:



Quindi D_3 è un gruppo non abeliano.

Usando la relazione (2.2) possiamo quindi calcolare i prodotti in D_3

Per esempio

$$s \circ r^2 = s \circ r \circ r = r^2 \circ s \circ r = r^4 \circ s = r \circ s$$

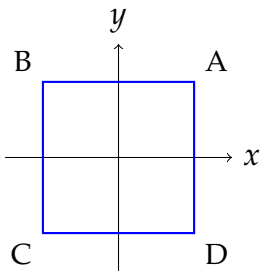
e analogamente per gli altri elementi.

Si ottiene quindi facilmente la seguente tavola moltiplicativa per il gruppo D_3.

$\cdot$	1	r	r^2	s	rs	r^2s
1	1	r	r^2	s	rs	r^2s
r	r	r^2	1	rs	r^2s	s
r^2	r^2	1	r	r^2s	s	rs
s	s	r^2s	rs	1	r	r^2
rs	rs	s	r^2s	r^2	1	r
r^2s	r^2s	rs	s	r	r^2	1

2.1.2 Il gruppo D_4

In questo caso il poligono regolare P_4 è un quadrato di vertici A, B, C e D come in figura, che possiamo pensare centrato nell'origine degli assi di un sistema di riferimento cartesiano xy.

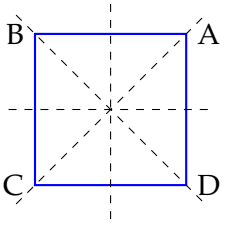


Le isometrie distinte del piano che fissano il quadrato sono 8:

- l'applicazione identica, denotata con 1;
- la rotazione $r_{\frac{\pi}{2}}$ in senso antiorario intorno all'origine di angolo $\frac{\pi}{2}$;
- la rotazione r_π in senso antiorario intorno all'origine di angolo π;
- la rotazione $r_{\frac{3\pi}{2}}$ in senso antiorario intorno all'origine di angolo $\frac{3\pi}{2}$;
- la riflessione s_{AC} rispetto alla diagonale AC;
- la riflessione s_{BD} rispetto alla diagonale BD;

- la riflessione s_x rispetto all'asse delle ascisse;
- la riflessione s_y rispetto all'asse delle ordinate.

Gli assi di simmetria sono rappresentati come segue.



Quindi D_4 è un gruppo di ordine 8.

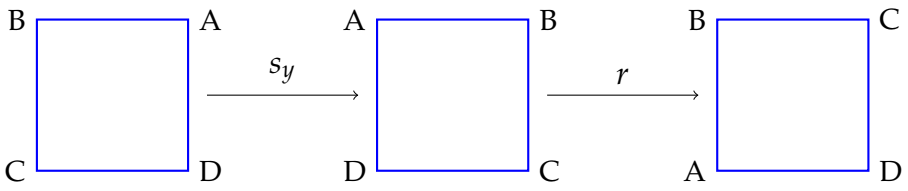
Se indichiamo con $r = r_{\frac{\pi}{2}}$ allora $r_\pi = r^2$, $r^3 = r_{\frac{3\pi}{2}}$ e $r^4 = 1$. Possiamo quindi scrivere

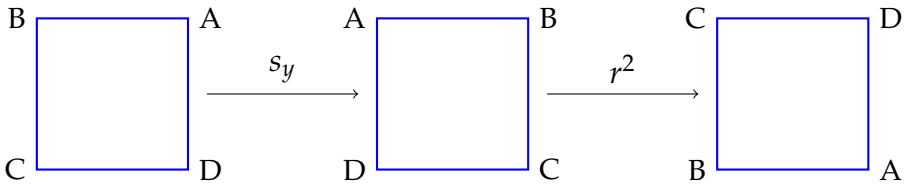
$$D_4 = \{1, r, r^2, r^3, s_{AC}, s_{BD}, s_x, s_y\}$$

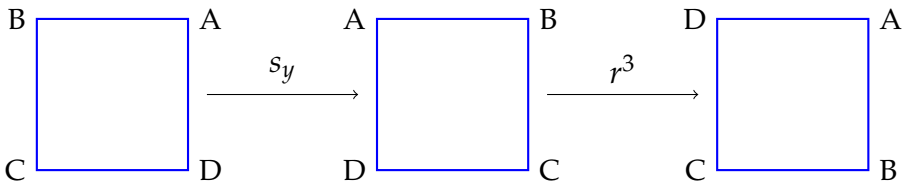
Osserviamo che

$$r^4 = s_{AC}^2 = s_{BD}^2 = s_x^2 = s_y^2 = 1$$

e che $r \circ s_y = s_{BD}$, $r^2 \circ s_y = s_x$, $r^3 \circ s_y = s_{AC}$ come mostrano i seguenti disegni:







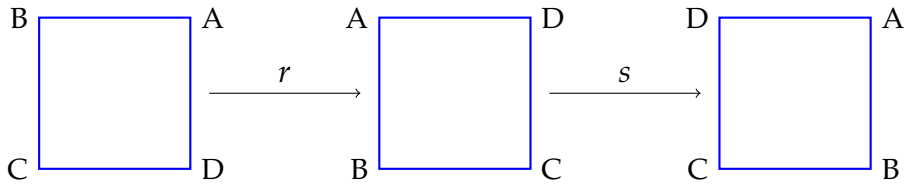
Possiamo quindi esprimene gli elementi di D_4 in funzione di r e di $s := s_y$ come

$$D_4 = \{1, r, r^2, r^3, s, r \circ s, r^2 \circ s, r^3 \circ s\}$$

Osserviamo anche che la rotazione r e la riflessione s non commutano. Più precisamente

$$s \circ r = r^3 \circ s = s_{AC}, \tag{2.2}$$

come si evince dal seguente disegno:



Quindi D_4 è un gruppo non abeliano.

Usando la relazione (2.2) possiamo quindi calcolare i prodotti in D_4 e ottenere la seguente tavola moltiplicativa per questo gruppo.

$\cdot$	1	r	r^2	r^3	s	rs	r^2s	r^3s
1	1	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	1	rs	r^2s	r^3s	s
r^2	r^2	r^3	1	r	r^2s	r^3s	s	rs
r^3	r^3	1	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	1	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	1	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	1	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	1

2.1.3 Il caso generale

Assumiamo che il poligono regolare P_n sia centrato nell'origine di un sistema di riferiemento cartesiano. Come osservato nei casi $n = 2$ e $n = 3$ gli assi di simmetria del poligono P_n sono disposti in maniera diversa, a seconda che il numero dei suoi lati sia pari (metá degli assi passano per i vertici opposti e metá passano per il centro dei lati opposti) oppure dispari (ogni asse passa per un vertice e il centro del lato opposto). Ovviamente tutti gli assi di simmetria passano per l'origine.

Quindi

$$D_n = \{1, r, \ldots, r^{n-1}, s_1, \ldots, s_n\},$$

dove r é la rotazione intorno all'origine in senso antiorario di angolo $\frac{2\pi}{n}$, $r^n = 1$ e s_h, $h = 1, \ldots, n$ é la riflessione rispetto al h-esimo asse di simmetria del poligono, $s_h^2 = 1$.

Dunque D_n è un gruppo di ordine $2n$.

Il seguente lemma segue dai corsi di geometria (si veda anche l'Osservazione 2.1.5).

Lemma 2.1.1 *Sia O un punto fissato del piano. Sia $\mathcal{R}$ l'insieme delle rotazioni piane intorno a O e sia $\mathcal{S}$ l'insieme delle riflessioni piane rispetto a rette passanti per O. Allora*

1. $r_1 \circ r_2 \in \mathcal{R}$, $\forall r_1, r_2 \in \mathcal{R}$;
2. $s \circ t \in \mathcal{R}$, $\forall s, t \in \mathcal{S}$;
3. $r \circ s \in \mathcal{S}$, $\forall r \in \mathcal{R}, \forall t \in \mathcal{S}$. *A parole: la composizione di due rotazioni o di due simmetrie è una rotazione, mantre la composizione di una simmetria e di una rotazione è un simmetria.*

Teorema 2.1.2 *D_n, $n \geq 3$ è un gruppo non abeliano di ordine $2n$. Sia s una qualunque riflessione in D_n, alllora*

$$D_n = \{1, r, \ldots, r^{n-1}, r \circ s, \ldots, r^{n-1} \circ s\}. \tag{2.3}$$

Inoltre,

$$s \circ r = r^{n-1} \circ r. \tag{2.4}$$

Dimostrazione: Abbiamo già osservato che D_n è un gruppo con $2n$ elementi. Per il lemma precedente, $\{r, \ldots, r^{n-1}\}$ sono tutte rotazioni distinte e conseguentemente $r^k \circ s$ sono n riflessioni distinte per $k = 1, \ldots, n-1$. Segue che $\{r, \ldots, r^{n-1}\} = \{s_1, \ldots, s_n\}$ e quindi vale la (2.3). Osserviamo ora che $s \circ r$ è una riflessione per il Lemma 2.1.1. Quindi

$$s \circ r \circ s \circ r = (s \circ r)^2 = 1$$

che implica $s \circ r = r^{-1} \circ s^{-1} = r^{n-1} \circ s$ ossia la (2.4). Infine la (2.4). mostra che D_n non è abeliano. □

Per induzione su n dalla (2.4) si ottiene facilmente il seguente corollario

Corollario 2.1.3 *Siano r e s come nel Teorema 2.1.2. Allora*

$$s \circ r^{n-k} = r^k \circ s, \ \forall k = 1, \ldots, n-1. \tag{2.5}$$

Notazione 2.1.4 Per esprimere in maniera concisa il gruppo diedrale si usa la notazione

$$D_n = \langle r, s \mid r^n = s^2 = 1, sr = r^n s \rangle$$

che viene chiamata una *presentazione* del gruppo diedrale con *generatori* r e s (non tratteremo le presentazioni di gruppi in queste note). Questa scrittura significa semplicemente che gli elementi del gruppo D_n si ottengono moltiplicando gli elementi di r e di s e tenendo conto del fatto che r ha ordine n, s ha ordine 2 e che vale la relazione $sr = r^n s = r^{-1}s$.

Osservazione 2.1.5 Se prensiamo a P_n com un poligono regolare inscritto nella circonferenza unitaria e prendiamo r come la rotazione di angolo $\frac{2\pi}{n}$ in senso antiorario rispetto all'origine possiamo scrivere

$$r^k = \begin{bmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{bmatrix}, \ k = 1, \ldots, n-1.$$

A meno dell'ordine le simmetrie $s_1, \ldots, s_n$ possono scriversi come

$$s_h = \begin{bmatrix} \cos\frac{4\pi h}{n} & \sin\frac{4\pi h}{n} \\ \sin\frac{4\pi h}{n} & -\cos\frac{4\pi h}{n} \end{bmatrix}, \ h = 1, \ldots, n.$$

Possiamo anche scegliere

$$s := s_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

ossia la rilfessione intorno all'asse delle ordinate (che è un asse di simmetria sia nel caso n pari che n dispari). Fatta questa scelta le (2.4) e (2.5) possono essere verificate molitpicando le matrici opportune. Anche il Lemma 2.1.1 può essere (ri)dimostrato usando le matrici. Infatti per $\alpha \in \mathbb{R}$ la rotazione r_α in senso antiorario intorno all'origine di angolo α è data da

$$r_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

Mentre la simmetria s_α rispetto ad una retta che passa per l'origine e forma un angolo α con l'asse positivo delle ascisse e data da

$$s_\alpha = \begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}.$$

Quindi i seguenti fatti seguono facilmente.

1. $r_\alpha \circ r_\beta = r_\beta \circ r_\alpha = r_{\alpha+\beta}$;
2. $s_\alpha \circ s_\beta = r_{2(\alpha-\beta)}$;
3. $r_\alpha \circ s_\beta = s_{\frac{\alpha}{2}+\beta}$.

2.2 Il gruppo delle permutazioni

SI VEDANO GLI APPUNTI PRESI IN CLASSE

2.3 Esercizi

Esercizio 2.1 Si descrive il gruppo dell'isometrie del piano che fissano un rettangolo (che non sia un quadrato).

Esercizio 2.2 Sia $G = D_n$, $n \geq 3$, il gruppo diedrale. Determinare il sottoinsieme $S \subset G$ costituito da tutti gli elementi di ordine 2 se n dispari solo le n riflessioni; se n pari tutte le riflessione e $r^{\frac{n}{2}}$

Esercizio 2.3 Sia f la permutazione di S_{12} data da

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 6 & 7 & 10 & 12 & 9 & 4 & 3 & 11 & 8 & 2 & 1 \end{pmatrix}.$$

Si scriva la decomposizione in cicli disgiunti di f, f^2, f^3 e f^5 e si calcolino gli ordini di queste permutazioni.

Esercizio 2.4 Siano f e g la permutazioni di S_{10} definite come segue:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 5 & 7 & 9 & 8 & 10 & 6 & 3 & 1 \end{pmatrix} \text{ e } g = (23).$$

Si trovi la decomposizione in cicli disgiunti delle permutazioni $f, g, f \circ g$ e $g \circ f$ e si calcolino gli ordini di queste permutazioni.

Esercizio 2.5 Dimostrare che due cicli σ e τ della stessa lunghezza sono coniugati, cioé esiste una permutazione f tale che $f^{-1} \circ \sigma \circ f = \tau$.

Esercizio 2.6 Sia σ un ciclo di lunghezza l e $k \in N_+$ tale che $\sigma^k \neq id$. Mostrare che esistono t cicli disgiunti $\sigma_1, \ldots, \sigma_t$ tutti della stessa lunghezza m, tali che $l = mt$ e

$$\sigma^k = \sigma_1 \circ \cdots \circ \sigma_t. \tag{2.6}$$

Mostrare, inoltre che $m = \frac{l}{(k,l)}$ e $t = (k, l)$. (Suggerimento: usare il fatto che $\text{supp}(\sigma^k) = \text{supp}(\sigma)$, il teorema fondamentale delle permutazioni e che se $\sigma = (a_1 \ldots a_l)$ allora $\sigma^k = (a_1 \ldots a_l)^k = (a_i \ldots a_l a_1 \ldots a_{i-1})^k$, per ogni $1 \leq i \leq l$. Per l'ultima parte si calcolino gli ordini di σ^k e $\sigma_1 \circ \cdots \circ \sigma_t$).

Esercizio 2.7 Mostrare che se $\sigma_1, \ldots, \sigma_t$ sono cicli disgiunti tutti della stessa lunghezza m allora esiste un ciclo σ di lunghezza $l = mt$ e $k \in N_+$ tali che $\sigma^k = \sigma_1 \circ \cdots \circ \sigma_t$. (Suggerimento: se $\sigma_j = (a_{j1} \cdots a_{jm})$, $j = 1, \ldots, t$, si definisca

$$\sigma = (a_{11}a_{21} \ldots a_{t1}a_{12}a_{22} \cdots a_{t2} \cdots a_{1m}a_{2m} \cdots a_{tm})$$

e si verifichi che $\sigma^t = \sigma_1 \circ \cdots \circ \sigma_t$.).

Esercizio 2.8 Dimostrare che S_n é generato da $\{A_n, \tau\}$ dove τ é una trasposizione arbitraria.

Esercizio 2.9 Sia σ un ciclo di lunghezza l. Dimostrare che

1. σ^2 é un ciclo se e solo se l é dispari;
2. se l é dispari allora σ é il quadrato di un ciclo di lunghezza l;
3. se l é pari, $l = 2m$, allora σ^2 é il prodotto di due cicli di lunghezza m;
4. se $l = tm$, allora σ^t é il prodotto di t cicli di lunghezza m;
5. se l é un numero primo allora ogni potenza di σ é un ciclo.

(Suggerimento: usare l'Esercizio 2.6).

Esercizio 2.10 Il cubo di Rubik puó essere visto come un gruppo algebrico $\mathcal{R}$, dove le operazioni sono rappresentate dalle mosse che si possono eseguire sulle facce del cubo (si veda anche wikipedia) Piú precisamente $\mathcal{R}$ é generato dalle seguenti mosse di base.

- U: Rotazione di 90 gradi della faccia superiore (Upper) in senso orario;
- D: Rotazione di 90 gradi della faccia inferiore (Down) in senso orario;
- L: Rotazione di 90 gradi della faccia sinistra (Left) in senso orario;
- R: Rotazione di 90 gradi della faccia destra (Right) in senso orario;
- F: Rotazione di 90 gradi della faccia frontale (Front) in senso orario;
- B: Rotazione di 90 gradi della faccia posteriore (Back) in senso orario.

1. Calcolare l'ordine di ogni mossa di base;
2. Calcolare l'ordine degli elementi RU e RU^{-1};
3. Dimostrare che la permutazione dei 20 cubetti del cubo di Rubik (8 angoli e 12 spigoli) indotta da una qualunque mossa é di classe pari.

Capitolo 3

Sottogruppi e classi laterali

SI VEDANO GLI APPUNTI PRESI IN CLASSE

3.1 Ordine del prodotto di due elementi

Proposizione 3.1.1 *Sia G un gruppo $x, y \in G$, $o(x) = m$ e $o(y) = n$ tali che $(m, n) = 1$. Se x e y commutano allora $o(xy) = mn = [m, n]$ ($[m, n]$ denota il minimo comune multiplo tra m e n).*

Dimostrazione: Il fatto che x e y commutano implica che

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1$$

dalla quale segue che $k := o(xy)|[m, n] = mn$. Osserviamo che $(m, n) = 1$ implica $< x > \cap < y >= \{1\}$ (se $z \in < x > \cap < y >$ allora $o(z)|m$ e $o(z)|n$ e quindi $o(z)|(m, n) = 1$ e $o(z) = 1$ ossia $z = 1$). Allora $(xy)^k = x^k y^k = 1$ ossia $x^k = y^{-k} \in < x > \cap < y >= \{1\}$ e quindi $x^k = y^k = 1$. Quindi $m|k$ e $n|k$ e $mn = [m, n]|k$ da cui $k = [m, n]$. □

Corollario 3.1.2 *Sia G un gruppo $x, y \in G$, $o(x) = m$ e $o(y) = n$. Se x e y commutano allora esiste $z \in G$ tale che $o(z) = [m, n]$.*

Dimostrazione: Esistono due interi positivi m' e n' tali che

$$m'|m,\ n'|n,\ (m', n') = 1,\ m'n' = [m, n].$$

Infatti se $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ e $n = p_1^{\beta_1} \cdots p_t^{\beta_t}$ possiamo scegliere

$$m' = \prod_{i, \alpha_i \geq \beta_i} p_i^{\alpha_i},\ n' = \prod_{i, \beta_i > \alpha_i} p_i^{\beta_i}.$$

Osserviamo che $o(x^{\frac{m}{m'}}) = m'$, $o(y^{\frac{n}{n'}}) = n'$, $(m', n') = 1$ e $[x^{\frac{m}{m'}}, y^{\frac{n}{n'}}] = 1$. Segue dalla Proposizione 3.1 che se $z = x^{\frac{m}{m'}} y^{\frac{n}{n'}}$

$$o(z) = o(x^{\frac{m}{m'}}) o(y^{\frac{n}{n'}}) = m'n' = [m, n].$$

□

Osservazione 3.1.3 I risultati precedenti non valgono se gli elementi non commutano. Per esempio in S_3 gli elementi $x = (12)$ e $y = (123)$ hanno ordini primi ($o(x) = 2$ e $o(y) = 3$), $xy = (23)$ e $o(xy) = o((23)) = 2 \neq 6 = [2, 3]$. Anche se gli elementi commutano ma gli ordini non sono primi il risultato non vale. per esempio la classe $[2]_4 \in \mathbb{Z}_4$ ha ordine due, commuta con se stessa ma l'ordine di $[0]_4 = [2]_4 + [2]_4$ é 1. Si dimostra (noi non lo faremo) che dati m, n, r numeri naturali diversi da 1 esiste sempre un gruppo finito G e $x, y \in G$ tali che $o(x) = m$, $o(y) = n$ e $o(xy) = r$.

3.2 Esercizi

Esercizio 3.1 Dire quali dei seguenti insiemi H sono sottogruppi del gruppo G indicato:

1. $G = (\mathbb{R}, +)$, $H = \{\ln a \mid a \in \mathbb{Q},\ a > 0\}$;
2. $G = (\mathbb{R}, +)$, $H = \{\ln n \mid n \in \mathbb{Z},\ n > 0\}$;
3. $G = (\mathbb{R}, +)$, $H = \{x \in \mathbb{R} \mid \tan x \in \mathbb{Q}\}$;
4. $G = (\mathbb{R}^*, \cdot)$, $H = \{2^n 3^m \mid m, n \in \mathbb{Z}\}$;
5. $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) \mid y = 2x\}$.

Esercizio 3.2 Si consideri l'insieme $G = \{(a, b) \mid a, b \in \mathbb{Q}, a \neq 0\}$ con l'operazione binaria definita da

$$(a, b) \cdot (c, d) = (ac, ad + b).$$

Dopo aver verificato che $(G, \cdot)$ é un gruppo, si verifichi che $H = \{(a, b) \mid a \in \mathbb{Q}^*\} < G$.

Esercizio 3.3 Sia X un insieme e sia Δ_X la differenza simmetrica, cioé l'operazione su $\mathcal{P}(X)$ definita da:

$$A, B \in \mathcal{P}(X), A\Delta_X B = (A \setminus B) \cup (B \setminus A).$$

Si dimostri che $(\mathcal{P}(X), \Delta_X)$ é un gruppo abeliano. Sia $Y \subseteq X$. Si dimostri che $(\mathcal{P}(Y), \Delta_Y) \leq (\mathcal{P}(X), \Delta_X)$.

Esercizio 3.4 Si dimostri che l'insieme G delle funzioni da $\mathbb{R}$ in $\mathbb{R}$ con l'operazione definita da

$$(f + g)(x) = f(x) + g(x).$$

é un gruppo abeliano e che i seguenti sottoinsiemi sono sottogruppi di G.

1. $C(\mathbb{R}) = \{\text{funzioni continue } f : \mathbb{R} \to \mathbb{R}\}$;
2. $D(\mathbb{R}) = \{\text{funzioni derivabili } f : \mathbb{R} \to \mathbb{R}\}$;
3. $I(\mathbb{R}) = \{\text{funzioni integrabili } f : \mathbb{R} \to \mathbb{R}\}$.

Esercizio 3.5 In ognuno dei casi seguenti mostrare che H é un sottogruppo di S_X.

1. $X = \{x \in \mathbb{R} \mid x \neq 0, 1\}$, $H = \{id, f, g\}$, dove $f(x) = \frac{1}{1-x}$, $g(x) = \frac{x-1}{x}$;
2. $X = \{x \in \mathbb{R} \mid x \neq 0\}$, $H = \{id, f, g, h\}$, dove $f(x) = \frac{1}{x}$, $g(x) = -x$ $h(x) = -\frac{1}{x}$;
3. $X = \{x \in \mathbb{R} \mid x \neq 0, 1\}$, $H = \{id, f, g, h, j, k\}$, dove $f(x) = 1 - x$, $g(x) = \frac{1}{x}$, $h(x) = -\frac{1}{1-x}$, $j(x) = -\frac{x-1}{x}$ e $k(x) = -\frac{x}{x-1}$.

Esercizio 3.6 Per ogni coppia di numeri reali a, b, $a \neq 0$, si definisca la funzione $f_{a,b} : \mathbb{R} \to \mathbb{R}$. Si dimostri che:

1. $f_{a,b} \in S_{\mathbb{R}}$;
2. $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$;
3. $f_{a,b}^{-1} = f_{a^{-1},-ba^{-1}}$;
4. $H = \{f_{a,b} \mid a \in \mathbb{R}, b \in \mathbb{R}^*\} < S_{\mathbb{R}}$.

Esercizio 3.7 Sia $G = D_n$, $n \geq 3$, il gruppo diedrale. Dimostrare che G ha esattemente n elementi di ordine 2 se e solo se n é dispari. Nel caso che n sia dispari dimostrare che gli n elementi di G che non hanno ordine 2 formano un sottogruppo abeliano di G.

Esercizio 3.8 Sia X un insieme finito e A un sottoinsieme di X. Sia H il sottoinsieme di S_X che consiste di tutte le permutazioni $f \in S_X$ tale che $f(x) \in A$, per ogni $x \in A$.

1. Dimostrare che $H < S_X$;
2. Fornire un esempio dove la conclusione del punto precedente non vale se X é un insieme infinito.

Esercizio 3.9

(1) Dimostrare che l'insieme delle trasposizioni di S_n genera S_n;

(2) Dimostrare che l'insieme $\{(12), (13), \ldots, (1n)\}$ genera S_n;

(3) Dimostrare che i cicli di lunghezza 3 generano A_n, for $n \geq 3$;

(4) Dimostrare che l'insieme $\{(123), (124), \ldots, (12n)\}$ genera A_n;

(5) Dimostrare che S_n é generato da $\{(12), (12 \ldots n)\}$.

(Suggerimento: per (3) usare $(13)(12) = (123)$ e $(12)(34) = (321)(134)$; per (4) usare $(abc) = (1ca)(1ab)$, $(1ab) = (1b2)(12a)(12b)$ e $(1b2) = (12b)^2$; per (5) usare $(1 \dots n)(12)(1 \dots n)^{-1} = (23)$ e $(12)(23)(12) = (13)$).

Esercizio 3.10 Siano H e K sottogruppi di un gruppo finito G tali che $H \leq K \leq G$. Si dimostri che $[G : H] = [G : K][K : H]$.

Capitolo 4

Sottogruppi normali e quozienti

SI VEDANO GLI APPUNTI PRESI IN CLASSE

4.1 Sottogruppi del gruppo lineare

Sia $\mathbb{K}$ un campo arbitrario $n \geq 1$ we consideriamo $\mathrm{GL}_n(\mathbb{K}) \subset M_n(\mathbb{K})$.

Esempio 4.1.1 Il gruppo lineare speciale

$$\mathbb{SL}_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \mid \det A = 1\} \triangleleft \mathrm{GL}_n(\mathbb{K})$$

Esempio 4.1.2

$$T_n^+(\mathbb{K}) = \{\text{triang. sup. inv. } A = (a_{ij}), a_{ij} = 0, \forall i > j\} < \mathrm{GL}_n(\mathbb{K}).$$

Siano $A = (a_{ik}), B = (b_{kj}) \in T_n^+(\mathbb{K})$ quindi $a_{ik} = 0$ se $i > k$ e $b_{kj} = 0$ se $k > j$ (ovviamente $a_{ii} \neq 0$ e $b_{ii} \neq 0$ essendo A e B invertibili). Sia $AB = (c_{ij} = \sum_{k=1}^n a_{ik}b_{kj})$. Supponiamo $i > j$ e mostriamo $c_{ij} = 0$: se $i > k$ allora $a_{ik} = 0$ se invece $j < i \leq k$, ossia $k > j$ allora $b_{kj} = 0$ e quindi $c_{ij} = 0$ se $i > j$; per dimostrare che se $A \in T_n^+(\mathbb{K})$ allora $A^{-1} \in T_n^+(\mathbb{K})$.

Osserviamo che: *una matrice T è triangolare (non necessariamente invertibile) se e solo se $T(S_k) \subset S_k$ per ogni $k = 1, \ldots, n$ dove $S_k =< e_1, \ldots e_k >$, $\{e_1, \ldots, e_n\}$ è la base canonica di $\mathbb{K}^n$.* segue che: *$A \in T_n^+(\mathbb{K})$ se e solo se $A(S_k) \subset S_k$ per ogni $k = 1, \ldots, n$.*

Quindi se $s' \in S_k$ esiste $s' \in S_k$ take che $As' = s$ ossia $A^{-1}s = s'$ e quindi $A^{-1}(S_k) \subset S_k$ e quindi $A^{-1} \in T_n^+(\mathbb{K})$.

Osserviamo che $T_n^*(\mathbb{K})$ non è normale in $\mathrm{GL}_n(\mathbb{K})$, $\forall n \geq 2$ e $\forall \mathbb{K}$.

Infatti

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}^{-1}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\notin T_2^+(\mathbb{K})$$

Il caso generale per ogni n si ottiene completando opportunamente le matrici.

Lo stesso ragionamento di applica a

$$T_n^-(\mathbb{K})=\{\text{triang sup. inv. } A=(a_{ij}), a_{ij}=0, \forall i<j\}<\underset{n}{\mathrm{GL}}(\mathbb{K})\}$$

Esempio 4.1.3 $D_n(\mathbb{K})=\{\text{matrici diagonali invertibili}\}<\mathrm{GL}_n(\mathbb{K})$. Osserviamo che $D_n(\mathbb{K})$ non è normale se $n\geq 2$ e $|\mathbb{K}|\geq 3$. Siano infatti $a,b\in\mathbb{K}$, $a\neq b$ e non nulli. Allora

$$\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}^{-1}\begin{bmatrix}a & 0\\ 0 & b\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\ -1 & 1\end{bmatrix}\begin{bmatrix}a & 0\\ 0 & b\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}a & 0\\ b-a & b\end{bmatrix}\notin D_2(\mathbb{K})$$

Il caso generale per ogni n si ottiene completando opportunamente le matrici.

Osserviamo che $D_n(\mathbb{K})=T_n^+(\mathbb{K})\cap T_n^-(\mathbb{K})$.

Esempio 4.1.4

$$Z_n(\mathbb{K})=\{\text{matrici scalari invertibili } aI_n, a\neq 0\}\triangleleft\mathrm{GL}_n(\mathbb{K}).$$

In effetti $Z_n(\mathbb{K})=Z(\mathrm{GL}_n(\mathbb{K}))$ dalla quale segue che $\mathrm{GL}_n(\mathbb{K})$ non è abeliano $\forall n\geq 2$ e $\forall\mathbb{K}$. L'inclusione $Z_n(\mathbb{K})\subset Z(\mathrm{GL}_n(\mathbb{K}))$ è chiara. Per dimostrare l'altra inclusione sia E_{ij} $i\neq j$ la matrice $n\times n$ che ha 1 nella posizione ij e 0 in altre posizioni. Allora I_n+E_{ij} è invertibile (il determinante è uguale a 1 e l'inversa è I_n-E_{ij}). Se $A\in Z(GL_n(\mathbb{K}))$ allora $AB_{ij}=B_{ij}A$ e quindi $AE_{ij}=E_{ij}A$. Osserviamo che AE_{rs} è la matrice $n\times n$ con tutte le colonne nulle tranne la colonna s-esima data da dal vettore colonna $(a_{1r}\dots a_{nr})$ mentre $E_{rs}A$ è la matrice $n\times n$ con tutte le righe nulle tranne la riga r-esima data da dal vettore riga $(a_{s1}\dots a_{sn})$. Segue che $a_{ir}=0$ per ogni $i\neq r$ e $a_{rr}=a_{ss}$ per ogni $r,s=1,\dots,n$ ossia $A\in Z(\mathrm{GL}_n(\mathbb{K}))$.

Esempio 4.1.5

$$O_n(\mathbb{K})=\{\text{matrici ortogonali } AA^T=A^TA=I_n\}<\underset{n}{\mathrm{GL}}(\mathbb{K})$$

(semplice verifica usando il fatto che $(A^T)^{-1}=(A^{-1})^T$). $D_n(\mathbb{K})$ non è normale in $\mathrm{GL}_n(\mathbb{K})$ per ogni $n\geq 2$. Infatti

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^{-1}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}-1 & 0\\ 1 & 1\end{bmatrix}\notin O_2(\mathbb{K})$$

Il caso generale per ogni n si ottiene completando opportunamente le matrici.

Esempio 4.1.6 Le matrici simmetriche $S_n(\mathbb{K}) = \{A \mid A^T = A\}$ non sono un sottogruppo di $\mathrm{GL}_n(\mathbb{K})$. Per esempio

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\notin S_2(\mathbb{K})$$

Osserviamo che $(S_n(\mathbb{K}),+) < (M_n(\mathbb{K}),+)$

Esempio 4.1.7

$$T_n^+(\mathbb{K})\cap O_n(\mathbb{K}) = \{diag(a_1,\dots a_n), a_j^2 = 1\}.$$

Infatti se $A \in T_n^+(\mathbb{K})$ allora $A^T = A^{-1} \in T_n^+(\mathbb{K}) \cap T_n^{-1}(\mathbb{K})$ e quindi $A = (a_1,\dots a_n) \in D_n(\mathbb{K})$. Usando di nuovo il fatto che $A = (a_1,\dots a_n) \in O_n(\mathbb{K})$ si ottiene che $a_j^2 = a_j, \forall j = 1,\dots,n$.

Esempio 4.1.8 Il gruppo dei quaternioni unitari è definito come.

$$Q_8 = \{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix},\begin{bmatrix}-i & 0\\ 0 & i\end{bmatrix},\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\begin{bmatrix}0 & i\\ i & 0\end{bmatrix},\begin{bmatrix}0 & -i\\ -i & 0\end{bmatrix}\} < \mathrm{GL}_2(\mathbb{C})$$

Indicando $I_2 := \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $I := \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}$, $J := \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$, $K := \begin{bmatrix}0 & i\\ i & 0\end{bmatrix}$ si ottiene $I^2 = J^2 = K^2 = -I_2$, $IJ = K$, $JK = I$, $KI = J$.

Valgono i seguenti fatti di facile verifica

- Q_8 è il più piccolo gruppo non abeliano potenza di un primo.
- Q_8 è il più piccolo gruppo non abeliano in cui tutti i suoi sottogruppi sono normali (i suoi sottogruppi sono (a parte quelli banali) $Z(Q_8) = \{\pm I_2\}$, $< I >, < J >, < K >$ ognuno costituito da 4 elementi).

Osserviamo che Q_8 è unione dei suoi tre sottogruppi propri $Q_8 =< I > \cup < J >=< K >$ anche se non è il più piccolo sottogruppo con questa proprietà (abbiamo visto $\mathbb{Z}_2 \times \mathbb{Z}_2$ è un altro esempio).

Esempio 4.1.9 Il gruppo di Heisenberg è definito come

$$Heis = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\} < \underset{3}{\mathrm{GL}}(\mathbb{Q})$$

La moltiplicazione e l'inversa sono date da

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$$

Si verifica immediatamente che

$$Z(Heis) = \{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mid b \in \mathbb{Z} \}$$

Infatti se $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ commuta con ogni $\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix}$ allora $ac' = a'c, \forall a', c'$ che implica $a = c = 0$.

4.2 Esercizi

Esercizio 4.1 Sia $G = Heis = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\} < \mathrm{GL}_3(\mathbb{Q})$ il gruppo di Heisenberg e sia N l'insieme delle matrici

$$\begin{pmatrix} 1 & 2b & 2c \\ 0 & 1 & 2a \\ 0 & 0 & 1 \end{pmatrix}$$

con $a, b, c \in \mathbb{Z}$. Dimostrare che N é un sottogruppo normale di G.

Esercizio 4.2 Sia $n \in \mathbb{N}_+$ e p un primo. Si calcolino le cardinalitá di $Z(\mathrm{GL}_n(\mathbb{Z}_p))$ e $\mathbb{SL}_n(\mathbb{Z}_p)$.

Esercizio 4.3 Sia G un gruppo finito e H un suo sottogruppo di indice p, con p primo. Supponiamo che esista $x \in G \setminus H$ tale che $xH = Hx$. Dimostrare che H é normale in G. (Suggerimento: si consideri il gruppo $K = \langle x, H \rangle$, si usi l'Esercizio 3.10 per dedurre che $K = G$ e si dimostri che H é normale in K).

Esercizio 4.4 Sia G un gruppo di ordine $|G| = 2n$, $n \geq 2$. Supponiamo che G abbia esattamente n elementi di ordine 2 e che i restanti n elementi formino un gruppo H. Dimostrare che H é un sottogruppo abeliano e normale di G di ordine dispari. (Suggerimento: per dimostrare che H é abeliano, si fissi $s \in G$ di ordine 2, si osservi che sh ha ordine 2 per ogni $h \in H$).

Esercizio 4.5 Sia $Z(G)$ il centro di un gruppo G e $H \leq G$. Si dimostri che

$$Z(G) \subseteq G \cap Z(H)$$

e che l'inclusione puó essere stretta.

Esercizio 4.6 Dimostrare che $o(xy) = o(yx)$ per ogni x, y in un gruppo G. Inoltre se x é l'unico elemento di G che ha ordine k allora $x \in Z(G)$.

Esercizio 4.7 Dimostrare che il centro del gruppo simmetrico S_n é banale per $n \geq 3$. Dedurre che $\mathrm{Inn}(S_n) \cong S_n$, per $n \geq 3$ e che $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$. (Suggerimento: sia $f \in S_n$, $f \neq id$. Allora esistono $i, j \in \{1, 2 \ldots, n\}$ tali che $i \neq j$ e $f(i) = j$. Sia $k = f(j)$. Allora $j \neq k$. Siccome $n \geq 3$ esiste $l \neq j$ e $l \neq k$ e possiamo scegliere la trasposizione $\tau = (jl)$. Allora $(f \circ \tau)(j) = f(l) \neq f(j) = (\tau \circ f)(j)$) (Curiositá: in generale si dimostra che $\mathrm{Aut}(S_n) \cong S_n$ per $n \neq 2, 6$. Per maggiori informazioni, consulta la pagina di Wikipedia su *Automorphisms of the symmetric and alternating groups*).

Esercizio 4.8 Dimostrare che il centro del gruppo alterno A_n é banale per $n \geq 4$. Dedurre che $\mathrm{Inn}(A_n) \cong A_n$, per $n \geq 3$. (Suggerimento: sia $f \in A_n$, $f \neq id$. Allora esistono $i, j \in \{1, 2 \ldots, n\}$ tali che $i \neq j$ e $f(i) = j$. Siccome $n \geq 4$ esistono $k, l \in \{1, 2 \ldots, n\}$, distinti e diversi da i e j. Allora $(f \circ (jkl))(i) = f(i) = j \neq k = ((jkl) \circ f)(i)$).

Esercizio 4.9 Sia $D_n = \{1, r, \ldots, r^{n-1}, rs, \ldots, r^{n-1}s\}$ il gruppo diedrale, $n \geq 3$. Dimostrare che $Z(D_n) = \{1\}$ se n é dispari e $Z(D_n) = \{1, r^{\frac{n}{2}}\}$ se n é pari. Dedurre che $\mathrm{Inn}(D_n) \cong D_n$, se n é dispari. (Suggerimento: mostrare preliminarmente che se $x \in Z(D_n)$ allora $x = r^k$ e dedurre che $r^{2k} = \mathrm{id}$).

Esercizio 4.10 Dimostrare che il sottogruppo di S_4 generato da $\{(13), (1234)\}$ é isomorfo al gruppo diedrale D_4. Dedurre che S_4 non é generato da $\{(13), (1234)\}$ (cfr. Esercizio 3.9 del Capitolo 3). (Curiositá: si dimostra che S_n é generato da $\{(ab), (12 \ldots n)\}$ se solo se $b - a$ é coprimo con n. Lo studente interessato potrá consultare: https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf per dettagli e altri risultati collegati).

Capitolo 5

Omomorfismi e isomorfismi

SI VEDANO GLI APPUNTI PRESI IN CLASSE

5.1 Esercizi

Esercizio 5.1 Sia G l'insieme $\{\mathbb{R} \mid x \neq -1\}$ con l'operazione $x \cdot y = x + y + xy$. Dimostrare che $f(x) = x - 1$ é un isomorfismo tra $\mathbb{R}^*$ e G.

Esercizio 5.2 Dimostrare i seguenti fatti.

1. Il gruppo $(\mathbb{R}/\mathbb{Z}, +)$ é isomorfo al gruppo $(S^1, \cdot)$, dove S^1 é l'insieme dei numeri complessi di modulo unitario;
2. Sia $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$, $n > 1$ l'insieme delle radici n-esime dell'unitá. Allora U_n é un sottogruppo di S^1 isomorfo a $\mathbb{Z}_n$;
3. Sia $u \in U_n$, $n \geq 3$ e $u \neq 1$ e siano $r, s \in \mathrm{Aut}(\mathbb{C}^*)$ definiti come $r(z) = uz$ e $s(z) = \bar{z}$ per ogni $z \in \mathbb{C}^*$. Dimostrare che il gruppo diedrale D_n é isomorfo al sottogruppo di $\mathrm{Aut}(\mathbb{C}^*)$ generato da r e s.

Esercizio 5.3 Sia $S^3 = \{(\alpha, \beta) \in \mathbb{C}^2 \mid |\alpha|^2 + |\beta|^2 = 1\}$ e sia

$$\cdot : S^3 \times S^3 \to S^3, ((\alpha, \beta), (\gamma, \delta)) \mapsto (\alpha, \beta) \cdot (\gamma, \delta) = \left(\alpha\gamma - \beta\bar{\delta}, \alpha\delta + \beta\bar{\gamma}\right).$$

1. Dimostrare che $(S^3, \cdot)$ é un gruppo non abeliano;
2. Dimostrare che

$$SU(2) = \left\{ A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \in GL_2(\mathbb{C}) \mid \det A = 1 \right\}$$

é un sottogruppo di $\mathrm{GL}_2(\mathbb{C})$ isomorfo a $(S^3, \cdot)$.

Esercizio 5.4 Dimostrare che $\mathbb{Z}$ non é isomorfo a $\mathbb{Q}$.

Esercizio 5.5 Dimostrare che i gruppi $(\mathbb{Q}, +)$ (risp. $(\mathbb{R}, +)$) e $(\mathbb{Q}^*, \cdot)$ ((risp. $(\mathbb{R}^*, +)$)) non son isomorfi.

Esercizio 5.6 Dimostrare che $\mathbb{R}$ é isomorfo a $\mathbb{R}^+$ ma $\mathbb{Q}$ non é isomorfo a $\mathbb{Q}^+$.

Esercizio 5.7 Siano G e H due gruppi e sia X un insieme di generatori di G. Se per ogni coppia di omomorfismi $f, g : G \to H$ si ha che $f(x) = g(x)$ per ogni $x \in X$, si dimostri che $f = g$.

Esercizio 5.8 Siano G e H gruppi finiti e $f : G \to H$ un omomorfismo. Si dimostri che:

1. per ogni $x \in G$ si ha che $o(f(x))$ divide $o(x)$;

2. se $o(f(x)) = o(x)$ per ogni $x \in G$, allora f é iniettivo.

Dedurre da (1) che se N é un sottogruppo normale di un gruppo G allora $o(xN)$ divide $o(x)$, per ogni $x \in G$.

Esercizio 5.9 Sull'insieme $G = \mathbb{Z}_2 \times \{-1, 1\}$ si definisca un'operazione binaria ponendo per ogni $(x, u), (y, v) \in G$

$$(x, u) \cdot (y, v) = (x + uy, uv).$$

1. Si dimostri che G con questa operazione é un gruppo non abeliano;

2. Si trovi un sottogruppo di G che non é normale.

Esercizio 5.10 Sia $\langle \pi \rangle$ il sottogruppo di $(\mathbb{R}^*, \cdot)$ generato da π. Dimostrare che nel quoziente $\mathbb{R}^*/\langle \pi \rangle$ ci sono $\varphi(n)$ elementi di ordine n se n é dispari e $2\varphi(n)$ elementi di ordine n se n é pari, dove $\varphi(n)$ é la funzione di Eulero. (Suggerimento: poniamo $N = \langle \pi \rangle$ e sia $xN \in \mathbb{R}^*/N$ un elemento di ordine n. Allora $x^n = \pi^m$, per un certo numero naturale m. Dimostrare che si puó supporre $m < n$ e che m non divide n).

Capitolo 6

Prodotto diretto di gruppi

SI VEDANO GLI APPUNTI PRESI IN CLASSE

6.1 Struttura dei gruppi di ordine 6, 8 e p^2 con p primo

Proposizione 6.1.1 *Sia G un gruppo tale che $|G| = 6$. Allora G è isomorfo a $\mathbb{Z}_6$ oppure a S_3.*

Dimostrazione: Consideriamo due casi distinti.
Caso 1: Esiste un elemento di ordine 6.
Se esiste $x \in G$ tale che $o(x) = 6$, allora $G \cong \mathbb{Z}_6$. Possiamo costruire un isomorfismo esplicito tra G e $\mathbb{Z}_6$ con l'applicazione:

$$x^n \mapsto [n]_6 \quad \text{per} \quad n = 1, \ldots, 6.$$

Caso 2: non esiste un elemento di ordine 6
Supponiamo ora che non esista un elemento di ordine 6 in G. Tutti gli elementi diversi da 1 devono avere ordine 2 o 3. Mostriamo che esistono $a, b \in G$ tali che $o(a) = 2$ e $o(b) = 3$ utilizzando un metodo di eliminazione.

Contraddizione con tutti gli elementi di ordine 2: Supponiamo per assurdo che tutti gli elementi diversi da 1 abbiano ordine 2. Allora:

$$G = \{1, x, y, z, t, u\},$$

dove $o(x) = o(y) = o(z) = o(t) = o(u) = 2$. In questo caso, G è abeliano. Inoltre, xy non può essere uguale ne a x ne a y (perchè x e y sono diversi da 1).

Senza ledere alla generalità, possiamo supporre $xy = z$. Allora $y = xz = zx$ e $x = zy = yz$. Segue che $H = \{1, x, y, z\}$ è un sottogruppo di G. Applicando il teorema di Lagrange, non può esistere un sottogruppo di ordine 4 in un gruppo di ordine 6, ottenendo così una contraddizione.

Contraddizione con tutti gli elementi di ordine 3
Supponiamo ora che tutti gli elementi diversi da 1 abbiano ordine 3. Sia $x \in G$ con $o(x) = 3$. Allora $1, x, x^2$ sono tutti e tre distinti. Consideriamo un altro elemento $y \in G$ distinto da $1, x, x^2$. Non è difficile vedere che che $y^2 \notin \{1, x, x^2, y\}$. Infatti $y^2 \neq 1$ ($o(y) = 3$), $y^2 \neq x$, altrimenti $1 = y^3 = yx$ e $y = x^2$, $y^2 \neq x^2$, altrimenti $1 = y^3 = yx^2$ e quindi $x = y$, $y^2 \neq y$, altrimenti $y = 1$.

Segue che l'insieme $\{1, x, x^2, y, y^2\}$ è costituito da 5 elementi distinti. Esiste quindi $z \in G$ tale che $G = \{1, x, x^2, y, y^2, z\}$. La contraddizione nasce dal fatto che $z^2 \notin G$. Infatti $z^2 \neq 1$ (o(z)=3), $z^2 \neq x$, altrimenti $1 = z^3 = z^2x$ e quindi $x = z$, $z^2 \neq x^2$, altrimenti $1 = z^3 = zx^2$ e $x = z$, $z^2 \neq y$, altrimenti $1 = z^3 = zy$ e $z = y^2$, $z^2 \neq y^2$; altrimenti $1 = z^3 = zy^2$ e $z = y$.

Conclusione della dimostrazione
Dunque, esistono $a, b \in G$ con $o(a) = 2$ e $o(b) = 3$. Possiamo supporre che G non sia abeliano. Se infatti lo fosse allora $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Con un ragionamento simile a quelli fatti in precedenza si dimostra che gli elementi $1, a, b, b^2, ab, ab^2$ sono distinti e che quindi.

$$G = \{1, a, b, b^2, ab, ab^2\}.$$

Inoltre il fatto che G non è abeliano implica che $ab \neq ba$. Ora, con una semplice ispezione di tutti i casi possibili si verifica che $ab^2 = ba$ e $b^2a = ab$. Allora si costruisce un isomorfismo tra G e S_3 come segue: $1 \mapsto id$, $a \mapsto (12)$, $b \mapsto (123)$, $b^2 \mapsto (132)$, $ab \mapsto (23)$, $b \mapsto (13)$. □

Corollario 6.1.2 *Il gruppo alterno A_4 non ha sottogruppi di ordine 6 (nonostante $6 \mid 12 = |A_4|$).*

Dimostrazione: Osserviamo che

$$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Supponiamo per assurdo che esista un sottogruppo $H < A_4$ tale che $|H| = 6$. Per i risultati precedenti, H dovrebbe essere isomorfo a $\mathbb{Z}_6$ oppure a S_3.

Consideriamo prima la possibilità che $H \cong \mathbb{Z}_6$. In A_4, non ci sono elementi di ordine 6. Infatti, gli ordini degli elementi di A_4 sono:

- 1 (l'identità),
- 2 (le permutazioni prodotto di due trasposizioni disgiunte),
- 3 (i 3-cicli).

Poiché nessun elemento di A_4 ha ordine 6, non può esistere un sottogruppo isomorfo a $\mathbb{Z}_6$.

Consideriamo ora la possibilità che H sia isomorfo a S_3. Un sottogruppo isomorfo a S_3 dovrebbe contenere 3 elementi di ordine 2 e 2 elementi di ordine 3. Tuttavia, un sottogruppo H di A_4 può contenere al più un elemento di ordine 2. Infatti, se H avesse almeno due elementi a e b di ordine 2, questi sarebbero necessariamente il prodotto di due trasposizioni disgiunte. Il loro prodotto $ab = c$ sarebbe ancora una permutazione prodotto di due trasposizioni disgiunte, diversa sia da a sia da b. Questo implicherebbe che l'insieme $\{1, a, b, c\}$ formerebbe un sottogruppo di H contenente 4 elementi, in contraddizione con il Teorema di Lagrange. □

Teorema 6.1.3 *Sia G un gruppo di 8 elementi. Allora G è isomorfo a uno dei seguenti cinque gruppi:*

$$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ D_4,\ Q_8.$$

Dimostrazione: Se esiste $x \in G$ tale che $o(x) = 8$, allora $G \cong \mathbb{Z}_8$.

Supponiamo che tutti gli elementi di G abbiano ordine 2. Allora G è abeliano. Siano a e b due elementi distinti e diversi da 1, e sia $c \in G$ distinto da 1, a, b, e ab (con $ab \neq 1$, poiché $a \neq b^{-1} = b$). Si può facilmente verificare che

$$G = \{1, a, b, c, ab, ac, bc, abc\},$$

poiché, ad esempio, se $ac = b$, allora $a^2c = c = ab$, ma $c \neq ab$. La tavola di moltiplicazione risulta chiara sfruttando il fatto che G è abeliano e che tutti gli elementi hanno ordine 2. Inoltre un ismorfismo tra G e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ è dato da: $1 \mapsto (0,0,0)$, $a \mapsto (1,0,0)$, $b \mapsto (0,1,0)$, $c \mapsto (0,0,1)$, $ab \mapsto (1,1,0)$, $ac \mapsto (1,0,1)$, $bc \mapsto (0,1,1)$, $abc \mapsto (1,1,1)$.

Sia ora $a \in G$ tale che $o(a) = 4$ e sia $H = \langle a \rangle = \{1, a, a^2, a^3\}$. Se $b \in G \setminus H$, allora la classe laterale destra $Hb \neq H$ e quindi $|Hb| = 4$, con $H \cap Hb = \emptyset$. Ne segue che:

$$G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}. \tag{6.1}$$

Questa uguaglianza vale per qualunque $b \in G \setminus H$, indipendentemente dall'ordine di b. Inoltre, $ba \neq b$, altrimenti $a = 1$, e $ba \notin H$ poiché $b \notin H$. Ne consegue che si hanno tre possibilità:

1. $ba = ab$
2. $ba = a^2b$
3. $ba = a^3b$

Supponiamo ora che esista $b \in G \setminus H$ tale che $o(b) = 2$ e osserviamo che $ba \neq a^2b$. Infatti, se fosse $ba = a^2b$, avremmo:

$$a = 1a = b^2a = bba = ba^2b = baab = a^2bab = a^4b^2 = 1,$$

in contraddizione con $a \neq 1$. Restano dunque due possibilità: $ba = ab$ oppure $ba = a^3b$.

Se $ba = ab$, allora G è abeliano e, applicando il Teorema del Prodotto ai sottogruppi $\{1, a, a^2, a^3\}$ e $\{1, b\}$, otteniamo $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Un isomorfismo esplicito è dato da:

$$f : G \to \mathbb{Z}_4 \times \mathbb{Z}_2, \quad 1 \mapsto ([0]_4, [0]_2),\ a \mapsto ([1]_4, [0]_2),\ a^2 \mapsto ([2]_4, [0]_2),\ a^3 \mapsto ([3]_4, [0]_2),$$

$$b \mapsto ([0]_4, [1]_2),\ ab \mapsto ([1]_4, [1]_2),\ a^2b \mapsto ([2]_4, [1]_2),\ a^3b \mapsto ([3]_4, [1]_2).$$

Se invece $ba = a^3b$, allora $G \cong D_4$, il gruppo diedrale con 8 elementi. Un isomorfismo esplicito è dato da:

$$f : G \to D_4, \quad 1 \mapsto 1,\ a \mapsto r,\ a^2 \mapsto r^2,\ a^3 \mapsto r^3,\ b \mapsto s,\ ab \mapsto rs,\ a^2b \mapsto r^2s,\ a^3b \mapsto r^3s,$$

poiché $ba = a^3b$ e $sr = r^3s$.

Infine, supponiamo che tutti gli elementi di $G \setminus H$ abbiano ordine 4 e scegliamo un $b \in G \setminus H$ tale che $o(b) = 4$. Dimostriamo che $G \cong Q_8$, il gruppo dei quaternioni. Mostriamo anzitutto che $a^2 = b^2$. Poiché $o(b) = 4$, allora $o(b^2) = 2$, e quindi $b^2 \in G \setminus H$. Siccome in $H = \langle a \rangle$ l'unico elemento di ordine 2 è a^2, segue che $a^2 = b^2$. Inoltre, $ba \neq a^2b = b^2b = b^3$, altrimenti $a = b^2 = a^2$, e quindi $a = 1$. Inoltre, $ab \neq ba$, poiché, se $ab = ba$, avremmo:

$$(ab)^2 = a^2b^2 = a^4 = 1,$$

in contraddizione con il fatto che $ab \in G \setminus H$ e quindi $o(ab) = 4$.

Pertanto, resta solo la possibilità che $ba = a^3b$. In questo caso, l'equazione (6.1) diventa:

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

con le condizioni $a^4 = b^4 = 1$, $a^2 = b^2$, e $a^3b = ba$. Un isomorfismo esplicito è dato da:

$$f : G \to Q_8, \quad 1 \mapsto I_2,\ a \mapsto I,\ a^2 \mapsto -I_2,\ a^3 \mapsto -I,\ b \mapsto J,\ ab \mapsto K,\ a^2b \mapsto -J,\ a^3b \mapsto -K.$$

□

Teorema 6.1.4 *Sia G un gruppo di ordine p^2, con p un numero primo. Allora G è isomorfo a uno dei seguenti due gruppi:*

$$\mathbb{Z}_{p^2}, \quad \mathbb{Z}_p \times \mathbb{Z}_p.$$

Dimostrazione: Per il teorema di Lagrange, gli elementi di G, escluso l'elemento neutro, possono avere ordine p^2 oppure p. Se esiste un elemento di ordine p^2, allora $G \cong \mathbb{Z}_{p^2}$.

Supponiamo ora che tutti gli elementi di G, diversi dall'identità, abbiano ordine p. Allora esistono due elementi $x, y \in G$ con $x \neq y$ e $o(x) = o(y) = p$. Siano $H := \langle x \rangle$ e $K := \langle y \rangle$. Vogliamo mostrare che sono soddisfatte le ipotesi del Teorema Prodotto, ovvero:

- H e K sono sottogruppi normali di G;
- $H \cap K = \{1\}$;
- $G = HK$.

Questo implicherà che $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Mostriamo che $H \lhd G$ (lo stesso ragionamento si applica a K). Se, per assurdo, H non fosse normale in G, allora esisterebbe un $x \in G$ tale che $H^x \neq H$, dove H^x è il coniugato di H tramite x. In tal caso, $H \cap H^x$ sarebbe un sottogruppo proprio di H. Poiché $|H| = p$, l'unico sottogruppo proprio di H è $\{1\}$, quindi $|H \cap H^x| = 1$. Ne consegue che:

$$|H^x H| = \frac{|H^x| \cdot |H|}{|H \cap H^x|} = \frac{p \cdot p}{1} = p^2,$$

quindi $G = H^x H$. In particolare, esistono $h, h' \in H$ tali che $x^{-1}hxh' = x^{-1}$, da cui segue $x = h^{-1}h'^{-1} \in H$, cioè $H^x = H$, in contraddizione con l'assunzione che $H^x \neq H$. Pertanto, $H \lhd G$.

Mostriamo che $H \cap K = \{1\}$: infatti, $H \cap K$ è un sottogruppo di H. Se $H \cap K$ fosse diverso da $\{1\}$, allora $H \subseteq K$, il che è impossibile poiché $x \notin K$. Per il teorema di Lagrange, $|H \cap K| = 1$ e quindi $H \cap K = \{1\}$.

Infine, la condizione $H \cap K = \{1\}$ implica che:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2,$$

e quindi $G = HK$.

Questo dimostra che $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

6.2 Sottogruppi del prodotto diretto di due gruppi

Osserviamo che, in generale, un sottogruppo del prodotto diretto di due gruppi non è il prodotto diretto di due sottogruppi. Ad esempio, se G è un gruppo non banale, il sottogruppo diagonale $D = \langle (x, x) \mid x \in G \rangle$ è un sottogruppo di $G \times G$, che però non è il prodotto diretto di due sottogruppi di G (infatti, $(x, y) \notin D$ se $x \neq y$). Osserviamo che $D \cong G \cong \{1\} \times G \leq G \times G$.

Ci si può quindi chiedere se esista un sottogruppo $A \leq H \times K$ tale che $A \ncong A_1 \times A_2$, dove $A_1 \leq H$ e $A_2 \leq K$. Il seguente esempio mostra che ciò è possibile.

Esempio 6.2.1 Consideriamo l'omomorfismo suriettivo

$$f : S_3 \times S_3 \to \{\pm 1\} \cong \mathbb{Z}_2, \quad (f, g) \mapsto \operatorname{sgn}(f \circ g).$$

Allora il suo nucleo $H = \ker(f) < S_3 \times S_3$ non è isomorfo al prodotto diretto di due sottogruppi di S_3. Infatti, $|H| = 18$ (per il primo teorema di isomorfismo e il teorema di Lagrange), e quindi, se fosse isomorfo al prodotto diretto di due sottogruppi di S_3, l'unica possibilità (a meno dell'ordine) sarebbe $H \cong A_3 \times S_3$.

Osserviamo ora che $((12), (123)) \in A_3 \times S_3$ è un elemento di ordine 6, mentre H non contiene elementi di ordine 6. Infatti, se ci fosse un elemento di ordine 6 in $H < S_3 \times S_3$, dovrebbe essere (a meno dell'ordine) della forma (τ, σ), con τ trasposizione e σ 3-ciclo. Ma $f(\tau \circ \sigma) = \operatorname{sgn}(\tau \circ \sigma) = -1$, quindi $(\tau, \sigma) \notin H$.

Se i gruppi sono finiti e di cardinalità coprime, vale il seguente risultato.

Teorema 6.2.2 *Siano H e K due gruppi tali che $|H| = m$ e $|K| = n$, con $(m, n) = 1$. Allora, per ogni $A \leq H \times K$, esistono $A_1 \leq H$ e $A_2 \leq K$ tali che $A = A_1 \times A_2$.*

Dimostrazione: Siano $A_1 := p_1(A)$ e $A_2 := p_2(A)$, dove p_i sono le proiezioni canoniche. Allora $A \subseteq A_1 \times A_2$, e quindi

$$|A| \mid |A_1 \times A_2| = |A_1| \cdot |A_2|. \tag{6.2}$$

Siccome $|A| \mid |H \times K| = mn$, segue che $|A| = ab$, con $a \mid m$ e $b \mid n$. Ora, $|A_1| \mid m$ (per Lagrange) e $|A_1| \mid |A| = ab$ (per un corollario del primo teorema di isomorfismo). Quindi, $|A_1| \mid \gcd(m, ab) = a$ (in quanto $a \mid m$, $b \mid n$ e $(m, n) = 1$). Analogamente, $|A_2| \mid b$.

Quindi,

$$|A_1 \times A_2| = |A_1| \cdot |A_2| \mid ab. \tag{6.3}$$

Dalle equazioni (6.2) e (6.3) otteniamo $|A| = ab = |A_1 \times A_2|$, da cui $A = A_1 \times A_2$. □

6.3 Automorfismi del prodotto diretto di due gruppi

Teorema 6.3.1 *Siano H e K due gruppi tali che $|H| = m$ e $|K| = n$ con $(m, n) = 1$. Allora, $Aut(H) \times Aut(K) \cong Aut(H \times K)$.*

Dimostrazione: Definiamo l'applicazione

$$\Phi : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \to \mathrm{Aut}(H \times K), \quad (\alpha, \beta) \mapsto \Phi(\alpha, \beta), \quad \Phi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)).$$

I seguenti fatti si verificano facilmente:

1. $\Phi(\alpha, \beta) \in \mathrm{End}(H \times K)$ per ogni $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$.

2. $\Phi(\alpha, \beta) \in \mathrm{Aut}(H \times K)$, per ogni $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$ (ovvero Φ è ben definita): infatti, se $(h, k) \in H \times K$ è tale che

   $$\Phi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) = (1_H, 1_K),$$

   allora, poiché α e β sono iniettive, segue che $(h, k) = (1_H, 1_K)$, e quindi $\Phi(\alpha, \beta)$ è iniettiva, e di conseguenza anche suriettiva.

3. Φ è un omomorfismo di gruppi:

   $$\Phi\left((\alpha_1, \beta_1)(\alpha_2, \beta_2)\right) = \Phi(\alpha_1, \beta_1) \circ \Phi(\alpha_2, \beta_2).$$

4. Φ è iniettivo: $\ker(\Phi) = (\mathrm{id}_H, \mathrm{id}_K)$.

Resta da dimostrare la suriettività di Φ, utilizzando l'ipotesi $(m, n) = 1$.
Sia $\omega \in \mathrm{Aut}(H \times K)$ e definiamo $\omega_1 : H \to H$ come

$$\omega_1(h) = p_1(\omega(h, 1_K)), \quad \forall h \in H, \tag{6.4}$$

e $\omega_2 : K \to K$ come

$$\omega_2(k) = p_2(\omega(1_H, k)), \quad \forall k \in K. \tag{6.5}$$

Mostriamo che $\omega_1 \in \mathrm{Aut}(H)$. Poiché ω_1 è composizione di omomorfismi, si ha $\omega_1 \in \mathrm{End}(H)$. Inoltre:

$$\ker(\omega_1) = \{h \in H \mid \omega_1(h) = p_1(\omega(h, 1_K)) = 1_H\}$$

$$= \{h \in H \mid \omega(h, 1_K) = (1_H, 1_K)\} = \{1_H\},$$

dove l'ultima uguaglianza segue dal fatto che $\omega \in \mathrm{Aut}(H \times K)$. La penultima uguaglianza deriva da:

$$p_2(\omega(h, 1_K)) = 1_K. \tag{6.6}$$

L'omomorfismo $\gamma \in \mathrm{Hom}(H, K)$ definito da $\gamma(h) = p_2(\omega(h, 1_K))$ è banale, ovvero $\gamma(h) = 1_K$ per ogni $h \in H$, cioè $\ker(\gamma) = H$.

Per dimostrarlo, notiamo che, essendo $(m, n) = 1$, esistono $u, v \in \mathbb{Z}$ tali che $um + vn = 1$, e quindi, usando Lagrange:

$$h^{um+vn} = h^{vn} = h.$$

Pertanto:

$$\gamma(h) = \gamma(h^{vn}) = \gamma(h^v)^n = 1.$$

In modo analogo, si dimostra che $\omega_2 \in \mathrm{Aut}(K)$, in quanto composizione di omomorfismi, utilizzando l'uguaglianza

$$p_1(\omega(1_H, k)) = 1_H. \tag{6.7}$$

Quindi, dalle equazioni (6.4), (6.5), (6.6) e (6.7), otteniamo:

$$\Phi(\omega_1, \omega_2)(h, k) = (\omega_1(h), \omega_2(k)) = (\omega_1(h), 1_K)(1_H, \omega_2(k))$$

$$= (p_1(\omega(h, 1_K)), p_2(\omega(1_H, k))) = \omega(h, k),$$

e quindi Φ è suriettiva. □

Osservazione 6.3.2 Senza l'ipotesi $(m, n) = 1$, il teorema non è vero. Ad esempio, $\mathrm{Aut}(\mathbb{Z}_2) \times \mathrm{Aut}(\mathbb{Z}_2)$ è il gruppo banale $\{1\}$, mentre $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, come si verifica facilmente osservando che è un gruppo non abeliano con 6 elementi, oppure costruendo un isomorfismo esplicito.

6.4 Esercizi

Esercizio 6.1 Dimostrare che $(\mathbb{R}^*, \cdot)$ é isomorfo a $\mathbb{R} \times \mathbb{Z}_2$. (Suggerimento: si usi $\mathbb{Z}_2 \cong \{\pm 1, \cdot\}$ e si consideri l'applicazione $\mathbb{R} \times \mathbb{Z}_2 \to R^*, (s, x) \mapsto (-1)^s e^x$).

Esercizio 6.2 Sia G un gruppo e sia $D = \{(x, x) \in G \times G \mid x \in G\}$. Si dimostri che:

1. D é un sottogruppo di $G \times G$;
2. D é normale in $G \times G$ se e solo se G é abeliano.

Esercizio 6.3 Sia G un gruppo e siano N_j, $j = 1, \ldots, r$, sottogruppi normali di G tali che:

1. $N_i \cap N_j = \{1\}, \forall i, j = 1, \ldots, n, i \neq j$;
2. $G = N_1 \ldots N_r$.

Dimostrare con un esempio che G non é isomorfo a $N_1 \times \cdots \times N_r$ (e che quindi il *Teorema prodotto* visto a lezione non si estende in questo modo a piú di due sottogruppi).

Esercizio 6.4 Sia G un gruppo abeliano e $f : G \to G$ un omomorfismo di gruppi tale che $f \circ f = f$. Dimostrare che $G \cong f(G) \times \operatorname{Ker} f$.

Esercizio 6.5 Sia $f_1 : K \to G$ e $f_2 : K \to H$ due omomorfismi e sia

$$F : K \to G \times H,\ x \mapsto (f_1(x), f_2(x)).$$

Dimostrare che:

1. F é un omomorfismo e $p_i \circ F = f_i$, $i = 1, 2$;
2. ogni omomorfismo $\tilde{F} : K \to G \times H$ si ottiene in questo modo cioé gli omomorfismi $f_1 : K \to G$ e $f_2 : K \to H$ dati da $f_i = p_i \circ \tilde{F}$, $i = 1, 2$, danno luogo ad un omomorfismo $F : K \to G \times H$ descritto sopra, che coincide con $\tilde{F}$.

Esercizio 6.6 Sia G un gruppo con 10 elementi. Dimostrare che

$$G = \{1, a, b, b^2, b^3, b^4, ab, ab^2, ab^3, ab^4\},$$

dove $o(a) = 2$ e $o(b) = 5$.

Esercizio 6.7 Sia G come nell'esercizio precedente. Dimostrare che ba non puó essere uguale a: 1, a, b, b^2, b^3, b^4.

Esercizio 6.8 Sia G come nell'Esercizio 6.6 Dimostrare che se $ba = ab$ allora $G \cong \mathbb{Z}_{10}$.

Esercizio 6.9 Sia G come nell'Esercizio 6.6 Dimostrare che $ba \neq ab^2$ e $ba \neq ab^3$.

Esercizio 6.10 Sia G come nell'Esercizio 6.6 Dimostrare che se $ba = ab^4$ allora $G \cong D_5$. Dedurre che un gruppo G di ordine 10 é isomorfo a $\mathbb{Z}_{10}$ oppure a D_5.

Capitolo 7

Gruppi abeliani finiti

7.1 Classificazione dei gruppi ciclici e dei loro sottogruppi

Sia C un gruppo ciclico e denotiamo con $\mathrm{Gen}(C) = \{x \in C \,|\langle x\rangle = C\}$ l'insieme dei generatori di C. Ricordiamo che la funzione di Eulero $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ è definita come

$$\varphi(n) = |\{a \in \mathbb{N} \mid 1 \leq a < n, (a,n) = 1\}|$$

e soddisfa le seguenti proprietà:

- $\varphi(p) = p - 1$ per un primo p;
- $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$;
- $\varphi(ab) = \varphi(a)\varphi(b)$ se $(a,b) = 1$;
- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, allora

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\cdots p_t^{\alpha_t - 1}(p_t - 1) = n\prod_{j=1}^{t}\left(1 - \frac{1}{p_j}\right).$$

Teorema 7.1.1 *(Classificazione dei gruppi ciclici)*
Sia C un gruppo ciclico. Allora si hanno i seguenti casi:

- $C = \{1\}$ *(il gruppo banale), e* $|Gen(C)| = 1$;
- *Se* $|C| = \infty$, *allora* $C \cong \mathbb{Z}$ *e* $|Gen(C)| = 2$;

- *Se $C \neq \{1\}$ e $|C| < \infty$, allora $C \cong \mathbb{Z}_m$ e $|\,Gen(C)| = \varphi(m)$.*

Dimostrazione: Sia $C = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ e consideriamo l'omomorfismo suriettivo di gruppi

$$f : \mathbb{Z} \to C, \quad n \mapsto x^n.$$

Per il primo teorema di isomorfismo, abbiamo $\mathbb{Z}/\ker f \cong C$. Si osserva che $\ker f = m\mathbb{Z}$ con $m \geq 0$. Ci sono quindi tre possibilità:

- Se $m = 1$, allora $C \cong \mathbb{Z}/\mathbb{Z} = \{1\}$;
- Se $m = 0$, allora $C \cong \mathbb{Z}/\{0\} = \mathbb{Z}$;
- Se $m \neq 0, 1$, allora $C \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Per identificare i generatori di C, consideriamo i casi $C = \mathbb{Z}$ e $C = \mathbb{Z}_m$, poiché un isomorfismo induce una bigezione tra i generatori dei due gruppi isomorfi.

Nel primo caso, è chiaro che $\pm 1 \in \mathrm{Gen}(\mathbb{Z})$. Se $a \in \mathrm{Gen}(\mathbb{Z})$, allora $a = \pm 1$ (dato che $1 \notin \langle a \rangle = a\mathbb{Z}$). Di conseguenza, $\mathrm{Gen}(\mathbb{Z}) = \{\pm 1\}$ e $|\,\mathrm{Gen}(\mathbb{Z})| = 2$.

Nel caso $C = \mathbb{Z}_m$, abbiamo $[k]_m \in \mathrm{Gen}(\mathbb{Z}_m)$ se e solo se

$$o([k]_m) = \frac{m}{(m,k)} = m$$

cioè se e solo se $(m, k) = 1$. Quindi

$$\mathrm{Gen}(\mathbb{Z}_m) = \{k \in \mathbb{N}_+ \mid 1 \leq k < m, (m,k) = 1\},$$

e quindi $|\,\mathrm{Gen}(\mathbb{Z}_m)| = \varphi(m)$. □

Teorema 7.1.2 *(Sottogruppi e quozienti di un gruppo ciclico)*

Sia $H \leq C$ un sottogruppo di un gruppo ciclico C. Allora H è ciclico e C/H è ciclico (dato che $H \lhd C$ in quanto C è abeliano). Inoltre, se $|C| < \infty$, per ogni $d \mid |C|$, esiste un unico $H \leq C$ tale che $|H| = d$. Conseguentemente, esiste una corrispondenza biunivoca tra i divisori positivi di $|C|$ e i sottogruppi di C.

Dimostrazione: Per dimostrare che $H \leq C$ è ciclico, possiamo seguire due approcci. Possiamo usare il teorema di classificazione e ridurci a dimostrare che i sottogruppi di $\mathbb{Z}$ e di $\mathbb{Z}_m$ sono ciclici. È noto che i sottogruppi di $\mathbb{Z}$ sono della forma $m\mathbb{Z} = \langle m \rangle$ e i sottogruppi di $\mathbb{Z}_m$ sono della forma $n\mathbb{Z}/m\mathbb{Z} = \langle [n]_m \rangle$ dove $n \mid m$. Oppure possiamo considerare l'omomorfismo suriettivo

$f : \mathbb{Z} \to C = \langle x \rangle, n \mapsto x^n$ e osservare che se $H \leq C$, allora $f^{-1}(H) \leq \mathbb{Z}$ e quindi $f^{-1}(H) = m\mathbb{Z}$ è ciclico, implicando che $H = f(f^{-1}(H))$ è ciclico in quanto immagine di un gruppo ciclico. Inoltre, il quoziente C/H è ciclico, essendo C/H immagine del gruppo ciclico C tramite l'omomorfismo canonico $\pi : C \to C/H$.

Ora, sia $d \mid |C|$. Sia $m_1 = \frac{m}{d}$ e $y = x^{m_1}$. Allora il gruppo ciclico $\langle y \rangle$ ha ordine d (infatti $o(y) = \frac{m}{(m,m_1)} = \frac{m}{m_1} = d$). Mostriamo che se $H \leq C$ con $|H| = d$, allora $H = \langle y \rangle$.

Essendo H ciclico (per la prima parte), possiamo scrivere $H = \langle z \rangle$ con $z \in C$. Supponiamo quindi $1 < k < m$ tale che $z = x^k$. Si ha quindi:

$$\frac{m}{m_1} = d = |H| = |\langle z \rangle| = o(z) = o(x^k) = \frac{m}{(m,k)}.$$

Da ciò segue che $m_1 = (m,k)$. In particolare, $m_1 \mid k$, quindi $k = m_1 k_1$ per un certo k_1. Riscriviamo:

$$z = x^k = x^{m_1 k_1} = (x^{m_1})^{k_1} = y^{k_1}.$$

Pertanto $z \in \langle y \rangle$, il che implica $H \leq \langle y \rangle$. Dato che $|H| = |\langle y \rangle| = d$, otteniamo $H = \langle y \rangle$.

Infine, consideriamo la funzione $F : \{d \in \mathbb{N}^+ \mid d \mid |C|\} \to S_C$ definita dall'insieme dei divisori positivi $d \mid |C|$ all'insieme S_C dei sottogruppi di C, dove $F(d) = H$ è l'unico sottogruppo di C tale che $|H| = d$. L'applicazione F è ben definita (per la prima parte) e iniettiva. Inoltre, F è suriettiva: dato $H \leq C$, per Lagrange abbiamo $d = |H| \mid |C|$, quindi $F(d) = H$. □

Osservazione 7.1.3 *Osserviamo che se m, n sono naturali tali che $n \mid m$, allora*

$$\mathbb{Z}_m/(n\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}_n.$$

Infatti, $|n\mathbb{Z}/m\mathbb{Z}| = \frac{m}{n}$ e $|\mathbb{Z}/m\mathbb{Z}/n\mathbb{Z}/m\mathbb{Z}| = \frac{m}{\left(\frac{m}{n}\right)} = n$. Essendo $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z})$ un gruppo ciclico finito, è isomorfo a $\mathbb{Z}_n$ (per il Teorema 7.1.2).

Corollario 7.1.4 *Sia K un sottogruppo ciclico e normale di un gruppo G. Allora ogni sottogruppo H di K è normale in G.*

Dimostrazione: Se $K = \langle x \rangle$ e sia $y \in G$, dato che K è normale in G, abbiamo $y^{-1}xy = x^m$ per un certo intero m. Inoltre, se $H = \langle x^k \rangle$ per un certo intero k, segue che

$$y^{-1}x^k y = (y^{-1}xy)^k = (x^m)^k = (x^k)^m \in H.$$

Poiché y è arbitrario, deduciamo che H è normale in G. □

Corollario 7.1.5 *Sia G un gruppo arbitrario con solo sottogruppi banali. Allora G è ciclico di ordine primo p.*

Dimostrazione: Se G non fosse ciclico, esisterebbero $x, y \in G$ tali che $y \notin \langle x \rangle$, in contraddizione con l'ipotesi. Quindi G è ciclico. Per il teorema di classificazione, abbiamo $G \cong \mathbb{Z}$ o $G \cong \mathbb{Z}_m$, con $m \geq 2$. Nel primo caso, il sottogruppo $2\mathbb{Z}$ è non banale. Resta quindi il caso $G \cong \mathbb{Z}_m$. Se m non fosse primo, $m = rs$ con $r, s > 1$. Allora, per il teorema precedente, esisterebbe un sottogruppo non banale di ordine r, in contraddizione con l'ipotesi. □

7.2 Prodotti diretti di gruppi ciclici

Consideriamo i gruppi ciclici C_1 e C_2. Se uno dei due gruppi è banale, allora $C_1 \times C_2 \cong C_2$ (o $C_1 \cong C_1$), e di conseguenza $C_1 \times C_2$ è ciclico se e solo se C_1 (o C_2) è ciclico.

Nel caso in cui entrambi i gruppi siano non banali, abbiamo il seguente teorema:

Teorema 7.2.1 *(Prodotti diretti di gruppi ciclici) Siano C_1 e C_2 due gruppi ciclici non banali. Allora il loro prodotto diretto $C_1 \times C_2$ è ciclico se e solo se C_1 e C_2 sono ciclici e hanno ordine finito con cardinalità coprime.*

Dimostrazione: Consideriamo i casi in cui C_1 e C_2 non sono entrambi finiti. Se almeno uno dei due gruppi è infinito, abbiamo $C_1 \times C_2 \cong \mathbb{Z} \times \mathbb{Z}$, che non è ciclico. Infatti, se supponiamo per assurdo che $(a, b) \in \mathrm{Gen}(\mathbb{Z} \times \mathbb{Z})$, allora, scegliendo (a, b') con $b' \neq b$, l'equazione $m(a, b) = (a, b')$ implicherebbe $ma = a$ e $mb = b'$, il che non ha soluzioni.

Se, invece, C_1 è finito e C_2 è infinito (o viceversa), allora $C_1 \times C_2 \cong \mathbb{Z}_m \times \mathbb{Z}$ con $m \geq 2$. Se questo prodotto fosse ciclico, dovrebbe essere isomorfo a $\mathbb{Z}$, ma l'elemento $([1]_m, 0) \in \mathbb{Z}_m \times \mathbb{Z}$ ha ordine m, mentre tutti gli elementi di $\mathbb{Z}$ diversi da 0 hanno ordine infinito.

Resta quindi da dimostrare che se $|C_1| = m$ e $|C_2| = n$, allora $C_1 \times C_2$ è ciclico se e solo se C_1 e C_2 sono ciclici e $(m, n) = 1$.

Supponiamo che $C_1 \times C_2$ sia ciclico. Allora C_1 e C_2 devono essere ciclici, essendo isomorfi a sottogruppi di un gruppo ciclico. Inoltre, esiste $z \in C_1 \times C_2$

tale che $o(z) = mn = [o(x), o(y)]$. Ne consegue che mn divide $o(x)o(y)$. D'altra parte, per il teorema di Lagrange, $m = o(x)a$ e $n = o(y)b$ per certi $a, b \in \mathbb{N}_+$. Così, abbiamo $mn = o(x)ao(y)b$ che divide $o(x)o(y)$, il che implica $ab = 1$, quindi $a = 1$ e $b = 1$. Questo implica che $o(x) = m$ e $o(y) = n$, e $mn = [m, n]$ implica che $(m, n) = 1$.

Viceversa, supponiamo che $(m, n) = 1$ e che C_1 e C_2 siano ciclici. Sia $x \in \mathrm{Gen}(C_1)$ e $y \in \mathrm{Gen}(C_2)$, con $o(x) = m$ e $o(y) = n$. Allora $z = (x, y) \in C_1 \times C_2$ ha ordine $o(z) = [o(x), o(y)] = [m, n] = mn$, quindi $z \in \mathrm{Gen}(C_1 \times C_2)$. □

Corollario 7.2.2 *Si ha $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ se e solo se $(m, n) = 1$.*

Corollario 7.2.3 *Il prodotto diretto $C_1 \times \cdots \times C_n$ di n gruppi è ciclico se e solo se ciascun C_i è ciclico e le loro cardinalità sono coprime tra loro.*

7.3 Il gruppo degli automorfismi di un gruppo ciclico

Il gruppo banale è un caso particolare di gruppo ciclico, il cui gruppo degli automorfismi è anch'esso banale. I casi non banali sono trattati dal seguente teorema.

Teorema 7.3.1 *(Automorfismi di un gruppo ciclico) Sia C un gruppo ciclico non banale. Allora:*

- *Se $|C| = \infty$, allora $Aut(\mathbb{Z}) \cong (U(\mathbb{Z}), \cdot) \cong \mathbb{Z}_2$.*
- *Se $|C| = m$, allora $Aut(C) \cong (U(\mathbb{Z}_m), \cdot)$ e $|Aut(C)| = \varphi(m)$.*

Dimostrazione: Se $|C| = \infty$, possiamo assumere, grazie al Teorema 7.1.2, che $C = \mathbb{Z}$. Un automorfismo $f \in \mathrm{Aut}(\mathbb{Z})$ deve mappare generatori in generatori, quindi $f(1) = \pm 1$. Se $f(1) = 1$, abbiamo $f(n) = n$ per ogni $n \in \mathbb{Z}$, il che implica $f = \mathrm{id}_{\mathbb{Z}}$. Se $f(1) = -1$, allora $f(n) = -n$. Ne segue che $\mathrm{Aut}(\mathbb{Z}) = \{\pm \mathrm{id}_{\mathbb{Z}}\}$, quindi $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Se $|C| = m$, possiamo sempre assumere, tramite il Teorema 7.1.2, che $C = \mathbb{Z}_m$ con $m \geq 2$. Osserviamo che $U(\mathbb{Z}_m) = \mathrm{Gen}(\mathbb{Z}_m) = \{[k]_m \in \mathbb{N}_+ \mid 1 \leq k < m,\ (m, k) = 1\}$. Infatti, $k \in U(\mathbb{Z}_m)$ se e solo se esiste $[h]_m \in \mathbb{Z}_m$ tale che $[hk]_m = [1]_m$, il che implica che $m \mid (hk - 1)$ e quindi $hk - ma = 1$ se e solo se $(k, m) = 1$.

Pertanto, per dimostrare il secondo punto, è sufficiente costruire un isomorfismo esplicito tra $\mathrm{Aut}(\mathbb{Z}_m)$ e $U(\mathbb{Z}_m)$.

Sia

$$\Phi : \mathrm{Aut}(\mathbb{Z}_m) \to U(\mathbb{Z}_m), \quad f \mapsto f([1]_m).$$

Questa applicazione è ben definita poiché un automorfismo $f \in \mathrm{Aut}(\mathbb{Z}_m)$ induce una bigezione tra $\mathrm{Gen}(\mathbb{Z}_m)$ e se stesso. Verifichiamo ora che Φ è un omomorfismo di gruppi: se $f, g \in \mathrm{Aut}(\mathbb{Z}_m)$ tali che $f([1]_m) = [h]_m$ e $g([1]_m) = [k]_m$, allora

$$\Phi(g \circ f) = (g \circ f)([1]_m) = g(f([1]_m)) = g([h]_m) = g(h[1]_m) = hg([1]_m) = [h]_m[k]_m = [hk]_m = \Phi(g)\Phi(f).$$

Inoltre, Φ è iniettivo:

$$\ker \Phi = \{f \in \mathrm{Aut}(\mathbb{Z}_m) \mid \Phi(f) = f([1]_m) = [1]_m\} = \{f \in \mathrm{Aut}(\mathbb{Z}_m) \mid f([a]_m) = [a]_m,\ \forall [a]_m \in \mathbb{Z}_m\} = \{\mathrm{id}_{\mathbb{Z}_m}\}$$

Mostriamo infine che Φ è suriettivo. Per ogni $n \in \mathbb{N}$, consideriamo l'applicazione $\psi_n : \mathbb{Z}_m \to \mathbb{Z}_m,\ [a]_m \mapsto [na]_m$. Questa è un omomorfismo:

$$\psi_n([a]_m + [b]_m) = [n(a+b)]_m = [na]_m + [nb]_m = \psi_n([a]_m) + \psi_n([b]_m).$$

Inoltre, se $(n, m) = 1$, allora $\psi_n \in \mathrm{Aut}(\mathbb{Z}_m)$. Verifichiamo che ψ_n è iniettivo se $(n, m) = 1$:

$$\ker \psi_n = \{[a]_m \mid \psi_n([a]_m) = [na]_m = [0]_m\} = \{[a]_m \mid m \mid na\} = \{[a]_m \mid m \mid a\} = \{[0]_m\}.$$

Segue che $\psi_n \in \mathrm{Aut}(\mathbb{Z}_m)$ e $\Phi(\psi_n) = \psi_n([1]_m) = [n]_m$, il che implica che Φ è suriettiva. □

Esempio 7.3.2 Calcoliamo $\mathrm{Aut}(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$. Tutti gli elementi di questo gruppo hanno ordine 2, quindi $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Osservazione 7.3.3 Il teorema precedente mostra, in particolare, che il gruppo degli automorfismi di un gruppo ciclico è abeliano. Cosa succede se il gruppo degli automorfismi di un gruppo G è ciclico? Si dimostra che G è abeliano (si vedano gli esercizi). Si osservi che $Z(G)$ può essere abeliano sia che G sia abeliano oppure no. Ad esempio, se $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, allora $\mathrm{Aut}(G) \cong S_3$, mentre esistono gruppi finiti non abeliani (complicati da descrivere) il cui gruppo di automorfismi è abeliano.

7.4 Il Lemma di Gauss

Lemma 7.4.1 *(Gauss) Il gruppo $Aut(\mathbb{Z}_{p^m})$ è ciclico per ogni primo dispari p e per ogni $m \geq 1$.*

Iniziamo con il caso base $m = 1$, in cui $\mathbb{Z}_p$ è un campo. Per procedere, utilizziamo il seguente lemma.

Lemma 7.4.2 *Sia $\mathbb{K}$ un campo. Allora:*

$$|\{x \in \mathbb{K} \mid x^d = 1\}| \leq d. \tag{7.1}$$

Dimostrazione: Un polinomio $p(x)$ di grado d con coefficienti in un campo $\mathbb{K}$ può avere al massimo d radici (si veda il corso di Algebra 1). Applicando questa osservazione al polinomio x^d, otteniamo (7.1). □

Osservazione 7.4.3 In un anello che non è un campo, il numero di radici di un polinomio può superare il suo grado. Ad esempio, in $\mathbb{Z}_{12}$, il polinomio $x^2 - 4$ ha quattro radici: $2, 4, 8, 10$.

Lemma 7.4.4 *(Lemma di Gauss per $m = 1$) $Aut(\mathbb{Z}_p)$, con p primo dispari, è ciclico.*

Dimostrazione: Dimostriamo che se $\mathbb{K}$ è un campo e $G \leq \mathbb{K}^*$ è un sottogruppo finito del gruppo moltiplicativo, allora G è ciclico (da ciò segue immediatamente che $\mathrm{Aut}(\mathbb{Z}_p) \cong U(\mathbb{Z}_p) = (\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ è ciclico).

Sia $k = \max\{o(a) \mid a \in G\}$ e sia $x \in G$ tale che $o(x) = k$. La dimostrazione sarà conclusa se dimostriamo che $|G| = k$.

Consideriamo $X = \{a \in G \mid a^k = 1\}$. Se per assurdo $X \subsetneq G$, allora esisterebbe $y \in G$ tale che $y^k \neq 1$, e quindi $o(y) \nmid k$. Per un corollario precedente, poiché x e y commutano (essendo G abeliano), esisterebbe $z \in G$ tale che $o(z) = [o(x), o(y)] = [k, o(y)] > k$, contraddicendo l'ipotesi.

Quindi $G = X$. Dato che $|G| \geq k$ e $|X| \leq k$ (per il Lemma 7.4.2), conclude che $|G| = k$. □

Trattiamo ora il caso $m = 2$.

Lemma 7.4.5 *(Lemma di Gauss per $m = 2$) $Aut(\mathbb{Z}_{p^2})$ è ciclico.*

Dimostrazione: Dal Lemma 7.4.4, esiste $[r]_p$, generatore di $\mathrm{Aut}(\mathbb{Z}_p) = U(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, con $o([r]_p) = p - 1$. Mostriamo che sia $[r]_{p^2}$ sia $[r + p]_{p^2}$ generano $\mathrm{Aut}(\mathbb{Z}_{p^2})$.

Sia $x = o([r]_{p^2})$. Allora:

$$([r]_{p^2})^x = [r^x]_{p^2} = [1]_{p^2} \Rightarrow p^2 \mid (r^x - 1) \Rightarrow p \mid (r^x - 1) \Rightarrow [r]_p^x = [1]_p \Rightarrow x = s(p-1)$$

per un certo $s \in \mathbb{N}$.

Inoltre, poiché $|\operatorname{Aut}(\mathbb{Z}_{p^2})| = \varphi(p^2) = p(p-1)$, si ha:

$$([r]_{p^2})^{p(p-1)} = [1]_{p^2} \Rightarrow x = s(p-1) \mid p(p-1),$$

dove $x = p^a(p-1)$ con $a = 0, \ldots, m-1$. Dimostreremo ora che $x = p^{m-1}(p-1)$.

Supponiamo per assurdo che $x = p^b(p-1)$ con $b = 0, \ldots, m-2$. Allora:

$$([r]_{p^2})^{p^{m-2}(p-1)} = [1]_{p^2}.$$

Ne consegue che:

$$[1]_{p^2} = ([r]_{p^2})^{p^{m-2}(p-1)} = ([r^{p-1}]_{p^2})^{p^{m-2}} = ([1+kp]_{p^2})^{p^{m-2}} = [1+kp^{m-1}]_{p^2},$$

dove abbiamo usato il Lemma 7.4.7 per ottenere l'ultima uguaglianza. Tuttavia, $[1+kp^{m-1}]_{p^2} \neq [1]_{p^2}$, poiché $p \nmid k$. Questa è l'assurdo che cercavamo.

Poiché $|\operatorname{Aut}(\mathbb{Z}_{p^2})| = p(p-1)$, segue che $\operatorname{Aut}(\mathbb{Z}_{p^2})$ è generato da $[r]_{p^2}$ o $[r+p]_{p^2}$ e quindi è ciclico. □

Esempio 7.4.6 Il generatore di $\operatorname{Aut}(\mathbb{Z}_3) = \{[1]_3, [2]_3\} \cong \mathbb{Z}_2$ è $[2]_3$. I generatori di $\operatorname{Aut}(\mathbb{Z}_9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\} \cong \mathbb{Z}_6$ sono $[2]_9$ e $[5]_9$. Osserviamo che $[8]_9 = [5+3]_9$ non è un generatore, poiché $[8]_9^2 = [1]_9$.

Prima di dimostrare il Lemma di Gauss in generale abbiamo bisogno di due lemmi aggiuntivi.

Lemma 7.4.7 *Siano $k \in \mathbb{Z}$ e p un primo dispari. Allora per ogni naturale $a \geq 1$ si ha*

$$\left([1+kp]_{p^{a+2}}\right)^{p^a} = [1+kp^{a+1}]_{p^{a+2}} \tag{7.2}$$

Dimostrazione: La (7.2) é equivalente all'esistenza di $m_a \in \mathbb{Z}$ tale che

$$(1+kp)^{p^a} = 1 + kp^{a+1} + m_a p^{a+2}, \tag{7.3}$$

per ogni $a \geq 1$.

Dimostriamo quindi la (7.3) per induzione su a. Se $a = 1$ allora

$$(1+kp)^p = \sum_{j=0}^{p} \binom{p}{j} k^j p^j = 1 + kp^2 + k^2 \binom{p}{2} p^2 + p^3 \sum_{j=3}^{p} \binom{p}{j} k^j p^{j-3}.$$

Siccome $p \neq 2$ e p é primo allora $p|\binom{p}{2}$ e quindi $k^2\binom{p}{2}p^2 = n_1 p^3$ per un certo naturale n_1. Segue che

$$(1+kp)^p = 1 + kp^2 + m_1 p^3.$$

con $m_1 = n_1 + \sum_{j=3}^{p} \binom{p}{j} k^j p^{j-3}$.

Supponiamo che la (7.3) sia vera e dimostriamola per $a+1$. Allora

$$(1+kp)^{p^{a+1}} = [(1+kp)^{p^a}]^p = (1+kp^{a+1}+m_a p^{a+2})^p = \sum_{i=0}^{p} \binom{p}{i} (1+kp^{a+1})^{p-i} m_a^i p^{i(a+2)}. \tag{7.4}$$

Osserviamo che per $i \geq 1$ tutti i termini della somma precedente sono divisibili per p^{a+3} (infatti per $i = 1$ compare il termine $\binom{p}{1}p^{a+2} = p^{a+3}$, mentre per $i \geq 2$ compare il termine $p^{i(a+2)}$ che é sempre divsibile per p^{a+3} essendo $a \geq 1$. Quindi esiste $n_a \in \mathbb{Z}$ tale che

$$\sum_{i=1}^{p} \binom{p}{i} (1+kp^{a+1})^{p-i} m_a^i p^{i(a+2)} = n_a p^{a+3}. \tag{7.5}$$

Osserviamo che il termine in (7.4) per $i = 0$ si scrive come

$$(1+kp^{a+1})^p = \sum_{j=0}^{p} \binom{p}{j} k^j p^{j(a+1)} = 1 + kp^{a+2} + \sum_{j=2}^{p} \binom{p}{j} k^j p^{j(a+1)} \tag{7.6}$$

e $p^{a+3}|p^{ja+j}$ per ogni $j \geq 2$. Esiste quindi $n'_a \in \mathbb{Z}$ tale che

$$\sum_{j=2}^{p} \binom{p}{j} k^j p^{j(a+1)} = n'_a p^{a+3}. \tag{7.7}$$

Mettendo insieme la (7.5), la (7.6) e la (7.7) e ponendo $m_{a+1} = n_a + n'_a$ possiamo scrivere la (7.4) come

$$(1+kp)^{p^{a+1}} = 1 + kp^{a+2} + m_{a+1} p^{a+3}$$

che é quello che volevamo dimostrare. □

Osservazione 7.4.8 Nel corso della dimostrazione del Lemma 7.4.7 abbiamo usato l'ipotesi che p fosse un primo dispari solo solo nell'ipotesi induttiva.

Lemma 7.4.9 *Sia p un primo (non necessariamente dispari). Se $Aut(\mathbb{Z}_{p^m})$ é ciclico e $[r]_{p^m}$ é un suo generatore allora $[r]_{p^{m-1}}$ é un generatore di $Aut(\mathbb{Z}_{p^{m-1}})$. Se $[r]_{p^2}$ é un generatore di $Aut(\mathbb{Z}_{p^2})$ allora*

$$r^{p-1} = 1 + kp \tag{7.8}$$

per qualche intero k tale che $p \nmid k$.

Dimostrazione: L'applicazione

$$\mathrm{Aut}(\mathbb{Z}_{p^m}) = U(\mathbb{Z}_{p^m}) \to \mathrm{Aut}(\mathbb{Z}_{p^{m-1}}) = U(\mathbb{Z}_{p^{m-1}}), [u]_{p^m} \mapsto [u]_{p^{m-1}}$$

è un omomorfismo suriettivo di gruppi e quindi se $\mathrm{Aut}(\mathbb{Z}_{p^m})$ é ciclico allora $\mathrm{Aut}(\mathbb{Z}_{p^{m-1}})$ é ciclico e se $[r]_{p^m}$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^m})$ allora generatore $[r]_{p^{m-1}}$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^{m-1}})$. Se, in particolare, $[r]_{p^2}$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^2})$ allora $[r]_p$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_p)$ e quindi $([r]_p)^{p-1} = [1]_p$ ossia $r^{p-1} = 1 + kp$, per qualche intero k. Inoltre $p \nmid k$ altrimenti $[r]_{p^2}^{p-1} = [1]_{p^2}$ in contrasto col fatto che $[r]_{p^2}$ genera $\mathrm{Aut}(\mathbb{Z}_{p^2})$ e quindi ha ordine $p(p-1)$. □

Dimostrazione del Lemma di Gauss (Lemma 7.4.1) Sia p un primo dispari. Dimostriamo che $\mathrm{Aut}(\mathbb{Z}_{p^m})$ è ciclico per ogni $m \geq 3$. Sia $[r]_{p^2}$ un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^2})$ la cui esistenza è garantita dal Lemma 7.4.5. Sia $x = o([r]_{p^m})$. Allora:

$$([r]_{p^m})^x = [r^x]_{p^m} = [1]_{p^m} \Rightarrow p^m | (r^x - 1) \Rightarrow p | (r^x - 1) \Rightarrow [r^x]_p = [1]_p \Rightarrow x = s(p-1),$$

per un certo $s \in \mathbb{N}_+$. Inoltre

$$[r^{p^{m-1}(p-1)}]_{p^m} = [1]_{p^m} \Rightarrow x = s(p-1) \mid p^{m-1}(p-1),$$

Allora $x = p^a(p-1)$ dove $a = 0, \ldots, m-1$. La dimostrazione sará conclusa se si dimostra che $x = p^{m-1}(p-1)$ (infatti in questo caso $[r]_{p^m}$ un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^m})$ che ha cardinalitá $p^{m-1}(p-1)$). Supponiamo per assurdo che $x = p^b(p-1)$, $b = 0, \ldots, m-2$. Allora, in particolare,

$$([r]_{p^m})^{p^{m-2}(p-1)} = [1]_{p^m}.$$

Segue che

$$[1]_{p^m} = ([r]_{p^m})^{p^{m-2}(p-1)} = ([r^{p-1}]_{p^m})^{p^{m-2}} = ([1+kp]_{p^m})^{p^{m-2}} = [1 + kp^{m-1}]_{p^m}$$

dove nell'ultima uguaglianza abbiamo usato la (7.2) del Lemma 7.4.7 con $m = a + 2$. D'altra parte $[1 + kp^{m-1}]_{p^m} \neq [1]_{p^m}$ in quanto $p \nmid k$. Questo é l'assurdo desiderato e la dimostrazione é conclusa. □

7.5 Il Teorema di Gauss

Teorema 7.5.1 (Gauss) *Il gruppo $Aut(\mathbb{Z}_n)$ è ciclico se e solo se $n \in \{1, 2, 4, p^m, 2p^m\}$, con p un primo dispari.*

Dimostrazione: Iniziamo dimostrando che se $n \in \{1, 2, 4, p^m, 2p^m\}$, con p primo dispari, allora $\mathrm{Aut}(\mathbb{Z}_n)$ è ciclico.

Per i casi $n = 1$ e $n = 2$, abbiamo rispettivamente il gruppo banale e $\mathbb{Z}_2$, i cui gruppi di automorfismi sono entrambi banali. Per $n = 4$, si ha $\mathrm{Aut}(\mathbb{Z}_4) = \mathbb{Z}_2$. Il caso $n = p^m$ segue dal Lemma di Gauss. Infine, se $n = 2p^m$, allora $\mathbb{Z}_n \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^m}$ e, poiché $\gcd(2, p^m) = 1$, si ha

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_2) \times \mathrm{Aut}(\mathbb{Z}_{p^m}) \cong \{0\} \times \mathrm{Aut}(\mathbb{Z}_{p^m}) \cong \mathrm{Aut}(\mathbb{Z}_{p^m}),$$

che è ciclico, ancora per il Lemma di Gauss.

Mostriamo ora che se $\mathrm{Aut}(\mathbb{Z}_n)$ è ciclico, allora $n \in \{1, 2, 4, p^m, 2p^m\}$, con p primo dispari.

Scriviamo

$$n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}, \quad \alpha_j \geq 0, \quad p_i \neq p_j,$$

dove i p_i sono primi dispari distinti.

Dimostriamo che può esserci al massimo un solo primo dispari nella scomposizione di n. Supponiamo per assurdo che esistano due primi dispari distinti, diciamo p_1 e p_2, con $\alpha_1 \geq 1$ e $\alpha_2 \geq 1$. In questo caso, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \mathbb{Z}_r$, dove $r = 2^{\alpha_0} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$. Allora, per il teorema sul prodotto diretto di gruppi con cardinalità coprime, si ha

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_1}}) \times \mathrm{Aut}(\mathbb{Z}_{p_2^{\alpha_2}}) \times \mathrm{Aut}(\mathbb{Z}_r).$$

Essendo $\mathrm{Aut}(\mathbb{Z}_n)$ ciclico, anche $\mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_1}})$ e $\mathrm{Aut}(\mathbb{Z}_{p_2^{\alpha_2}})$ devono essere ciclici, e i loro ordini devono essere primi tra loro. Tuttavia,

$$|\mathrm{Aut}(\mathbb{Z}_{p_i^{\alpha_i}})| = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1),$$

che è pari per $i = 1, 2$, portando così a una contraddizione. Quindi, $n = 2^{\alpha_0} p^{\alpha}$, con p un primo dispari.

Restano ora da esaminare i casi $n = 2^{\alpha_0}$ con $\alpha_0 \geq 3$ e $n = 2^{\alpha_0} p^{\alpha}$ con $\alpha_0 \geq 2$ e $\alpha \geq 1$, per mostrare che in questi casi $\mathrm{Aut}(\mathbb{Z}_n)$ non è ciclico.

Consideriamo innanzitutto il caso $n = 2^{\alpha_0}$ con $\alpha_0 \geq 3$. Se per assurdo $\mathrm{Aut}(\mathbb{Z}_{2^{\alpha_0}})$ fosse ciclico, allora, per il Lemma 7.4.9, $\mathrm{Aut}(\mathbb{Z}_8)$ dovrebbe essere ciclico, ma sappiamo che $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, che non è ciclico.

Infine, consideriamo il caso $n = 2^{\alpha_0} p^{\alpha}$ con $\alpha_0 \geq 2$ e $\alpha \geq 1$. Dall'isomorfismo $\mathbb{Z}_n \cong \mathbb{Z}_{2^{\alpha_0}} \times \mathbb{Z}_{p^{\alpha}}$, si ottiene

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{2^{\alpha_0}}) \times \mathrm{Aut}(\mathbb{Z}_{p^{\alpha}}),$$

nuovamente per il teorema sul prodotto diretto di gruppi con cardinalità coprime. Tuttavia, le cardinalità sono

$$|\operatorname{Aut}(\mathbb{Z}_{2^{\alpha_0}})| = \varphi(2^{\alpha_0}) = 2^{\alpha_0-1}, \quad |\operatorname{Aut}(\mathbb{Z}_{p^\alpha})| = p^{\alpha-1}(p-1),$$

entrambe pari (poiché $\alpha_0 \geq 2$ e p è un primo dispari), il che implica che $\operatorname{Aut}(\mathbb{Z}_n)$ non è ciclico, ottenendo così la contraddizione cercata. □

7.6 Esercizi

Esercizio 7.1 Sia G un gruppo abeliano e siano H e K sottogruppi finiti di G. Dimostrare che:

1. $|H+K|$ divide $|H||K|$;
2. se gli ordini di H e K sono coprimi. allora $H+K \cong H \times K$.

Esercizio 7.2 Sia G un gruppo abeliano di ordine n, dove $n = 28, 30, 130, 131$. Si dica per quali valori di n si puó affermare che G é necessariamente ciclico.

Esercizio 7.3 Dimostrare che se il gruppo $\mathrm{Aut}(G)$ degli automorfismi di un gruppo G é ciclico allora il gruppo é abeliano. (Suggerimento: se $\mathrm{Aut}(G)$ é ciclico anche $G/Z(G) \cong \mathrm{Inn}(G)$ é ciclico e quindi esiste $x \in G$ tale che $< xZ(G) >= G/Z(G)$. Segue che per ogni $y_1, y_2 \in G$ esistono $z_1, z_2 \in Z(G)$, $n_1, n_2 \in \mathbb{Z}$ tali che $y_1 = x^{n_1} z_1$ $y_2 = x^{n_2} z_2$. Dimostrare che $y_1 y_2 = y_2 y_1$).

Esercizio 7.4 Sia G un gruppo abeliano di ordine pq, con p e q primi non necessariamente distinti. Si trovi il numero dei sottogruppi di G. (Suggerimento: dimostrare che G é isomorfo a $\mathbb{Z}_{p^2}$ oppure a $\mathbb{Z}_p \times \mathbb{Z}_p$ oppure a $\mathbb{Z}_p \times \mathbb{Z}_q$ con $p \neq q$. Dimostrare che il gruppo ciclico $\mathbb{Z}_{p^2}$ ha 3 sottogruppi; il gruppo $\mathbb{Z}_p \times \mathbb{Z}_q$ ha 4 sottogruppi e il gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$ ha $p+1$ sottogruppi).

Esercizio 7.5 Sia p un numero primo. Dimostrare che $\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \cong \mathrm{GL}_2(\mathbb{Z}_p)$. (Suggerimento: ogni atuomorfismo di $\mathbb{Z}_p \times \mathbb{Z}_p$ puó essere visto come un'isomorfismo dello spazio vettoriale $\mathbb{Z}_p \times \mathbb{Z}_p$ sul campo $\mathbb{Z}_p$).

Esercizio 7.6 Siano m e n due interi positivi coprimi. Dimostrare che ogni omomorfismo φ da $\mathbb{Z}_m \times \mathbb{Z}_n$ in se stesso ha la forma $\varphi = (\varphi_1, \varphi_2)$, dove $\varphi_j : \mathbb{Z}_m \to \mathbb{Z}_n$, $j = 1, 2$, sono oppurtuni omomorfismi. (Suggerimento: usare il fatto, dimostrato a lezione, che un omomorfismo $\varphi : H \to K$ tra due gruppi H e K di ordini coprimi é banale, cioé $\ker \varphi = H$).

Esercizio 7.7 Sia G un gruppo abeliano finito generato da due elementi x, y, $G = \langle x, y \rangle$. Sia p un numero primo che divide $|G|$, ma p non divide $o(x)$. Dimostrare che p divide $o(y)$. (Suggerimento: dimostrare che $G = \langle x \rangle + \langle y \rangle$ e che, per la parte (a) dell'Esercizio 7.1, $|\langle x \rangle + \langle y \rangle|$ divide $|\langle x \rangle||\langle y \rangle|$).

Esercizio 7.8 Sia G un gruppo abeliano finito e sia $\hat{G}$ l'insieme di tutti gli omomorfismi $\varphi : G \to \mathbb{R}/\mathbb{Z}$, sul quale definiamo un'operazione

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x).$$

Dimostrare che $\hat{G}$ é un gruppo e che se $G \cong H \times K$ allora $\widehat{H \times K} \cong \hat{H} \times \hat{K}$.

Esercizio 7.9 Sia $\hat{G}$ come nell'Esercizio 7.8. Si dimostri che se G é ciclico allora $\hat{G} \cong G$. (Suggerimento: per $n \geq 2$ si dimostri che l'applicazione $\hat{\mathbb{Z}}_n \to U_n$, $\varphi \mapsto \varphi([1]_n)$, dove U_n é il sottogruppo di $S^1 = \mathbb{R}/\mathbb{Z}$ costituito dalle radici n-esime dell'unitá, é un isomorfismo).

Esercizio 7.10 Sia $\hat{G}$ come nell'Esercizio 7.8. Si dimostri che $\hat{G} \cong G$. (Suggerimento: usare gli Esercizi 7.8, 7.9 e il Teorema di Frobenius-Stickelberger).

Bibliografia

[1] Boothby W., *An introduction to Differentiable Manifolds and Riemannian Geometry*, Second Edition, Academic Press 1986.