Dispense di Algebra 1 - Gruppi

Dikran Dikranjan e Maria Silvia Lucido

Dipartimento di Matematica e Informatica
Università di Udine
via delle Scienze 200, I-33100 Udine

gennaio 2005

"*L'algébre est généreuse, elle donne souvent plus qu'on lui demande.*"

d'Alembert

L'algebra è uno dei settori più antichi della matematica. Le operazioni aritmetiche sui numeri interi e sui numeri razionali positivi, così come alcune formule algebriche in geometria e astronomia, erano note ai tempi dei Babilonesi, degli Egiziani e degli antichi Greci. Fin dalle sue origini l'algebra si può considerare come l'arte di manipolare somme, prodotti e potenze di numeri (interi). Le regole di queste manipolazioni valgono per tutti i numeri, e quindi i numeri possono essere sostituiti da lettere. Così l'algebra moderna, nata tra la fine dell'ottocento (in seguito ai contributi fondamentali di David Hilbert) e gli anni venti-trenta del novecento, studia le strutture algebriche, ovvero insiemi dotati di una o più operazioni. Più precisamente, l'oggetto principale dell'algebra sono *le operazioni* (e le loro proprietà), mentre l'insieme-supporto è di secondaria importanza.

Prerequisito principale per il corso di Algebra 1 è il corso di Aritmetica, ma saranno indispensabili anche le conoscenze delle nozioni di base del corso di Analisi 1 (insiemi finiti e infiniti, numeri reali) e Geometria 1 (spazio vettoriale, calcolo matriciale). L'obbiettivo del corso è di introdurre le strutture algebriche più semplici – i gruppi e i semigruppi. Non è esagerato dire che i semigruppi presentano la principale e la più importante struttura algebrica. Ogni altra struttura algebrica infatti, sia essa anello o campo, modulo o spazio vettoriale, dominio o algebra, ha come struttura soggiacente almeno un semigruppo. Ma il concetto di semigruppo trapassa i confini dell'algebra e della teoria dei numeri e trova molte applicazioni nella geometria, nell'analisi e nella fisica. Un caso particolare di questa struttura è quella di gruppo, isolato implicitamente dal geniale matematico francese Galois nell'ambito della soluzione delle equazioni di grado maggiore di quattro. Nel caso dei gruppi l'operazione è più ricca di proprietà – oltre all'elemento neutro si richiede anche l'esistenza di un inverso per ogni elemento.

Nel primo capitolo vengono introdotte le strutture algebriche principali, che saranno studiate durante i corsi di Algebra 1 e Algebra 2. Si comincia con i semigruppi, insiemi dotati di un'operazione associativa, e i monoidi, semigruppi dotati di un elemento neutro. Si introduce anche il concetto di gruppo, un monoide in cui ogni elemento è invertibile, che permette di definire anche la seconda struttura algebrica importante, ovvero quella di anello e in particolare, di campo. Gli anelli ed i campi saranno studiati nel corso di Algebra 2, mentre i gruppi saranno oggetto di studio in Algebra 1.

Il secondo capitolo contiene alcune proprietà immediate del calcolo con le potenze in un gruppo e anche un paragrafo dedicato all'esempio di gruppi *par excellance*, ovvero i gruppi di permutazioni. Infatti ogni gruppo può essere visto come un gruppo di permutazioni.

Nel terzo capitolo si espone il concetto fondamentale di sottogruppo: sottoinsieme del gruppo che risulta gruppo esso stesso se considerato con l'operazione che proviene dal gruppo. L'idea di introdurre i sottogruppi è di semplificare lo studio del gruppo perché i sottogruppi hanno spesso una struttura molto più semplice. Ogni sottogruppo H di un gruppo G dà luogo a due relazioni di equivalenza su G, le cui classi di equivalenza sono chiamate classi laterali. Il numero $[G : H]$ di queste classi laterali è un invariante importante del sottogruppo H e nel caso dei gruppi finiti si calcola tramite il teorema di Lagrange.

Il quarto capitolo è dedicato ai sottogruppi normali N che hanno l'ulteriore proprietà che le due relazioni di equivalenza associate a N di cui sopra, coincidono. Di conseguenza questa unica relazione che risulta è compatibile con l'operazione del gruppo. Questo permette l'introduzione del gruppo

quoziente avente come sostegno l'insieme quoziente G/N. I sottogruppi normali rappresentano la controparte dei sottospazi degli spazi vettoriali. Inoltre, nel caso dei gruppi finiti, permettono di studiare la struttura di un gruppo tramite due gruppi di ordine più piccolo, N e G/N. Presentiamo poi i gruppi lineari, ovvero i sottogruppi del gruppo delle trasformazioni lineari invertibili di uno spazio vettoriale. Introduciamo inoltre i quaternioni, i numeri particolari "quattro-dimensionali" inventati dal matematico irlandese William Rowan Hamilton 160 anni fa. I quaternioni hanno molte applicazioni in geometria, in meccanica razionale e in fisica.

Il quinto capitolo è dedicato al concetto importantissimo di *omomorfismo* che permette di collegare diversi gruppi tra loro. Come nel caso delle trasformazioni lineari in Geometria, un omomorfismo è una applicazione tra gruppi che rispetta l'operazione. Gli omomorfismi biiettivi, detti isomorfismi, permettono di identificare molti gruppi apparentemente diversi e facilitano lo studio della struttura dei gruppi.

Il sesto capitolo è dedicato ai gruppi ciclici, ovvero i gruppi generati da un singolo elemento. Questa classe di gruppi permette una descrizione completa e abbastanza semplice (ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ oppure al gruppo $\mathbb{Z}_m$ per qualche m).

I capitoli successivi affrontano i seguenti quattro argomenti: i prodotti diretti, la struttura dei gruppi abeliani finiti, gli automorfismi e le proprietà dei gruppi non abeliani. Come nel caso degli spazi vettoriali, alcuni gruppi ammettono una rappresentazione come prodotto diretto di altri gruppi (più semplici); in particolare, ogni gruppo abeliano è prodotto diretto di gruppi ciclici.

Il processo di creare e trasmettere matematica ha due componenti molto diverse – l'idea ispiratrice di ogni dimostrazione è il cuore (il nocciolo) che il lettore deve capire e ricordare, mentre la costruzione di un argomento rigoroso è la "spina dorsale" senza la quale non è possibile trasmettere correttamente la dimostrazione. Abbiamo cercato, per quanto possibile, di dare l'idea principale della dimostrazione in un breve commento iniziale e poi esporre con rigore tutti i dettagli della dimostrazione stessa. La lettura di questi appunti deve essere accompagnata da un lavoro serio sugli esercizi.

Desideriamo ringraziare la Dott-ssa Chiara Milan per i miglioramenti e le correzioni apportate in questa (quarta) edizione degli appunti.

Contents

1 Strutture algebriche

1.1 Operazioni su un'insieme

Sia G un insieme. Un'*operazione binaria* su G è un'applicazione $\bullet : G \times G \to G$. Se a e b sono elementi di G, l'immagine tramite $\bullet$ della coppia (a, b) si dice *prodotto* di a e b e si indica con $a \bullet b$. Per indicare le operazioni useremo di solito i simboli $\cdot$ e $+$. L'operazione $\cdot$ è *associativa*, se vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni a, b e c in G.

1.2 Semigruppi

Definizione 1.1 Un *semigruppo* è una coppia $(G, \cdot)$ dove G è un insieme (detto *supporto* del semigruppo), $\cdot$ è un'operazione binaria associativa su G.

Per comodità, d'ora in poi, quando non sarà necessario specificare l'operazione, scriveremo S al posto di $(S, \cdot)$ e scriveremo semplicemente ab al posto di $a \cdot b$.

Definizione 1.2 La cardinalità dell'insieme S si indica con $|S|$ e si dice *ordine* di S. Un semigruppo si dice *finito* se il suo ordine è un numero naturale.

Per due elementi $a, b \in G$ si dice che a e b *commutano* (o sono *permutabili*) se $ab = ba$.
Un semigruppo A si dice *abeliano* o *commutativo* se per ogni a, b in A risulta $ab = ba$.

Esempio 1.3

1. Se $\mathbb{N}$ è l'insieme dei numeri naturali, le coppie $(\mathbb{N}, +)$ e $(\mathbb{N}, \cdot)$ risultano semigruppi.
2. Se $\mathbb{Z}$ è l'insieme dei numeri interi, le coppie $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \cdot)$ risultano semigruppi.
3. Se $\mathbb{Q}$ è l'insieme dei numeri razionali, le coppie $(\mathbb{Q}, +)$ e $(\mathbb{Q}, \cdot)$ risultano semigruppi.
4. Se $\mathbb{R}$ è l'insieme dei numeri reali, le coppie $(\mathbb{R}, +)$ e $(\mathbb{R}, \cdot)$ risultano semigruppi.
5. Se $\mathbb{C}$ è l'insieme dei numeri complessi, le coppie $(\mathbb{C}, +)$ e $(\mathbb{C}, \cdot)$ risultano semigruppi.
6. Se $m > 1$ è intero e $\mathbb{Z}_m$ è l'insieme delle classi resto modulo m, allora le coppie $(\mathbb{Z}_m, +)$ e $(\mathbb{Z}_m, \cdot)$ risultano semigruppi.
7. Se $\mathbb{N}_+$ è l'insieme dei numeri naturali positivi, le coppie $(\mathbb{N}_+, +)$ e $(\mathbb{N}_+, \cdot)$ risultano semigruppi.
8. Se $\mathbb{Q}_+$ è l'insieme dei numeri razionali positivi, le coppie $(\mathbb{Q}_+, +)$ e $(\mathbb{Q}_+, \cdot)$ risultano semigruppi.

Tutti i semigruppi nell'esempio 1.3 sono commutativi.

La legge di cancellazione in un semigruppo. In un semigruppo $(S, \cdot)$ si dice che si può *cancellare l'elemento x a sinistra* in S se da $xb = xc$ segue sempre $b = c$ per ogni coppia di elementi $b, c \in S$. Analogamente, se da $bx = cx$ si conclude $b = c$ per ogni coppia di elementi $b, c \in S$, si dice che si può *cancellare x a destra*. Si dirà che il semigruppo $(S, \cdot)$ soddisfa *la legge di cancellazione*, se ogni elemento di S si può cancellare a destra e a sinistra.

Esempio 1.4 I semigruppi $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_m, +), (\mathbb{N}_+, \cdot)$ e $(\mathbb{Q}_+, \cdot)$ soddisfano la legge di cancellazione, ma i semigruppi $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot), (\mathbb{Z}_m, \cdot)$
no.

Per un semigruppo $(S, \cdot)$ e un elemento $x \in S$ definiamo le potenze di x nel modo seguente. Poniamo $x^1 = x$ e per $n \in \mathbb{N}$ con $n > 1$ poniamo $x^n = x^{n-1}x$.

Esercizio 1.5 *Dimostrare che $x^{n+m} = x^n x^m$ per tutti i numeri naturali positivi n, m.*

Un elemento b di un semigruppo si dice *idempotente* se $b = b^2$. In generale, un semigruppo potrebbe non avere degli idempotenti (per esempio, $(\mathbb{N}^*, +)$), ma ogni semigruppo finito ha almeno un idempotente (vedi l'Esercizio 1.20).

Notazione additiva. In molti casi, soprattutto quando il semigruppo è abeliano, si usa anche la notazione additiva (vedi gli esempi in 1.3). Allora l'operazione viene denotata con $+$. Ecco, per esempio, in notazione additiva:
a) la legge associativa, $a + (b + c) = (a + b) + c$ per ogni a, b e c in G;
b) la legge di cancellazione, $a + b = a + c$ implica $b = c$ e $b + a = c + a$ implica $b = c$ per ogni coppia di elementi $b, c \in S$.
c) le potenze di x si chiamano adesso *multipli* di x e si scrivono nx, ponendo $nx = (n-1)x + x$ e pertanto la formula del Lemma 1.5 diventa $(n + m)x = nx + mx$.

1.3 Monoidi

Un semigruppo $(M, \cdot)$ si dice *monoide* se esiste un *elemento neutro* 1 di M, tale che

$$1 \cdot a = a \cdot 1 = a \text{ per ogni } a \in M. \tag{1}$$

Vediamo subito che l'elemento neutro 1 di M di un monoide è unico. Infatti, se per qualche elemento e di M risulta $e \cdot a = a \cdot e = a$ per ogni a in M, allora $e = e \cdot 1 = 1$.

Questo suggerisce di considerare il monoide anche come una terna $(M, \cdot, 1)$ dove M è un insieme, $\cdot$ è un'operazione binaria su M e 1 è un elemento di M, che verifica la proprietà (1).

Per comodità, d'ora in poi, quando non sarà necessario specificare l'operazione e l'elemento neutro, scriveremo M al posto di $(M, \cdot)$ o $(M, \cdot, 1)$.

Se $(S, \cdot, 1)$ è un monoide e $x \in S$ poniamo anche $x^0 = 1$. Allora la formula del Lemma 1.5 vale per tutti i numeri naturali n, m.

Notazione additiva. In molti casi, soprattutto quando il monoide è abeliano, si usa anche la notazione additiva. Allora l'operazione viene denotata con $+$, l'elemento neutro con 0. Quindi, l'elemento neutro 0 di $(G, +)$, soddisfa $0 + a = a + 0 = a$ per ogni a in G.

In un monoide l'elemento neutro è ovviamente un idempotente. Il seguente lemma dimostra che per i semigruppi con la legge di cancellazione questi due proprietà coincidono.

Lemma 1.6 *Un elemento e di un semigruppo con la legge di cancellazione è idempotente se e solo se e è l'elemento neutro.*

Dimostrazione. Sia $(S, \cdot)$ semigruppo con la legge di cancellazione e sia e un idempotente di S. Allora per ogni $a \in S$ si ha $ae = ae^2$ in quanto $e = e^2$. Adesso cancellando e a destra ricaviamo $a = ae$. Analogamente si prova che $ea = a$. Quindi e è l'elemento neutro. □

Esempio 1.7

1. Le terne $(\mathbb{N}, +, 0)$ e $(\mathbb{N}, \cdot, 1)$ risultano monoidi.
2. Le terne $(\mathbb{Z}, +, 0)$ e $(\mathbb{Z}, \cdot, 1)$ risultano monoidi.
3. Le terne $(\mathbb{Q}, +, 0)$ e $(\mathbb{Q}, \cdot, 1)$ risultano monoidi.
4. Le terne $(\mathbb{R}, +, 0)$ e $(\mathbb{R}, \cdot, 1)$ risultano monoidi.
5. Le terne $(\mathbb{C}, +, 0)$ e $(\mathbb{C}, \cdot, 1)$ risultano monoidi.
6. Se $m > 1$ è intero, le terne $(\mathbb{Z}_m, +, 0)$ e $(\mathbb{Z}_m, \cdot, 1)$ risultano monoidi.
7. La terna $(\mathbb{N}_+, \cdot, 1)$ è un monoide.
8. Siano $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ e $\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}$. Allora le terne $(\mathbb{Q}^*, \cdot, 1)$ e $(\mathbb{Q}_+, \cdot, 1)$ risultano monoidi.
9. Siano $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ e $\mathbb{R}_+ = \{r \in \mathbb{R} : r > 0\}$. Allora le terna $(\mathbb{R}^*, \cdot, 1)$ e $(\mathbb{R}_+, \cdot, 1)$ risultano monoidi.
10. Sia $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Allora la terna $(\mathbb{C}^*, \cdot, 1)$ è un monoide.
11. Se $\mathbb{S}$ è l'insieme dei numeri complessi z con $|z| = 1$, la terna $(\mathbb{S}, \cdot, 1)$ è un monoide.

Tutti i monoidi sopra elencati sono abeliani.

1.4 Esempi di semigruppi provenienti da insiemi ordinati

Esempio 1.8 *Sia $(X, \leq)$ un insieme ordinato che risulta un reticolo.*

(a) Possiamo considerare $\vee$ e $\wedge$ come operazioni binarie su X. E' facile verificare che entrambe le operazioni sono associative. Quindi, $(X, \vee)$ e $(X, \wedge)$ risultano semigruppi.

(b) Se il reticolo $(X, \leq)$ è limitato, allora $(X, \vee, 0)$ e $(X, \wedge, 1)$ risultano monoidi.

I semigruppi ottenuti in questo modo nell'esempio 1.8 sono commutativi e hanno tutti gli elementi idempotenti.

Questo esempio assai generico ci permette di ottenere anche degli esempi più concreti come segue.

Esempio 1.9 *Sia X un insieme, allora:*

a) $\mathcal{P}(X)$ risulta un monoide rispetto all'unione, con elemento neutro $\emptyset$;

b) $\mathcal{P}(X)$ risulta un monoide rispetto all'intersezione, con elemento neutro X.

Infatti, $\mathcal{P}(X)$, ordinato con l'inclusione è un reticolo limitato. Quindi si applica l'Esempio 1.8 (b).

c) L' insieme di tutte le applicazioni $X \to X$ risulta un monoide rispetto alla composizione $\circ$, con elemento neutro id_X.

1.5 Gruppi

Definizione 1.10 Sia M un monoide. Un elemento $a \in M$ si dice *invertibile* se esiste un elemento $x \in M$ tale che $ax = xa = 1$.

Vediamo subito che l'inverso x dell'elemento a è univocamente determinato da a. Infatti, se vale $a \cdot x' = x' \cdot a = 1$ per qualche elemento $x' \in G$, si ha (usando la proprietà associativa)

$$x = 1 \cdot x = (x' \cdot a) \cdot x = x' \cdot (a \cdot x) = x' \cdot 1 = x'.$$

L'unicità dell'elemento inverso x di a, determinato dalla proprietà $a \cdot x = x \cdot a = 1$, ci suggerisce di indicarlo di con a^{-1}.

Possiamo finalmente dare la definizione più importante per questo corso.

Definizione 1.11 Un monoide $(M, \cdot, 1)$ si dice un *gruppo* se ogni elemento di M è invertibile.

Un gruppo si dice *abeliano*, se risulta abeliano quale semigruppo, ovvero, soddisfa la legge commutativa.

Teorema 1.1 *Ogni gruppo soddisfa la legge di cancellazione.*

Dimostrazione. Se $ab = ac$ in un gruppo G, allora vale

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = 1c = c.$$

Quindi, si può cancellare a a sinistra. Analogamente, si conclude che si può cancellare a a destra. □

Più in generale, da $ab = cd$ si può dedurre, ragionando nello stesso modo, che $b = a^{-1}cd$ e $a = cdb^{-1}$.

Teorema 1.2 *Un monoide finito $(M, \cdot, 1)$ è gruppo se e solo se soddisfa la legge di cancellazione.*

Dimostrazione. Se $(M, \cdot, 1)$ è gruppo, allora il teorema precedente ci garantisce che $(M, \cdot, 1)$ soddisfa la legge di cancellazione.

Supponiamo adesso che $(M, \cdot, 1)$ soddisfi la legge di cancellazione. Per vedere che $(M, \cdot, 1)$ risulta un gruppo basta far vedere che ogni elemento $a \in G$ è invertibile. L'applicazione $f : M \to M$ definita da $f(x) = ax$ per ogni $x \in M$ risulta iniettiva. Infatti, se $f(x) = f(y)$, allora $ax = ay$ e per la legge di cancellazione posiamo concludere che $x = y$. Essendo M finito, l'applicazione f è anche suriettiva. Quindi esiste $x \in M$ tale che $ax = 1$. Nello stesso modo si vede che esiste $y \in M$ con $ay = 1$. Ora $x = x \cdot 1 = x \cdot (a \cdot y) = (x \cdot a) \cdot y = 1 \cdot y = y$. Quindi, $x = a^{-1}$ è l'inverso di a. □

Notazione additiva. In molti casi, soprattutto quando il gruppo è abeliano, si usa anche la notazione additiva. Allora l'operazione viene denotata con $+$, l'elemento neutro con 0 e l'elemento inverso di x con $-x$ e chiamato *opposto di* x. Allora l'opposto $-a$ di a è definito dalla proprietà $(-a)+a = a+(-a) = 0$. Per semplicità ometteremo le parentesi e scriveremo nel seguito $-a + b$ e $a - b$ al posto da $(-a) + b$ e $a + (-b)$.

Esempio 1.12

- I monoidi $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ sono gruppi.
- I monoidi $(\mathbb{Q}^*, \cdot, 1)$, $(\mathbb{Q}_+, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{R}_+, \cdot, 1)$ e $(\mathbb{C}^*, \cdot, 1)$ sono gruppi.
- Se $\mathbb{S}$ è l'insieme dei numeri complessi z con $|z| = 1$, il monoide $(\mathbb{S}, \cdot, 1)$ è un gruppo.
- Se $m > 1$ è intero, allora il monoide $(\mathbb{Z}_m, +, [0]_m)$ è un gruppo.
- Se p è un numero primo e $\mathbb{Z}_p^*$ è l'insieme delle classi $[k]_p \neq [0]_p$, allora il monoide $(\mathbb{Z}_p^*, \cdot, [1]_p)$ è un gruppo.

Tutti questi gruppi sono abeliani. E' facile vedere che i monoidi $(\mathbb{N}, +, 0)$ e $(\mathbb{N}, \cdot, 1)$ non sono gruppi.

1.6 Anelli e campi

In questo paragrafo introduciamo anche la definizione di anello e campo, che utilizzeremo talvolta nel corso di Algebra 1, essenzialmente nel paragrafo dei Gruppi Lineari.

Definizione 1.13 Un *anello* è una terna $(A, +, \cdot)$ dove A è un insieme, $+$ e $\cdot$ sono operazioni binarie su A che verificano le seguenti proprietà:

1. la coppia $(A, +)$ è un gruppo abeliano con elemento neutro che denoteremo con 0.
2. l'operazione $\cdot$ è *associativa*, cioè $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni a, b e c in A;
3. vale la legge distributiva, cioè $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot c$ per ogni a, b e c in A.

Un anello $(A, +, \cdot)$ si dice

1. *unitario*, se il semigruppo $(A, \cdot)$ risulta un monoide;
2. *commutativo*, se il semigruppo $(A, \cdot)$ risulta commutativo;
3. un *dominio di integrità* (o brevemente, *dominio*), se è unitario e commutativo, e nel semigruppo $(A \setminus \{0\}, \cdot)$ vale la legge di cancellazione;
4. un *campo*, se è un dominio, e il semigruppo $(A \setminus \{0\}, \cdot)$ risulta un gruppo.

Per comodità denoteremo un anello $(A, +, \cdot)$ anche semplicemente con A, quando non c'è pericolo di confusione.

Ricordiamo che una *matrice* è una tabella rettangolare costituita da elementi di uno stesso insieme numerico X, disposti secondo un certo numero di righe e un certo numero di colonne. In generale una matrice di m righe e n colonne si dice una matrice $m \times n$, viene indicata con $A = (a_{ij})$ e ha la seguente configurazione:

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix}$$

con $i = 1, 2..., m$ e $j = 1, 2, ..., n$.

Denoteremo con $M_{m\times n}(X)$ l'insieme di tutte le matrici $m \times n$ a elementi in X. Una matrice si dice *quadrata* se $m = n$, cioè se ha lo stesso numero di righe e di colonne. Denoteremo con $M_n(X)$ l'insieme delle matrici quadrate $n \times n$ a elementi in X.

Sia ora $\mathbb{K}$ un campo e $M_n(\mathbb{K})$ l'insieme delle matrici quadrate $n \times n$ a elementi in $\mathbb{K}$. Chiameremo *matrice nulla* la matrice 0_n avente tutti gli elementi uguali a 0, cioè $0_n = (a_{ij})$, in cui $a_{ij} = 0$ per ogni $i, j = 1, ..., n$. Chiameremo *matrice identica* la matrice $I_n = (a_{ij})$, in cui $a_{ij} = 0$ se $i \neq j$ e $a_{ii} = 1$, per ogni $i, j = 1, ..., n$.

Date due matrici $A = (a_{ij})$ e $B = (b_{ij})$ in $M_n(\mathbb{K})$, si definisce la somma $+$ ponendo $A + B = C = (c_{ij})$ dove $c_{ij} = a_{ij} + b_{ij}$. Ovviamente, $A + 0_n = A$ per ogni $A \in M_n(\mathbb{K})$.

Date due matrici $A = (a_{ij})$ e $B = (b_{ij})$ in $M_n(\mathbb{K})$, si definisce un prodotto $\cdot$ "righe per colonne" nel modo seguente:

$$A \cdot B = C = (c_{ij}) \quad \text{dove} \quad c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj}.$$

A volte è comodo presentare l'operazione in una struttura algebrica tramite una tabella. Come esempio diamo la tabella delle due operazioni $+$ e $\cdot$ nell'anello $(\mathbb{Z}_5, +, \cdot)$

Tabella della $+$ in $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

,

Tabella della $\cdot$ in $\mathbb{Z}_5$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Supponiamo ora di avere due semigruppi G ed H. Come si possono costruire nuovi semigruppi a partire da G ed H? Si è visto nel corso di Aritmetica che dati due insiemi possiamo costruire il prodotto cartesiano dei due insiemi. Quando questi due insiemi sono dotati anche di una struttura algebrica è possibile dotare l'insieme prodotto della stessa struttura algebrica, definendo "componente per componente" l'operazione sul prodotto. Diamo quindi la definizione precisa di quanto detto.

Siano G e H due semigruppi. Nel prodotto cartesiano $G \times H$ si introduce la seguente operazione:

$$\text{per } g, g_1 \in G,\ h, h_1 \in H,\ \text{poniamo } (g,h)\cdot(g_1,h_1) = (gg_1, hh_1).$$

Teorema 1.14 *Siano $(G,\cdot)$ e $(H,\cdot)$ due semigruppi. Allora $(G\times H,\cdot)$ risulta un semigruppo, detto prodotto diretto di G e H.*

(a) Se $(G,\cdot,1_G)$ e $(H,\cdot,1_H)$ sono monoidi, allora $(G\times H,\cdot,(1_G,1_H))$ risulta un monoide.

(b) Se $(G,\cdot,1_G)$ e $(H,\cdot,1_H)$ sono gruppi, allora anche $(G\times H,\cdot)$ risulta un gruppo.

(c) Se $(G,+,\cdot)$ e $(H,+,\cdot)$ sono anelli, allora la terna $(G\times H,+,\cdot)$ risulta un anello, dove $(G\times H,+)$ e $(G\times H,\cdot)$ sono i prodotti diretti di $(G,+)$ e $(H,+)$ (rispettivamente di $(G,\cdot)$ e $(H,\cdot)$).

DIMOSTRAZIONE. Verifichiamo che l'operazione $\cdot$ è associativa. Siano $g, g_1, g_2 \in G$ e $h, h_1, h_2 \in H$. Allora

$$((g,h)(g_1,h_1))(g_2,h_2) = (gg_1, hh_1)(g_2,h_2) = ((gg_1)g_2, (hh_1)h_2) = (g(g_1g_2), h(h_1h_2)) =$$

$$(g,h)(g_1g_2, h_1h_2) = (g,h)((g_1,h_1)(g_2,h_2)).$$

(a) Verifichiamo che $(1_G,1_H)$ è l'elemento neutro. Per ogni coppia $(g,h)\in G\times H$ risulta

$$(1_G,1_H)(g,h) = (1_Gg, 1_Hh) = (g,h) = (g1_G, h1_H) = (g,h)(1_G,1_H).$$

(b) Per ogni coppia $(g,h)\in G\times H$ la coppia (g^{-1},h^{-1}) risulta l'inverso di (g,h):

$$(g^{-1},h^{-1})(g,h) = (g^{-1}g, h^{-1}h) = (1_G,1_H) = (gg^{-1}, hh^{-1}) = (g,h)(g^{-1},h^{-1}).$$

(c) Infine, se $(G,+,\cdot)$ e $(H,+,\cdot)$ sono anelli, si verifica facilmente, che vale la legge distributiva per la $+$ e la $\cdot$ definite nel prodotto $G\times H$. Quindi, $G\times H$ risulta un anello. □

1.7 Esercizi

Esercizio 1.15 *Se e è un elemento idempotente in semigruppo S, allora, $e^n = e$ per ogni intero positivo n.*

Esercizio 1.16 *(a) Se S è l'insieme dei numeri complessi z con $|z|>1$, allora $(S,\cdot)$ è un semigruppo, ma non un monoide.*

(b) Se S è l'insieme dei numeri complessi z con $|z|\geq 1$, allora $(S,\cdot,1)$ è un monoide con legge di cancellazione.

(c) Se S è l'insieme dei numeri complessi z con $|z|<1$, allora $(S,\cdot)$ è un semigruppo, ma non un monoide.

(d) Se S è l'insieme dei numeri complessi z con $|z|\leq 1$, allora $(S,\cdot,1)$ è un monoide.

Esercizio 1.17 *Si dimostri che:*

(a) $(M_n(\mathbb{K}),+,0_n)$ è un monoide abeliano.

(b) $(M_n(\mathbb{K}),\cdot)$ è un monoide con elemento identico la matrice I_n. Se $n>1$, allora $M_n(\mathbb{K})$ non è abeliano.

Esercizio 1.18 *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 può affermare che S non è un monoide?*

Esercizio 1.19 *Quali dei monoidi dell'Esempio 1.9 soddisfano la legge di cancellazione?*

Esercizio 1.20* *Dimostrare che ogni semigruppo finito contiene idempotenti.*

Esercizio 1.21* *Dimostrare che ogni semigruppo finito S con la legge di cancellazione risulta un gruppo.*

Esercizio 1.22* *Dimostrare che sull'insieme finito $S = \{a, b\}$ ci sono precisamente 8 strutture di semigruppo, di cui 6 abeliane e 2 non abeliane. Di questi solo 2 risultano gruppi.*

Esercizio 1.23 *Sia $(S, \cdot)$ un monoide. Per $a, b \in S$ poniamo $a|b$ se esiste $c \in S$ tale che $b = ac$. Dimostrare che:*

(a) la relazione binaria $|$ è di preordine;

(b) se $(S, \cdot)$ è un monoide con la legge di cancellazione e un unico elemento invertibile, allora $|$ è un ordine e l'insieme ordinato $(S, |)$ ha un elemento minimo.

2 Proprietà elementari dei gruppi e primi esempi

Cominciamo con la regola di calcolo dell'inverso di un prodotto.

Lemma 2.1 *Sia G un gruppo e siano $a, b \in G$. Allora*

a) l'inverso del prodotto ab è l'elemento $b^{-1}a^{-1}$;

b) a e b commutano se e solo se vale $a^{-1}b^{-1}ab = 1$.

DIMOSTRAZIONE. La dimostrazione è un facile esercizio. □

Definizione 2.2 Dati due elementi a, b di un gruppo G, si denota con $[a, b]$ l'elemento $a^{-1}b^{-1}ab$, che si chiama *commutatore di a e b.*

Si osservi che $ab = ba(ba)^{-1}ab = ba(a^{-1}b^{-1}ab) = ba[a, b]$, da cui segue immediatamente $[a, b] = 1$ se e solo se a, b commutano, come appena visto nel Lemma 2.1.

2.1 Calcolo con potenze e multipli

Per un gruppo $(G, \cdot)$ e un elemento $x \in G$ abbiamo già definito le potenze x^n per $n \in \mathbb{N}$. Ora per $n < 0$ poniamo $x^n = (x^{-1})^{-n}$. La formula $x^n = x^{n-1}x$ resta vera anche per gli interi $n < 0$:

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

Lemma 2.3 *Sia $(G, \cdot)$ un gruppo e $x \in G$. Allora per ogni coppia $m, n \in \mathbb{Z}$ vale:*

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

(b) $(x^n)^{-1} = x^{-n}$ e $x^m x^n = x^n x^m$;

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

DIMOSTRAZIONE.

(a) Nel caso $n \geq 0$ proviamo per induzione che $x^m x^n = x^{m+n}$ vale per ogni $m \in \mathbb{Z}$. Per $n = 0$ questo è ovvio. Supponiamo allora per ipotesi induttiva (su n) che $x^m x^{n-1} = x^{m+n-1}$ per ogni $m \in \mathbb{Z}$. Allora

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

Nel caso $n < 0$, si ha

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

(b) Segue immediatamente da (a).

(c) Nel caso $n \geq 0$ proviamo per induzione che $(x^m)^n = x^{mn}$ vale per ogni $m \in \mathbb{Z}$. Per $n = 0$ questo è ovvio. Per ipotesi induttiva su n si ha dunque $(x^m)^{n-1} = x^{m(n-1)}$ per ogni $m \in \mathbb{Z}$. Allora

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

Nel caso $n < 0$, si ha

$$(x^m)^n = ((x^m)^{-1})^{-n} = (x^{-m})^{-n} = x^{(-m)(-n)} = x^{mn}.\square$$

Lemma 2.4 *Sia $(G, \cdot)$ un gruppo e $x, y \in G$ due elementi permutabili. Allora:*

a) x^n e y sono permutabili per ogni $n \in \mathbb{Z}$;

b) $(xy)^n = x^n y^n$ per ogni $n \in \mathbb{Z}$ (in particolare, $(xy)^{-1} = x^{-1}y^{-1}$);

b) x^n e y^m sono permutabili per ogni $n, m \in \mathbb{Z}$.

DIMOSTRAZIONE. a) Si dimostra prima per induzione che x^n e y sono permutabili per ogni $n \geq 0$ e con il Lemma 2.3 (b) questo si estende per ogni $n \in \mathbb{Z}$.

b) Per ogni $n \in \mathbb{N}$ si può dimostrare per induzione che vale $(xy)^n = x^n y^n$. Per $n < 0$ si applichi il Lemma 2.3 (b).

c) Per il punto a), applicato a x e y, si ha che x^n e y sono permutabili. Applicando nuovamente il punto a) a y e $z = x^n$ si deduce che per ogni $m \in \mathbb{Z}$, x^n e y^m sono permutabili. □

Riformuliamo gli enunciati di questi due lemmi in notazione additiva. Innanzitutto, per un gruppo abeliano $(G, +)$ e $x \in G$ introduciamo i *multipli* nx di x per ogni $n \in \mathbb{Z}$ come segue. Per $n \geq 0$ induttivamente, ponendo $0x = 0$, e $nx = (n-1)x + x$ per $n > 0$. Per $n < 0$ si pone $nx = (-n)(-x)$. Allora per ogni coppia $m, n \in \mathbb{Z}$ risulta

(a) $mx + nx = (m+n)x$;
(b) $-(nx) = (-n)x$;
(c) $n(mx) = nmx$;
(d) $n(x+y) = nx + ny$.

Definizione 2.5 Dato un gruppo G e un suo elemento x, consideriamo il seguente sottoinsieme dei numeri naturali $S(x) = \{n \in \mathbb{N}_+ : x^n = 1\}$. Se $S(x)$ non è vuoto, per il principio del buon ordinamento di $\mathbb{N}$, S ammette un minimo elemento non nullo, che denoteremo con $o(x)$ e chiameremo *ordine* (o *periodo*) di x. Se $S(x)$ è vuoto, definiamo $o(x) = \infty$. Se $o(x) = m$ allora si dice che x è *periodico* di periodo m, mentre se $o(x) = \infty$, si dice che x è *aperiodico*.

Vogliamo ora provare alcune proprietà sugli elementi periodici.

Lemma 2.6 *Sia G un gruppo e $x \in G$ tale che $o(x) = m$ è finito Allora:*
(a) $x^k = 1$ per qualche $k \in \mathbb{Z}$ se e solo se m divide k;
(b) $x^n = x^k$ per $n, k \in \mathbb{Z}$ se e solo se $n \equiv_m k$.
(c) $o(x^k) = \frac{m}{(m,k)}$.
(d) $o(x^{-1}) = m$.

DIMOSTRAZIONE. a) Se m divide k, allora $m = qk$, da cui $x^{qm} = (x^m)^q = 1$.

Viceversa sia $x^k = 1$, per qualche $k \in \mathbb{Z}$. Dividiamo k per m con resto e troviamo $q \in \mathbb{Z}$ e $0 \leq r < m$ tali che $k = qm + r$. Ora $1 = x^k = x^{qm+r} = x^{qm}x^r = x^r$. Se fosse $r > 0$, si avrebbe $r \in S(x)$ contraddicendo la minimalità di m. Pertanto $r = 0$ e m divide k.

(b) Dalla congruenza $n \equiv_m k$ e da (a) deduciamo che $x^{n-k} = 1$. Quindi, $x^n x^{-k} = x^{n-k} = 1$ e di conseguenza $x^n = x^k$. Supponiamo adesso che $x^n = x^k$. Allora $x^n x^{-k} = 1$ e di conseguenza m divide $n - k$ (vedi (a)), cioè $n \equiv_m k$.

(c) Se $d = (m, k)$, allora $m = dm_1$ e $k = dk_1$, con $(k_1, m_1) = 1$. Sia $s = o(x^k)$. Allora $(x^k)^s = x^{ks} = 1$ e dal punto (a) si deduce che m divide ks. Di conseguenza dm_1 divide $dk_1 s$, e cancellando d concludiamo che m_1 divide $k_1 s$. Ora $(k_1, m_1) = 1$ implica che m_1 divide s. Poiché $(x^k)^{m_1} = x^{k_1 dm_1} = (x^m)^{k_1} = 1$, dal punto (a) segue che s divide m_1 e quindi $s = m_1 = \frac{m}{(m,k)}$.

(d) Segue da (c). □

Per calcolare l'inverso di una potenza $b = a^k$ di un elemento a di ordine m basta risolvere la congruenza $kx \equiv_m 1$. Allora la potenza a^x coincide con b^{-1}.

In caso di notazione additiva, avremo $kx = 0$ per un multiplo di x se e solo se $o(x)$ divide k.

2.2 Un esempio: i gruppi di permutazioni

In questo paragrafo vogliamo studiare i *gruppi di permutazioni* (detti anche gruppi simmetrici), cioè insiemi di funzioni biiettive su un insieme, che sono gruppi con l'operazione di composizione di applicazioni. Questi gruppi sono importanti perché sono esempi concreti di gruppi e ogni gruppo astratto si può immergere in un gruppo di permutazioni. Questo significa che, in modo opportuno, possiamo immaginare ogni gruppo astratto come un un gruppo di permutazioni. Studiamo in particolare i gruppi simmetrici finiti, che forniranno i primi esempi di gruppi non abeliani.

Definizione 2.7 Sia X un insieme. Denotiamo con S_X l'insieme di tutte le *permutazioni* di X, cioè delle applicazioni biiettive di X in se'.

Nel corso di aritmetica avevamo già calcolato la cardinalità di S_X, nel caso in cui $|X| = n$, e avevamo visto che $|S_n| = n!$.

Lemma 2.8 *Sia S_X l'insieme delle permutazioni su un insieme non vuoto X. Sia $\circ$ la composizione di applicazioni e id_X l'applicazione identica. Allora la terna $(S_X, \circ, id_X)$ è un gruppo; se $|X| > 2$, allora S_X non è abeliano.*

DIMOSTRAZIONE. Siano $f, g, h \in S_X$. Vogliamo dimostrare che $f \circ (g \circ h) = (f \circ g) \circ h$. A tal scopo, verifichiamo che queste due applicazioni coincidono sugli elementi di X. Infatti, per ogni $x \in X$ risulta:

$$(f \circ (g \circ h))(x) = f(g(h(x)) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

Inoltre $(f \circ id_X)(x) = f(id_X(x)) = f(x)$ e poiché f è biiettiva, esiste l'inversa f^{-1} tale che $f \circ f^{-1} = id_X$. Pertanto $(S_X, \circ, id_X)$ è un gruppo. Proviamo ora che, se $|X| \geq 3$, allora S_X non è un gruppo abeliano.

Siano x, y, z tre elementi distinti di X. Definiamo l'applicazione $f : X \longrightarrow X$ tale che $f(x) = y$, $f(y) = x$ e $f(t) = t$ per ogni $t \in X \setminus \{x, y\}$. Sia g l'applicazione $g : X \longrightarrow X$ tale che $g(x) = z$, $g(z) = x$ e $g(t) = t$ per ogni $t \in X \setminus \{x, z\}$.

Allora $(f \circ g)(x) = f(g(x)) = f(z) = z$ mentre $(g \circ f)(x) = g(f(x)) = g(y) = y$ con $y \neq z$. Pertanto $(f \circ g)(x) \neq (g \circ f)(x)$ e quindi S_X non è abeliano. □

Se l'insieme X è finito e di cardinalità n, X è in biiezione con l'insieme $I_n = \{1, 2, \ldots, n\}$. Denotiamo pertanto $S_X = S_n$ e gli elementi di X con $1, 2, \ldots, n$. Possiamo rappresentare una permutazione di S_n nel modo seguente

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ f(1) & f(2) & \ldots & f(i) & \ldots & f(n) \end{pmatrix}.$$

In particolare S_3 non è abeliano. Vedremo più avanti che S_3 è il più piccolo gruppo non abeliano e fornirà spesso un esempio (negativo) per mostrare che talune proprietà non valgono in generale.

Per una permutazione f di X con inversa f^{-1} definiamo anche le potenze negative ponendo $f^{-n} = (f^{-1})^n = (f^n)^{-1}$ per $n \in \mathbb{N}$ (cioè $x = f^n(y) \Leftrightarrow y = f^{-n}(x)$).

Definizione 2.9 Data $f \in S_X$ definiamo il *supporto* di f come l'insieme degli elementi che non vengono fissati da f, cioè *supp(f)*$=\{x \in X : f(x) \neq x\}$.

Sia f la permutazione di S_{12} definita come segue:

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

Allora $supp(f) = \{2, 3, 4, 6, 7, 8, 9, 10\}$.

Definizione 2.10 Diremo che due permutazioni $f, g \in S_X$ sono *disgiunte* se $supp(f) \cap supp(g) = \emptyset$.

Osserviamo che se $x \in supp(f)$, allora anche $f(x) \in supp(f)$. Infatti se $f(x) \notin supp(f)$, allora $f(f(x)) = f(x)$, da cui deduciamo per l'iniettività di f che $f(x) = x$, contro l'ipotesi.

Lemma 2.1 *Se f e g sono due permutazioni disgiunte, allora f e g commutano.*

DIMOSTRAZIONE. Se $x \in supp(f)$, allora dall'ipotesi che f e g sono disgiunte deduciamo che $g(x) = x$. Quindi $(f \circ g)(x) = (f(g(x)) = f(x)$ e anche $(g \circ f)(x) = (g(f(x)) = f(x)$, in quanto dall'osservazione precedente il Lemma sappiamo che anche $f(x) \in supp(f)$. In modo del tutto analogo si prova che se $y \in supp(g)$, allora $(f \circ g)(y) = (f(g(y)) = g(y) = g(f(y)) = (g \circ f)(y)$. Infine se $z \notin supp(f) \cup supp(g)$, si ha $(f \circ g)(z) = (f(g(z)) = f(z) = z = g(z) = g(f(z)) = (g \circ f)(z)$. Concludiamo che f e g commutano. □

Data $f \in S_X$ definiamo un relazione in X nel modo seguente:

$$a \sim_f b \quad \Longleftrightarrow \quad \text{esiste} \quad i \in \mathbb{Z} \ \text{ tale che } b = f^i(a).$$

Allora $\sim_f$ è una relazione di equivalenza. Infatti è
riflessiva: $a = f^0(a) = id(a)$,
simmetrica: se $b = f^i(a)$ allora $a = f^{-i}(b)$,
transitiva: se $b = f^i(a)$ e $c = f^j(b)$ allora $c = f^j(b) = f^j(f^i(a)) = f^{i+j}(a)$.
Pertanto l'insieme X si ripartisce in classi di equivalenza rispetto a questa relazione.

Definizione 2.11 La classe di un elemento $a \in X$ si dice l'*orbita* di a rispetto ad f, e si denota

$$[a]_f = \{\ldots, f^{-i}(a), \ldots, f^{-1}(a), a, f(a), \ldots f^i(a), \ldots\}.$$

Supponiamo ora che X sia finito, allora l'orbita di a rispetto ad f è finita, pertanto si avrà $[a]_f = \{a, f(a), \ldots, f^d(a)\}$ per qualche $d \in \mathbb{N}$. Cioè f ristretta a $[a]_f$ agisce *ciclicamente*, cioè manda $a_0 = a$ in $a_1 = f(a)$, manda a_1 in $a_2 = f(a_1)$, ..., infine, manda $a_d = f^d(a)$ in $a_0 = a$. Motivati da questa osservazione definiamo adesso un tipo relativamente semplice di permutazioni, ossia quelle che agiscono ciclicamente sul loro supporto.

Definizione 2.12 Sia $l > 1$, un *ciclo di lunghezza* l è una permutazione σ di X tale che $supp(\sigma) = \{a_1, \ldots, a_l\} \subseteq X$ e $\sigma(a_i) = a_{i+1}$ per ogni $i = 1, \ldots, l-1$ e $\sigma(a_l) = a_1$.

Denoteremo il ciclo σ con $(a_1 a_2 \ldots a_l)$ e notiamo subito che anche $(a_2 a_3 \ldots a_l a_1)$, $(a_3 a_4 \ldots a_l a_1 a_2)$, ecc. definiscono lo stesso ciclo σ.

Particolare importanza avranno i cicli di lunghezza 2:

Definizione 2.13 Un ciclo (ab) di lunghezza due si chiama *trasposizione*.

Se consideriamo una permutazione f e scriviamo i cicli relativi alle orbite di f, allora questi cicli sono disgiunti, proprio perché le orbite costituiscono una partizione di X. Si avrà pertanto:

Teorema 2.14 *Ogni permutazione si può scrivere in modo essenzialmente unico come prodotto di cicli disgiunti.*

Infatti ogni permutazione si scrive come prodotto di cicli disgiunti e i cicli sono univocamente determinati, ma non così l'ordine con cui vengono moltiplicati. Quindi, a meno di scambiare l'ordine dei fattori, che in questo caso commutano poiché sono cicli disgiunti, la scrittura è unica.

Vediamo come si moltiplicano tra di loro due permutazioni scritte in cicli disgiunti.

Esempio 2.15 *Calcoliamo in* S_7

$$(3457) \circ (1234) = (124)(357) \quad e \quad (1237) \circ (3245) \circ (53) = (537124)$$

Sia dunque $f \in S_n$ una permutazione e $f = \sigma_1 \circ \sigma_2 \ldots \circ \sigma_t$ sia la fattorizzazione di f in cicli disgiunti, con σ_i ciclo di lunghezza l_i.

Definizione 2.16 Possiamo definire il numero intero

$$N(f) = (l_1 - 1) + (l_2 - 1) + \ldots + (l_t - 1) = \Sigma_{i=1}^t (l_i - 1) = \Sigma_{i=1}^t l_i \ - \ t.$$

Una permutazione f si dice di *classe pari* o *dispari* a seconda che $N(f)$ sia pari o dispari.

Sia ora $(a_1 a_2 \ldots a_l)$ un ciclo di lunghezza l. Allora

$$(a_1 a_2 \ldots a_l) = (a_1 a_l) \circ (a_1 a_{l-1}) \circ \ldots \circ (a_1 a_3) \circ (a_1 a_2).$$

Poiché ogni permutazione è prodotto di cicli, abbiamo provato il seguente:

Lemma 2.2 *Ogni permutazione si può scrivere come prodotto di trasposizioni.*

Osservazione 2.17 Attenzione che in questo caso non si tratta di trasposizioni disgiunte e nemmeno tale scrittura è unica!

Vediamo un esempio di come si possa scrivere una permutazione come prodotto di cicli disgiunti e di come calcolare $N(f)$.

Esempio 2.18 Si scriva la permutazione

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

come prodotto di cicli disgiunti, come prodotto di trasposizioni e se ne calcoli il segno. $f = (124569)(378)$ è la fattorizzazione di f in cicli disgiunti e $N(f) = (6-1) + (3-1) = 7$ e quindi f è dispari. Infine $f = (124569)(378) = (19)(16)(15)(14)(12)(38)(37)$, è una fattorizzazione di f come prodotto di trasposizioni.

2.3 Esercizi

Come alla fine di ogni capitolo, riportiamo alcuni esercizi che riguardano i gruppi in generale. Si chiederà per lo più di dimostrare che un insieme sul quale è definita un'operazione è un gruppo. Seguiranno alcuni esercizi sulle permutazioni.

Esercizio 2.19 *Sia A un gruppo abeliano, a e b elementi di A di ordine rispettivamente m ed n (n,m interi). Allora l'ordine di ab divide mn.*

Esercizio 2.20 *Sia G un gruppo e siano $a_1, a_2, a_3 \in G$. Provare che l'inverso del prodotto $a_1a_2a_3$ è l'elemento $a_3^{-1}a_2^{-1}a_1^{-1}$.*

Esercizio 2.21 *Sia G il prodotto cartesiano $\mathbb{Q} \times \mathbb{Z}^*$ ove $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Definiamo un'operazione su G nel modo seguente: $(q, m) \cdot (q', m') = (q + mq', mm')$. Si provi che $(G, \cdot)$ è un monoide e si calcolino gli elementi invertibili. E' G abeliano? E' G un gruppo?*

Esercizio 2.22 *Sia X un insieme e sia $\triangle$ la differenza simmetrica, cioè l'operazione su $\mathcal{P}(X)$ così definita :*

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

Si provi che $(\mathcal{P}(X), \triangle)$ è un gruppo abeliano. Si calcolino i periodi degli elementi di $(\mathcal{P}(X), \triangle)$.

Esercizio 2.23 *Si dica quali dei seguenti monoidi sono dei gruppi: $(\{0\}, +)$, $(\{0, 1\}, \cdot)$, $(\{1, -1\}, \cdot)$, $(\mathbb{Q}_+, \cdot)$, ove $\cdot$ è l'usuale moltiplicazione di $\mathbb{Q}$.*

Esercizio 2.24 *Si calcolino gli elementi invertibili dei seguenti monoidi e si dica se sono dei gruppi: $(\mathcal{P}(X), \cup)$, $(\mathcal{P}(X), \cap)$.*

Esercizio 2.25 *Sia G il prodotto cartesiano $\mathbb{Q}^* \times \mathbb{Q}$. Definiamo un'operazione su G nel modo seguente: $(a, b) \cdot (a', b') = (aa', ab' + b/a')$. Si provi che $(G, \cdot)$ è un gruppo. E' abeliano?*

Esercizio 2.26 *Sia $G = \{$funzioni $f : \mathbb{R} \to \mathbb{R}.\}$. Si definisca la funzione somma $f + g$ nel modo seguente $(f + g)(x) = f(x) + g(x)$. Si dimostri che $(G, +)$ è un gruppo abeliano.*

Esercizio 2.27 *Sia $G = \{f : \mathbb{R} \to \mathbb{R}$, tali che $f(x) = ax + b$ con $a, b \in \mathbb{R}$, $a \neq 0\}$. Si dimostri che G è un sottoinsieme di $S_{\mathbb{R}}$, l'insieme di tutte le applicazioni biiettive di $\mathbb{R}$ in se'. Si provi che G è un gruppo rispetto alla composizione di funzioni. G è abeliano?*

Esercizio 2.28 *Sia $(M, \cdot)$ un monoide. Sia $U = \{u \in M : u$ è invertibile$\}$. Si dimostri che $(U, \cdot)$ è un gruppo.*

Esercizio 2.29 *Se σ è un ciclo è vero che anche il suo quadrato σ^2 è un ciclo?*

Esercizio 2.30 *Dimostrare che:*

(a) ogni permutazione in S_3 è un ciclo;

(b) le uniche permutazioni in S_4 che non sono cicli sono $(12)(34), (13)(24)$ e $(14)(23)$;

(c) descrivere tutte le permutazioni di S_5 e S_6 che non sono cicli.

Esercizio 2.31 *Sia σ la permutazione di S_{12} definita come segue:*

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

Si trovi la decomposizione in cicli disgiunti delle permutazioni σ, σ^2, σ^3 e σ^5.

Esercizio 2.32 *Siano σ e τ le permutazioni di S_{10} definite come segue:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 5 & 7 & 9 & 8 & 10 & 6 & 3 & 1 \end{pmatrix}, \qquad \tau = (23).$$

i) Si trovi la decomposizione in cicli disgiunti di σ, τ, $\sigma\tau$ e $\tau\sigma$.

Esercizio 2.33 *Siano σ e τ le permutazioni di S_8 definite rispettivamente come segue:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 & 3 & 2 & 1 & 4 \end{pmatrix}.$$

i) Si dimostri che $\sigma\tau = \tau^{-1}\sigma$.

ii) Si trovi la decomposizione in cicli disgiunti di σ, τ e $\sigma\tau$.

3 Sottogruppi e classi laterali

3.1 Sottogruppi

Definizione 3.1 Un sottoinsieme non vuoto H di un gruppo G si dice *sottogruppo* se:

(S1) H è *stabile*, cioè $xy \in H$ per ogni coppia di elementi $x, y \in H$;

(S2) se $x \in H$, allora anche $x^{-1} \in H$.

Per indicare che H è un sottogruppo di G scriveremo $H \leq G$.

Chiaramente, $1 \in H$ per ogni sottogruppo H, poiché (S1) implica $1 = xx^{-1} \in H$ per ogni elemento $x \in H$ in quanto $x^{-1} \in H$ per (S2).

Esempio 3.2 Ci sono sempre i sottogruppi $G \leq G$ e $\{1\} \leq G$, che chiameremo *banali*. In certi casi non ci sono sottogruppi non banali, come vedremo nel Lemma 3.29 nel gruppo $(\mathbb{Z}_p, +)$, con p primo.

Un sottogruppo H di G si dice *proprio* se $H < G$, cioé $\neq G$.

I sottogruppi di un gruppo G sono precisamente i sottoinsiemi H di G che risultano dei gruppi con la *stessa* operazione di G, cioè con la restrizione dell'operazione di G in H. Di conseguenza l'operazione del sottogruppo H ha le stesse proprietà di quella di G: ad esempio se G è abeliano, anche il suo sottogruppo H lo è.

Vediamo ora qualche esempio di sottogruppo. Iniziamo con gli esempi numerici, la cui dimostrazione è un facile esercizio.

Esempio 3.3 Alcuni sottogruppi del gruppo additivo dei numeri complessi sono:

$$(\mathbb{Z}, +) \ \leq \ (\mathbb{Q}, +) \ \leq (\mathbb{R}, +) \ \leq (\mathbb{C}, +).$$

E alcuni sottogruppi del gruppo moltiplicativo dei numeri complessi non nulli:

$$(\mathbb{Q}^*, \cdot) \ \leq \ (\mathbb{R}^*, \cdot) \ \leq (\mathbb{C}^*, \cdot) \ \text{ e } \ \text{ anche } \ (\mathbb{S}, \cdot) \leq (\mathbb{C}^*, \cdot).$$

Infine $(\mathbb{Z}^*, \cdot)$ eredita la struttura di gruppo moltiplicativo per esempio da $(\mathbb{Q}^*, \cdot)$ ma, pur essendo stabile rispetto alla moltiplicazione, non è un sottogruppo di $(\mathbb{Q}^*, \cdot)$, in quanto gli unici elementi invertibili sono $1, -1$.

Vediamo ora alcuni esempi di sottogruppi di un gruppo non abeliano.

Esempio 3.4 Sia S_X il gruppo delle permutazioni su un insieme X. Sia $A \subseteq X$ e sia

$$H = \{f \in S_X : f(a) = a \text{ per ogni } a \in A\}.$$

Allora H è un sottogruppo. Infatti l'identità appartiene ad H, che pertanto non è vuoto. Inoltre se $f, g \in H$, si ha $(f \circ g)(a) = f(g(a)) = f(a) = a$ per ogni $a \in A$, da cui segue che $f \circ g \in H$. Infine se $f \in H$ e $a \in A$, si ha $a = f(a)$, da cui, applicando f^{-1}, $f^{-1}(a) = f^{-1}(f(a)) = (f^{-1} \circ f)(a) = id(a) = a$. Concludiamo che anche f^{-1} appartiene ad H.

Esempio 3.5 Sia S_n il gruppo delle permutazioni su un insieme con n elementi. Consideriamo

$$A_n = \{f \in S_n : f \text{ e' di classe pari}\}.$$

Innanzitutto A_n non è vuoto, perché l'identità ha classe pari. Come dimostrato nel corso di Aritmetica, se f e g sono due permutazioni di classe pari, allora anche $f \circ g$ è di classe pari. Inoltre se $f = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_t$ è la fattorizzazione di f in cicli disgiunti, $f^{-1} = \sigma_1^{-1} \circ \sigma_2^{-1} \ldots \circ \sigma_t^{-1}$ è la fattorizzazione di f^{-1} in cicli disgiunti (perché?). Poiché la lunghezza di σ_i^{-1} coincide con la lunghezza di σ_i, si ha $N(f) = N(f^{-1})$. Abbiamo così dimostrato che A_n è un sottogruppo di S_n. Il sottogruppo A_n si chiama *gruppo alterno*.

Il lemma seguente fornisce un criterio per verificare se un sottoinsieme è un sottogruppo.

Lemma 3.6 *Un sottoinsieme non vuoto H di un gruppo G è un sottogruppo se e solo se*

$$x^{-1}y \in H \text{ per ogni coppia di elementi } x, y \in H. \tag{1}$$

DIMOSTRAZIONE. Sia $H \leq G$. Se $x, y \in H$, allora $x^{-1} \in H$ per (S2), e quindi $x^{-1}y \in H$ per (S1).

Supponiamo adesso che valga (1). Essendo H non vuoto esiste almeno un elemento $x_0 \in H$. Allora ponendo $y = x_0$ ricaviamo $1 = x_0^{-1}x_0 \in H$. Per verificare (S2) prendiamo un elemento $x \in H$. Allora applicando (1) ad x e $y = 1$ troviamo $x^{-1} = x^{-1}1 \in H$. Per dimostrare che vale anche (S1) prendiamo due elementi $x, y \in H$. Per (S2) già dimostrata, vale $x^{-1} \in H$. Quindi, dalla (1) applicata a x^{-1} e y ricaviamo $xy = (x^{-1})^{-1}y \in H$. □

Applicando il Lemma 3.6 si può provare:

Corollario 3.7 *Se H e K sono sottogruppi di un gruppo G, allora $H \cap K$ è un sottogruppo di G.*

Lemma 3.8 *L'intersezione di una famiglia qualsiasi di sottogruppi di un gruppo G è ancora un sottogruppo di G.*

DIMOSTRAZIONE. Sia $\{H_i\}_{i \in I}$ una famiglia di sottogruppi del gruppo G e sia $H = \bigcap_{i \in I} H_i$. Allora $1 \in H_i$ per ogni $i \in I$, quindi $1 \in H$. Per $x, y \in H$ si ha $x, y \in H_i$ per ogni $i \in I$. Quindi (1) implica $x^{-1}y \in H_i$ per ogni $i \in I$. Di conseguenza $x^{-1}y \in H$. Per il Lemma 3.6 H è un sottogruppo. □

Se X è un sottoinsieme di G, l'intersezione di tutti i sottogruppi di G contenenti X è un sottogruppo di G che si chiama *sottogruppo generato da X* e si denota con $\langle X \rangle$. Chiaramente, $\langle X \rangle$ è *il più piccolo sottogruppo di G contenente X*.

In particolare, se $G = \langle X \rangle$ diremo che X è un *sistema di generatori* di G oppure che G è *generato* da X. Inoltre, per alleggerire la notazione, se X è un insieme finito, $X = \{x_1, x_2, ..., x_n\}$ scriveremo $\langle X \rangle = \langle x_1, x_2, ..., x_n \rangle$ e diremo che G è *finitamente generato*.

Lemma 3.9 *Sia $X = \{x\}$. Allora il sottogruppo generato da X coincide con l'insieme $\{x^n : n \in \mathbb{Z}\}$ di tutte le potenze di x.*

DIMOSTRAZIONE. Poiché $\langle X \rangle$ è un sottogruppo, sfruttando (S1) e (S2) si può dimostrare per induzione che $x^n \in \langle X \rangle$ per ogni $n \in \mathbb{Z}$. Pertanto l'insieme delle potenze $H = \{x^n : n \in \mathbb{Z}\}$ è contenuto in $\langle X \rangle$. Per l'altra inclusione basta vedere che H è un sottogruppo. Infatti, se $x^n, x^m \in H$, allora $x^m x^n = x^{m+n} \in H$ e $(x^n)^{-1} = x^{-n} \in H$. Allora H è un sottogruppo che contiene x e pertanto contiene $\langle x \rangle$. □

Definizione 3.10 Un gruppo che sia generato da un solo elemento si dice *ciclico*.

I gruppi ciclici sono importanti per lo studio dei gruppi, perché un gruppo arbitrario è ricoperto dai suoi sottogruppi ciclici. Ovviamente $\mathbb{Z}$ è un gruppo ciclico essendo generato dal suo elemento 1. Vediamo ora altri esempi di sottogruppo generato da un elemento. Calcoliamo i sottogruppi di $(\mathbb{Z}, +)$ e dimostriamo che tutti i sottogruppi di $(\mathbb{Z}, +)$ sono di questo tipo.

Lemma 3.11 *Sia $n \in \mathbb{N}$. Allora*
(i) l'insieme $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\} = \langle n \rangle$ è un sottogruppo di $\mathbb{Z}$;
(ii) se H è un sottogruppo di $\mathbb{Z}$, allora esiste $n \in \mathbb{Z}$ tale che $H = n\mathbb{Z}$.

DIMOSTRAZIONE. (i) Per il Lemma 3.9 in notazione additiva, il sottogruppo $\langle n \rangle$ è proprio $\{nz : z \in \mathbb{Z}\}$.

(ii) Se $H = \{0\}$, basta prendere $n = 0$. Supponiamo ora $H \neq 0$. Allora esiste un elemento $h \in H$, $h \neq 0$. Se $h < 0$, allora $-h \in H$ e $-h > 0$. Possiamo quindi supporre che esista $h_1 \in H$ con $h_1 > 0$. Per il principio del buon ordinamento in N, esiste $h_0 \in H$ tale che $h_0 > 0$ e h_0 è minimale tra tutti gli elementi positivi di H. Ovviamente, $\langle h_0 \rangle \leq H$. Sia $x \in H$. Dividendo x per h_0 con resto troviamo $q \in \mathbb{Z}$ e $0 \leq r < h_0$ tali che $x = qh_0 + r$. Poiché $qh_0 \in H$ e $x \in H$, ne deduciamo che anche $r = x - qh_0 \in H$. Essendo $r < h_0$, r non può essere positivo. Quindi $r = 0$ e pertanto $x = qh_0 \in \langle h_0 \rangle$. Questo dimostra che $H = \langle h_0 \rangle$. □

Dato un elemento x di un gruppo G, possiamo considerare l'ordine del sottogruppo generato da x e il suo ordine come elemento di G, definito in 2.5. Dimostriamo ora che questa duplice definizione di "ordine" non da' luogo a nessuna contraddizione, perché in effetti coincidono.

Lemma 3.12 *Sia G un gruppo e x un suo elemento. Allora $|\langle x \rangle| = o(x)$.*

DIMOSTRAZIONE. Se $o(x) = m$, per il Lemma 2.6 b), avremo $x^n = x^k$ per $n, k \in \mathbb{Z}$ se e solo se $n \equiv_m k$. Allora, per quanto dimostrato nel corso di Aritmetica, $\{x^n : n \in \mathbb{Z}\} = \{x^0, x^1, ...x^{m-1}\}$, da cui concludiamo per il Lemma 3.9 che $|\langle x\rangle| = |\{x^0, x^1, ...x^{m-1}\}| = m$.

Viceversa supponiamo $|\langle x\rangle| = m$, allora per il Lemma 3.9, esistono $n_1, n_2 \in \mathbb{Z}$, con $n_1 < n_2$ tali che $x^{n_1} = x^{n_2}$. Moltiplicando a destra e a sinistra per x^{-n_1}, otteniamo $x^{n_2-n_1} = 1$ e $n_2 - n_1 > 0$, da cui segue che $S(x) = \{n \in \mathbb{N}^* : x^n = 1\}$ non è vuoto. Dalla definizione 2.5 sappiamo che allora $o(x) = d < \infty$. Per quanto appena dimostrato, $o(x) = d$ implica $d = |\langle x\rangle| = m$.

Abbiamo dimostrato che $o(x) = m$ se e solo se $|\langle x\rangle| = m$, da cui segue $o(x) = \infty$ se e solo se $|\langle x\rangle| = \infty$. □

Si osservi che l'unione di sottogruppi non è in generale un sottogruppo. Vale infatti il seguente fatto.

Lemma 3.13 *Siano H e K sottogruppi di un gruppo G. Allora $H \cup K$ è un sottogruppo di G se e solo se $H \subseteq K$ oppure $K \subseteq H$.*

DIMOSTRAZIONE. Ovviamente, $H \cup K$ è un sottogruppo se $H \subset K$ oppure $K \subset H$ poiché in tal caso $H \cup K$ coincide con K o con H rispettivamente.

Supponiamo adesso che $H \cup K$ sia un sottogruppo di G e che $H \not\subseteq K$. Allora esiste $h \in H$ con $h \notin K$. Per dimostrare che $K \subseteq H$ prendiamo un elemento arbitrario $k \in K$. Allora $k \in H \cup K$ e anche $h \in H \cup K$. Poiché $H \cup K$ è un sottogruppo di G avremo anche $hk \in H \cup K$, ma $hk \notin K$. Infatti, se hk fosse un elemento di K, moltiplicandolo a destra per $k^{-1} \in K$ troveremmo $h = (hk)k^{-1} \in K$, assurdo. Quindi, $hk \notin K$ e di conseguenza $hk \in H$. Moltiplicando a sinistra per $h^{-1} \in H$ troviamo $k = h^{-1}(hk) \in H$. □

Corollario 3.14 *Un gruppo G non può essere unione di due suoi sottogruppi propri.*

DIMOSTRAZIONE. Supponiamo per assurdo che esistano due sottogruppi propri H, K di G tali che $G = H \cup K$. Allora per il Lemma 3.13, $H \leq K$ oppure $K \leq H$. Supponiamo per esempio $H \leq K$. Allora $G = H \cup K = K$, in contraddizione col fatto che K è un sottogruppo proprio di G. □

Vedremo nell'Esercizio 4.23 che un gruppo può essere unione di tre sottogruppi propri.

Siano H e K sottogruppi di G; in seguito denoteremo con $\langle H, K\rangle$ il sottogruppo $\langle H \cup K\rangle$. Con il simbolo HK indichiamo l'insieme dei prodotti $\{hk \mid h \in H, k \in K\}$. Chiaramente HK è contenuto in $\langle H, K\rangle$ ma in generale non coincide con $\langle H, K\rangle$.

Lemma 3.15 *Siano H e K sottogruppi di un gruppo G. Allora $HK = KH$ se e solo se $\langle H, K\rangle = HK$.*

DIMOSTRAZIONE. Se $\langle H, K\rangle = HK$, allora HK è un sottogruppo di G, che contiene sia H che K e pertanto contiene anche i loro prodotti, cioè $KH \subseteq HK$. Se consideriamo gli inversi di entrambi i lati, otteniamo $HK \subseteq KH$, e pertanto $HK = KH$. Viceversa, se $HK = KH$, basterà dimostrare che HK è un sottogruppo di G. Se $h_1, h_2 \in H$ e $k_1, k_2 \in K$, allora

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1}h_2) = h_1(h_3k_3)$$

per qualche $h_3 \in H$, $k_3 \in K$. Pertanto $h_1k_1(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$ e quindi HK è un sottogruppo. □

Se due sottogruppi sono nella particolare situazione del Lemma 3.15, diremo che permutano. Infatti

Definizione 3.16 Siano H, K sottogruppi di un gruppo G. Se $HK = KH$ si dice che H e K *permutano*.

È noto che vale la legge distributiva dell'unione rispetto all'intersezione di insieme. Vediamo che in generale la legge distributiva del prodotto di sottogruppi rispetto all'intersezione non vale, cioè dati 3 qualsiasi sottogruppi H, K, L di un gruppo G, NON vale

$$(HK) \cap L = (H \cap L)(K \cap L). \qquad (*)$$

Di certo si ha $(H \cap L)(K \cap L) \subseteq (HK) \cap L$, perché $H \cap L \subseteq H$ e $K \cap L \subseteq K$, da cui $(H \cap L)(K \cap L) \subseteq HK$, ma anche $H \cap L \subseteq L$, $K \cap L \subseteq L$, da cui $(H \cap L)(K \cap L) \subseteq L$, in quanto L è un sottogruppo. Il seguente esempio dimostra che l'altra inclusione non vale in generale.

Esempio 3.17 Siano $G = S_3$, $H = \langle(123)\rangle$, $K = \langle(12)\rangle$ e $L = \langle(13)\rangle$. Allora $HK = G$, $H \cap L = \{1\}$ e $K \cap L = \{1\}$ da cui

$$(HK) \cap L = G \cap L = L = \langle(13)\rangle > (H \cap L)(K \cap L) = \{1\}.$$

Vale però una forma particolare della legge distributiva.

Teorema 3.18 (Legge modulare di Dedekind) *Siano H, K, L sottogruppi di un gruppo e sia $K \subseteq L$. Allora $(HK) \cap L = (H \cap L)K$. In particolare se H e K permutano, si ha $\langle H, K\rangle \cap L = \langle H \cap L, K\rangle$.*

DIMOSTRAZIONE. La prima inclusione è già stata dimostrata nel caso più generale in $(*)$. Viceversa supponiamo $x \in (HK) \cap L$, allora $x = hk$ per qualche $h \in H$ e $k \in K$, da cui $h = xk^{-1} \in LK = L$, cioè $h \in H \cap L$. Ma allora $x \in (H \cap L)K$. La seconda parte discende direttamente dal Lemma 3.15. □

3.2 Classi laterali di un sottogruppo

Se H è un sottogruppo di un gruppo G, introduciamo in G una relazione binaria ponendo $x \sim y$ quando $x^{-1}y \in H$.

Lemma 3.19 *(a) $\sim$ è una relazione di equivalenza.*
(b) la classe di equivalenza $[x]_\sim$ coincide con l'insieme $\{xh : h \in H\}$, che denoteremo brevemente con xH.
(c) $\{xH : x \in G\}$ è una partizione di G.

DIMOSTRAZIONE. (a) Sia $x \in G$. Allora $x \sim x$ in quanto $x^{-1}x \in H$. Se $x \sim y$, allora $x^{-1}y \in H$. Per la proprietà (S2) ricaviamo $y^{-1}x = (x^{-1}y)^{-1} \in H$, e di conseguenza $y \sim x$. Se $x \sim y$ e $y \sim z$, allora $x^{-1}y \in H$ e $y^{-1}z \in H$. Moltiplicando questi due elementi di H si ricava da (S1) $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$. Questo dimostra (a).
(b) Sia $y \in [x]_\sim$. Allora $x \sim y$ e quindi $x^{-1}y \in H$. Pertanto $x^{-1}y = h$ per qualche elemento $h \in H$. Deduciamo che $y = xh$.
Viceversa, se $y = xh$ per qualche elemento $h \in H$, allora $x^{-1}y = h \in H$, e quindi $x \sim y$ e $y \in [x]_\sim$.
(c) Le classi di equivalenza di una relazione di equivalenza costituiscono una partizione, quindi per (a) e (b) $\{xH : x \in G\}$ è una partizione di G. □

In seguito chiameremo la classe di equivalenza xH *classe laterale sinistra* di H in G.
Analogamente, per un sottogruppo H del gruppo G, si introduce la relazione $x \sim' y$ quando $xy^{-1} \in H$. Il seguente lemma è un facile esercizio.

Lemma 3.20 *Verificare che*
(a) $\sim'$ è una relazione di equivalenza.
(b) la classe di equivalenza $[x]_{\sim'}$ coincide con l'insieme $\{hx : h \in H\} = Hx$.
(c) $\{Hx\}_{x \in G}$ è una partizione di G.

Analogamente la classe di equivalenza Hx si dice *classe laterale destra* di H in G.
Vediamo alcuni esempi.

Esempio 3.21 Sia $G = (\mathbb{Z}, +)$ e sia $H = 4\mathbb{Z}$. Abbiamo visto nel Lemma 3.11 che H è un sottogruppo di G. Troviamo le classi laterali sinistre di H (in notazione additiva):
$0 + 4\mathbb{Z} = \{4m : m \in \mathbb{Z}\}$, $1 + 4\mathbb{Z} = \{1 + 4m : m \in \mathbb{Z}\}$,
$2 + 4\mathbb{Z} = \{2 + 4m : m \in \mathbb{Z}\}$, $3 + 4\mathbb{Z} = \{3 + 4m : m \in \mathbb{Z}\}$.
Poiché il gruppo è abeliano le classi laterali destre coincidono con le classi laterali sinistre.

Vediamo ora un esempio di un sottogruppo di un gruppo finito non abeliano, in cui le classi laterali sinistre non coincidono con le classi laterali destre.

Esempio 3.22 Sia $G = S_3$ il gruppo delle permutazioni su 3 oggetti e sia $H = \langle(12)\rangle$. Troviamo le classi laterali sinistre di H:
$id \circ H = \{id, (12)\}$, $(123) \circ H = \{(123), (13)\}$, $(132) \circ H = \{(132), (23)\}$.
Mentre le classi laterali destre sono:
$H \circ id = \{id, (12)\}$, $H \circ (123) = \{(123), (23)\}$, $(132) \circ H = \{(132), (13)\}$.

In generale quindi le classi laterali destre e sinistre non coincidono. Si può invece dimostrare che hanno la stessa cardinalità:

Lemma 3.23 *Sia G un gruppo ed $H \leq G$. Ogni classe laterale di H in G ha la stessa cardinalità di H.*

DIMOSTRAZIONE. Sia $x \in G$. Definiamo un'applicazione $f : H \to xH$ ponendo $f(h) = xh$. Per la definizione di xH, f è suriettiva. Verifichiamo ora che f è anche iniettiva. Infatti, se $f(h) = f(h')$, allora $xh = xh'$ e per la legge di cancellazione si ricava $h = h'$. Quindi, xH ha la stessa cardinalità di H. Allo stesso modo si verifica che anche le classi laterali destre hanno la stessa cardinalità di H. □

Lemma 3.24 *Sia G un gruppo ed $H \leq G$. La cardinalità dell'insieme $\{xH\}_{x\in G}$ delle classi laterali sinistre di H in G coincide con la cardinalità dell'insieme $\{Hx\}_{x\in G}$ delle classi laterali destre di H in G.*

DIMOSTRAZIONE. Infatti, ad ogni classe laterale sinistra xH corrisponde la classe laterale destra Hx^{-1} e questa corrispondenza definisce una biiezione tra i due insiemi. □

Definizione 3.25 La cardinalità comune degli insiemi $\{xH\}_{x\in G}$ e $\{Hx\}_{x\in G}$ si indica con $[G : H]$ e si dice *indice* del sottogruppo H in G.

Il seguente celebre teorema di Lagrange rivela una relazione semplice, ma molto utile tra la cardinalità di un sottogruppo H di un gruppo finito e l'indice di H:

Teorema 3.1 (Teorema di Lagrange) *Sia G un gruppo finito ed H un suo sottogruppo. Allora $|G| = [G : H]|H|$.*

DIMOSTRAZIONE. Abbiamo dimostrato che la relazione $\sim$ definita nel Lemma 3.19 è una relazione di equivalenza. Pertanto G è unione disgiunta delle classi di questa equivalenza, che sono le classi laterali sinistre di H in G. Ci sono esattamente $[G : H]$ di queste classi e abbiamo dimostrato nel Lemma 3.23 che ognuna di queste ha la stessa cardinalità di H. Allora $|G| = [G : H]|H|$. □

Il Teorema di Lagrange ha due importantissimi corollari che permettono di mettere in relazione l'ordine di un gruppo finito e quello dei suoi sottogruppi:

Corollario 3.26 *Sia G un gruppo finito e H un sottogruppo di G. Allora $|H|$ divide $|G|$.*

Quindi se consideriamo un gruppo di ordine 12, come ad esempio $G = \mathbb{Z}_{12}$, G non potrà avere sottogruppi di ordine 5 o 10, ma potrà avere sottogruppi di ordine $2, 3, 4$ o 6, oltre a quelli banali di ordine 1 e 12. Come vedremo più avanti, non è detto che li abbia.

Il Teorema di Lagrange ci permette inoltre di conoscere i possibili periodi degli elementi di un certo gruppo finito G. Infatti

Corollario 3.27 *Sia G un gruppo finito e x un elemento di G. Allora $o(x)$ divide $|G|$.*

DIMOSTRAZIONE. Per il Lemma 3.12, $o(x) = |\langle x\rangle|$, da cui per il Corollario 3.26, $o(x)$ divide $|G|$. □

Applichiamo il Teorema di Lagrange per calcolare tutti i sottogruppi di un gruppo.

Esempio 3.28 Calcoliamo tutti i sottogruppi di $G = (\mathbb{Z}_3, +)$. Se H è un sottogruppo di G, $|H|$ deve dividere 3. Quindi le sole possibilità sono $|H| = 1, 3$, da cui segue che H può essere solo $\{0\}$ o G.

Come si vede dall'esempio 3.28, lo stesso ragionamento vale ogni qualvolta si abbia un gruppo di ordine un primo. Inoltre i gruppi di ordine un primo sono sempre ciclici.

Lemma 3.29 *Sia G un gruppo di ordine p. Allora*
i) gli unici sottogruppi di G sono $\{1_G\}$ e G;
ii) G è ciclico;
iii) tutti gli elementi non nulli di G hanno ordine p e generano G.

DIMOSTRAZIONE. *i)* Se H è un sottogruppo di G, $|H|$ deve dividere p, per il Teorema di Lagrange. Quindi le sole possibilità sono $|H| = 1, p$, da cui segue che H può essere solo $\{1_G\}$ o G.

ii) e *iii)*. Sia x un elemento di G, $x \neq 1$. Allora per *i)*, $|\langle x \rangle| = p$ e quindi coincide con G. Per il Lemma 3.12 si ha infine $o(x) = p$. □

Il Teorema di Lagrange vale solo per gruppi finiti. Anche per i gruppi infiniti però si può dire qualcosa, come si dimostra nel seguente Lemma.

Lemma 3.30 *Se H e K sono sottogruppi di indice finito del gruppo G, allora anche il sottogruppo $H \cap K$ ha indice finito.*

DIMOSTRAZIONE. Basta provare che il sottogruppo $H \cap K$ ha un numero finito di classi laterali sinistre. Ricordiamo adesso che le classi laterali sinistre di $H \cap K$ sono le classi di equivalenza della relazione di equivalenza $\sim$ definita da $x \sim y$ se e solo se $x^{-1}y \in H \cap K$. Chiaramente, questo è equivalente a $x^{-1}y \in H$ e $x^{-1}y \in K$, cioè $x \sim_H y$ e $x \sim_K y$, dove $\sim_H$ e $\sim_K$ sono le relazione di equivalenza relative ai sottogruppi H e K. Queste ultime relazioni di equivalenza danno luogo alle partizioni $G = \bigcup_{x \in G} xH$ e $G = \bigcup_{x \in G} xK$ di G che sono finite per ipotesi. Le classi di equivalenza della relazione $\sim$ sono intersezioni delle classi di equivalenza delle relazioni $\sim_H$ e $\sim_K$. Pertanto, tutte le intersezioni non vuote $\{xH \cap yK\}_{x,y \in G}$ danno luogo ad una partizione nuova che corrisponde alla relazione di equivalenza $\sim$. Ovviamente, esse sono un numero finito. □

In generale se G è un gruppo infinito e H un sottogruppo di G, si ha $|G| = max\{[G : H], |H|\}$. La dimostrazione di questo fatto, che utilizza proprietà dei numeri cardinali infiniti, viene lasciata negli esercizi (vedi esercizio 3.43).

3.3 Esercizi sui sottogruppi

Concludiamo il capitolo con alcuni esercizi sui sottogruppi.

Esercizio 3.31 *Sia $X = \{x, y\}$. Allora il sottogruppo generato da X coincide con l'insieme dei prodotti*

$$H = \{x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k} : k \in \mathbb{N}_+, n_i, m_i \in \mathbb{Z} \text{ per } i = 1, 2, \dots, k\}.$$

Se x e y sono permutabili, allora $\langle X \rangle$ coincide con l'insieme $\{x^n y^m : n, m \in \mathbb{Z}\}$.

Esercizio 3.32 *Sia $X = H \cup K$, dove H e K sono sottogruppi di G. Provare che:*

(a) Il sottogruppo generato da X coincide con l'insieme

$$\{h_1k_1h_2k_2 \dots h_sk_s : s \in \mathbb{N}_+, h_i \in H, k_i \in K \text{ per } i = 1, 2, \dots, s\}.$$

(b) Se G è abeliano, il sottogruppo generato da X coincide con l'insieme $\{hk : h \in H,\ k \in K\}$.

Esercizio 3.33 *Ricavare la conclusione dell'Esercizio 3.31 dal Lemma 3.9 e dall' Esercizio 3.32.*

Esercizio 3.34 *Si dimostri che l'insieme $\{(12)(34), (13)(24), (14)(23), id\}$ è un sottogruppo di S_4.*

Esercizio 3.35 *Sia G un gruppo finito. Un sottoinsieme non vuoto H di G è un sottogruppo se H è stabile, ovvero $ab \in H$ per ogni a, b in H.*

Esercizio 3.36 *Sia G il gruppo delle funzioni reali a variabile reale con la somma, come definito nell'esercizio 2.26. Si dimostri che i seguenti insiemi sono dei sottogruppi di G:*
i) $\mathcal{C}(\mathbb{R}) = \{$funzioni continue $f : \mathbb{R} \to \mathbb{R}\}$,
ii) $\mathcal{D}(\mathbb{R}) = \{$funzioni derivabili $f : \mathbb{R} \to \mathbb{R}\}$,
iii) $\mathcal{I}(\mathbb{R}) = \{$funzioni integrabili $f : \mathbb{R} \to \mathbb{R}\}$.

Esercizio 3.37 *Siano G ed H due gruppi e sia $G \times H$ il gruppo prodotto diretto definito nel Teorema 1.14. Si dimostri che i seguenti sottoinsiemi sono sottogruppi:*
i) $G_1 = \{(g, 1_H) : g \in G\}$,
ii) $H_1 = \{(1_G, h) : h \in H\}$.

Esercizio 3.38 *Sia G un gruppo e sia $G \times G$ il gruppo prodotto diretto definito nel Teorema 1.14. Si dimostri che $D = \{(g, g) : g \in G\}$ è un sottogruppo di $G \times G$.*

Esercizio 3.39 *Sia V uno spazio vettoriale di dimensione 3 sul campo $\mathbb{R}$, generato dai vettori e_1, e_2 ed e_3. Si dimostri che il sottoinsieme $W = \{ae_1 + be_2 : a, b \in \mathbb{R}\}$ è un sottogruppo di V. Si descrivano le classi laterali destre e sinistre di W.*

Esercizio 3.40 *Sia V uno spazio vettoriale di dimensione n sul campo $\mathbb{R}$ e sia W un sottospazio proprio di V. Si descrivano le classi laterali destre e sinistre di W.*

Esercizio 3.41 *Sia $n \in \mathbb{N}$. Dato il sottogruppo $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ di $(\mathbb{Z}, +)$ si calcoli $[\mathbb{Z} : n\mathbb{Z}]$.*

Esercizio 3.42 *Per i gruppi $G = (\mathbb{Z}_2, +)$, $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_6, +)$, $(\mathbb{Z}_7, +)$, $(\mathbb{Z}_8, +)$, $(\mathbb{Z}_9, +)$ $(\mathbb{Z}_{10}, +)$ descrivere tutti i sottogruppi H di G e calcolare l'indice $[G : H]$. Determinare qual è il gruppo con il maggior numero di sottogruppi.*

Esercizio 3.43* *Sia G un gruppo infinito e H un sottogruppo di G. Allora $|G| = max\{[G : H], |H|\}$.*

Esercizio 3.44 *Si dimostri che $H = \{x + iy : 5x + 3y = 0\}$ è un sottogruppo del gruppo additivo dei numeri complessi.*

Esercizio 3.45 *Elencare tutti i sottogruppi di A_4 di ordini 2, 3, 4 (vedere l' Esempio 3.5 per la definizione di A_4).*

Esercizio 3.46 *Elencare tutti i sottogruppi di S_3.*

Esercizio 3.47 *Si provi che l'insieme*

$$S = \{\rho(\cos(2k\pi/3) + i\sin(2k\pi/3))|\ \rho \in \mathbb{R}, \rho > 0, k \in \mathbb{Z}\}$$

è un sottogruppo di $(\mathbb{C}^*, \cdot, 1)$. Calcolare la cardinalità di S.

Esercizio 3.48 *Sia $\mathbb{Q}$ il campo dei numeri razionali e si consideri il gruppo $G = \{(a, b)|a, b \in \mathbb{Q}, a \neq 0\}$ con l'operazione di moltiplicazione definita dalla posizione $(a, b) \cdot (c, d) = (ac, ad + b)$.*
i) Si determini l'unità di G e l'inverso dell'elemento $(a, b) \in G$.
ii) Si verifichi che $H = \{(a, 0)|a \in \mathbb{Q}, a \neq 0\}$ è un sottogruppo di G.

Esercizio 3.49 *Dimostrare che se H, K ed L sono sottogruppi di un gruppo abeliano G, non è detto che valga la legge distributiva del prodotto rispetto all'intersezione (vedi $(*)$ prima del Teorema 3.18 sulla Legge modulare di Dedekind).*

Esercizio 3.50* *Si deduca dal Lemma 3.8 che l'insieme $\mathcal{L}(G)$ dei sottogruppi di G ordinato per inclusione è un reticolo limitato avente G come elemento massimo e $\{1\}$ come minimo.*

4 Sottogruppi normali e quozienti

4.1 Sottogruppi normali

Definizione 4.1 Un sottogruppo H di un gruppo G si dice *normale* se vale $xH = Hx$ per ogni elemento $x \in G$. Si denota brevemente $H \trianglelefteq G$.

Chiaramente, quando $H \leq G$ è normale, non c'è più distinzione tra classi laterali *sinistre* e classi laterali *destre*. L'insieme delle classi laterali di H in G si indica con G/H.

Lemma 4.2 *Se G è un gruppo abeliano, allora tutti i sottogruppi sono normali.*

DIMOSTRAZIONE. Se G è abeliano e H è un sottogruppo di G, allora $xh = hx$ per ogni $x \in G$, $h \in H$ e quindi $xH = Hx$ per ogni $x \in G$, cioè H è normale. □

Non è però vero il viceversa. Esistono cioè dei gruppi in cui tutti i sottogruppi sono normali, ma che non sono abeliani, come vedremo nell'esercizio 4.23.

Se il gruppo non è abeliano, non tutti i sottogruppi sono normali, come dimostra il gruppo S_3. Infatti nell'esempio 3.22 vengono calcolate le classi laterali di $H = \langle(12)\rangle$ e si verifica $(123) \circ H \neq H \circ (123)$.

Dimostriamo ora un utile criterio per verificare se un sottogruppo di un gruppo G è normale, senza dover controllare l'uguaglianza delle classi laterali destre e sinistre.

Lemma 4.3 *Un sottogruppo H di un gruppo G è normale se e solo se*

$$x^{-1}hx \in H \text{ per ogni } x \in G \text{ e per ogni } h \in H. \qquad (*)$$

DIMOSTRAZIONE. Supponiamo che H sia normale. Sia $x \in G$ e $h \in H$. Allora $hx \in Hx = xH$, quindi esiste $h' \in H$ tale che $hx = xh'$. Di conseguenza $x^{-1}hx = h' \in H$. Questo dimostra $(*)$.

Supponiamo ora che valga $(*)$. Per dimostrare che H è normale bisogna provare che $xH = Hx$ per ogni elemento $x \in G$. Sia $x \in G$. Per vedere che $xH \subseteq Hx$ prendiamo un elemento $xh \in xH$. Per $(*)$ applicata all'elemento x^{-1}, esiste un elemento $h' \in H$ tale che $xhx^{-1} = h'$. Allora $xh = h'x$, e quindi $xh \in Hx$. Per dimostrare l'inclusione $Hx \subseteq xH$ si prenda un elemento $hx \in Hx$. Per $(*)$ abbiamo $x^{-1}hx \in H$ e quindi $x^{-1}hx = h'$ per qualche $h' \in H$. Di conseguenza $hx = xh' \in xH$. Quindi anche l'inclusione $Hx \subseteq xH$ è stata dimostrata. □

Osservazione 4.4 Nella dimostrazione precedente, abbiamo sfruttato il fatto che $(*)$ significa $x^{-1}hx = h'$ per *ogni elemento $x \in G$, ogni elemento $h \in H$ e un opportuno elemento $h' \in H$.* In generale, h' può non coincidere con h. Tuttavia, questa regola di *scambio* ci permette di avere per ogni $x \in G$ e per ogni $h \in H$ un certo $h' \in H$ tale che $xh = h'x$ (più precisamente, $h' = x^{-1}hx$).

Definizione 4.5 Sia G un gruppo e $x \in G$. Allora il *coniugato* di x tramite g è l'elemento $g^{-1}xg$, che denotiamo con x^g. Se H è un sottogruppo di G, il *coniugato* di H tramite g è il sottoinsieme $\{h^g : g \in G\}$, che denotiamo con H^g.

In questi termini, nell'Osservazione 4.4 h' è il coniugato di h tramite x. È facile verificare che H^g è un sottogruppo di G (vedi Esercizio 4.26).

Usando il Lemma 4.3 e la notazione appena introdotta si dimostra

Lemma 4.6 *Sia N un sottogruppo di G. Allora sono equivalenti:*
(a) N è normale in G;
(b) $N^g \leq N$ per ogni $g \in G$;
(c) $N = N^g$ per ogni $g \in G$.

DIMOSTRAZIONE. (a) è equivalente a (b) per il Lemma 4.3.

(c) implica (b) è ovvio. Verifichiamo che (b) implica (c). Sia $g \in G$, allora per (b) applicata a g^{-1} si ha $N^{g^{-1}} \leq N$, cioè $gNg^{-1} \leq N$, da cui si ottiene, moltiplicando a destra per g e a sinistra per g^{-1}, $N \leq g^{-1}Ng$, da cui la tesi. □

Lemma 4.7 *Se H è un sottogruppo di un gruppo G e K è un sottogruppo normale di G allora $HK = KH$. In particolare, HK è un sottogruppo di G (vedi Esercizio. 3.15). Se anche H è normale, allora HK è un sottogruppo normale di G.*

DIMOSTRAZIONE. Poiché K è normale, $hK = Kh$ per ogni $h \in H$ e quindi $HK = \bigcup_{h\in H} hK = \bigcup_{h\in H} Kh = KH$. Usiamo il Lemma 4.3 per dimostrare che HK è normale se H e K lo sono. Sia $x \in G$ e $hk \in HK$, cioè $h \in H$ e $k \in K$. Allora $x^{-1}hkx = x^{-1}h(xx^{-1})kx = (x^{-1}hx)(x^{-1}kx) \in HK$, in quanto $x^{-1}hx \in H$ e $x^{-1}kx \in K$ perché H e K sono normali. □

Abbiamo visto che l'intersezione di sottogruppi è ancora un sottogruppo. Vediamo se vale lo stesso anche per i sottogruppi normali.

Lemma 4.8 *Sia $\{N_i : i \in I\}$ una famiglia di sottogruppi normali di un gruppo G. Allora*
(a) $\bigcap_{i\in I} N_i$ è un sottogruppo normale di G.
(b) $\langle N_i : i \in I\rangle$ è un sottogruppo normale di G

DIMOSTRAZIONE. (a) Sia $x \in \bigcap_{i\in I} N_i$, allora $x \in N_i$, per ogni $i \in I$ e, per il Lemma 4.6, si ha $x^g \in N_i$, per ogni $i \in I$ e per ogni $g \in G$. Allora $x^g \in \bigcap_{i\in I} N_i$ e quindi $(\bigcap_{i\in I} N_i)^g \leq \bigcap_{i\in I} N_i$, che ci permette di concludere nuovamente grazie al Lemma 4.6.

(b) Sia $x \in \langle N_i : i \in I\rangle$. Per il Lemma 4.7 $x = x_1x_2 \dots x_r$ con $x_j \in N_{i_j}$ per qualche $i_1, \dots, i_r \in I$. Quindi

$$x^g = g^{-1}xg = (g^{-1}x_1g)(g^{-1}x_2g) \dots (g^{-1}x_rg) \in \langle N_i : i \in I\rangle$$

per il Lemma 4.6 visto che N_{i_j} è normale per ogni $j = 1, \dots, r$. Abbiamo dimostrato che $\langle N_i : i \in I\rangle^g \leq \langle N_i : i \in I\rangle$ e quindi concludiamo nuovamente per il Lemma 4.6. □

Il Lemma 4.8 ci permette di osservare che l'insieme di tutti i sottogruppi normali di un gruppo G, che denoteremo con $\mathcal{N}(G)$ è un reticolo, come verrà richiesto di dimostrare nell'Esercizio 4.27.

Potrebbe accadere che il reticolo dei sottogruppi normali $\mathcal{N}(G)$ contenga solo i sottogruppi banali $\{1\}$ e G. Allora

Definizione 4.9 Un gruppo privo di sottogruppi normali non banali si dice *semplice*.

Abbiamo già osservato nel Lemma 3.29 che un gruppo di ordine un primo p non ha sottogruppi non banali, quindi a maggior ragione non ha sottogruppi normali non banali. Pertanto i gruppi $(\mathbb{Z}_p, +)$ sono gruppi semplici. Si può dimostrare anzi che sono i soli gruppi abeliani semplici. Ci sono anche gruppi semplici non abeliani, che hanno invece "molti" sottogruppi non normali. Un' intera famiglia di gruppi semplici non abeliani è data dai gruppi alterni A_n, come dimostreremo più avanti.

Per ogni gruppo G possiamo definire un sottogruppo che è senz'altro normale, ma potrebbe essere banale. Un sottogruppo che "misura" quanti elementi commutano con tutti gli elementi del gruppo.

Definizione 4.10 Un elemento $x \in G$ si dice *centrale* in G se $xg = gx$ per ogni $g \in G$. L'insieme degli elementi centrali $Z(G) = \{z \in G \mid zg = gz \text{ per ogni } g \in G\}$ si chiama *centro* di G.

Lemma 4.11 *Il centro di un gruppo G è un sottogruppo abeliano normale di G.*

Dimostrazione. Sia $Z(G)$ il centro di G, allora $1 \in Z(G)$, che è pertanto non vuoto. Siano $z, w \in Z(G)$ e $x \in G$. Dimostriamo che z^{-1}, zw e $x^{-1}zx$ appartengono a $Z(G)$. Sia $g \in G$, dal fatto che $z \in Z(G)$ segue che $zg = gz$, da cui, moltiplicando per z^{-1} a destra e a sinistra, ricaviamo $gz^{-1} = z^{-1}g$, cioè $z^{-1} \in Z(G)$. Inoltre $(zw)g = z(wg) = z(gw) = (zg)w = g(zw)$, cioè anche $zw \in Z(G)$

Dalla definizione segue che $zw = wz$ e quindi $Z(G)$ è abeliano. Infine $x^{-1}zx = x^{-1}(zx) = x^{-1}(xz) = (x^{-1}x)z = z \in Z(G)$, da cui segue che $Z(G)$ è normale, per il Lemma 4.3. □

Osserviamo che, come accennato prima, se G è abeliano, allora $Z(G) = G$, mentre se G è un gruppo semplice non abeliano, si dimostra nell'esercizio 4.28 che $Z(G) = \{1\}$.

4.2 Quozienti

Sia G un gruppo e sia N un sottogruppo normale di G. Nel paragrafo 3.2 sono state definite due relazioni di equivalenza $\sim$ nel lemma 3.19 e $\sim'$ nel successivo esercizio 3.20, entrambe relative al sottogruppo N. Dal fatto che N è normale segue che queste due relazioni di equivalenza coincidono. Vediamo ora che questa relazione di equivalenza è compatibile con l'operazione del gruppo G nel senso che

$$\text{se } x \sim x_1 \text{ e } y \sim y_1, \text{ allora } xy \sim x_1y_1. \qquad (**)$$

Infatti, per la definizione di $\sim$ si ha $x_1 = xh$ e $y_1 = yh'$ per opportuni $h, h' \in N$. Allora, per il Lemma 4.3 e l'Osservazione 4.4 si ha $x_1y_1 = xhyh' = xyh''h' \in xyN$, dove h'' è un opportuno elemento di N.

Nell'insieme quoziente G/H delle classi laterali si introduce un operazione binaria nel modo seguente. Notiamo che per ogni coppia di elementi $x, y \in G$ il prodotto x_1y_1 appartiene sempre alla classe xyN se $x_1 \sim x$ e $y_1 \sim y$. Poniamo dunque $xN \cdot yN = xyN$.

Teorema 4.12 *Con il prodotto così definito $(G/N, \cdot)$ risulta un gruppo (detto gruppo quoziente).*

Dimostrazione. Verifichiamo la legge associativa.

$$(xN \cdot yN) \cdot zN = (xyN) \cdot zN = ((xy)z)N = (x(yz))N = xN \cdot (yzN) = xN \cdot (yN \cdot zN).$$

La classe N dell'elemento 1 risulta elemento neutro di $(G/N, \cdot)$:

$$N \cdot xN = 1N \cdot xN = (1 \cdot x)N = xN \;\; e \;\; xN \cdot 1N = xN \cdot 1N = (x \cdot 1)N = Nx$$

per ogni $x \in G$.

Infine,

$$(xN) \cdot (x^{-1}N) = (x \cdot x^{-1})N = 1N = N \;\; e \;\; (x^{-1}N) \cdot (xN) = (x^{-1}xN) = 1N = N,$$

quindi la classe $x^{-1}N$ è l'inversa della classe xN. □

Esempio 4.13 Sia $m > 1$ un intero. Allora $m\mathbb{Z} = \langle m \rangle$ è un sottogruppo normale di $\mathbb{Z}$. La relazione di equivalenza associata al sottogruppo $m\mathbb{Z}$ è definita con $x \sim y$ se e solo se $y - x \in m\mathbb{Z}$, ovvero $x \equiv_m y$. In altre parole, in questo caso troviamo la congruenza modulo m introdotta in precedenza. Quindi, le classi laterali $x + m\mathbb{Z}$ coincidono con le classi $[x]_m$ dei resti modulo m. Perciò il gruppo quoziente $(\mathbb{Z}/m\mathbb{Z}, +)$ in questo caso coincide con il gruppo $(\mathbb{Z}_m, +)$ introdotto in precedenza.

Quando si definisce una funzione su un insieme quoziente, bisogna fare attenzione a come la si definisce. Infatti, poiché gli elementi di un insieme quoziente sono classi di equivalenza, quando si definisce l'immagine di una classe, dando l'immagine di un rappresentante della classe, bisogna verificare che poi la funzione sia *ben definita*, cioè che se si sceglie un altro rappresentante l'immagine sia effettivamente la stessa.

Vediamolo meglio con un esempio.

Esempio 4.14 Sia $(\mathbb{Z}_6, +)$ il gruppo delle classi resto modulo 6 e $(\mathbb{Z}_8, +)$ il gruppo delle classi resto modulo 8. Siano $f : \mathbb{Z}_6 \to \mathbb{Z}_8$ definita da $f([x]_6) = [2x]_8$ e $g : \mathbb{Z}_6 \to \mathbb{Z}_8$ definita da $g([x]_6) = [4x]_8$. Si dica se sono ben definite.

DIMOSTRAZIONE. Osserviamo che $[1]_6 = [7]_6$, mentre $f([1]_6) = [2]_8 \neq f([7]_6) = [6]_8$; quindi f non è ben definita.

Verifichiamo se g è ben definita. Se $[x]_6 = [y]_6$, allora $x = y + 6k$ per qualche $k \in \mathbb{Z}$. Allora $4x = 4y + 24k$ e pertanto $[4x]_8 = [4y]_8$, quindi g è ben definita. □

4.3 Un altro esempio: i gruppi lineari

In questo paragrafo vogliamo studiare i *gruppi lineari*, cioè insiemi di trasformazioni lineari invertibili su uno spazio vettoriale di dimensione finita che sono gruppi con l'operazione di composizione di applicazioni. Anche questi gruppi, come i gruppi di permutazioni, sono importanti perché sono esempi concreti di gruppi. In questo caso, ogni gruppo astratto finito si può immergere in un gruppo lineare, cioè ogni gruppo astratto finito può essere visto come un sottogruppo di un gruppo lineare. E' chiaro proprio dalla loro definizione come automorfismi di spazi vettoriali, che i gruppi lineari costituiscono un legame importante tra la Geometria e l'Algebra.

Nell' Esercizio 1.17, si dimostra che se $\mathbb{K}$ è un campo, allora $(M_n(\mathbb{K}), \cdot)$ è un monoide. Consideriamo l'insieme $GL_n(\mathbb{K})$ degli elementi invertibili di $(M_n(\mathbb{K}), \cdot)$. Allora $(GL_n(\mathbb{K}), \cdot)$ è un gruppo (si veda l'esercizio 2.28).

Dalla Geometria è noto che $GL_n(\mathbb{K})$ è in corrispondenza biunivoca con il gruppo delle trasformazioni lineari biiettive dello spazio vettoriale $\mathbb{K}^n$. Inoltre è noto che $A \in M_n(\mathbb{K})$ è invertibile se e solo se $det(A)$ è invertibile (equivalentemente, $det(A) \neq 0$). Un ultimo teorema di Geometria che utilizzeremo è il seguente:

Teorema 4.15 (Teorema di Binet) *Siano $A, B \in M_n(\mathbb{K})$. Allora $det(AB) = det(A)det(B)$.*

Una immediata conseguenza del Teorema di Binet è il seguente corollario:

Corollario 4.16 *Siano $A, B \in GL_n(\mathbb{K})$. Allora*
i) $det(A^{-1}) = det(A)^{-1}$;
ii) $det(A^{-1}BA) = det(B)$.

DIMOSTRAZIONE. *i)* Per il Teorema di Binet, si ha $1 = det(I_n) = det(AA^{-1}) = det(A)det(A^{-1})$, da cui l'asserto.

i) Per il Teorema di Binet, si ha $det(A^{-1}BA) = det(A^{-1})det(B)det(A) = det(A)^{-1}det(A)det(B) = det(B)$, per il punto *i)*. □

Introduciamo ora altri sottogruppi di $GL_n(\mathbb{K})$.

Lemma 4.17 *Siano $n > 1$ un intero e $\mathbb{K}$ un campo. Provare che:*
a) il sottoinsieme $SL_n(\mathbb{K})$ del gruppo lineare $GL_n(\mathbb{K})$ formato dalle matrici con determinante uguale a 1 è un sottogruppo normale.
b) Il sottoinsieme $\mathrm{T}_n^+(\mathbb{K}) = \{(a_{ij}) \in GL_n(\mathbb{K}) : a_{ij} = 0 \text{ se } i > j\}$ di $GL_n(\mathbb{K})$ formato delle matrici triangolari superiori è un sottogruppo di $GL_n(\mathbb{K})$; $\mathrm{T}_n^+(\mathbb{K})$ non è normale.
c) Il sottoinsieme $\mathrm{D}_n(\mathbb{K}) = \{(a_{ij}) \in GL_n(\mathbb{K}) : a_{ij} = 0 \text{ se } i \neq j\}$ di $GL_n(\mathbb{K})$ formato delle matrici diagonali è un sottogruppo di $GL_n(\mathbb{K})$.

DIMOSTRAZIONE. *a)* Innanzitutto $SL_n(\mathbb{K})$ non è vuoto, perché la matrice identica $I_n \in SL_n(\mathbb{K})$. Inoltre, se $A, B \in SL_n(\mathbb{K})$, $det(A) = det(B) = 1$ da cui, per il Teorema di Binet e per il Corollario 4.16 i),

$$det(A^{-1}B) = det(A^{-1})det(B) = det(A)^{-1}det(B) = 1.$$

Quindi $SL_n(\mathbb{K})$ è un sottogruppo. Dimostriamo che è normale. Se $C \in GL_n(\mathbb{K})$, allora $det(C^{-1}AC) = det(A) = 1$ per il Corollario 4.16 ii), da cui segue che $SL_n(\mathbb{K})$ è normale.

b) Innanzitutto $\mathrm{T}_n^+(\mathbb{K})$ non è vuoto, perché la matrice identica $I_n \in \mathrm{T}_n^+(\mathbb{K})$. Siano $A, B \in \mathrm{T}_n^+(\mathbb{K})$. Utilizzando la definizione dell'inversa di A, si può provare che anche $A^{-1} \in \mathrm{T}_n^+(\mathbb{K})$. Inoltre se $AB = C = (c_{ij})$ e $i > j$ si ha $c_{ij} = \sum_{l=1}^{n} a_{il}b_{lj}$, ove se $i > l$, $a_{il} = 0$ e se $i \leq l$, allora $j < i \leq l$, da cui $b_{lj} = 0$. Pertanto $c_{ij} = 0$ per ogni $i, j = 1, .., n$ e $i > j$, cioè $AB = C \in \mathrm{T}_n^+(\mathbb{K})$.

Per dimostrare che non è un sottogruppo normale, lo dimostriamo dapprima nel caso $n = 2$, prendendo la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{T}_n^+(\mathbb{K})$ e la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_n(\mathbb{K})$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

che non appartiene a $\mathrm{T}_n^+(\mathbb{K})$. Il caso $n > 2$ si ottiene allo stesso modo, "completando" opportunamente le matrici utilizzate nel caso $n = 2$.

c) Innanzitutto $\mathrm{D}_n(\mathbb{K})$ non è vuoto, perché la matrice identica $I_n \in \mathrm{D}_n(\mathbb{K})$. Siano $A = (a_{ii}), B = (b_{ii}) \in \mathrm{D}_n(\mathbb{K})$. Utilizzando la definizione dell'inversa di A, si può provare che $A^{-1} = (a_{ii}^{-1}) \in \mathrm{D}_n(\mathbb{K})$. Inoltre se $C = AB = (c_{ij})$, una semplice verifica prova che $c_{ij} = 0$ se $i \neq j$ e $c_{ii} = a_{ii}b_{ii}$ per ogni $i, j = 1, ..., n$. □

In modo del tutto analogo si dimostra che anche il sottoinsieme delle matrici triangolari inferiori $\mathrm{T}_n^-(\mathbb{K}) = \{(a_{ij}) \in GL_n(\mathbb{K}) : a_{ij} = 0 \text{ se } i < j\}$ è un sottogruppo di $GL_n(\mathbb{K})$. Allora vale il seguente facile Lemma

Lemma 4.18 *L'intersezione del sottogruppo delle matrici triangolari superiori con il sottogruppo delle matrici triangolari inferiori è il sottogruppo delle matrici diagonali, cioè*

$$\mathrm{T}_n^+(\mathbb{K}) \cap \mathrm{T}_n^-(\mathbb{K}) = \mathrm{D}_n(\mathbb{K}).$$

DIMOSTRAZIONE. Sia $A = (a_{ij}) \in \mathrm{T}_n^+(\mathbb{K}) \cap \mathrm{T}_n^-(\mathbb{K})$ allora $a_{ij} = 0$ per ogni $i < j$ e $j < i$, $i, j = 1, 2, ..., n$, da cui $a_{ij} = 0$ per ogni $i \neq j$, $i, j = 1, 2, ..., n$, cioè $A = (a_{ij}) \in \mathrm{D}_n(\mathbb{K})$. L'altra inclusione è ovvia. □

Vogliamo ora introdurre un altro gruppo lineare, cioè un sottogruppo di $GL_n(\mathbb{K})$. Per far questo abbiamo bisogno della seguente definizione.

Definizione 4.19 Sia $A = (a_{ij}) \in M_{m\times n}(\mathbb{K})$, definiamo la *matrice trasposta* di A come la la matrice che si ottiene da A mettendo nel posto (lk) l'elemento a_{kl} che si trova nel posto (kl) di A. Denotiamo la matrice trasposta di A con $A^t = (a_{ji})$.

E' noto dalla Geometria che per $A, B \in \mathrm{M}_n(\mathbb{K})$, si ha $(AB)^t = B^tA^t$. Ci si può chiedere quando una matrice $A \in \mathrm{M}_n(\mathbb{K})$ coincide con la sua trasposta. Le matrici di questo tipo hanno un nome:

Definizione 4.20 Una matrice $A \in \mathrm{M}_n(\mathbb{K})$ tale che $A^t = A$ si dice *simmetrica*.

L'insieme di tutte le matrici simmetriche di $GL_n(\mathbb{K})$ non forma un sottogruppo di $GL_n(\mathbb{K})$, come si chiede di dimostrare nell'esercizio 4.40. Pertanto proviamo invece a considerare il sottoinsieme di tutte le matrici di $GL_n(\mathbb{K})$ tali che l'inversa coincide con la trasposta. Dimostriamo nel seguente Lemma che questo insieme è un sottogruppo di $GL_n(\mathbb{K})$.

Lemma 4.21 *(a) Sia $A \in GL_n(\mathbb{K})$, allora $(A^t)^{-1} = (A^{-1})^t$.*
(b) Sia $\mathrm{O}_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) : A^{-1} = A^t\}$. Allora $\mathrm{O}_n(\mathbb{K})$ è un sottogruppo di $GL_n(\mathbb{K})$.

DIMOSTRAZIONE. *(a)* Sia $A \in GL_n(\mathbb{K})$ e I_n la matrice identica di $GL(n, \mathbb{K})$. Allora

$$I_n = (I_n)^t = (AA^{-1})^t = (A^{-1})^tA^t$$

da cui segue che l'inversa di A^t, cioè $(A^t)^{-1}$ è proprio $(A^{-1})^t$.

(b) $\mathrm{O}_n(\mathbb{K})$ non è vuoto perché la matrice identica $I_n \in \mathrm{O}_n(\mathbb{K})$. Inoltre se $A, B \in \mathrm{O}_n(\mathbb{K})$, per (a), e per la definizione di $\mathrm{O}_n(\mathbb{K})$ si ha $(A^{-1})^t = (A^t)^{-1} = (A^{-1})^{-1} = A$, da cui segue che $A^{-1} \in \mathrm{O}_n(\mathbb{K})$. Inoltre

$$(AB)^{-1} = B^{-1}A^{-1} = B^tA^t = (AB)^t,$$

da cui segue che $AB \in \mathrm{O}_n(\mathbb{K})$. □

I sottogruppi definiti nei Lemma 4.17 e 4.21 hanno i seguenti nomi:

Definizione 4.22 Il gruppo $SL_n(\mathbb{K})$ si chiama il *gruppo speciale lineare*, il gruppo $\mathrm{O}_n(\mathbb{K})$ si chiama il *gruppo ortogonale lineare*.

I gruppi lineari fino ad ora considerati possono essere definiti su qualsiasi campo. Infatti nelle definizioni non abbiamo introdotto nessuna ipotesi sul campo $\mathbb{K}$. Passiamo ora a considerare alcuni casi particolari, specializzando lo studio per esempio al campo dei complessi o ai campi finiti.

Cominciamo con il gruppo $\mathbb{H}$ dei *quaternioni*, che verrà talvolta denotato anche con Q_8, visto che è un gruppo di ordine 8. Lo definiamo come sottogruppo del gruppo lineare $GL_2(\mathbb{C})$. Anche Q_8, come S_3, è il più piccolo gruppo che gode di diverse proprietà. Ad esempio è il più piccolo gruppo non abeliano di ordine una potenza di un primo, o ancora è il più piccolo gruppo non abeliano in cui tutti i sottogruppi sono abeliani. Infine, come dimostriamo nel seguente Lemma 4.23, Q_8 è l'unione di suoi 3 sottogruppi propri. E' il più piccolo gruppo che gode di questa proprietà? (si veda l'esercizio 4.39)

Lemma 4.23 *Sia $\mathbb{H}$ il seguente sottoinsieme di $GL_2(\mathbb{C})$, il gruppo delle matrici invertibili 2×2 a elementi nel campo dei numeri complessi: $\mathbb{H} = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, ove 1 denota la matrice identica I_2 e*

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Si provi che

i) $\mathbf{i}^4 = \mathbf{j}^4 = \mathbf{k}^4 = 1$, $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$, $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$, $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$, $\mathbf{i}^3 = -\mathbf{i}$, $\mathbf{j}^3 = -\mathbf{j}$, $\mathbf{k}^3 = -\mathbf{k}$.

ii) $\mathbb{H}$ è un sottogruppo non abeliano di $GL_2(\mathbb{C})$.

iii) Si verifichi che i sottogruppi di $\mathbb{H}$ sono $\langle\mathbf{i}\rangle$, $\langle\mathbf{j}\rangle$, $\langle\mathbf{k}\rangle$, $Z(\mathbb{H})$ e che sono tutti normali.

iv) Si provi che $\mathbb{H} = \langle\mathbf{i}\rangle \cup \langle\mathbf{j}\rangle \cup \langle\mathbf{k}\rangle$.

Dimostrazione. *i)* E' un facile esercizio (si veda l' Esercizio 4.39).

ii) Bisogna verificare che prodotti di elementi di $\mathbb{H}$ sono ancora elementi di $\mathbb{H}$, ricordando che la verifica per l'inverso di un elemento di $\mathbb{H}$ non è necessaria poiché $\mathbb{H}$ è finito, grazie all' Esercizio 3.35. Per esempio $\mathbf{i}^{-1} = \mathbf{i}^3 = -\mathbf{i}$.

iii) $\mathbb{H}$ è un gruppo di ordine 8, quindi, per il teorema di Lagrange, i suoi sottogruppi propri possono avere solo ordine 4 o 2. Se un sottogruppo K contiene $\mathbf{i}$, allora contiene $\langle\mathbf{i}\rangle$ e quindi o $K = \mathbb{H}$ oppure $K = \langle\mathbf{i}\rangle$, poiché $\langle\mathbf{i}\rangle = \{1, i, -i, -1\}$. Analogamente per **i, j, k, -i, -j, -k**. Allora l'unica altra possibilità è che K non contenga nessuno di quegli elementi, cioè $K = \langle -1\rangle$. Infine, i primi 3 sottogruppi sono normali perché hanno indice 2 (vedi l' Esercizio 4.36) e il quarto è normale perché è il centro del gruppo $\mathbb{H}$.

iv) Ogni elemento di $\mathbb{H}$ è contenuto in uno dei 3 sottogruppi $\langle\mathbf{i}\rangle$, $\langle\mathbf{j}\rangle$, $\langle\mathbf{k}\rangle$. □

Passiamo ora a considerare un esempio di un gruppo lineare infinito. Il sottogruppo definito nel seguente Lemma 4.24 si dice *gruppo di Heisenberg* e viene utilizzato in Fisica.

Lemma 4.24 *Sia G l'insieme delle matrici $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ con $a, b, c \in \mathbb{Z}$. Allora G è un sottogruppo di $GL_3(\mathbb{Q})$ e il centro di G è*

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

Dimostrazione. G non è vuoto perché la matrice identica $I_3 \in G$. E' facile verificare che

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+ac'+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e}$$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = I_3.$$

Da questo segue che G è un gruppo e che il centro di G è esattamente $\left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$. $\square$

Concludiamo il paragrafo, con alcune osservazioni riguardanti i gruppi lineari definiti su campi finiti. Consideriamo l'insieme $\mathbb{Z}_p$ delle classi resto modulo p, ove p è un primo. Abbiamo dimostrato che $(\mathbb{Z}_p, +)$ è un gruppo e che $(\mathbb{Z}_p^*, \cdot)$ è pure un gruppo. Allora $(\mathbb{Z}_p, +, \cdot)$ è un campo, che denoteremo con $\mathbb{F}_p$ per ricordare che stiamo parlando della struttura di campo definita sull'insieme $\mathbb{Z}_p$. ($\mathbb{F}$ spesso denota un campo, dall'inglese "field"). Possiamo quindi parlare di spazi vettoriali sul campo $\mathbb{F}_p$. Dalla Geometria è noto che ogni spazio vettoriale di dimensione n su $\mathbb{F}_p$ è isomorfo a $\mathbb{F}_p^n$. Inoltre possiamo fissare la base canonica di $\mathbb{F}_p^n$, definita da $e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0), ..., e_n = (0, 0, ..., 1)$. Osserviamo infine che uno spazio vettoriale di dimensione n su $\mathbb{F}_p$ ha ordine p^n.

E' inoltre possibile definire $GL_n(\mathbb{F}_p)$, il gruppo lineare a elementi nel campo $\mathbb{F}_p$. Il gruppo $GL_n(\mathbb{F}_p)$ è finito, in quanto si tratta di un insieme di matrici i cui elementi stanno in un insieme finito. E' facile calcolare la cardinalità di $M_n(\mathbb{F}_p)$ e ci proponiamo ora di calcolare anche quella di $GL_n(\mathbb{F}_p)$, utilizzando alcune proprietà degli spazi vettoriali.

Lemma 4.25 *Sia $\mathbb{F}_p$ il campo con p elementi appena definito. Allora:*
i) $|M_n(\mathbb{F}_p)| = p^{n^2}$;
ii) $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{n-2})(p^n - p^{n-1}) =$
$= p^{n(n-1)/2}(p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1)...(p^2 - 1)(p - 1)$.

DIMOSTRAZIONE. *i)* Per ogni elemento di una matrice di $M_n(\mathbb{F}_p)$ si hanno p scelte e quindi in totale si avranno p^{n^2} possibili matrici.

ii) Utilizziamo la definizione geometrica di $GL_n(\mathbb{F}_p)$: ogni matrice di $GL_n(\mathbb{F}_p)$ rappresenta una trasformazione lineare biiettiva f dello spazio vettoriale $\mathbb{F}_p^n$ in se stesso, in cui la i-esima colonna rappresenta l'immagine $v_i = f(e_i)$ dell'i-esimo vettore della base canonica e_i di $\mathbb{F}_p^n$, per $i = 1, 2, ..., n$. Pertanto contiamo quante scelte si hanno per ogni colonna. Per la prima colonna abbiamo $p^n - 1$ scelte, poiché ogni vettore non nullo di $\mathbb{F}_p^n$ può essere immagine di e_1 tramite f. Il vettore $v_2 = f(e_2)$ non deve appartenere al sottospazio generato da v_1, in quanto f è biiettiva. Allora per v_2 abbiamo $p^n - p$ scelte. In generale il vettore v_i non deve essere combinazione lineare dei precedenti vettori $v_1, ..., v_{i-1}$ già fissati, cioè non deve appartenere al sottospazio vettoriale da essi generato che deve avere dimensione $i - 1$. Quindi si hanno $p^n - p^{i-1}$ scelte per l'i-esimo vettore colonna v_i. Concludiamo che $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{n-2})(p^n - p^{n-1})$. $\square$

4.4 Esercizi su sottogruppi normali e quozienti

Esercizio 4.26 *Sia H un sottogruppo di G e g un elemento di G. Si dimostri che H^g è un sottogruppo di G.*

Esercizio 4.27 *Si dimostri che l'insieme $\mathcal{N}(G)$ dei sottogruppi normali di G ordinato per inclusione è un reticolo limitato avente G come elemento massimo e $\{1\}$ come minimo.*

Esercizio 4.28 *Sia $Z(G)$ il centro di un gruppo G. Si dimostri*
i) $Z(G) = G$ se e solo se G è abeliano;
ii) se G è un gruppo semplice non abeliano, allora $Z(G) = \{1\}$.

Esercizio 4.29 *Se H è un sottogruppo di G, si dimostri che $Z(H)$ contiene $Z(G) \cap H$. Si mostri con un esempio che l'inclusione può essere stretta.*

Esercizio 4.30 *Si dimostri che l'insieme $G = GL_3(\mathbb{Z})$ delle matrici quadrate di ordine 3 a coefficienti interi con determinante ± 1 forma un sottogruppo di $GL_3(\mathbb{R})$.*

Esercizio 4.31 *Sia G il gruppo $GL_3(\mathbb{F}_2)$.*
(a) Si calcoli l'ordine di G.
(b) Si descriva il centro di G.

(b) Sia N l'insieme delle matrici $\begin{pmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}$ *con* $a, b, c \in \mathbb{F}_2$. *Si dimostri che N è un sottogruppo di G.*

Esercizio 4.32 *Sia G il gruppo $GL_2(\mathbb{F}_3)$.*
(a) Si calcoli l'ordine di G.
(b) Si descriva il centro Z di G.
(c) Si trovino almeno due sottogruppi di ordine 3 di G.

Esercizio 4.33 *Si dimostri che il sottogruppo $\mathrm{D}_n(\mathbb{R})$ delle matrici diagonali a coefficienti in $\mathbb{R}$ non è un sottogruppo normale di $GL_n(\mathbb{R})$.*

Esercizio 4.34 *Sia G un gruppo e Z il suo centro.*
(a) Dimostrare che per ogni elemento a di G il sottogruppo di G generato da Z e a è abeliano.
(b) Dimostrare che se $ab \in Z(G)$, allora $ab = ba$.
(c) Mostrare che l'implicazione inversa in (b) non vale.

Esercizio 4.35 *Determinare $Z(S_2)$, $Z(S_3)$, $Z(S_4)$.*

Esercizio 4.36 *Sia G un gruppo e sia N un sottogruppo di G di indice 2.*
(a) Dimostrare che N è normale.
(b) Dare un esempio di un gruppo G e di un sottogruppo N di G di indice 3 che non è normale.

Esercizio 4.37 *Sia $G = GL_3(\mathbb{Z})$ (vedi l'esercizio 4.30). Assegnati tre interi positivi l, m, n si consideri il sottoinsieme $H_{l,m,n}$ delle matrici della forma*

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \quad x \in l\mathbb{Z}, y \in m\mathbb{Z}, z \in n\mathbb{Z}.$$

i) Si calcoli l'inverso di $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ *in G.*
ii) Si dimostri che $H_{l,m,n}$ è un sottogruppo di G se e solo se m divide ln.
iii) Si verifichi che l'insieme N di tutte le matrici della forma $\begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *con $y \in 6\mathbb{Z}$ è un sottogruppo normale di $H_{2,6,3}$.*

Esercizio 4.38 *Sia G un gruppo finito, H un suo sottogruppo di indice p, con p primo. Supponiamo che esista $g \in G \setminus H$ tale che $gH = Hg$. Dimostrare che H è normale in G.*

Esercizio 4.39 *Sia Q_8 il gruppo dei quaternioni definito nel Lemma 4.23:*
i) si provi i) *del Lemma 4.23.*
ii) Si consideri il sottogruppo $V = \langle (12)(34), (13)(24) \rangle$ di S_4. Si provi che V è l'unione di 3 sottogruppi propri e si calcoli $|V|$.

Esercizio 4.40 *Sia $H = \{A \in GL_n(\mathbb{K}) : A^t = A\}$ l'insieme delle matrici simmetriche di $GL_n(\mathbb{K})$, definite in 4.20. Si dimostri che H non è un sottogruppo di $GL_n(\mathbb{K})$, se $n > 1$.*

Esercizio 4.41 *Determinare l'intersezione $\mathrm{O}_n(\mathbb{K}) \cap \mathrm{T}_n^-(\mathbb{K})$, dove $\mathrm{T}_n^-(\mathbb{K})$ è il sottogruppo delle matrici triangolari inferiori.*

Esercizio 4.42 *Dimostrare che $\mathrm{O}_2(\mathbb{K})$ non è un sottogruppo normale di $\mathrm{GL}_2(\mathbb{K})$.*

Esercizio 4.43 *Si considerino i seguenti insiemi di matrici in $SL_2(\mathbb{R})$:*

$$U^+ = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}, \quad U^- = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} : x \in \mathbb{R} \right\}, \quad D = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} : x \in \mathbb{R}, x \neq 0 \right\}.$$

a) Dimostrare che U^+, U^- e D sono sottogruppi di $SL_2(\mathbb{R})$. Determinare quali di questi sottogruppi sono normali.

b) Descrivere l'insieme U^-DU^+ dei prodotti $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ al variare di $x, y, d \in \mathbb{R}$ con $d \neq 0$.

c) Sia $\varepsilon = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Dimostrare che $SL_2(\mathbb{R}) = U^-DU^+ \cup U^-D\varepsilon$.

Esercizio 4.44 *Sia G il gruppo di Heisenberg, definito nel Lemma 4.24 e sia N l'insieme delle matrici $\begin{pmatrix} 1 & 2b & 2c \\ 0 & 1 & 2a \\ 0 & 0 & 1 \end{pmatrix}$ con $a, b, c \in \mathbb{Z}$. Si dimostri che N è un sottogruppo normale di G.*

Esercizio 4.45 *Si calcoli l'ordine del gruppo $G = GL_2(\mathbb{F}_p)$, dove p è un numero primo. Quanti elementi ha il centro di G?*

Esercizio 4.46 *Nel gruppo additivo $\mathbb{Q}$ dei numeri razionali si dimostri che il sottoinsieme H dei razionali con denominatore "square-free", cioè $H = \{m/n \in \mathbb{Q} : m, n$ interi e n prodotto di primi distinti $\}$ è un sottogruppo.*

Si determini l'ordine dell'elemento $\frac{5}{36} + H$ in $\mathbb{Q}/H$.

Esercizio 4.47 *Sia H l'insieme delle matrici $\begin{pmatrix} 1 & x & y & z \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}$ con $a, b, x, y, z \in \mathbb{F}_2$.*

(a) Si dimostri che H è un sottogruppo del gruppo $GL_4(\mathbb{F}_2)$ e si calcolino gli ordini di $GL_4(\mathbb{F}_2)$ e H.

(b) Si descriva il centro Z di H.

(c) Si descriva il quoziente H/Z. Si determini, in particolare se H/Z è ciclico.

5 Omomorfismi

Un omomorfismo tra due gruppi G ed H è un'applicazione da G in H che *rispetta* la struttura di gruppo. Più precisamente:

Definizione 5.1 Se G e H sono gruppi, un *omomorfismo* di G in H è un'applicazione $\varphi\colon G \to H$ tale che per ogni $a, b \in G$ risulti $\varphi(ab) = \varphi(a)\varphi(b)$.

Se φ è anche biiettiva, si dice un *isomorfismo*.

Nei gruppi moltiplicativi si usa talvolta la notazione g^φ per indicare $\varphi(g)$.

L'insieme di tutti gli omomorfismi di G in H si denota con $Hom(G, H)$. Questo insieme non è mai vuoto, infatti esiste sempre un omomorfismo da un gruppo G ad un gruppo H: l'omomorfismo banale $b : G \to H$ che manda ogni elemento di G nell'identità 1_H di H.

Un omomorfismo di un gruppo G in se stesso si dice un *endomorfismo* di G.

5.1 Prime proprietà degli omomorfismi

Lemma 5.2 *Sia $\varphi : G \to H$ un omomorfismo tra due gruppi G e H. Allora*

i) $\varphi(1_G) = 1_H$;

ii) $\varphi(x^{-1}) = (\varphi(x))^{-1}$, per ogni $x \in G$;

iii) $\varphi(x^n) = (\varphi(x))^n$ per ogni $x \in G$, $n \in \mathbb{Z}$.

Dimostrazione. i) $\varphi(1_G)1_H = \varphi(1_G) = \varphi(1_G1_G) = \varphi(1_G)\varphi(1_G)$, da cui, applicando la legge di cancellazione, si ottiene $1_H = \varphi(1_G)$.

ii) $1_H = \varphi(1_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, da cui segue, per l'unicità dell'inverso, che $(\varphi(x))^{-1} = \varphi(x^{-1})$.

iii) Lo proviamo per induzione su n, nel caso in cui $n \geq 0$. Il caso $n = 0$ lo abbiamo provato in i). Supponiamo ora vero l'enunciato per $n - 1$, allora

$$\varphi(x^n) = \varphi(x^{n-1}x) = \varphi(x^{n-1})\varphi(x) = (\varphi(x))^{n-1}\varphi(x) = (\varphi(x))^n.$$

Per $n < 0$, si pone $x^n = (x^{-1})^{-n}$ e si utilizza ii) e la formula dimostrata per $n > 0$. □

Definizione 5.3 Un esempio molto importante di isomorfismo di un gruppo G in se stesso è il *coniugio* φ_a per un elemento $a \in G$, $\varphi_a : G \to G$ definito da $\varphi_a(x) = a^{-1}xa$.

Lemma 5.4 *Sia G un gruppo e sia $a \in G$. Allora l'applicazione φ_a è un isomorfismo per ogni $a \in G$.*

Dimostrazione. Come abbiamo già più volte osservato, si ha:

$$\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y)$$

Dimostriamo che $\varphi_{a^{-1}}$ è l'inversa di φ_a. Infatti

$$(\varphi_a \circ \varphi_{a^{-1}})(x) = \varphi_a(\varphi_{a^{-1}}(x)) = \varphi_a(axa^{-1}) = a^{-1}(axa^{-1})a = (a^{-1}a)x(aa^{-1}) = x = id(x).$$

Quindi $\varphi_a \circ \varphi_{a^{-1}} = \varphi_1 = id_G$. □

Osserviamo che φ_a risulta essere l'identità se e solo se a è un elemento centrale. In particolare φ_a è l'identità per ogni elemento a, nel caso dei gruppi abeliani.

Dato un omomorfismo $\varphi : G \to H$, possiamo definire l'*immagine* di φ, $Im(\varphi) = G^\varphi = \{x^\varphi : x \in G\}$ e il *nucleo* di φ, $\ker(\varphi) = \{x \in G : x^\varphi = 1_H\}$.

Proposizione 5.1 *Sia $\varphi: G \to H$ un omomorfismo di gruppi. Allora*
(a) $Im(\varphi)$ è un sottogruppo di H;
(b) $\ker(\varphi)$ è un sottogruppo normale di G.

Dimostrazione. (a) Dati $y, z \in Im(\varphi)$, si ha $y = \varphi(x)$ e $z = \varphi(t)$ per qualche $x, t \in G$. Allora

$$y^{-1}z = (\varphi(x))^{-1}\varphi(t) = \varphi(x^{-1})\varphi(t) = \varphi(x^{-1}t) \in Im(\varphi).$$

Quindi per il Lemma 3.6, $Im(\varphi)$ è un sottogruppo.

(b) Per (i) del Lemma 5.2 si ha $1_G \in \ker\varphi$. Inoltre, se $x, y \in \ker\varphi$ si ha

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

poiché $\varphi(x) = \varphi(y) = 1$. Per il Lemma 3.6, $\ker\varphi$ è un sottogruppo. Verifichiamo che $\ker\varphi$ è un sottogruppo normale. Sia $x \in G$ e $a \in \ker\varphi$. Allora

$$\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x^{-1}) = \varphi(x)1\varphi(x)^{-1} = \varphi(x(x)^{-1}) = 1,$$

quindi $xax^{-1} \in \ker\varphi$. □

Vediamo ora che ogni sottogruppo normale risulta essere il nucleo di qualche omomorfismo.

Esempio 5.5 Sia G un gruppo e sia N un sottogruppo normale di G. Si consideri l'applicazione canonica $\pi : G \to G/N$ definita da $\pi(x) = xN$. E' facile vedere che π è un omomorfismo. Inoltre, π è suriettivo e $\ker\pi = N$.

Chiameremo $\pi : G \to G/N$ *omomorfismo canonico.*

Lemma 5.6 *Sia $f : G \to G_1$ un omomorfismo di gruppi. Allora:*
(a) $f(x) = f(y)$ per $x, y \in G$ se e solo se $y \in x\ker f$;
(b) $f^{-1}(f(x)) = x\ker f$ per ogni $x \in G$;
(d) f è iniettivo se e solo se $\ker(f) = \{1\}$.

Dimostrazione. (a) Abbiamo

$$f(x) = f(y) \Leftrightarrow f(x)^{-1}f(y) = 1 \Leftrightarrow f(x^{-1})f(y) = 1 \Leftrightarrow f(x^{-1}y) = 1 \Leftrightarrow x^{-1}y \in \ker f \Leftrightarrow y \in x\ker f.$$

(b) segue da (a)

(c) Da (b) segue che $\ker(f) = \{1\}$ se f è iniettivo. Se $\ker(f) = \{1\}$, allora (a) implica che f è iniettivo. □

5.2 I Teoremi di omomorfismo

In questa sezione vogliamo presentare i teoremi di omomorfismo che mettono in luce le relazioni esistenti tra i gruppi quozienti e gli omomorfismi.

Lo scopo del seguente teorema è di presentare un omomorfismo arbitrario $f : G \to H$ come composizione di due omomorfismi più semplici, dei quali il primo è l'omomorfismo canonico $\pi : G \to G/\ker f$ mentre il secondo è iniettivo.

Teorema 5.7 *Sia $f : G \to H$ un omomorfismo e $\pi : G \to G/\ker f$ l'omomorfismo canonico. Allora:*
1) esiste un omomorfismo iniettivo $\tilde{f} : G/\ker f \to H$ tale che $\tilde{f} \circ \pi = f$;
2) $\tilde{f}$ è un isomorfismo se e solo se f è suriettivo.

DIMOSTRAZIONE. Definiamo l'applicazione $\tilde{f}$ ponendo $\tilde{f}(x \ker f) = f(x)$ per ogni $x \in G$ (la definizione è corretta poiché $x \ker f = y \ker f$ implica $f(x) = f(y)$). Poiché $x \ker f = \pi(x)$, questo ci garantisce che vale $\tilde{f} \circ \pi = f$. Per vedere che $\tilde{f}$ è un omomorfismo notiamo che

$$\tilde{f}(x \ker f \cdot y \ker f) = \tilde{f}(xy \ker f) = f(xy) = f(x)f(y) = \tilde{f}(x \ker f)\tilde{f}(y \ker f).$$

Inoltre, se $\tilde{f}(x \ker f) = 1$, allora $f(x) = 1$, e quindi $x \in \ker f$. Pertanto $\tilde{f}$ è iniettivo. Questo conclude la dimostrazione del punto 1).

Per il punto 2) basta notare che essendo $\tilde{f}$ iniettivo, $\tilde{f}$ è un isomorfismo se e solo se $\tilde{f}$ è suriettivo. Poiché π è suriettivo, questo è equivalente al fatto che $f = \tilde{f} \circ \pi$ è suriettivo. □

Ricaviamo immediatamente il seguente corollario.

Corollario 5.8 (Primo Teorema di Omomorfismo) *Sia $f : G \to H$ un omomorfismo di gruppi. Allora*

$$G/\ker(f) \cong Im(f).$$

I seguenti Teoremi prendono il nome di **Teoremi di corrispondenza** e mettono in relazione i sottogruppi di un gruppo con le loro immagini tramite un omomorfismo.

Teorema 5.2 *Sia $f : G \to H$ un omomorfismo di gruppi e $N = \ker f$.*
(a) Per ogni $K \leq G$ risulta $f(K) \leq H$, in particolare $f(G) \leq H$. Inoltre, se $K \trianglelefteq G$, allora $f(K) \trianglelefteq f(G)$.
(b) Per ogni $L \leq H$ risulta $f^{-1}(L) \leq G$ e $N \leq f^{-1}(L)$. Inoltre, se $L \trianglelefteq H$, allora $f^{-1}(L) \trianglelefteq G$.
(c) $f^{-1}(f(K)) = KN = \{xN : x \in K\}$ per ogni $K \leq G$ e $f(f^{-1}(L)) = L \cap f(G)$ per ogni $L \leq H$

DIMOSTRAZIONE. (a) Sia $K \leq G$. Allora $1_G \in K$ e pertanto $1_H = f(1_G) \in f(K)$. Se $u, v \in f(K)$, allora esistono $x, y \in K$ tali che $u = f(x)$ e $v = f(y)$. Ora $u^{-1}v = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y) \in f(K)$, poiché $x^{-1}y \in K$ in quanto $K \leq G$. Ora supponiamo $K \trianglelefteq G$. Allora per ogni $u \in f(G)$ e $v \in f(K)$ si ha $uvu^{-1} \in f(K)$. Infatti, se $u = f(x)$ e $v = f(y)$ con $x \in G$ e $y \in K$, si ha $xyx^{-1} \in K$ poiché $K \trianglelefteq G$. Quindi $uvu^{-1} = f(xyx^{-1}) \in f(K)$.

(b) Analogamente al punto (a) si dimostra che $f^{-1}(L) \leq G$ per ogni $L \leq H$. Ora supponiamo $L \trianglelefteq H$. Per verificare che $f^{-1}(L) \trianglelefteq G$ prendiamo un elemento $x \in G$ e $z \in f^{-1}(L)$. Allora $f(z) \in L$ e quindi $f(xzx^{-1}) = f(x)f(z)f(x)^{-1} \in L$ poiché $L \trianglelefteq H$. Questo implica $xzx^{-1} \in f^{-1}(L)$ e prova che $f^{-1}(L) \trianglelefteq G$.

(c) Osserviamo che $x \in f^{-1}(f(K))$ se e solo se $f(x) \in f(K)$. In altre parole, $x \in f^{-1}(f(K))$ se e solo se $f(x) = f(y)$ per qualche $y \in K$. Ma questo significa che $x \in f^{-1}(f(K))$ se e solo se $y^{-1}x \in N$ per qualche $y \in K$. L'ultimo fatto è equivalente a $x \in yN$ per qualche $y \in K$. Questo dimostra che $f^{-1}(f(K)) = \bigcup_{y \in K} yN = KN$.

Resta da notare che $f(f^{-1}(L)) \subseteq L$ e $f(f^{-1}(L)) \subseteq f(G)$. Da queste due inclusioni segue immediatamente $f(f^{-1}(L)) \subseteq L \cap f(G)$. L'inclusione $L \cap f(G) \subseteq f(f^{-1}(L))$ è ovvia. □

Corollario 5.9 *Sia $f : G \to H$ un omomorfismo di gruppi e $N = \ker f$. Siano*

- *$\mathcal{S}$ l'insieme dei sottogruppi di G* contenenti *N e*
- *$\mathcal{S}'$ l'insieme dei sottogruppi di H* contenuti in *$f(G)$.*

Allora l'applicazione che ad ogni $K \in \mathcal{S}$ associa $f(K)$ è una biiezione tra $\mathcal{S}$ e $\mathcal{S}'$. Inoltre, $K \in \mathcal{S}$ è normale se e solo se $f(K) \trianglelefteq f(G)$.

DIMOSTRAZIONE. Poiché $f(K) \in \mathcal{S}'$ per ogni $K \in \mathcal{S}$, si definisce così un'applicazione $\Phi : \mathcal{S} \to \mathcal{S}'$ ponendo $\Phi(K) = f(K)$. Per i punti (b) e (c) del Teorema 5.2, $f^{-1}(L) \in \mathcal{S}$ e $L = f(f^{-1}(L))$ per ogni $L \leq f(G)$. Quindi Φ è suriettiva. Per vedere che Φ è anche iniettiva, prendiamo $K, K_1 \in \mathcal{S}$ con $f(K) = f(K_1)$. Di nuovo per il punto (c) del teorema 5.2 e dal fatto che $N \leq K$, si ha

$$K = f^{-1}(f(K)) = f^{-1}(f(K_1)) = K_1.$$

Osserviamo infine che $f(k^g) = f(g^{-1}kg) = f(g)^{-1}f(k)f(g) = f(k)^{f(g)}$ per ogni $g \in G$, $k \in K$, poiché f è un omomorfismo. Pertanto $K^g = K$ se e solo se $f(K)^{f(g)} = f(K)$. □

Corollario 5.10 *Sia $f : G \to H$ un omomorfismo suriettivo di gruppi e $N = \ker f$. Siano*

- *$\mathcal{S}$ l'insieme dei sottogruppi di G contenenti N e*
- *$\mathcal{S}'$ l'insieme di tutti sottogruppi di H.*

Allora l'applicazione che ad ogni $K \in \mathcal{S}$ associa $f(K)$ è una biiezione tra $\mathcal{S}$ e $\mathcal{S}'$. Inoltre, $K \in \mathcal{S}$ è normale se e solo se $f(K) \trianglelefteq H$; in tal caso $G/K \cong H/f(K)$.

DIMOSTRAZIONE. Segue dal Corollario 5.9. Per dimostrare l'isomorfismo $G/K \cong H/f(K)$ si consideri l'omomorfismo canonico $\pi' : H \to H/f(K)$ e sia $g = \pi' \circ f : G \to H/f(K)$. Allora $\ker g = \{x \in G : g(x) = 1\} = \{x \in G : f(x) \in f(K)\} = K$. Per il Teorema 5.7, $G/\ker g = G/K \cong H/f(K)$. □

Un caso particolare dell'ultimo corollario ha rilevanza particolare. Si tratta dell'omomorfismo canonico $\pi : G \to G/N$ rispetto ad un sottogruppo normale N di un gruppo G. Abbiamo già visto che il nucleo di un omomorfismo è un sottogruppo normale. In effetti i sottogruppi normali sono in biiezione con i nuclei di omomorfismi, come è stato visto nell'esempio 5.5.

Corollario 5.11 (Secondo teorema di omomorfismo) *Siano K un sottogruppo e N un sottogruppo normale di un gruppo G. Allora $N \cap K \trianglelefteq K$ e $K/K \cap N \cong KN/N$.*

DIMOSTRAZIONE. Consideriamo la restrizione $f = \pi|_K : K \to f(K)$ dell'omomorfismo $\pi : G \to G/N$. Poiché $f(K) = f(KN)$, il sottogruppo $f(K)$ coincide con il quoziente KN/N. D'altra parte, $\ker f = \{x \in K : f(x) = 1\} = K \cap \ker f = K \cap N$. Per il Teorema 5.7 risulta $K/K \cap N \cong KN/N$. □

Osserviamo ancora che per ogni sottogruppo L di G/N il sottogruppo $K = \pi^{-1}(L)$ di G contiene N e quindi N è un sottogruppo normale di K. Il quoziente $K/N = \{xN : x \in K\}$ si può considerare in modo naturale come sottoinsieme di G/N essendo ogni classe laterale xN, con $x \in K$, uguale a $\pi(x)$. In altre parole, $K/N = \pi(K) = L$. Ora supponiamo che L sia un sottogruppo normale di G/N. In tal caso K risulta normale in G e $G/K \cong (G/N)/(K/N) = (G/N)/L$ (vedi Corollario 5.10). Abbiamo così dimostrato il

Corollario 5.12 (Terzo Teorema di omomorfismo) *Siano N, K sottogruppi normali di un gruppo G e $N \leq K$. Allora $K/N \trianglelefteq G/N$ e $G/K \cong (G/N)/(K/N)$.*

Come applicazione determiniamo adesso i sottogruppi di $\mathbb{Z}_m$.

Esempio 5.13 Applicando i risultati precedenti al caso $G = \mathbb{Z}$, $N = m\mathbb{Z}$ e $\pi : \mathbb{Z} \to \mathbb{Z}_m$ si ricava la seguente descrizione dei sottogruppi di $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Sia $L \leq \mathbb{Z}_m$. Per $K = \pi^{-1}(L)$ si ha $K = n\mathbb{Z}$ per qualche $n > 0$. Poiché $m\mathbb{Z} \leq n\mathbb{Z}$, si ha $m \in n\mathbb{Z}$ e di conseguenza n divide m. Quindi i sottogruppi L di $\mathbb{Z}_m$ hanno la forma $L = n\mathbb{Z}/m\mathbb{Z}$ per qualche n che divide m. Per esempio, i soli sottogruppi propri di $\mathbb{Z}_6$ sono $2\mathbb{Z}/6\mathbb{Z}$ e $3\mathbb{Z}/6\mathbb{Z}$.

Vediamo un altro esempio di omomorfismo. Sia σ una permutazione in S_n e sia $\mathbb{R}$ il campo dei numeri reali. Sia V uno spazio vettoriale su $\mathbb{R}$ di dimensione n e $\mathcal{B} = \{v_1 \dots v_n\}$ una base di V. Sia f_σ la funzione lineare così definita sugli elementi della base di V: $f_\sigma(v_i) = v_{\sigma(i)}$. Denotiamo con A_σ la matrice di f_σ rispetto alla base $\mathcal{B}$. Allora A_σ è una matrice di $GL_n(\mathbb{R})$ tale che in ogni colonna c'è un unico 1 e gli altri elementi sono uguali a 0. Una matrice siffatta si dice *matrice di permutazione*.

L'omomorfismo definito nel lemma seguente è importante perché permette di "rappresentare" il gruppo delle permutazioni su un insieme finito come un sottogruppo di matrici.

Lemma 5.14 *L'applicazione $f : S_n \longrightarrow GL_n(\mathbb{R})$ tale che $f(\sigma) = A_\sigma$ è un omomorfismo di gruppi.*

DIMOSTRAZIONE. Siano $\sigma, \tau \in S_n$, allora $f_{\sigma\circ\tau}(v_i) = v_{\sigma\circ\tau(i)} = v_{\sigma(\tau(i))} = f_\sigma(v_{\tau(i)}) = f_\sigma(f_\tau(v_i)) = (f_\sigma \circ f_\tau)(v_i)$. Poiché la matrice della composizione $f_\sigma \circ f_\tau$ delle funzioni lineari f_σ e f_τ coincide con il prodotto delle matrici di f_σ e f_τ, possiamo concludere che $A_{\sigma\circ\tau} = A_\sigma A_\tau$. □

Consideriamo ora una trasposizione $\tau = (ij)$ e la matrice A_τ. Osserviamo che scambiando la i-esima colonna con la j-esima colonna di A_τ, otteniamo la matrice identica I_n e quindi $det(A_\tau) = -det(I_n) = -1$. Ora ogni $\sigma \in S_n$ è un prodotto di trasposizioni, $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$. Pertanto, utilizzando il lemma appena dimostrato e il Teorema di Binet che ci garantisce che il determinante è moltiplicativo, $det(A_\sigma) = det(A_{\tau_1} A_{\tau_2} \ldots A_{\tau_r}) = det(A_{\tau_1}) det(A_{\tau_2}) \ldots det(A_{\tau_r}) = (-1)^r$.

Definizione 5.15 Definiamo la funzione *segno* da S_n nel gruppo $\{1, -1\}$ nel modo seguente $sgn(\sigma) = det(A_\sigma)$.

Allora la funzione *sgn* è un omomorfismo suriettivo di gruppi.

Possiamo calcolare il segno di una permutazione scrivendola come prodotto di cicli disgiunti e poi osservando che il segno di un ciclo di lunghezza l è 1 se l è dispari, -1 se l è pari. Infatti se $(a_1 a_2 \ldots a_l)$ è un ciclo di lunghezza l, allora

$$(a_1 a_2 \ldots a_l) = (a_1 a_l) \circ (a_1 a_{l-1}) \circ \ldots \circ (a_1 a_3) \circ (a_1 a_2),$$

$(a_1 a_2 \ldots a_l)$ è il prodotto di $l-1$ trasposizioni, da cui $sgn((a_1 a_2 \ldots a_l)) = (-1)^{l-1}$.

Vogliamo trovare il nucleo della funzione *sgn*. Osserviamo che $sgn(\sigma) = (-1)^{N(\sigma)}$ dove $N(\sigma)$ è l'intero della definizione 2.16. Pertanto il nucleo dell'applicazione *sgn* è esattamente il sottogruppo di tutte le permutazioni pari, cioè il gruppo alterno A_n. Allora il gruppo alterno è un sottogruppo normale di indice due di S_n.

5.3 Esercizi sugli omomorfismi

Esercizio 5.16 *Verificare che la funzione logaritmo (con base arbitraria) definisce un isomorfismo tra i gruppi* $(\mathbb{R}_+, \cdot)$ *e* $(\mathbb{R}, +)$.

Esercizio 5.17 *Verificare che la composizione di omomorfismi è un omomorfismo.*

Esercizio 5.18 *Si consideri l'applicazione* $\tau : GL_2(\mathbb{R}) \to GL_2(\mathbb{R})$ *che manda ogni matrice A nella sua trasposta* A^t*, cioè*

$$\tau\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}.$$

L'applicazione τ *così definita è un omomorfismo?*

Esercizio 5.19 *Dimostrare che:*

(a) il gruppo quoziente $\mathbb{R}/\mathbb{Z}$ *è isomorfo al gruppo* $(\mathbb{S}, \cdot)$*, se* $\mathbb{S}$ *è l'insieme dei numeri complessi z con* $|z| = 1$.

(b) l' insieme $(\mathbb{U}_n, \cdot)$ *delle radici n-esime dell' unità,* $n > 1$ *è un sottogruppo di* $\mathbb{S}$.

(c) ll gruppo quoziente $\mathbb{Z}/n\mathbb{Z}$ *è isomorfo al gruppo* $(\mathbb{U}_n, \cdot)$.

Esercizio 5.20 *Provare che i gruppi* $(\mathbb{Q}, +)$ *e* $(\mathbb{Q} \setminus \{0\}, \cdot)$ *non sono isomorfi.*

6 I gruppi ciclici

In questo capitolo intendiamo studiare i gruppi ciclici (vedi Definizione 3.10). Dapprima vogliamo "classificarli". Quando in Teoria dei gruppi si usa la parola "classificare" si intende trovare tutti i gruppi, a meno di isomorfismo, con una certa proprietà. Nel caso specifico, dato un qualunque gruppo ciclico G, dimostriamo che in realtà G è isomorfo ad un gruppo che già conosciamo. Studiamo poi i generatori dei gruppi ciclici e infine ne determiniamo la "struttura". Che cosa significa "determinare la struttura di un gruppo"? Significa descrivere tutti i suoi sottogruppi, i suoi sottogruppi normali e i suoi quozienti. In generale, non è facile determinare la struttura di un gruppo, ma nel caso dei gruppi ciclici, questa viene determinata completamente.

Iniziamo quindi con la classificazione dei gruppi ciclici. Come già osservato, nella dimostrazione del seguente Teorema sarà determinante l'utilizzo del primo teorema di omomorfismo e la conoscenza dei sottogruppi dei numeri interi $(\mathbb{Z}, +)$.

Teorema 6.1 *Sia $(G, \cdot)$ un gruppo ciclico, allora:*
(a) $G \cong \mathbb{Z}$, se G è infinito; oppure
(b) G è isomorfo a $\mathbb{Z}_m$ se G è finito con m elementi.

DIMOSTRAZIONE. Sia x un generatore di G. Allora l'applicazione $f : \mathbb{Z} \to G$ definita da $f(n) = x^n$ è suriettiva. Dal Lemma 2.3 segue che f è un omomorfismo. Allora il suo nucleo $\ker f$ è un sottogruppo di $\mathbb{Z}$. Per l'esercizio 3.11 esiste $m \geq 0$ tale che $\ker f = m\mathbb{Z}$. Consideriamo due casi:
(a) $m = 0$, allora $\ker f = \{0\}$ e quindi f è iniettiva. Di conseguenza f è un isomorfismo, quindi $G \cong \mathbb{Z}$.
(b) $m > 0$, allora per il teorema dell'omomorfismo $G \cong \mathbb{Z}/\ker f = \mathbb{Z}_m$. □

Vogliamo studiare ora la struttura di un gruppo ciclico e cominciamo a capire quanti possono essere i generatori di un gruppo ciclico. Ci sarà una differenza tra i casi in cui G è ciclico infinito e G è finito.

Lemma 6.2 *(a) $\mathbb{Z}$ ha due generatori.*
(b) $\mathbb{Z}_m$ ha $\varphi(m)$ generatori.

DIMOSTRAZIONE. (a) Ovviamente ± 1 sono generatori di $\mathbb{Z}$. Se a è un generatore di $\mathbb{Z}$, allora $\langle a \rangle = a\mathbb{Z} = \mathbb{Z}$. Questo è possibile se e solo se $a = \pm 1$.
(b) Per vedere che $\mathbb{Z}_m$ ha $\varphi(m)$ generatori, basta notare che per un generatore a di $\mathbb{Z}_m$ un multiplo ka risulta generatore se e solo se k è coprimo con m (vedi (c) del Lemma 2.6). Quindi i generatori di $\mathbb{Z}_m$ corrispondono ai numeri interi k che soddisfano $0 \leq k < m$ e sono coprimi con m. □

Un'altra importante proprietà che riguarda in generale i generatori di un gruppo, non necessariamente ciclico, e gli omomorfismi, è la seguente:

Lemma 6.3 *Sia $f : G \to H$ un omomorfismo suriettivo. Se a è generatore di G, allora $f(a)$ è un generatore di H.*

DIMOSTRAZIONE. Sia $G = \langle a \rangle$. Allora per ogni $x \in H$ esiste $y \in G$ tale che $x = f(y)$. Essendo $G = \langle a \rangle$ troviamo $n \in \mathbb{Z}$ tale che $y = a^n$. Adesso $x = f(a^n) = f(a)^n$, quindi $x \in \langle f(a) \rangle$. Pertanto, $H = \langle f(a) \rangle$. □

Ora dimostriamo che un sottogruppo di un gruppo ciclico è ciclico, generalizzando (e sfruttando) ciò che abbiamo visto nell'esercizio 3.11. Vediamo inoltre che la classe dei gruppi ciclici è stabile anche per il passaggio ai quozienti (cioè il quoziente di un gruppo ciclico è ciclico):

Proposizione 6.4 *Sia C un gruppo ciclico. Allora:*
(a) ogni quoziente di C è ciclico;
(b) ogni sottogruppo di C è ciclico.

DIMOSTRAZIONE. (a) Sia a un generatore di C e sia N un sottogruppo di C. Poiché C è abeliano, N è un sottogruppo normale. Sia $\pi : C \to C/N$ l'omomorfismo canonico. Allora $\pi(a)$ è un generatore di C/N per il Lemma 6.3.
(b) Sia $f : \mathbb{Z} \to C$ un omomorfismo suriettivo (vedi la dimostrazione del Teorema 6.1). Allora per ogni $L \leq C$ si ha $L = f(f^{-1}(L))$. Per l'esercizio 3.11 il sottogruppo $f^{-1}(L)$ di $\mathbb{Z}$ è ciclico. Ora, per il Lemma 6.3 anche L risulta ciclico. □

Dal Teorema di Lagrange segue che per ogni gruppo finito G l'ordine dei sottogruppi di G divide $|G|$. Come già accennato, non è detto che per ogni divisore di $|G|$ esista un sottogruppo. Questo accade invece nei gruppi ciclici. Anzi ogni divisore dell'ordine di $|G|$ risulta essere l'ordine di un unico sottogruppo di G.

Teorema 6.5 *Sia C un gruppo ciclico finito. Allora per ogni divisore d di $m = |C|$ esiste un unico sottogruppo di C di ordine d.*

DIMOSTRAZIONE. Sia x un generatore di C. Allora per $m_1 = m/d$ l'elemento $y = x^{m_1}$ ha ordine d e pertanto il sottogruppo $\langle y \rangle$ ha ordine d. Ora supponiamo di avere un sottogruppo H di C di ordine d. Sia y un generatore di H. Allora $o(y) = d$ ed esiste un unico $1 \leq k \leq m$ tale che $y = x^k$. Poiché $d = m/(k, m)$, concludiamo che $(k, m) = m_1$, quindi $k = m_1 k_1$, con $(k_1, d) = 1$. Quindi, $d = o(y) = o(x^{m_1})$. Si ha $H = \langle y \rangle \leq \langle x^{m_1} \rangle$. Essendo anche $\langle x^{m_1} \rangle$ un sottogruppo di ordine d, abbiamo $H = \langle x^{m_1} \rangle$. □

Questo teorema stabilisce una biiezione tra i sottogruppi di un gruppo ciclico finito G e i divisori dell'ordine $|G|$. Inoltre completa lo studio dei gruppi ciclici finiti.

Esaminiamo alcune proprietà dei gruppi infiniti più noti, cioè i numeri razionali e i numeri reali.

Lemma 6.6 *Ogni sottogruppo finitamente generato di $(\mathbb{Q}, +)$ è ciclico.*

DIMOSTRAZIONE. Sia $H = \langle r_1, \ldots, r_n \rangle$ un sottogruppo finitamente generato di $\mathbb{Q}$. Procediamo per induzione sul numero n di generatori di H. Consideriamo prima il caso $n = 2$ (essendo il caso $n = 1$ banale). Sia $H = \langle r, s \rangle$, con $r, s \in \mathbb{Q}$. Allora $r = a/b, s = c/d$, con $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$. Ovviamente, $r \in \langle 1/b \rangle$ e $s \in \langle 1/d \rangle$, pertanto H è contenuto in $K = \langle 1/b, 1/d \rangle$. Ora, $1/b \in \langle 1/bd \rangle$ e $1/d \in \langle 1/bd \rangle$. Quindi $K \leq \langle 1/bd \rangle$. Questo dimostra che H è sottogruppo del gruppo ciclico $\langle 1/bd \rangle$, e quindi H è ciclico. Abbiamo così dimostrato che ogni sottogruppo di $\mathbb{Q}$ generato da due elementi è ciclico. Sia ora $n > 2$. Per dimostrare che $H = \langle r_1, \ldots, r_n \rangle$ è ciclico poniamo $K = \langle r_1, \ldots, r_{n-1} \rangle$ e notiamo che $K = \langle k \rangle$ è ciclico per l' ipotesi induttiva. Allora $H = \langle k, r_n \rangle$ è ciclico per l' argomento nel caso $n = 2$. □

Proposizione 6.1 *Sia $(G, +)$ un gruppo abeliano infinito tale che ogni sottogruppo proprio di G ha indice finito. Dimostrare che G è ciclico.*

DIMOSTRAZIONE. Sia $x \in G$, $x \neq 0$. Allora $H = \langle x \rangle$ ha indice finito, quindi H è infinito. Questo dimostra che $o(x) = \infty$ per ogni $x \in G$, $x \neq 0$. Fissiamo un elemento non nullo $a \in G$ e sia $H_0 = \langle a \rangle$. Se $H_0 = G$ la dimostrazione è finita. Supponiamo che $H_0 \neq G$. Per $y \in G$, $y \neq 0$, il sottogruppo $\langle y \rangle$ ha indice finito, pertanto anche $\langle y \rangle \cap H$ ha indice finito (vedi il Lemma 3.30). In particolare, $\langle y \rangle \cap H_0 \neq 0$. Quindi esistono $n, m \in \mathbb{Z}$ con $na = my$ e $n \neq 0, m \neq 0$. Adesso consideriamo l'applicazione $f : G \to \mathbb{Q}$ definita da $f(y) = n/m$ per $y \neq 0$ in G e con $f(0) = 0$. Per vedere che la definizione è corretta, supponiamo di avere $m'y = n'a$ per un'altra coppia di interi $m', n' \in \mathbb{Z}$ e $m' \neq 0$. Allora moltiplicando per m si trova $mm'y = mn'a = nm'a$ perché $na = my$. Ora $mn'a = nm'a$ implica $mn' = nm'$ perché a ha ordine infinito e $(mn' - nm')a = 0$. Concludiamo che $m/n = m'/n'$ e quindi f è definita correttamente. Inoltre f è un omomorfismo in quanto se $y, z \in G$ e uno dei due è 0, allora $f(y + z) = f(y) + f(z)$. Se $y \neq 0 \neq z$, allora si ha $n_1 a = m_1 y$ e $n_2 a = m_2 z$ per qualche $n_1, n_2, m_1, m_2 \in \mathbb{Z}$. Moltiplicando la prima uguaglianza per m_2 e la seconda per m_1, si ottiene $m_2 n_1 a = m_2 m_1 y$ e $m_1 n_2 a = m_1 m_2 z$ da cui segue $(m_2 n_1 + m_1 n_2)a = m_2 m_1 (y + z)$. Pertanto $f(y + z) = m_2 n_1 + m_1 n_2 / m_2 m_1 = n_1/m_1 + n_2/m_2 = f(y) + f(z)$. Inoltre f ha nucleo $\{0\}$, quindi $G \cong f(G)$ e $f(G)$ ha la stessa proprietà. In particolare, $\mathbb{Z} = f(H_0)$ ha indice finito in $f(G)$, quindi il gruppo $f(G)$ è finitamente generato. Per il Lemma 6.6, $f(G)$ è ciclico e quindi $G \cong f(G)$ è pure ciclico. □

7 Prodotti diretti

Nel Capitolo 2 sui gruppi, abbiamo introdotto il prodotto diretto $H \times K$ di due gruppi H e K e abbiamo dimostrato nel Teorema 1.14 come risulti essere un gruppo con l'operazione definita "componente per componente".

In questo capitolo analizziamo meglio la struttura dei prodotti diretti. Mostreremo in particolare che un gruppo G è (isomorfo ad) un prodotto diretto di due gruppi se e solo se G possiede due sottogruppi normali che generano tutto G e la cui intersezione è identica.

Ricordiamo che in generale il prodotto di due sottogruppi non è in generale un sottogruppo, ma nel caso di sottogruppi normali è ancora un sottogruppo normale, come dimostrato nel Lemma 4.8.

Cominciamo dunque partendo da un gruppo G che possiede due sottogruppi *normali* H e K che godono delle seguenti due proprietà:

(a) $H \cap K = \{1\}$, e

(b) $G = HK$.

Osserviamo che i due sottogruppi H e K di G sono in particolare dei gruppi. Quindi possiamo considerare il loro prodotto diretto $H \times K$. Dimostriamo nel seguente Teorema 7.2 che, in questo caso, G ha la stessa struttura del prodotto diretto $H \times K$. Per far questo necessitiamo prima di un Lemma:

Lemma 7.1 *Sia G un gruppo e siano H e K due sottogruppi normali di G, tali che $H \cap K = \{1\}$. Allora ogni elemento di H è permutabile con ogni elemento di K.*

DIMOSTRAZIONE. Siano $h \in H$ e $k \in K$. Allora $hkh^{-1} \in K$ per il Lemma 4.3 poiché K è normale. Inoltre, $k^{-1} \in K$, perciò concludiamo che $hkh^{-1}k^{-1} \in K$. Analogamente, il Lemma 4.3 ci permette di

scrivere $kh^{-1}k^{-1} \in H$ poiché $h^{-1} \in H$ e H è normale. Di conseguenza anche $hkh^{-1}k^{-1} \in H$. Questo dimostra che $hkh^{-1}k^{-1} \in K \cap H = \{1\}$. Pertanto $hkh^{-1}k^{-1} = 1$ e di conseguenza $hk = kh$. □

Dimostriamo ora il Teorema.

Teorema 7.2 *Sia G un gruppo e siano H ed K due sottogruppi normali di G, tali che*

(a) $H \cap K = \{1\}$, e

(b) $G = HK$.

Allora $G \cong H \times K$.

DIMOSTRAZIONE. Definiamo $f : H \times K \to G$ con $f(h, k) = hk$. Per il punto (b) f è un'applicazione suriettiva. Proviamo che f è un omomorfismo. Infatti, siano $h, h_1 \in H$ e $k, k_1 \in K$. Allora $h_1k = kh_1$ per il punto (a) e il Lemma 7.1. Quindi

$$f((h, k)(h_1, k_1)) = f((hh_1, kk_1)) = hh_1kk_1 = hkh_1k_1 = f((h, k))f((h_1, k_1)).$$

Per verificare che f è iniettiva basta vedere che $\ker f = \{1\}$. Se $f(h, k) = 1$, allora $hk = 1$ e quindi $h = k^{-1} \in H \cap K$ e per il punto (a) abbiamo $h = k = 1$. Abbiamo così dimostrato che f è un isomorfismo. □

Le condizioni (a) e (b) del Teorema 7.2 si ricordano facilmente. Si tende invece a dimenticare l'altra ipotesi essenziale del Teorema e cioè che i due sottogruppi H e K devono essere normali. Tale condizione è invece essenziale: infatti se non sono normali, il Teorema non è più vero, come dimostreremo nell'esempio 7.6.

Le condizioni richieste nel precedente Teorema 7.2 sono in particolare soddisfatte nel caso di un gruppo finito con due sottogruppi normali propri di ordine coprimo.

Teorema 7.3 *Sia G un gruppo finito e siano H ed K due sottogruppi normali di G, tali che $H = |m|$ e $K = |n|$. Supponiamo che*
(a) $(m, n) = 1$, e
(b) $|G| = mn$.
Allora $G \cong H \times K$.

DIMOSTRAZIONE. Applicheremo il Teorema 7.2. A questo scopo bisogna verificare che $H \cap K = \{1\}$ e $G = HK$.

Poniamo $l = |H \cap K|$. Applicando il Teorema di Lagrange al gruppo H e al suo sottogruppo $H \cap K$ ricaviamo che l divide m. Analogamente, applicando il Teorema di Lagrange al gruppo K e al suo sottogruppo $H \cap K$ ricaviamo che l divide n. Allora l divide (m, n). Da $(m, n) = 1$ concludiamo che $l = 1$ e quindi $H \cap K = \{1\}$.

Ora poniamo $s = |HK|$. Applicando il Teorema di Lagrange al gruppo HK e al suo sottogruppo H ricaviamo che m divide s. Analogamente, applicando il Teorema di Lagrange al gruppo HK e al suo sottogruppo K ricaviamo che n divide s. Allora anche il minimo comune multiplo mn (per $(m, n) = 1$) di m ed n divide s. Poiché $s \leq |G| = mn$, concludiamo che $s = mn$ e quindi $HK = G$. □

Nel caso dei gruppi abeliani, poiché ogni sottogruppo è normale, le due precedenti condizioni si ridurranno a:

Corollario 7.4 *Sia G un gruppo abeliano e siano H ed K due sottogruppi di G, tali che $|H| = m$ e $|K| = n$. Supponiamo che*
(a) $H \cap K = \{1\}$ oppure $(m, n) = 1$
(b) $|G| = mn$.
Allora $G \cong H \times K$.

Vediamo ora alcune applicazioni di quanto appena dimostrato, nel caso di alcuni gruppi abeliani di ordine piccolo.

Esempio 7.5 Sia H il sottogruppo di $\mathbb{Z}_6$ generato da $[2]_6$ e sia K il sottogruppo generato da $[3]_6$. Allora $|K| = 2$ e $|H| = 3$ sono coprimi e $|\mathbb{Z}_6| = 2 \cdot 3$. Per il corollario precedente, $\mathbb{Z}_6 \cong H \times K$.

Esempio 7.6 Consideriamo il gruppo $G = S_3$ e i suoi due sottogruppi $H = \langle(12)\rangle$ e $K = \langle(123)\rangle$. Allora

a) $H \cap K = \{1\}$, e

b) $G = HK$.

Pertanto per il Teorema 7.2, $S_3 \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Quindi S_3 è isomorfo ad un gruppo ciclico di ordine 6 e pertanto contiene un elemento di ordine 6. Ma gli elementi di S_3 hanno tutti ordine 1,2 o 3. Dov'è l'errore?

Abbiamo dimostrato che se G possiede due sottogruppi normali che generano tutto G e la cui intersezione è identica, allora G è (isomorfo ad) un prodotto diretto di due gruppi. Come promesso all'inizio del capitolo, dimostriamo ora il viceversa.

Cominciamo dimostrando che le proiezioni, come sono state definite sugli insiemi, sono degli omomorfismi.

Lemma 7.7 *Siano* $p_1 : H \times K \to H$ *e* $p_2 : H \times K \to K$ *le due proiezioni definite da* $p_1((h,k)) = h$ *e* $p_2((h,k)) = k$. *Allora* p_1 *e* p_2 *sono omomorfismi. Inoltre* $\ker p_1 \cong K$ *e* $\ker p_2 \cong H$.

Dimostrazione. Se $h, h_1 \in H$ e $k, k_1 \in K$ si ha

$$p_1((h,k)(h_1,k_1)) = p_1((hh_1, kk_1)) = hh_1 = p_1((h,k))p_1((h_1,k_1)).$$

Analogamente si dimostra che p_2 è un omomorfismo. I nuclei $K_1 = \ker p_1$ e $H_1 = \ker p_2$ sono sottogruppi normali di $H \times K$. Questo si vede facilmente anche dalla forma esplicita

$$K_1 = \{(1_H, k) : k \in K\} = \{1_H\} \times K \quad \text{e} \quad H_1 = \{(h, 1_K) : h \in H\} = H \times \{1_K\}.$$

Infine, $i : K_1 \to K$ e $j : H_1 \to H$ definiti da $i(1_H, k) = k$ e $j(h, 1_K) = h$ sono isomorfismi che ci permettono di identificare i gruppi H e K rispettivamente con i sottogruppi H_1 e K_1 del prodotto diretto $H \times K$. □

Dalla dimostrazione del Lemma 7.7 segue il Corollario 7.8 che permette di scrivere G come prodotto di due suoi sottogruppi normali.

Corollario 7.8 *Sia* $G = H \times K$ *il prodotto diretto di due gruppi* H *e* K. *Allora esistono due sottogruppi normali* H_1 *e* K_1 *di* $H \times K$, *tali che:*

(a) $H_1 \cap K_1 = \{1\}$,

(b) $G = H_1 K_1$.

Dimostrazione. Basta prendere $K_1 = \ker p_1$ e $H_1 = \ker p_2$, come nel Lemma 7.7. K_1 e H_1 sono normali perché sono nuclei di omomorfismi. Inoltre (a) è ovvia dalla definizione di H_1 e K_1. Per (b) basta notare che se $(h,k) \in H \times K$, allora $(h,k) = (h, 1_K)(1_H, k)$. Ovviamente, possiamo scrivere anche $(h,k) = (1_H, k)(h, 1_K)$ poiché ogni elemento di H_1 è permutabile con ogni elemento di K_1. □

Le dimostrazioni fatte finora, non richiedono nessuna ipotesi sul gruppo G. Iniziamo a "specializzare" il nostro studio per avviarci a studiare i gruppi abeliani finiti. Infatti, con il seguente Teorema 7.9, ci proponiamo di studiare l'ordine degli elementi di un prodotto di gruppi H e K in funzione dell'ordine delle loro proiezioni.

Teorema 7.9 *Siano* H *ed* K *due gruppi e sia* $z = (x, y)$ *un elemento del prodotto diretto* $H \times K$. *Allora l' ordine di* z *è finito se e solo se sono finiti gli ordini di* x *e* y. *In tal caso, l' ordine di* z *è il minimo comune multiplo degli ordini* $o(x)$ *e* $o(y)$.

Dimostrazione. Se $z^m = 1$ per qualche intero m, allora $(x^m, y^m) = (1_H, 1_K)$, e quindi $x^m = 1_H$ e $y^m = 1_K$. Di conseguenza, gli ordini di x e y sono finiti qualora sia finito l'ordine di z. Supponiamo adesso che $o(x) = m$ e $o(y) = n$ siano finiti. Dimostreremo che anche $o(z)$ è finito e coincide con il minimo comune multiplo l di m e n. Infatti dall'esercizio 2.19 segue che $o(z)$ divide l. Se $z^s = 1$, allora $x^s = 1_H$ e $y^s = 1_K$, quindi m divide s e n divide s. Di conseguenza anche l divide s. Quindi $o(z) = l$. □

Applichiamo il Teorema 7.9 appena dimostrato, per dimostrare che alcuni prodotti diretti di gruppi non possono essere ciclici.

Esempio 7.10 (a) Il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico.
(b) Sia p un numero primo. Il gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$ non è ciclico.

DIMOSTRAZIONE. (a) Ogni elemento $x \in \mathbb{Z}_2$ soddisfa $2x = 0$, quindi $\mathbb{Z}_2 \times \mathbb{Z}_2$ non ha elementi di ordine 4.
(b) Per il Teorema 7.9 ogni elemento non nullo di $\mathbb{Z}_p \times \mathbb{Z}_p$ ha ordine p, quindi non può generare tutto il gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$. Pertanto $\mathbb{Z}_p \times \mathbb{Z}_p$ non è ciclico. □

I gruppi considerati nell' Esempio 7.10 stimolano allora una domanda: il prodotto diretto di 2 gruppi ciclici è ancora ciclico? Il seguente Teorema 7.11 da' la risposta.

Teorema 7.11 *Siano m e n due numeri naturali. Allora $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ se e solo se m ed n sono coprimi.*

DIMOSTRAZIONE. Supponiamo che m ed n siano coprimi. Sia x un generatore di $\mathbb{Z}_m$ e sia y un generatore di $\mathbb{Z}_n$. Allora $o(x) = m$ e $o(y) = n$. Per il Teorema 7.9 l'elemento $z = (x, y)$ di $\mathbb{Z}_m \times \mathbb{Z}_n$ ha ordine $o(z) = mn$. Quindi il sottogruppo ciclico $\langle z \rangle$ di $\mathbb{Z}_m \times \mathbb{Z}_n$ ha mn elementi. Pertanto, $\mathbb{Z}_{mn} \cong \langle z \rangle = \mathbb{Z}_m \times \mathbb{Z}_n$.
Ora dimostriamo che se il gruppo $\mathbb{Z}_m \times \mathbb{Z}_n$ è ciclico, allora m e n sono coprimi. Supponendo per assurdo che m ed n non siano coprimi si trova un numero primo p che divide sia m che n. Allora, per il Teorema 6.5 esiste un sottogruppo H di $\mathbb{Z}_m$ di ordine p ed esiste un sottogruppo K di $\mathbb{Z}_n$ di ordine p. Ora $H \times K$ è un sottogruppo di $\mathbb{Z}_m \times \mathbb{Z}_n$ isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$, quindi non può essere ciclico per il punto (b) dell' Esempio 7.10, assurdo (vedi la Proposizione 6.4). □

I prodotti diretti si possono definire anche per più di due gruppi. Se H_1, H_2 e H_3 sono tre gruppi, si può definire il prodotto diretto $H_1 \times H_2 \times H_3$ come $(H_1 \times H_2) \times H_3$. Proviamo che l'ordine in cui viene scritto il prodotto diretto di due gruppi non è influente sulla struttura del gruppo.

Lemma 7.12 *Siano H_1 e H_2 due gruppi. Allora $H_1 \times H_2 \cong H_2 \times H_1$.*

DIMOSTRAZIONE. L'applicazione $f : H_1 \times H_2 \to H_2 \times H_1$ definita da $f(x, y) = (y, x)$ è un isomorfismo. □

Utilizzando lo stesso ragionamento della dimostrazione del Lemma 7.12, si può dimostrare che

$$(H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3).$$

Quindi, questi due gruppi si possono identificare. Un terzo modo per definire il prodotto diretto $H_1 \times H_2 \times H_3$ è quello di introdurre un'operazione binaria nel prodotto cartesiano $H_1 \times H_2 \times H_3$ ponendo $(g_1, g_2, g_3) \cdot (h_1, h_2, h_3) = (g_1h_1, g_2h_2, g_3h_3)$ per ogni coppia di terne $(g_1, g_2, g_3), (h_1, h_2, h_3) \in H_1 \times H_2 \times H_3$. Si dimostra facilmente, seguendo la dimostrazione del Teorema 1.14, che $(H_1 \times H_2 \times H_3, \cdot)$ risulta un gruppo isomorfo a $(H_1 \times H_2) \times H_3$. In seguito penseremo il prodotto diretto $H_1 \times H_2 \times H_3$ definito nell'ultimo modo. In maniera analoga si può introdurre anche il prodotto diretto $H_1 \times H_2 \times \ldots \times H_n$ di n gruppi $H_1, H_2, \ldots, H_n$.

Esempio 7.13 Applicando due volte il Teorema 7.11 è facile dimostrare, che $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Più in generale, se m, n e k sono tre numeri interi positivi a due a due coprimi, allora $\mathbb{Z}_{kmn} \cong \mathbb{Z}_k \times \mathbb{Z}_m \times \mathbb{Z}_n$.

Questa decomposizione di un gruppo ciclico in prodotto diretto di gruppi ciclici di ordini coprimi è un caso particolare di un procedimento che si può applicare più in generale ad un gruppo abeliano finito. Il seguente Teorema infatti descrive la struttura dei gruppi abeliani finiti.

Teorema 7.14 (Teorema di Frobenius-Stickelberger) *Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici.*

Il capitolo seguente sarà interamente dedicato alla dimostrazione del Teorema 7.14

7.1 Esercizi sui prodotti diretti

Esercizio 7.15 *Sia G un gruppo e sia $D = \{(g, g) : g \in G\}$ il sottogruppo diagonale del prodotto diretto $G \times G$. Dimostrare che D è un sottogruppo normale di $G \times G$ se e solo se G è abeliano.*

Esercizio 7.16 *Siano H ed K due gruppi. Dimostrare che $H \times K$ è abeliano se e solo se H e K sono abeliani.*

Esercizio 7.17 *Sia A un sottogruppo del prodotto diretto $H \times K$ contenente il sottogruppo $H \times \{1\}$. Allora $A = H \times (A \cap K)$.*

Esercizio 7.18 *Sia G un gruppo, e siano H e K sottogruppi di G tali che $G = H \times K$. Provare che:*
(a) $Z(G) = Z(H) \times Z(K)$;
(b) se $N \triangleleft G$ e $N \not\subseteq Z(G)$ allora risulta $H \cap N \neq \{1\}$ oppure $K \cap N \neq \{1\}$;
(c)* se H e K sono semplici e non abeliani, allora H e K sono gli unici sottogruppi normali non banali di G.

Esercizio 7.19 *Si consideri il gruppo $G = \{(a, b, c,)|a, b, c \in \mathbb{Z}\}$ con il prodotto definito dalla posizione*

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

i) Si determini l'identità e l'inverso dell'elemento (a, b, c).
ii) Sia $\mathbb{Z}\times\mathbb{Z}$ il gruppo prodotto diretto del gruppo additivo degli interi per se stesso e sia $f : G \to \mathbb{Z}\times\mathbb{Z}$ definito da $f((a, b, c)) = (a, c)$. Si verifichi che f è un omomorfismo e si determini $\ker(f)$.
iii) Si verifichi che $ker(f)$ coincide con il centro $Z(G)$ di G.

Esercizio 7.20 *Siano $f : G \to G_1$ e $t : H \to H_1$ due omomorfismi. Sia $F : G \times H \to G_1 \times H_1$ l'applicazione definita da $F(g, h) = (f(g), t(h))$. Allora:*
(a) F è un omomorfismo;
(b) F è iniettivo se e solo se lo sono f e t;
(c) F è suriettivo se e solo se lo sono f e t;
(d) F è un isomorfismo se e solo se lo sono f e t.

Esercizio 7.21 *Sia G un gruppo abeliano e siano H e K sottogruppi di G. Dimostrare che:*
a) il sottoinsieme $K + H = \{k + h : k \in K, h \in H\}$ di G è un sottogruppo,
b) il sottogruppo $K + H$ è isomorfo ad un quoziente del prodotto diretto $K \times H$, e quindi $|K + H|$ divide $|K| \cdot |H|$ nel caso in cui H e K siano finiti,
c) se gli ordini $|K|$ e $|H|$ sono coprimi, allora $K + H \cong K \times H$ e pertanto $|K + H| = |K| \cdot |H|$.

Esercizio 7.22 *Sia G un gruppo abeliano non ciclico di ordine 9. Dimostrare che $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.*

Esercizio 7.23 *Siano p e q due numeri primi distinti. Si trovi il numero dei sottogruppi del gruppo $G = \mathbb{Z}_p \times \mathbb{Z}_q$.*

Esercizio 7.24 *Sia p un numero primo. Si trovi il numero dei sottogruppi del gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Esercizio 7.25 *Dimostrare che il gruppo simmetrico S_3 non è prodotto diretto di due suoi sottogruppi propri.*

8 Gruppi abeliani finiti

In questa sezione vogliamo dimostrare il Teorema 7.14 di struttura dei gruppi abeliani finiti. Ci serviranno diversi lemmi sulle proprietà riguardanti i gruppi abeliani. Dapprima esaminiamo alcuni casi di gruppi "piccoli". Il primo lemma classifica tutti i gruppi di ordine un primo p (ce n'è uno solo!)

Lemma 8.1 *Per ogni primo p esiste esattamente (a meno di isomorfismi) un gruppo di ordine p.*

Dimostrazione. Sia $(G, \cdot)$ un gruppo di ordine p. Applicare il Teorema di Lagrange per concludere che ogni elemento $a \neq 1$ di G ha ordine p e quindi è un generatore di G in quanto $|G| = p$. In particolare, $G \cong \mathbb{Z}_p$. □

Vediamo ora i gruppi in cui tutti gli elementi hanno ordine 2.

Lemma 8.2 *Sia G un gruppo tale che tutti i suoi elementi diversi da 1 hanno periodo 2. Allora G è abeliano.*

DIMOSTRAZIONE. Siano $x, y \in G$. Allora $x^2 = y^2 = (xy)^2 = 1$. Pertanto, $x = x^{-1}, y = y^{-1}$ e $xy = (xy)^{-1}$. Ma $(xy)^{-1} = y^{-1}x^{-1} = yx$. Quindi $xy = yx$. □

Poiché 4 è il più piccolo numero naturale che non è un primo, studiamo ora i gruppi di ordine 4.

Lemma 8.3 *Sia G un gruppo di ordine 4; allora $G \cong \mathbb{Z}_4$ o $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

DIMOSTRAZIONE. Se G ha un elemento di ordine 4, allora G è ciclico e pertanto $G \cong \mathbb{Z}_4$. Altrimenti, tutti gli elementi diversi da 1 di G hanno periodo 2. Quindi G è abeliano. Si scelga un elemento non nullo $a \in G$. Allora $H = \langle a \rangle$ ha due elementi. Sia $b \in G \setminus H$. Allora $K = \langle b \rangle$ ha due elementi e $K \not\subseteq H$, quindi $H \cap K = \{1\}$ e HK contiene propriamente K. Poiché $d = |HK|$ divide $4 = |G|$, concludiamo che $HK = G$. Ora si applica Corollario 7.4. □

È relativamente facile descrivere tutti i gruppi abeliani di ordine ≤ 15 senza far ricorso al Teorema di struttura 7.14 come verrà chiesto di fare nell' Esercizio 8.10.

Iniziamo ora la dimostrazione del Teorema di Frobenius-Stickelberger.

Lemma 8.4 *Sia G un gruppo, H un sottogruppo di G ed $a \in G$. Se esistono due interi coprimi m ed n tali che $ma \in H$ e $na \in H$, allora $a \in H$.*

DIMOSTRAZIONE. Siano $u, v \in \mathbb{Z}$ tali che $1 = um + vn$. Allora $a = u(ma) + v(na) \in H$. □

Abbiamo visto nel Corollario 3.27 al Teorema di Lagrange che l'ordine di un elemento divide sempre l'ordine del gruppo e abbiamo anche visto che non sempre dato un divisore dell'ordine del gruppo esiste un sottogruppo di quell'ordine. Ci sono però alcuni casi particolari in cui ciò accade. E' il caso di un divisore primo dell'ordine del gruppo. Il seguente Lemma, noto come Lemma di Cauchy, vale per tutti i gruppi finiti, ma per ora lo dimostriamo solo nel caso abeliano.

Lemma 8.5 (Lemma di Cauchy) *Sia p un numero primo e G un gruppo abeliano finito tale che p divide $|G|$. Allora G ha elementi di ordine p.*

DIMOSTRAZIONE. L'asserto segue dal Teorema 6.5 se G è ciclico. Scriviamo $m = |G| = pn$ e procediamo per induzione su n. Per $n = 1$ ogni elemento non nullo di G ha ordine p. Supponiamo $n > 1$. Sia $a \in G$ un elemento non nullo. Se p divide l'ordine k di $H = \langle a \rangle$, si applica l'osservazione iniziale per trovare un elemento di ordine p di H. Supponiamo che p non divida k. Consideriamo il gruppo quoziente $G_1 = G/H$ e l'omomorfismo canonico $\pi : G \to G_1$. Ora $m_1 = |G_1| = m/k < m$ e $p|m_1$ poiché p divide km_1 e $(p, k) = 1$. Per l'ipotesi induttiva esiste $y \in G_1$ di ordine p. Sia $x \in G$ con $\pi(x) = y$. Allora se $K = \langle x \rangle$ si ha che p divide $|K|$. Infatti, supponiamo per assurdo che p non divida s. Allora $px \in H \cap K$ (poiché $o(y) = p$) e $sx = 0 \in H \cap K$, quindi $x \in H$ per il Lemma 8.4. Pertanto $\pi(x) = 0$, assurdo. Quindi, possiamo concludere che p divide s. Allora il sottogruppo ciclico K contiene un elemento di ordine p per il Teorema 6.5. □

Il seguente Lemma serve per la dimostrazione del Teorema successivo.

Lemma 8.6 *Sia $(G, +)$ un gruppo abeliano finito e sia m un intero positivo tale che $mx = 0$ per ogni $x \in G$. Allora $|G|$ divide qualche potenza di m.*

DIMOSTRAZIONE. Sia p un primo che divide $|G|$, allora esiste $x \in G$ di ordine p. Se p fosse coprimo con m, da $mx = 0$ e dal Lemma 8.4 si deduce, con $H = \{0\}$, che $x = 0$, assurdo. Quindi p divide m. Abbiamo così dimostrato che ogni numero primo che divide $|G|$ divide anche m. Per il Teorema fondamentale dell'aritmetica, questo implica che $|G|$ divide qualche potenza opportuna di m. □

Siamo ora giunti alla parte cruciale della dimostrazione. Il Teorema 8.7 e il successivo Corollario 8.8 garantiscono che se G è un gruppo abeliano di ordine finito $n = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}$, con p_i primo per ogni $i = 1, ..., t$ e $p_i \neq p_j$ se $i \neq j$; allora G si può scrivere come prodotto diretto di t gruppi P_1,..., P_t di ordini rispettivamente $p_1^{a_1}$, $p_2^{a_2}$, ..., $p_t^{a_t}$.

Teorema 8.7 *Siano m e n due numeri interi positivi coprimi e G un gruppo abeliano di ordine mn. Allora:*

a) $H = \{x \in G : nx = 0\}$ è un sottogruppo di G di ordine n;

b) $K = \{x \in G : mx = 0\}$ è un sottogruppo di G di ordine m;

c) $G \cong H \times K$.

DIMOSTRAZIONE. Se $nx = 0$ e $ny = 0$ per $x, y \in G$, allora anche $n(x-y) = nx - ny = 0$. Poiché anche $0 \in H$, questo ci permette di affermare che $H \leq G$. Analogamente si prova che $K \leq G$ e la prima parte di a) e b) sono così concluse.

c) Per provare che $G \cong H \times K$ proviamo adesso che $H \cap K = \{0\}$. Infatti, se $x \in H \cap K$, allora $nx = 0$ e $mx = 0$. Essendo m e n coprimi, si deduce dal Lemma 8.4, con $H = \{0\}$, che $x = 0$. Per verificare che $G = H + K$ prendiamo $y \in G$. Essendo m ed n coprimi esistono $u, v \in \mathbb{Z}$ tali che $1 = um + vn$. Allora avremo $y = u(my) + v(ny)$. Ora $n(my) = (nm)y = 0$ essendo $|G| = nm$. Quindi, $my \in H$. Analogamente si vede che $ny \in K$. Quindi, $y \in H + K$. Per il Teorema 7.2 si conclude che $G \cong H \times K$.

Per finire la dimostrazione, notiamo adesso che per il Lemma 8.6, $|H|$ divide qualche potenza di n, e pertanto $|H|$ è coprimo con m. D'altra parte, essendo un sottogruppo di G, $|H|$ divide $|G| = mn$. Quindi $|H|$ divide n. Analogamente $|K|$ divide m. L'isomorfismo $G \cong H \times K$ ci da' $|H| \cdot |K| = mn$. Quindi, $|H| = n$ e $|K| = m$. $\square$

Corollario 8.8 *Sia G gruppo finito di ordine n e sia $n = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}$, con p_i primo e $a_i \in \mathbb{N}^*$ per ogni $i = 1, ..., t$, la decomposizione di n in prodotto di primi distinti. Allora esistono t sottogruppi P_1, P_2, ..., P_t di ordini rispettivamente $p_1^{a_1}$, ..., $p_t^{a_t}$, tali che $G \cong P_1 \times P_2 \times ... \times P_t$.*

DIMOSTRAZIONE. La dimostrazione è per induzione su t. Se $t = 1$ il Corollario è ovvio. Supponiamo $t \geq 2$ e sia $m = p_1^{a_1} ... p_{t-1}^{a_{t-1}}$: allora m e $p_t^{a_t}$ sono coprimi e $mp_t^{a_t} = n$. Applichiamo il Teorema 8.7 per ottenere due sottogruppi H e P_t di ordini rispettivamente m e $p_t^{a_t}$ e tali che $G \cong H \times P_t$. Applichiamo ora l'ipotesi induttiva al gruppo H ed otteniamo $H \cong P_1 \times ... \times P_{t-1}$ per certi sottogruppi P_1, ..., P_{t-1} di ordini rispettivamente $p_1^{a_1}$, ..., $p_{t-1}^{a_{t-1}}$. Si conclude sostituendo H

$$G \cong H \times P_t \cong (P_1 \times ... \times P_{t-1}) \times P_t \cong P_1 \times ... \times P_{t-1} \times P_t. \square$$

Ora ci resta solo da dimostrare che i sottogruppi P_i definiti nel Corollario 8.8 si possono scrivere come prodotto di gruppi ciclici.

Teorema 8.9 *Sia p un numero primo, sia n un intero positivo e sia G un gruppo abeliano di ordine p^n. Allora G si scompone in prodotto diretto di gruppi ciclici.*

DIMOSTRAZIONE. Procediamo per induzione su n. Per $n = 1$ il gruppo stesso è ciclico, quindi non c'è niente da dimostrare. Se $n > 1$, scegliamo $b \in G$ con massimo ordine $p^k = o(b)$. Per il sottogruppo $B = \langle b \rangle$ scegliamo un sottogruppo $C \leq G$ tale che $B \cap C = \{0\}$ e C è massimo per questa proprietà (avendo G solo un numero finito di sottogruppi, questo è possibile). Dimostreremo che

$$G \cong B \times C. \tag{1}$$

Ora, $|C| = |G|/|B| = p^{n-k}$ e quindi per l'ipotesi induttiva C è prodotto diretto di gruppi ciclici. Essendo B ciclico, questo dimostra la tesi. Per dimostrare (1) basta verificare che sono soddisfatte le condizioni del Teorema 7.2. Essendo $B \cap C = \{0\}$ per ipotesi, basta verificare che

$$G = B + C. \tag{2}$$

Per un elemento $x \in G$ l'ordine $o(x)$ divide $|G|$, pertanto $o(x) = p^s$ per qualche intero s con $0 \leq s \leq k$. Dimostreremo che

$$x \in B + C \tag{3}$$

per induzione su s. Per $s = 0$ questo è banale perché allora $o(x) = 1$ e quindi $x = 0$. Supponiamo $s > 0$ e (3) vale per tutti gli elementi di ordine $s - 1$ di G. Allora per $y = px$ si ha $o(y) = p^{s-1}$. Per l'ipotesi induttiva, $y \in B + C$. Quindi, esistono $c \in C$ e $m \in \mathbb{Z}$ tali che $y = px = mb + c$. Moltiplicando per p^{s-1} troviamo $0 = p^{s-1}mb + p^{s-1}c$. Quindi $p^{s-1}mb \in C \cap B = \{0\}$. Allora $p^{s-1}mb = 0$ e per la scelta di b si ha p^k divide $p^{s-1}m$. Di conseguenza p divide m e $m = pm_1$ con $m_1 \in \mathbb{Z}$, poiché $k > s - 1$. Quindi, $px = m_1 pb + c$. Allora per l'elemento $a = x - m_1 b$ si ha $pa = c \in C$. Se $a \in C$, allora $x = a + m_1 b \in B + C$ e (3) è dimostrato. Se invece $a \notin C$, il sottogruppo $C_1 = \langle C, a \rangle$ contiene propriamente C, quindi $B \cap C_1 \neq \{0\}$ per la scelta di C. Sia $b' \in B \cap C_1$, $b' \neq 0$. Allora esistono $c \in C$ e $l \in \mathbb{Z}$ tali che $b' = c + la$. Allora p non divide l per la scelta di $b' \neq 0$; altrimenti $la \in C$ e $b' \in B \cap C = \{0\}$. Quindi, $la \in B + C$ e $pa \in C \leq B + C$. Per il Lemma 8.4, $a \in B + C$. Ora anche $x = a + m_1 b \in B + C$. Questo dimostra (3). $\square$

Possiamo ora dimostrare il Teorema di Frobenius Stickelberger.

(Teorema di Frobenius-Stickelberger) *Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici.*

DIMOSTRAZIONE. Sia G un gruppo abeliano di ordine n. Sia $n = p_1^{a_1} \dots p_t^{a_t}$ la scomposizione di n in prodotto di numeri primi distinti $p_1, \dots, p_t$. Per il Corollario 8.8, G è isomorfo al prodotto diretto $P_1 \times \dots \times P_t$, dove $|P_i| = p_i^{a_i}$ per ogni $i = 1, ..., t$. Per il Teorema 8.9, i sottogruppi P_i sono prodotti diretti di gruppi ciclici. Pertanto G è isomorfo a un prodotto diretto di gruppi ciclici. □

8.1 Esercizi sui gruppi abeliani finiti

Esercizio 8.10 *Descrivere tutti i gruppi abeliani di ordine minore o uguale a 15 senza far ricorso al Teorema 7.14.*

Esercizio 8.11 *Sia G un gruppo abeliano di ordine: a) 6; b) 12; c) 18; d) 22; e) 24; f) 28; g) 30 h) 33; i) 35; j) 42; k) 46; l) 66; m) 69; n) 78; o) 102; p) 105; q) 106; r) 110; s) 114; t) 119; u) 130; v) 131. In quale di questi casi si può affermare che G è necessariamente ciclico ?*

Esercizio 8.12 *Determinare il numero dei gruppi abeliani di ordine 24 a meno di isomorfismo. Lo stesso per quelli di ordine 100 e 144. Sia p un numero primo: quanti sono (a meno di isomorfismo) i gruppi abeliani di ordine p^5 ?*

Esercizio 8.13 *Siano p, q e r tre numeri primi distinti. Quanti sono (a meno di isomorfismo) i gruppi abeliani di ordine $p^5q^4r^3$?*

Esercizio 8.14 *Sia G un gruppo abeliano finito. Sia G^* l'insieme di tutti gli omomorfismi $f : G \to \mathbb{R}/\mathbb{Z}$ sul quale definiamo un'operazione $(f+g)(x) = f(x)+g(x)$. Si dimostri che G^* è un gruppo e che se $G = H \times K$, allora $G^* \cong H^* \times K^*$.*

Esercizio 8.15 *Sia G un gruppo abeliano finito e G^* il gruppo degli omomorfismi $f : G \to \mathbb{R}/\mathbb{Z}$, definito nell'esercizio 8.14. Si dimostri che se G è ciclico, allora $G \cong G^*$.*

Esercizio 8.16 * *Sia G un gruppo abeliano finito e G^* il gruppo degli omomorfismi $f : G \to \mathbb{R}/\mathbb{Z}$, definito nell'esercizio 8.14. Si dimostri che $G \cong G^*$.*

Esercizio 8.17 *Siano H e K due sottogruppi del gruppo abeliano finito G tali che $G = H+K$. Allora l'ordine di G divide $|H| \cdot |K|$.*

Esercizio 8.18 *Se p è un numero primo e $G = \langle x, y \rangle$ è un gruppo abeliano finito tale che p divide $|G|$, ma p non divide $o(x)$, allora p divide $o(y)$.*

Esercizio 8.19 *Se p è un numero primo e $G = \mathbb{Z}_{p^k}^m$ calcolare il numero degli elementi $x \in G$ con $o(x) = p^s$.*

Esercizio 8.20 *Se p è un numero primo e $G = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_{p^2}^{m_2} \times \dots \times \mathbb{Z}_{p^s}^{m_s}$ con $m_s > 0$, calcolare il numero degli elementi $x \in G$ con $o(y) = p^r$.*

Esercizio 8.21 * *Siano G e H due gruppi abeliani finiti. Se per ogni k c'è un numero uguale di elementi di periodo k in G ed H, allora G ed H sono isomorfi.*

9 Automorfismi di un gruppo

Sia G un gruppo. Un isomorfismo $f : G \to G$ di G in se stesso si dice un *automorfismo* di G. Si vede facilmente che l'insieme $Aut(G)$ degli automorfismi di un gruppo G è un gruppo rispetto alla composizione di applicazioni. Infatti, la composizione di applicazioni è associativa, la mappa identica id_G è l'elemento neutro e l'applicazione inversa di un automorfismo è ancora un automorfismo. Tale gruppo si chiama *gruppo degli automorfismi* del gruppo G. Se f è un automorfismo di G, allora f preserva l'ordine degli elementi.

Lemma 9.1 *Sia G un gruppo, $f \in Aut(G)$ e $a \in G$. Allora*

a) $o(f(a)) = o(a)$*;*

b) se a *è generatore di* G*, allora anche* $f(a)$ *è un generatore di* G*.*

DIMOSTRAZIONE. a) Ovviamente, f induce un isomorfismo tra i sottogruppi ciclici $\langle a\rangle$ e $\langle f(a)\rangle$ di G. Di conseguenza $o(f(a)) = o(a)$.

b) Segue dal Lemma 6.3. □

Esempio 9.2 Sia $(G, \cdot)$ un gruppo abeliano. L'applicazione $f : G \to G$ definita da $f(x) = x^{-1}$ per ogni $x \in G$ è un automorfismo. In particolare, l'applicazione $x \mapsto -x$ nel gruppo $\mathbb{Z}$ è un automorfismo, che denoteremo anche con $-id_{\mathbb{Z}}$.

Vediamo adesso che $Aut(\mathbb{Z}) = \{id_{\mathbb{Z}}, -id_{\mathbb{Z}}\}$. Infatti, sia $f \in Aut(\mathbb{Z})$ e $a = f(1)$. Allora $f(n) = f(n \cdot 1) = nf(1) = na$. Quindi, il sottogruppo $f(\mathbb{Z})$ coincide con il sottogruppo $a\mathbb{Z}$ di tutti i multipli di a. Poiché f è suriettiva, si ha $f(\mathbb{Z}) = \mathbb{Z}$, quindi $a\mathbb{Z} = \mathbb{Z}$, cioè a è un generatore di $\mathbb{Z}$. Questo è possibile se e solo se $a = \pm 1$. Se $a = 1$ abbiamo $f = id_{\mathbb{Z}}$, se $a = -1$, abbiamo $f = -id_{\mathbb{Z}}$.

Abbiamo dimostrato nell'esercizio 5.4 che per un gruppo G l'applicazione $\varphi_a : G \to G$ definita da $\varphi_a(x) = a^{-1}xa$ è un isomorfismo per ogni $a \in G$. L'automorfismo φ_a si dice *automorfismo interno* (spesso anche *coniugio* per l'elemento a, si veda anche la definizione 5.3). Si denoti con *Inn(G)* l'insieme $\{\varphi_a : a \in G\}$ degli automorfismi interni di un gruppo G.

Lemma 9.3 *Sia* G *un gruppo. Allora*

$$Inn(G) \cong \frac{G}{Z(G)}.$$

DIMOSTRAZIONE. Definiamo la seguente applicazione $F : G \to Aut(G)$ tramite $F(a) = \varphi_{a^{-1}}$. Dimostriamo che F è un omomorfismo, cioè per $a, b \in G$ si ha $F(ab) = F(a) \circ F(b)$, cioè $\varphi_{(ab)^{-1}} = \varphi_{a^{-1}} \circ \varphi_{b^{-1}}$. Infatti

$$\varphi_{(ab)^{-1}}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = \varphi_{a^{-1}}(b^{-1}xb) = \varphi_{a^{-1}}(\varphi_{b^{-1}}(x)) = (\varphi_{a^{-1}} \circ \varphi_{b^{-1}})(x).$$

L'immagine di F è per costruzione $Inn(G)$. Vediamo qual è il nucleo di F: $\ker(F) = \{a \in G : \varphi_{a^{-1}} = id_G\}$, cioè $\varphi_{a^{-1}}(x) = axa^{-1} = x$ per ogni $x \in G$. Allora a è un elemento centrale e quindi $\ker(F)$ è il centro di G. Applicando il primo Teorema di omomorfismo, si ottiene

$$\frac{G}{\ker(F)} \cong Im(F) \quad \Longrightarrow \quad \frac{G}{Z(G)} \cong Inn(G). \square$$

9.1 Automorfismi di $\mathbb{Z}_m$

Denotiamo con $U(\mathbb{Z}_m)$ l'insieme delle classi $\{[k]_m : \text{ con } (k, m) = 1\}$ in $\mathbb{Z}_m$. Dalla definizione della funzione $\varphi(m)$, sappiamo che $U(\mathbb{Z}_m)$ ha cardinalità $\varphi(m)$. Poiché il prodotto di due numeri n e k entrambi coprimi con m è sempre coprimo con m, il sottoinsieme $U(\mathbb{Z}_m)$ di $\mathbb{Z}_m$ è chiuso rispetto alla moltiplicazione e $[1]_m$ risulta il suo elemento neutro. Inoltre, per ogni a coprimo con m la congruenza $ax \equiv_m 1$ ha una soluzione che fornisce l'elemento inverso di $[a]_m$ in $U(\mathbb{Z}_m)$. In questo modo, $(U(\mathbb{Z}_m), \cdot)$ risulta un gruppo di cardinalità $\varphi(m)$.

Esempio 9.4 Descriviamo il gruppo $G = (U(\mathbb{Z}_8), \cdot)$. Poiché $\varphi(8) = 4$, G ha quattro elementi, più precisamente $G = \{[1]_8, [3]_8, [5]_8, [7]_8\}$. Ovviamente $[3]_8^2 = [5]_8^2 = [7]_8^2 = [1]_8$. Pertanto $o([3]_8) = o([5]_8) = o([7]_8) = 2$. Quindi i sottogruppi $H = \langle[3]_8\rangle$ e $K = \langle[5]_8\rangle$ hanno entrambi due elementi e $H \cap K = \{[1]_8\}$. Inoltre, il sottogruppo HK di G contiene propriamente H, quindi $d = |HK| > 2$ e divide $4 = |G|$. Quindi $d = 4$ e $HK = G$. Ora il Teorema 7.2 implica $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, essendo $H \cong K \cong \mathbb{Z}_2$.

Questa descrizione produce esplicitamente i sottogruppi H e K per i quali risulta $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Per concludere che $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, possiamo applicare direttamente il Teorema di Frobenius-Stickelberger e notare che essendo $|G| = 4$ abbiamo $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ o $G \cong \mathbb{Z}_4$. Ora $o([3]_8) = o([5]_8) = o([7]_8) = 2$ implica $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ perché G non ha elementi di ordine 4.

Teorema 9.5 *Sia $m > 1$ un numero intero. Allora $Aut(\mathbb{Z}_m) \cong (U(\mathbb{Z}_m), \cdot)$.*

DIMOSTRAZIONE. L'elemento $[1]_m$ è un generatore del gruppo ciclico $\mathbb{Z}_m = G$, cioè, $G = \langle [1]_m \rangle$. Allora ogni elemento di $\mathbb{Z}_m$ è del tipo $k[1]_m$ con $k \in \mathbb{Z}$. Sia $f \in Aut(\mathbb{Z}_m)$. Posto $a = f([1]_m)$, avremo quindi $f(s[1]_m) = sa$ per ogni $s \in \mathbb{Z}$. In altre parole, $a = f([1]_m)$ determina univocamente f. Sia $a = k[1]_m$, con $0 \leq k < m$. Poiché $f([1]_m)$ è un generatore di $\mathbb{Z}_m$ (vedi 6.3), si ha $o(a) = m$ e quindi $(k, m) = 1$. Poniamo $\Phi(f) = f([1]_m)$. Abbiamo così definito un'applicazione $\Phi : Aut(\mathbb{Z}_m) \to U(\mathbb{Z}_m)$. Per vedere che Φ è iniettiva supponiamo di avere $\Phi(f) = \Phi(g)$ per $f, g \in Aut(\mathbb{Z}_m)$. Allora $f = g$ poiché $f([1]_m) = g([1]_m)$ determina univocamente f e g.

Per vedere che Φ è suriettiva definiamo per ogni intero n un'applicazione Ψ_n da $\mathbb{Z}_m$ in sè con $\Psi_n([k]_m) = [nk]_m = n[k]_m$ per ogni $[k]_m \in \mathbb{Z}_m$. Si vede facilmente che Ψ_n è un omomorfismo da $\mathbb{Z}_m$ in se stesso. Inoltre, $\Psi_n = \Psi_{n'}$ se $n \equiv_m n'$. Quindi, Ψ_n dipende solo dalla classe laterale $n + m\mathbb{Z} = [n]_m$ di n modulo m. Poniamo intanto $\Psi([n]_m) = \Psi_n$. Se $(n, m) = 1$, allora Ψ_n è iniettiva (poiché $nt \equiv_m 0$ implica $t \equiv_m 0$ per ogni $t \in \mathbb{Z}$). Essendo $\mathbb{Z}_m$ finito, Ψ_n è un automorfismo per ogni n coprimo con m. Possiamo quindi parlare di un'applicazione $\Psi : U(\mathbb{Z}_m) \to Aut(G)$. Per la definizione di Ψ, si ha $f = \Psi(\Phi(f))$ per ogni $f \in Aut(\mathbb{Z}_m)$. Inoltre, per ogni $[n]_m \in U(\mathbb{Z}_m)$ si ha $\Psi([n]_m)([1]_m) = [n]_m$, cioè $\Phi(\Psi([n]_m) = [n]_m$. Questo dimostra che $\Phi : Aut(\mathbb{Z}_m) \to U(\mathbb{Z}_m)$ è una biiezione con inversa Ψ.

Adesso dimostriamo che Φ è un isomorfismo. Per $f, g \in Aut(\mathbb{Z}_m)$ con $f([1]_m) = [n]_m$ e $g([1]_m) = [k]_m$ si ha

$$\Phi(f \circ g) = (f \circ g)([1]_m) = f(g([1]_m)) = f([k]_m) =$$

$$f(k[1]_m) = kf([1]_m) = k[n]_m = [kn]_m = [k]_m[n]_m = \Phi(f)\Phi(g). \square$$

9.2 Esercizi sugli automorfismi

Esercizio 9.6 *Si dimostri che i gruppi $(U(\mathbb{Z}_3), \cdot)$, $(U(\mathbb{Z}_5), \cdot)$, $(U(\mathbb{Z}_7), \cdot)$, $(U(\mathbb{Z}_{11}), \cdot)$, $(U(\mathbb{Z}_{13}), \cdot)$, $(U(\mathbb{Z}_{17}), \cdot)$ e $(U(\mathbb{Z}_{19}), \cdot)$ sono ciclici.*

Esercizio 9.7 *Descrivere il gruppo $G = (U(\mathbb{Z}_{20}), \cdot)$.*

Esercizio 9.8 *Sia A un gruppo non identico e sia $\tau : A \to A$, l'applicazione definita da $\tau(a) = a^{-1}$. Si dimostri che*

i) τ è biiettiva;

ii) l'applicazione τ è un omomorfismo (quindi un automorfismo) di gruppi se e solo se A è abeliano;

iii) se ogni elemento non identico di A ha ordine 2, allora τ è l'identità, altrimenti τ ha ordine 2 quale elemento del gruppo $Aut(A)$.

Esercizio 9.9 *(1) Sia $f \in Aut(\mathbb{Q}, +)$. Allora esiste un $r \in \mathbb{Q}$, $r \neq 0$, tale che $f(x) = rx$ per ogni $x \in \mathbb{Q}$.*

(2) Dimostrare che $Aut(\mathbb{Q}, +) \cong (\mathbb{Q}^*, \cdot)$.

(3) Dimostrare che $Aut(\mathbb{Q} \times \mathbb{Q}, +) \cong GL_2(\mathbb{Q})$.

(4) Dimostrare che $Aut(\mathbb{Q}^n, +) \cong GL_n(\mathbb{Q})$.

Esercizio 9.10 *Sia G un gruppo e sia X un insieme di generatori di G.*

(a) Per ogni omomorfismo suriettivo $f : G \to H$ l'insieme $f(X)$ genera il gruppo H.

(b) Se per una coppia di omomorfismi $f, g : G \to H$ si ha $f(x) = g(x)$ per ogni $x \in X$, allora $f = g$.

Esercizio 9.11 *Siano τ_1, τ_2 e τ_3 le tre trasposizioni nel gruppo simmetrico S_3 e siano σ_1 e σ_2 i due cicli di lunghezza tre.*

(a) Dimostrare che ci sono sei automorfismi interni di S_3 e:

(a_1) ogni automorfismo interno φ_{τ_i} fissa la trasposizione τ_i e scambia tra loro sia le altre due trasposizioni, sia i cicli σ_1, σ_2.

(a_2) ogni automorfismo interno φ_{σ_i} fissa entrambi i cicli σ_1, σ_2 e scambia tra loro le trasposizioni τ_i senza lasciarne una fissa.

(b^*)Dimostrare che ogni automorfismo di S_3 è interno.

Vediamo ora un altro esempio di automorfismo interno del gruppo $GL_2(\mathbb{R})$.

Esercizio 9.12 *In $G = GL_2(\mathbb{R})$, si consideri il coniugio tramite la matrice $\eta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$. Si calcoli l'immagine tramite φ_η dei seguenti sottogruppi:*

i) il sottogruppo delle matrici triangolari superiori $T_2^+ = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$;

ii) il sottogruppo delle matrici triangolari inferiori $T_2^- = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$;

iii) il sottogruppo delle matrici diagonali $D_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in \mathbb{R}, ac \neq 0 \right\}$.

Esercizio 9.13 *Descrivere $Aut(\mathbb{Z}_3)$, $Aut(\mathbb{Z}_5)$, $Aut(\mathbb{Z}_7)$, $Aut(\mathbb{Z}_8)$, $Aut(\mathbb{Z}_{11})$, $Aut(\mathbb{Z}_{13})$, $Aut(\mathbb{Z}_{17})$, $Aut(\mathbb{Z}_{19})$ e $Aut(\mathbb{Z}_{20})$.*

Esercizio 9.14 *Descrivere $Aut(\mathbb{Z}_{22})$, $Aut(\mathbb{Z}_{33})$, $Aut(\mathbb{Z}_{35})$, $Aut(\mathbb{Z}_{42})$, $Aut(\mathbb{Z}_{44})$, $Aut(\mathbb{Z}_{52})$.*

Esercizio 9.15 *Trovare i generatori del gruppo $Aut(\mathbb{Z}_{29})$.*

Esercizio 9.16 *Si descriva il gruppo $Aut(\mathbb{Z}_{21})$.*

Esercizio 9.17 *Si descriva il gruppo $G = Aut(\mathbb{Z}_{36})$ degli automorfismi del gruppo $\mathbb{Z}_{36}$. Si determini se G è ciclico.*

Esercizio 9.18 *Sia $n \geq 3$ un intero. Dimostrare che il numero $|Aut(\mathbb{Z}_n)|$ è pari.*

Esercizio 9.19 *Sia $f : G \to H$ un omomorfismo di gruppi abeliani tali che $|G| = m$ e $|H| = n$ sono coprimi. Allora f è banale, cioè* $\ker f = G$.

Esercizio 9.20 *Siano m ed n interi positivi coprimi. Allora ogni omomorfismo $f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ ha la forma $f = (f_1, f_2)$, dove $f_1 : \mathbb{Z}_m \to \mathbb{Z}_m$ e $f_2 : \mathbb{Z}_n \to \mathbb{Z}_n$ sono opportuni omomorfismi (cf. Esercizio 7.20).*

Esercizio 9.21 *Sia $G = \mathbb{Z}_m \times \mathbb{Z}_n$, con $(m, n) = 1$. Allora $Aut(G) \cong Aut(\mathbb{Z}_m) \times Aut(\mathbb{Z}_n)$.*

Esercizio 9.22 *Descrivere tutti gli automorfismi dei gruppi $\mathbb{Z}_{68}$ e $\mathbb{Z}_{210}$.*

Esercizio 9.23 *Descrivere $Aut(\mathbb{Z}_{24})$, $Aut(\mathbb{Z}_{60})$ e $Aut(\mathbb{Z}_{72})$.*

Esercizio 9.24 *Siano m e n interi positivi coprimi e siano G e H gruppi abeliani con $|G| = m$ e $|H| = n$. Allora ogni automorfismo $f : G \times H \to G \times H$ ha la forma $f = (f_1, f_2)$, dove $f_1 \in Aut(G)$ e $f_2 \in Aut(H)$.*

Esercizio 9.25 *Sia p un numero primo. Dimostrare che $Aut(\mathbb{Z}_p \times \mathbb{Z}_p) \cong GL_2(\mathbb{F}_p)$.*

10 I gruppi non abeliani: un primo approccio

In questo capitolo ci proponiamo di introdurre lo studio dei gruppi non abeliani. Rivolgeremo il nostro studio quasi prevalentemente ai gruppi non abeliani finiti.

Come dimostrato nel Capitolo 8, tutti i gruppi di ordine minore o uguale a 5 sono abeliani. Quindi per trovare un gruppo non abeliano dobbiamo supporre $|G| \geq 6$. Conosciamo già un gruppo non abeliano di ordine 6, il gruppo simmetrico S_3. Abbiamo dimostrato nell'esempio 7.6, che per S_3 non vale il Teorema di struttura dei gruppi abeliani finiti 7.14.

Proviamo che S_3 è l'unico gruppo non abeliano di ordine 6.

Lemma 10.1 *Sia G un gruppo non abeliano di ordine 6, allora $G \cong S_3$.*

Dimostrazione. Supponiamo che G non sia abeliano e che $1 \neq a$ sia un elemento di G. Allora $o(a)$ divide 6, ma non può essere 6 perché altrimenti G risulterebbe ciclico e quindi abeliano. Pertanto $o(a) = 2$ o 3. Se $o(a) = 2$ poniamo $H = \langle a \rangle$. Per il Lemma 8.2, G deve avere almeno un elemento b di ordine 3. Poniamo $K = \langle b \rangle$. Se $x \in G$ e $x \notin K$, il sottogruppo $L = \langle x \rangle$ non può avere ordine 3. Infatti se $|L| = 3$, allora K ed L sarebbero sottogruppi normali (avendo indice 2; vedi Esercizio 4.36) con $K \cap L = \{1\}$ e quindi il sottogruppo KL di G sarebbe isomorfo a $K \times L \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, assurdo. Quindi $o(x) = 2$. G risulta allora generato da a e b, e quindi $ab \neq ba$, essendo G non abeliano. Poiché

$aba^{-1} = aba \in K \triangleleft G$ ma non può coincidere con b, concludiamo che $aba = b^{-1}$ ha ordine 3. Adesso si può definire un omomorfismo $f : G \to S_3$ che manda a in (12), b in (123), $b^2 = b^{-1}$ in (132), ab in $(12)(123) = (23)$, ecc. $\square$

Abbiamo così classificato tutti i gruppi di ordine minore o uguale a 7. Di ordine 8 ci sono due gruppi non abeliani: uno è il gruppo dei quaternioni, l'altro verrà introdotto nell'Esercizio 11.1. È relativamente facile descrivere tutti i gruppi non abeliani di ordine ≤ 15.

La conseguenza più "pesante" del fatto che il gruppo non sia abeliano, non è tanto che ci siano elementi che non commutano, quanto che non tutti i sottogruppi siano normali.

Iniziamo quindi lo studio dei gruppi non abeliani, cercando innanzitutto di capire quali sottogruppi sono normali. Abbiamo già visto che ad esempio il centro di un gruppo è un sottogruppo normale (vedi Lemma 4.11).

Nel Capitolo 3 avevamo inoltre introdotto la definizione di *commutatore* di due elementi a e b di un gruppo (vedi Definizione 3.2) $[a, b] = a^{-1}b^{-1}ab$.

Consideriamo ora il sottogruppo generato da tutti i commutatori di un gruppo. Anche questo sottogruppo risulta essere normale:

Lemma 10.2 *Sia $G' = \langle [a, b] : a, b \in G \rangle$ il sottogruppo generato dai commutatori di G. Allora G' è un sottogruppo normale.*

Dimostrazione. Utilizziamo il Lemma 4.3 per dimostrare che G' è normale. E' sufficiente verificare che se x è un generatore di G' e $g \in G$, allora $g^{-1}xg \in G'$. Sia $x = [a, b]$ e $g \in G$, allora:

$$g^{-1}xg = g^{-1}[a, b]g = g^{-1}(a^{-1}b^{-1}ab)g = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = (a^g)^{-1}(b^g)^{-1}a^g b^g = [a^g, b^g],$$

che appartiene a G'. Poiché vale per i generatori di G', vale anche per elementi arbitrari di G'. $\square$

Il sottogruppo normale G' di G definito nel Lemma 10.2 si chiama il *sottogruppo derivato di G*, o più semplicemente il *derivato* di G. Verifichiamo che il quoziente G/G' è abeliano e anzi dimostriamo che G' è il più piccolo sottogruppo con questa proprietà.

Lemma 10.3 *Sia G' il sottogruppo derivato di un gruppo G. Allora*
i) G/G' è abeliano;
ii) se $N \triangleleft G$ e G/N è abeliano, allora $N \geq G'$.

Dimostrazione. *i)* Siano aG', bG' due elementi di G/G'. Allora

$$aG'bG' = abG' = baG' = bG'aG' \quad \Leftrightarrow \quad a^{-1}b^{-1}ab \in G'.$$

Dalla definizione di G' si ha che $a^{-1}b^{-1}ab \in G'$ per ogni $a, b \in G$, da cui segue che G/G' è abeliano.

ii) Supponiamo che G/N sia abeliano, allora per ogni $a, b \in G$, si ha $aNbN = abN = baN = bNaN$, ma questo accade se e solo se $a^{-1}b^{-1}ab \in N$. Allora $[a, b] \in N$, per ogni $a, b \in G$, cioè $G' \leq N$. $\square$

10.1 Centralizzanti, equazione delle classi e Lemma di Cauchy

Abbiamo visto la definizione di elemento centrale. Può accadere però che in un gruppo non ci siano elementi centrali non banali (vedi ad esempio l'esercizio 4.35). Diamo la definizione di centralizzante di un sottoinsieme X di un gruppo G, che è una richiesta più debole rispetto a quella di essere centrale.

Definizione 10.4 Un elemento g di G *centralizza* X se $gx = xg$ per ogni $x \in X$.

L'insieme $C_G(X) = \{g \in G : gx = xg \ \forall x \in X\}$ degli elementi di G che centralizzano X si chiama il *centralizzante di X in G*.

Per non appesantire la notazione, scriveremo $C_G(x)$ per indicare il centralizzante dell'insieme $\{x\}$. Calcoliamo il centralizzante di alcuni elementi.

Esempio 10.5 Consideriamo l'elemento (12) di $G = S_3$. Allora $C_{S_3}((12)) = \langle (12) \rangle$. Se invece consideriamo (12) come elemento di S_4, avremo $C_{S_4}((12)) = \langle (12), (34) \rangle$

Dato un gruppo G, possiamo definire la seguente relazione $x \sim_G y$ se e solo se esiste $g \in G$ tale che $y = x^g$. Si dimostra facilmente che $\sim_G$ è una relazione di equivalenza (vedi l'esercizio 11.19). Possiamo allora considerare le classi di equivalenza rispetto a $\sim_G$.

Definizione 10.6 Sia G un gruppo e x un elemento di G. La *classe di coniugio* di x è la classe di equivalenza di x rispetto a $\sim_G$, cioè l'insieme dei coniugati di x in G. Si denota con $x^G = \{x^g : g \in G\}$.

Ovviamente, $1^G = \{1\}$. Più in generale, la classe di coniugio di un elemento x di un gruppo G coincide con il singoletto $\{x\}$ precisamente quando x è un elemento centrale. Infatti $x^G = \{x\}$ se e solo se $x^g = x$ per ogni $g \in G$, cioè x commuta con tutti gli elementi di G.

Supponiamo ora che G sia un gruppo finito. Siano $x_1, ..., x_t$ i rappresentanti delle classi di coniugio di G di elementi non centrali, cioè $|x_i^G| > 1$ per ogni $i = 1, ..., t$. Le classi di equivalenza costituiscono una partizione e, se si raggruppano tutte le classi di equivalenza che contengono un solo elemento, allora $\{x \in G : |x^G| = 1\} = Z(G)$. Otteniamo quindi

$$G \ = Z(G) \ \cup \ x_1^G \ \cup \ x_2^G \ \cup ... \cup \ x_t^G,$$

ove l'unione è disgiunta. Allora calcolando la cardinalità di questi insiemi segue l'*equazione delle classi*:

$$|G| = \ |Z(G)| \ + \ \sum_{i=1}^{t} |x_i^G|. \qquad (*)$$

La prossima proposizione mette in relazione il numero dei coniugati di un elemento con il suo centralizzante.

Proposizione 10.7 *Sia G un gruppo e X un sottoinsieme di G. Allora:*
(a) $C_G(X)$ è un sottogruppo di G che contiene il centro di G,
(b) per ogni sottogruppo H di G si ha $C_G(H) \cap H = Z(H)$, in particolare $C_G(G) = Z(G)$,
(c) se G è finito, allora il numero dei coniugati di un elemento $x \in G$ coincide con l'indice del centralizzante di x in G.

Dimostrazione. *(a)* Siano $g_1, g_2 \in C_G(X)$ e sia $x \in X$. Allora $g_1 x = x g_1$ e $g_2 x = x g_2$ implicano

$$x g_1^{-1} = g_1^{-1} x \quad \text{e} \quad (g_1 g_2)x = g_1(g_2 x) = (g_1 x) g_2 = x(g_1 g_2).$$

Quindi $C_G(X)$ è un sottogruppo e contiene il centro di G perché ogni elemento del centro commuta in particolare con gli elementi di X.
(b) $C_G(H) \cap H = \{g \in H : gh = hg \ \ \forall h \in H\} = Z(H)$.
(c) Supponiamo ora che G sia finito. Sia x^G la classe di coniugio di x in G. Sia $C = C_G(x)$ e $\mathcal{C}$ l'insieme delle classi laterali destre del sottogruppo C in G. Definiamo $f : \mathcal{C} \to x^G$ con la posizione $f(Cg) = x^g$. Dimostriamo che f è ben definita e che è iniettiva:

$$Cg = Ch \Leftrightarrow gh^{-1} \in C \Leftrightarrow (gh^{-1})x = x(gh^{-1}) \Leftrightarrow g^{-1}xg = h^{-1}xh \Leftrightarrow f(g) = f(h).$$

Dalla definizione di x^G, segue immediatamente che f è suriettiva. Pertanto f è una biiezione e quindi gli insiemi $\mathcal{C}$ e x^G hanno la stessa cardinalità. Si conclude osservando che $|\mathcal{C}| = [G : C_G(x)]$. □

Abbiamo dimostrato il Lemma 8.5 di Cauchy nel caso dei gruppi abeliani finiti. Siamo ora in grado di provarlo per un qualsiasi gruppo finito G.

Lemma 10.8 (Lemma di Cauchy) *Sia p un primo che divide l'ordine di G. Allora esiste in G un elemento di ordine p.*

Dimostrazione. Sia $|G| = pm$, dimostriamo il lemma per induzione su m. Per $m = 1$, il Lemma è ovvio, anzi ogni elemento $\neq 1$ di G ha ordine proprio p.

Supponiamo $m > 1$. Se esiste $H < G$, tale che p divide $|H|$, per induzione esiste un elemento x in H tale che $o(x) = p$ e tale x appartiene anche a G. Supponiamo che p non divida l'ordine di alcun sottogruppo di G. In particolare se $a \notin Z(G)$, si ha $C_G(a) < G$ e p divide $[G : C_G(a)]$ e quindi p divide $|a^G|$ da (c) della Proposizione 10.7. Allora dall'equazione delle classi ricaviamo che $|G| \equiv_p |Z(G)|$ e poiché $|G| \equiv_p 0$, e $|Z(G)| \geq 1$, si conclude che p divide $|Z(G)|$. Per l'ipotesi fatta sui sottogruppi propri di G, si conclude che $G = Z(G)$, cioè G è abeliano. Per il lemma di Cauchy 8.5 dimostrato nel caso abeliano, possiamo concludere. □

Diamo ora una definizione per indicare i gruppi in cui ogni elemento ha ordine una potenza di un primo p.

Definizione 10.9 Sia p un primo fissato. Un gruppo G in cui ogni elemento ha ordine p^n, per qualche $n \in \mathbb{N}$, si dice un *p-gruppo.*

Grazie al Lemma di Cauchy possiamo ora trovare l'ordine di un p-gruppo finito.

Lemma 10.10 *Sia G un p-gruppo finito. Allora $|G| = p^m$ per qualche m in $\mathbb{N}$.*

DIMOSTRAZIONE. Per ipotesi sappiamo che ogni elemento di G ha ordine una potenza di p. Supponiamo per assurdo che esista un primo $q \neq p$ tale che q divide l'ordine di G. Allora, per il Lemma di Cauchy, esiste un elemento di ordine q, contraddicendo l'ipotesi. □

Un'altra importante conseguenza dell'equazione delle classi, nel caso dei p-gruppi, è la seguente.

Lemma 10.11 *Sia G un p-gruppo finito, p un primo. Allora il centro di G non è banale.*

DIMOSTRAZIONE. Consideriamo l'equazione delle classi applicata a G. Siano $x_1, \ldots, x_t$ i rappresentanti delle classi di coniugio di G di elementi non centrali. Cioè $|x_i^G| > 1$ e $G = Z(G) \cup x_1^G \cup x_2^G \cup ... \cup x_t^G$. Allora per il Lemma 10.7, $|x_i^G| = [G : C_G(x_i)] > 1$ e per il Teorema di Lagrange si ha che $[G : C_G(x_i)]$ divide l'ordine di G per $i = 1, 2, \ldots, t$. Allora per il Lemma 10.10, si ha $|x_i^G| = [G : C_G(x_i)] \equiv_p 0$ per ogni $i = 1, 2, \ldots, t$. Segue

$$0 \equiv_p |G| = |Z(G)| + |x_1^G| + |x_2^G| + \ldots + |x_t^G| \equiv_p |Z(G)|.$$

Quindi p divide $|Z(G)|$ e poiché $Z(G)$ non è vuoto perché contiene almeno l'elemento identico, segue che $|Z(G)| \geq p$. □

Concludiamo questo paragrafo con una conseguenza del Lemma 10.11 appena visto e del seguente Lemma 10.12.

Lemma 10.12 *Sia G un gruppo e $Z(G)$ il centro di G. Se $G/Z(G)$ è ciclico, allora G è abeliano.*

DIMOSTRAZIONE. Supponiamo che G non sia abeliano, allora $|G/Z(G)| > 1$. Poichè $G/Z(G)$ è ciclico, esiste $g \in G$ tale che $G/Z(G) = \langle \overline{g} \rangle$, con $\overline{g} = gZ(G)$. Allora per ogni $x, y \in G$, si ha che $xZ(G) = \overline{g}^i$ e $yZ(G) = \overline{g}^j$, per qualche $i, j \in \mathbb{N}$. Da questo si ricava che $x = z_1 g^i$ e $y = z_2 g^j$ con $z_1, z_2 \in Z(G)$ e quindi

$$xy = z_1 g^i z_2 g^j = z_1 z_2 g^i g^j = z_2 z_1 g^j g^i = z_2 g^j z_1 g^i = yx,$$

che contraddice l'ipotesi che G non sia abeliano. □

Proposizione 10.1 *Sia G un gruppo di ordine p^2. Allora G è abeliano.*

DIMOSTRAZIONE. Poiché G è un p-gruppo, si ha $\{1\} \neq Z(G)$, per il Lemma 10.11. Per il Teorema di Lagrange allora $|Z(G)| = p$ o p^2. Se $Z(G) = p^2$, $Z(G) = G$ e G è abeliano. Se fosse $|Z(G)| = p$, allora $G/Z(G)$ avrebbe ordine p e pertanto sarebbe un gruppo ciclico di ordine p. Per il Lemma 10.12 questo non può accadere. □

10.2 Teorema di Cayley

In questo paragrafo vogliamo dimostrare quanto affermato all'inizio del paragrafo 2.2 e cioè che ogni gruppo può essere visto come sottogruppo di un gruppo di permutazioni. Questo significa che dato un qualsiasi gruppo G esiste un omomorfismo iniettivo da G nel gruppo S_X di tutte le permutazioni di un insieme X.

Teorema 10.13 (Teorema di Cayley) *Sia G un gruppo. Allora G è (isomorfo ad) un sottogruppo di un gruppo di permutazioni.*

DIMOSTRAZIONE. Sia S_G il gruppo delle permutazioni sull'insieme supporto di G. Per ogni $g \in G$, definiamo $\mu_g : G \to G$ con $\mu_g(x) = gx$. Dimostriamo che μ_g è una biiezione per ogni $g \in G$. Infatti $\mu_g(x) = \mu_g(y)$ se e solo se $gx = gy$, da cui segue per la legge di cancellazione che $x = y$. Inoltre se $y \in G$, poniamo $x = g^{-1}y$, da cui segue che $\mu_g(x) = gx = y$. Allora μ_g è biiettiva ed è pertanto un elemento di S_G. Sia ora $\mu : G \to S_G$ definita da $\mu(g) := \mu_g$. Dimostriamo che μ è un omomorfismo iniettivo di gruppi. Siano $g_1, g_2 \in G$, allora $\mu(g_1 g_2) = \mu_{g_1 g_2}$. Per far vedere che coincide con $\mu_{g_1} \circ \mu_{g_2}$,

dimostriamo che queste due permutazioni coincidono su ogni elemento dell'insieme su cui sono definite. Sia dunque $x \in G$

$$(\mu_{g_1} \circ \mu_{g_2})(x) = \mu_{g_1}(\mu_{g_2}(x)) = \mu_{g_1}(g_2 x) = g_1(g_2 x) = (g_1 g_2)x = \mu_{g_1 g_2}(x).$$

Allora μ è un omomorfismo. Per controllare che è iniettivo è pertanto sufficiente calcolare $\ker(\mu) = \{g \in G : \mu(g) = id\}$. Allora $g \in \ker(\mu)$ se e solo se $\mu_g = id$, cioè $\mu_g(x) = gx = x$ per ogni $x \in G$, in particolare per $x = 1$ e quindi $g = 1$. Concludiamo che G è isomorfo a $\mu(G)$, sottogruppo di S_G. □

10.3 Sulla normalità dei sottogruppi

In quest'ultimo paragrafo consideriamo alcuni sottogruppi di un gruppo G, collegati ad un sottogruppo fissato H. Innanzitutto osserviamo che se H è un sottogruppo di G, in generale H non è normale in G, ma potrebbe essere normale in un altro sottogruppo più piccolo di G. Per esempio H risulta sempre normale in H stesso. Consideriamo pertanto il massimo di questi sottogruppi.

Definizione 10.14 Sia G un gruppo e X un sottoinsieme di G. Un elemento g *normalizza* X se $X^g = X$. L'insieme $N_G(X) = \{g \in G : X^g = X\}$ degli elementi di G che normalizzano X si chiama il *normalizzante di* X *in* G.

Come per il centralizzante di un sottoinsieme di G, esaminiamo alcune semplici proprietà del normalizzante.

Lemma 10.15 *Siano G un gruppo e H un sottogruppo di G. Allora*
a) $N_G(H)$ è un sottogruppo di G.
b) H è un sottogruppo normale di $N_G(H)$.
c) $N_G(H)$ è il più grande sottogruppo di G in cui H è normale.

Dimostrazione. a) Osserviamo che se $xH = Hx$, moltiplicando a destra e a sinistra per x^{-1} otteniamo $Hx^{-1} = x^{-1}H$, da cui si ricava immediatamente che $x^{-1} \in N_G(H)$. Se ora $x, y \in N_G(H)$, allora $(xy)H = x(yH) = x(Hy) = (xH)y = (Hx)y = H(xy)$. Quindi $xy \in N_G(H)$.

b) Se $h \in H$, allora per la proprietà di chiusura del sottogruppo si ha che $hH = Hh$, pertanto $h \in N_G(H)$, cioè $H \leq N_G(H)$. Il fatto che H sia normale in $N_G(H)$ viene direttamente dalla definizione.

c) Sia ora K un sottogruppo di G tale che H è normale in K. Vogliamo dimostrare che $K \leq N_G(H)$. Sia dunque $k \in K$, poiché H è normale in K, si avrà $kH = Hk$, cioè $k \in N_G(H)$, per la definizione di normalizzante. □

Il seguente lemma permette di calcolare il numero di coniugati di un sottogruppo H tramite il normalizzante di H.

Lemma 10.16 *Sia H un sottogruppo del gruppo G. Allora il numero dei coniugati di H coincide con l'indice del normalizzante di H in G.*

Dimostrazione. Vogliamo dimostrare che $|\{H^g : g \in G\}| = [G : N_G(H)]$ e, ricordando che vale $[G : N_G(H)] = |\{gN_G(H) : g \in G\}|$, costruiamo un biiezione tra questi due insiemi. Sia $N = N_G(H)$ e

$$f : \{H^g : g \in G\} \to \{gN : g \in G\}$$

definita da $f(H^g) = gN$. Dimostriamo che f è ben definita e che è iniettiva:

$$gN = xN \Leftrightarrow x^{-1}g \in N \Leftrightarrow (x^{-1}g)H(g^{-1}x) = H \Leftrightarrow gHg^{-1} = xHx^{-1} \Leftrightarrow f(g) = f(h).$$

Controlliamo infine che f è suriettiva. Infatti $gN_G(H) = f(H^g)$ per ogni $g \in G$. □

Sia G un gruppo e H un sottogruppo. Abbiamo introdotto $N_G(H)$ come il massimo sottogruppo di G in cui H è normale. Ma in generale $N_G(H)$ non sarà normale in G. Vogliamo ora introdurre degli altri sottogruppi legati ad H, che sono normali in G.

Definizione 10.17 Si dice *cuore* di H in G e si denota con H_G il sottogruppo generato dai sottogruppi normali di G contenuti in H.

Si dice *chiusura normale* di H in G e si denota H^G l'intersezione dei sottogruppi normali che contengono H.

Osserviamo che grazie al Lemma 4.8, H_G risulta essere il più grande sottogruppo normale di G contenuto in H e H^G il più piccolo sottogruppo normale di G contenente H.

Possiamo caratterizzare questi due sottogruppi nel modo seguente.

Proposizione 10.18 *Sia G un gruppo e H un sottogruppo di G. Allora*

$$H_G = \bigcap_{x\in G} H^x \text{ e } H^G = \langle H^x : x \in G\rangle.$$

DIMOSTRAZIONE. Per il Lemma 4.8, H_G è normale e pertanto per ogni $x \in G$ si ha $H_G = H_G^x \leq H^x$ da cui segue che $H_G \leq \bigcap_{x\in G} H^x$. Viceversa sia $g \in G$ e $u \in \bigcap_{x\in G} H^x$. Dal fatto che $u \in (xg^{-1})^{-1}H(xg^{-1}) = gx^{-1}Hxg^{-1}$, segue che esiste $h \in H$ tale che $u = gx^{-1}hxg^{-1}$ e quindi $g^{-1}ug = x^{-1}hx$, quindi $g^{-1}ug \in \bigcap_{x\in G}(x^{-1}Hx)$: allora $\bigcap_{x\in G} H^x$ è un sottogruppo normale contenuto in H e quindi è contenuto in H_G.

Sia ora $x \in G$, allora $H^x \leq (H^G)^x \leq H^G$ perché H^G è normale per il Lemma 4.8. Pertanto $\langle H^x : x \in G\rangle \leq H^G$. Vediamo viceversa che $\langle H^x : x \in G\rangle$ è un sottogruppo normale che contiene H, da cui seguirà che $H^G \leq \langle H^x : x \in G\rangle$. Intanto per $a \in \langle H^x : x \in G\rangle$, si ha $a = a_1 \dots a_n$, con $a_i \in H^{x_i}$ per $i = 1, \dots, n$. Se $g \in G$, allora $a_i^g \in (H^{x_i})^g = g^{-1}x_i^{-1}Hx_ig = (x_ig)^{-1}H(x_ig)$. Pertanto

$$a^g = g^{-1}ag = (g^{-1}a_1g)(g^{-1}a_2g)\dots(g^{-1}a_ng) \in \langle H^x : x \in G\rangle.$$

Quindi per il Lemma 4.6, $\langle H^x : x \in G\rangle$ è normale e contiene H e quindi contiene H^G. □

Chiaramente H_G è contenuto in H e risulta $H_G = H$ se e solo se il sottogruppo H è normale. Si può provare che H_G contiene l'intersezione $H \cap Z(G)$ (vedi l' Esercizio 10.26) e ciò fornisce un limite *inferiore* per il cuore H_G.

Daremo alcuni esempi in cui l'uguaglianza $H \cap Z(G) = H_G$ vale. Affinché ciò accada, è sufficiente che sia verificata l'inclusione $\bigcap_{x\in G} H^x \leq Z(G)$. Nei casi concreti vedremo che bastano addirittura anche intersezioni di due o tre coniugati di H (vedi ad esempio l'Esercizio 11.33).

10.4 La semplicità di A_n

In questa sezione vogliamo dimostrare che i gruppi alterni A_n sono gruppi semplici non abeliani, per ogni $n \geq 5$. Dimostriamo dapprima una proposizione.

Proposizione 10.19 *Se $n \geq 3$, ogni elemento di A_n è prodotto di 3-cicli.*

DIMOSTRAZIONE. Se $\sigma = id$ è l'identità allora $\sigma = (123) \circ (123) \circ (123)$. Sia $\sigma \neq id$ un elemento di A_n: allora σ si può scrivere come prodotto di un numero pari di trasposizioni $\sigma = (a_{11}a_{12}) \circ (a_{21}a_{22}) \circ \dots \circ (a_{t1}a_{t2})$, ove $t = 2r$. Se si dimostra che ogni coppia di trasposizioni è il prodotto di 3-cicli, si conclude che ogni permutazione pari è il prodotto di 3-cicli. Sia dunque $(ab) \circ (cd)$ prodotto di 2 trasposizioni.

Se $\{a, b\} = \{c, d\}$, allora $(ab) \circ (cd) = id$ è prodotto di 3-cicli.

Se $\{a, b\} \cap \{c, d\} = \{b\}$, allora $(ab) \circ (bd) = (abd)$.

Se $\{a, b\} \cap \{c, d\} = \emptyset$, allora $(ab) \circ (cd) = (ab) \circ (bc) \circ (bc) \circ (cd) = (abc) \circ (bcd)$. □

In generale non è facile capire quando due elementi di un gruppo sono coniugati. Nel caso dei gruppi simmetrici però c'è un utile criterio per riconoscere quando due permutazioni sono coniugate.

Lemma 10.20 *Sia $(a_1a_2 \dots a_d)$ un ciclo in S_n e $\sigma \in S_n$. Allora il coniugato di $(a_1a_2 \dots a_d)$ tramite σ è l'elemento $(\sigma(a_1)\sigma(a_2) \dots \sigma(a_d))$.*

DIMOSTRAZIONE. Ricordando la definizione di ciclo come funzione biiettiva dell'insieme $\{1, 2, ..., n\}$ su se stesso, dimostriamo che l'azione di $(a_1 \dots a_d)^\sigma$ su $\{1, 2, ..., n\}$ coincide con l'azione di $(\sigma(a_1) \dots \sigma(a_d))$. Denotiamo con f il ciclo $(a_1a_2 \dots a_d)$. Poiché σ è una biiezione, esiste un unico $b_i \in \{1, 2, ..., n\}$ tale che $\sigma(b_i) = a_i$. Allora $f(\sigma(b_i)) = f(a_i) = a_{i+1}$ se $i = 1, 2, ...d - 1$ e $f(\sigma(b_d)) = f(a_d) = a_1$, da cui

$$(\sigma^{-1} \circ f \circ \sigma)(b_i) = \sigma^{-1}(f(\sigma(b_i))) = \sigma^{-1}(a_{i+1}) = b_{i+1} \text{ per } i = 1, 2, ..., d-1 \text{ e } (\sigma^{-1} \circ f \circ \sigma)(b_d) = b_1.$$

Da questo si ricava che $(\sigma^{-1} \circ f \circ \sigma)$ agisce sull'insieme $\{b_1, b_2, ..., b_d\}$ esattamente come il ciclo $(b_1, ..., b_d)$ $= (\sigma(a_1)\sigma(a_2) \dots \sigma(a_d))$. Infine dalla definizione di ciclo, risulta $f(\sigma(i)) = \sigma(i)$ se $\sigma(i) \notin supp(f) = \{a_1, a_2, ..., a_d\}$, cioè se $i \notin \sigma^{-1}(\{a_1, a_2, ..., a_d\}) = \{b_1, b_2, ..., b_d\}$. Allora per ogni $i \notin \{b_1, b_2, ..., b_d\}$, si ha

$$(\sigma^{-1} \circ f \circ \sigma)(i) = \sigma^{-1}(f(\sigma(i)) = \sigma^{-1}(\sigma(i)) = i.$$

Da quest'ultima uguaglianza, deduciamo che $\sigma^{-1} \circ f \circ \sigma = (\sigma(a_1)\sigma(a_2)\dots\sigma(a_d))$. $\square$

Come conseguenza del Lemma 10.20, si ha che la struttura della decomposizione in cicli disgiunti viene preservata dal coniugio. Infatti, se $\rho = (a_{11}a_{12}\dots a_{1d_1}) \circ (a_{21}a_{22}\dots a_{2d_2}) \circ \dots \circ (a_{n1}a_{n2}\dots a_{nd_n})$, si ha

$$\rho^\sigma = ((a_{11}a_{12}\dots a_{1d_1}) \circ (a_{21}a_{22}\dots a_{2d_2}) \circ \dots \circ (a_{n1}a_{n2}\dots a_{nd_n}))^\sigma =$$

$$= (a_{11}a_{12}\dots a_{1d_1})^\sigma \circ (a_{21}a_{22}\dots a_{2d_2})^\sigma \circ \dots \circ (a_{n1}a_{n2}\dots a_{nd_n})^\sigma =$$

$$= (\sigma(a_{11})\sigma(a_{12})\dots\sigma(a_{1d_1})) \circ (\sigma(a_{21})\sigma(a_{22})\dots\sigma(a_{2d_2})) \circ \dots \circ (\sigma(a_{n1})\sigma(a_{n2})\dots\sigma(a_{nd_n})).$$

D'altra parte, se ρ' è un'altra permutazione con decomposizione in prodotto di cicli disgiunti

$$\rho' = (b_{11}b_{12}\dots b_{1d_1}) \circ (b_{21}b_{22}\dots b_{2d_2}) \circ \dots \circ (b_{n1}a_{n2}\dots b_{nd_n})$$

possiamo facilmente definire una permutazione σ tale che $\sigma(a_{ij}) = b_{ij}$ per tutti i possibili i, j (l'azione di σ sul resto dell'insieme di indici è del tutto irrilevante). Allora è chiaro che $\rho' = \rho^\sigma$. Abbiamo così dimostrato la seguente:

Proposizione 10.21 *Due permutazioni sono coniugate se e solo se hanno la stessa struttura ciclica.*

Applicando la Proposizione 10.21 al caso particolare dei cicli di lunghezza d, come dimostrato già nel lemma 10.20 si ottiene che tutti i cicli della stessa lunghezza sono coniugati in S_n. In generale non è detto però che questo avvenga anche in A_n, come si vede dal seguente esempio:

Esempio 10.22 Siano $\sigma = (12345)$ e $\rho = (12435)$ due cicli di S_5. Allora, poiché sono cicli di lunghezza 5, sono permutazioni pari e appartengono entrambi ad A_5. Per il lemma 10.20, σ e ρ sono coniugati in S_5, per esempio tramite $\tau = (34)$. Per l'esercizio 10.36, non c'è nessuna permutazione $\alpha \in A_5$ tale che $\sigma^\alpha = \rho$.

Il seguente Lemma 10.23 garantisce che, nel caso particolare dei 3-cicli, questo avviene anche in A_n.

Lemma 10.23 *Sia $n \geq 5$, allora i 3-cicli formano un'unica classe di coniugio.*

Dimostrazione. Siano $\sigma = (abc)$ e τ due 3-cicli. Allora esiste una permutazione $\psi \in S_n$ tale che $\sigma^\psi = \tau$. Se $\psi \in A_n$, allora σ e τ sono coniugati anche in A_n. Poiché $n \geq 5$, esistono due elementi d, e tali che $\{a, b, c\} \cap \{d, e\} = \emptyset$. Se $\psi \notin A_n$, la permutazione ψ è dispari e quindi la permutazione $\alpha = (de) \circ \psi$ è pari e appartiene ad A_n. Inoltre, $\sigma^\alpha = (\sigma^{(de)})^\psi = \sigma^\psi = \tau$ che prova che σ e τ sono coniugate anche in A_n. $\square$

Siamo ora in grado di dimostrare il seguente Teorema.

Teorema 10.24 *Per $n \geq 5$, il gruppo alterno A_n è semplice non abeliano.*

Dimostrazione. Sia N un sottogruppo normale non identico di A_n. Se N contiene un 3-ciclo, poiché N è normale, contiene tutti i coniugati di questo 3-ciclo. Ma i 3-cicli di A_n costituiscono un'unica classe di coniugio per il Lemma 10.23. Quindi N contiene tutti i 3-cicli di A_n, e pertanto tutto A_n in quanto A_n è generato dai 3-cicli per la Proposizione 10.19. Si cercherà di dimostrare che N contiene un 3-ciclo. Si osservi che se $\sigma \in N$, e $\tau \in A_n$, allora l'elemento $(\tau^{-1})^\sigma \circ \tau = \sigma^{-1} \circ \tau^{-1} \circ \sigma \circ \tau = \sigma^{-1} \circ \sigma^\tau \in N$. Dato $\sigma \in N$ cercheremo di dimostrare che esiste un'opportuna permutazione $\tau \in A_n$ tale che $(\tau^{-1})^\sigma \circ \tau$ sia un 3-ciclo, che quindi appartiene ad N.

Sia $\sigma = \sigma_1 \circ \dots \circ \sigma_r$ la decomposizione in cicli disgiunti di σ e siano l_i le lunghezze dei cicli σ_i per $i = 1, \dots, r$. Poniamo $l = max\{l_i | i = 1, \dots r\}$. Poiché i cicli disgiunti commutano, possiamo supporre che $l = l_1$. Distinguiamo vari casi.

i) Se $l \geq 4$, allora $\sigma_1 = (a_1a_2a_3a_4\dots)$. Sia $\tau = (a_1a_3a_2)$, allora $\tau^{-1} = (a_1a_2a_3)$ e

$$(\tau^{-1})^\sigma \circ \tau = (a_2a_3a_4) \circ (a_1a_3a_2) = (a_1a_4a_2) \in N.$$

ii) Se $l = 3$ e $r = 1$, σ è un 3-ciclo.

Se $l = 3$ e $r > 1$, allora possiamo supporre $\sigma_1 = (a_1a_2a_3)$ e $\sigma_2 = (a_4a_5\dots)$. Sia $\tau = (a_1a_4a_2)$, allora $\tau^{-1} = (a_1a_2a_4)$ e

$$(\tau^{-1})^\sigma \circ \tau = (a_2a_3a_5) \circ (a_1a_4a_2) = (a_1a_4a_3a_5a_2) \in N.$$

Concludiamo in quanto $(a_1a_4a_3a_5a_2)$ rientra nel caso i).

iii) Se $l = 2$, allora $r \geq 2$ perché $N \leq A_n$. Possiamo supporre $\sigma_1 = (a_1a_2)$ e $\sigma_2 = (a_3a_4)$. Poiché $n \geq 5$, esiste $a_5 \notin \{a_1, a_2, a_3, a_4\}$. Sia $\tau = (a_1a_5a_3)$ allora $\tau^{-1} = (a_1a_3a_5)$, da cui $(\tau^{-1})^\sigma = (a_2a_4a_6)$, ove $\sigma(a_5) = a_6 \notin \{a_1, a_2, a_3, a_4\}$. Dobbiamo distinguere due ulteriori casi.

Se $a_6 = a_5$, allora

$$(\tau^{-1})^\sigma \circ \tau = (a_2a_4a_5) \circ (a_1a_5a_3) = (a_1a_2a_4a_5a_3) \in N.$$

Possiamo concludere per il caso i).

Se $a_6 \neq a_5$, allora $(\tau^{-1})^\sigma \circ \tau = (a_2a_4a_6) \circ (a_1a_5a_3) \in N$. Possiamo concludere per il caso ii). □

10.5 Esercizi sui gruppi non abeliani

Esercizio 10.25 *Sia p un numero primo. È possibile trovare un gruppo di ordine p^3 non abeliano?*

Esercizio 10.26 *Sia G un gruppo e sia H un sottogruppo di G. Per ogni $x \in G$ denotiamo con H^x il sottogruppo coniugato $x^{-1}Hx$ di H. Dimostrare che*

(a) H^x contiene l'intersezione $H \cap Z(G)$, in particolare, $H \cap Z(G)$ è contenuto nel cuore H_G di H;

(b) esistono gruppi G per i quali l'uguaglianza $H \cap Z(G) = H_G$ fallisce per qualche sottogruppo proprio H.

Esercizio 10.27 *Sia $n \geq 4$, allora $Z(A_n) = \{1\}$.*

Esercizio 10.28 *Se $n \geq 5$, allora A_n è l'unico sottogruppo normale non banale di S_n.*

Esercizio 10.29 *Sia H un sottogruppo di un gruppo G. Provare che $N_G(H) = H$, se l'indice $[G : H]$ è primo e H non è normale.*

Esercizio 10.30 *Sia $H = \langle(123)\rangle$ il sottogruppo del gruppo alterno $G = A_4$. Calcolare $N_G(H)$.*

Esercizio 10.31 *Sia G un gruppo finito e sia H un sottogruppo proprio di G. Provare che l'insieme $\bigcup_{x\in G} H^x$ è una parte propria di G (dove H^x denota il sottogruppo coniugato $x^{-1}Hx$ di H).*

Esercizio 10.32 *Se il gruppo G non è abeliano, allora il gruppo $Aut(G)$ non può essere ciclico.*

Esercizio 10.33 *Non esiste un gruppo G tale che $Aut(G) \cong \mathbb{Z}$.*

Esercizio 10.34 *Sia $m > 1$ un intero dispari. Allora non esiste un gruppo G tale che $Aut(G) \cong \mathbb{Z}_m$.*

Esercizio 10.35 *Decomporre $(23)(432)(12)(13) \in S_4$ nel prodotto di cicli disgiunti. Dimostrare che S_4 è generato da $\{(12), (13), (14)\}$.*

Esercizio 10.36 *Siano $\sigma = (12345)$, $\rho = (12435)$ e $\tau = (34)$ cicli di S_5.*

i) Si verifichi che $\sigma^\alpha = \rho$ se e solo se $\alpha \in \{(34), (1245), (14)(235), (13)(254), (1532)\}$.

ii) Sia $H = \langle\sigma\rangle$. Si provi che $C_{S_5}(H) = H$.

iii) Si descriva la classe laterale $H\tau$ e si concluda che $\sigma^\alpha = \rho$ se e solo se $\alpha \in H\tau$.

Esercizio 10.37 *Sia G un gruppo e $x, y \in G$ due elementi coniugati, cioé esiste $g \in G$ tale che $x^g = y$. Allora $x^h = y$ se e solo se $h \in C_G(x)g$.*

Esercizio 10.38 *Dimostrare che S_4 è generato da $\{(12), (1234)\}$.*

Esercizio 10.39 *Si dimostri che esiste un omomorfismo $f : S_4 \to S_3$ tale che*

$$\ker f = \{id, (12)(34), (13)(24), (14)(23)\}.$$

È tale omomorfismo suriettivo?

Esercizio 10.40 * *Provare che il gruppo alterno A_4 non ha sottogruppi di ordine 6.*

Esercizio 10.41 *Siano σ e τ le permutazioni di S_9 definite rispettivamente come segue:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 5 & 6 & 4 & 8 & 9 & 7 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \end{pmatrix}.$$

(i) Si dimostri che $\sigma\tau = \tau\sigma$.

(ii) Si trovi la decomposizione in cicli disgiunti di σ, τ e $\sigma\tau$.

(iii) Si calcoli l'ordine di σ, τ e $\sigma\tau$.

(iv) Sia H il sottogruppo di S_9 generato da σ e τ. H è ciclico? H è abeliano? Quanti elementi ha H?

11 Esercizi vari

Esercizio 11.1 *Si consideri un quadrato inscritto in un cerchio di raggio 1. Sia σ la rotazione antioraria di $\pi/2$ radianti del cerchio su se stesso: σ trasforma il quadrato in se stesso.*

i) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano il quadrato in sé?

ii) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?

iii) Sia τ il ribaltamento del quadrato rispetto ad una delle sue diagonali. Qual è l'ordine di τ?

iv) Si provi che $\tau\sigma\tau = \sigma^{-1}$.

v) Che ordine ha il gruppo $G = \langle\sigma, \tau\rangle$?

vi) Qual è il centro di G?

Il gruppo G definito nell' Esercizio 11.1 (v) viene chiamato *gruppo diedrale* e denotato con D_8.

Esercizio 11.2 *Sia H il sottogruppo di S_4 generato dai cicli (1234) e (13). Dimostrare che $H \cong D_8$.*

Esercizio 11.3 ** *Si consideri un pentagono regolare inscritto in un cerchio di raggio 1. Sia σ la rotazione antioraria di 72 gradi del cerchio su se stesso: σ trasforma il pentagono in se stesso.*

i) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano il pentagono in sé?

ii) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?

iii) Sia τ il ribaltamento del pentagono rispetto ad uno dei suoi assi di simmetria. Qual è l'ordine di τ?

iv) Si provi che $\tau\sigma\tau = \sigma^{-1}$.

v) Provare che il gruppo $G = \langle\sigma, \tau\rangle$ ha ordine 10 e $Z(G) = \{1\}$.

Esercizio 11.4 ** *Si consideri un esagono regolare inscritto in un cerchio di raggio 1. Sia σ la rotazione antioraria di 60 gradi del cerchio su se stesso: σ trasforma l'esagono in se stesso.*

i) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano l'esagono in sé?

ii) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?

iii) Sia τ il ribaltamento dell'esagono rispetto ad una una delle sue diagonali grandi. Qual è l'ordine di τ ?

iv) Si provi che $\tau\sigma\tau = \sigma^{-1}$.

v) Provare che il gruppo $G = \langle\sigma, \tau\rangle$ ha ordine 12 e $|Z(G)| = 2$.

Esercizio 11.5 ** *Si consideri un poligono regolare P di 7 lati inscritto in un cerchio di raggio 1. Sia σ la rotazione antioraria di $2\pi/7$ radianti del cerchio su se stesso: σ trasforma P in se stesso.*

i) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano P in sé?

ii) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?

iii) Sia τ il ribaltamento di P rispetto ad uno dei suoi assi di simmetria. Qual è l'ordine di τ?

iv) Si provi che $\tau\sigma\tau = \sigma^{-1}$.

v) Provare che il gruppo $G = \langle\sigma, \tau\rangle$ ha ordine 14 e $Z(G) = \{1\}$.

Esercizio 11.6 *Siano H ed N due sottogruppi di un gruppo finito G, tali che $H \leq N \leq G$. Allora $[G : H] = [G : N][N : H]$.*

Esercizio 11.7 *Siano G un gruppo finito ed H e K sottogruppi di G. Si dica se le seguenti affermazioni sono vere o false, fornendo una breve dimostrazione o un controesempio.*

a) Se $[G : H] = 3$, e $|G|$ è dispari, allora $H \triangleleft G$.

b) Se $[G : H] = p$, p primo allora $H \triangleleft G$;

c) Se $[G : H] = p$, p primo allora H è massimale in G, cioè non esiste nessun sottogruppo $K \leq G$ tale che $H < K < G$.

Esercizio 11.8 *Provare che ogni gruppo G di ordine 15 è ciclico.*

Esercizio 11.9 *Sia p un numero primo tale che $p > 3$ e 3 non divide $p - 1$. Provare che ogni gruppo G di ordine $3p$ è ciclico.*

Esercizio 11.10 *Siano p e q numeri primi distinti. Provare che ogni gruppo abeliano di ordine pq è ciclico.*

Esercizio 11.11 *Sia p un numero primo e sia G un gruppo di ordine p^n per qualche $n \in \mathbb{N}$. Dimostrare che per ogni divisore d di $|G|$ esiste un sottogruppo di G di ordine d.*

Esercizio 11.12 *Sia $(G, \cdot)$ un gruppo e sia $* : G \times G \to G$ l'operazione così definita: per ogni $a, b \in G$ sia $a * b := b \cdot a$. Si dimostri che $(G, *)$ è un gruppo in cui l'identità per $*$ coincide con l'identità per $\cdot$ e anche l'inverso di un elemento a rispetto all'operazione $*$ coincide con l'inverso di a rispetto all'operazione $\cdot$. Si osservi che $\cdot$ coincide con $*$ se il gruppo G è abeliano.*

Esercizio 11.13 *Sia G un gruppo. Definiamo una relazione $\sim$ in G ponendo $x \sim y$ se e solo se $\langle x \rangle = \langle y \rangle$.*

i) Si verifichi che $\sim$ è una equivalenza.

ii) Si verifichi che per ogni $g \in G$ risulta $g \sim g^{-1}$.

iii) È vero che se $g \in G$ è aperiodico allora la classe $[g]_\sim$ di g rispetto a $\sim$ contiene esattamente due elementi?

iv) Si dimostri che se G è infinito, allora G ha infiniti sottogruppi.

Esercizio 11.14 *Siano G ed H gruppi finiti e $f : G \to H$ un omomorfismo. Si dimostri che*

a) per ogni $g \in G$ si ha $o(f(g))$ divide $o(g)$;

b) se $o(f(g)) = o(g)$ per ogni $g \in G$, allora f è iniettivo;

c) se f è suriettivo, allora $|H|$ divide $|G|$;

d) se f è iniettivo, allora $|G|$ divide $|H|$.

Esercizio 11.15 *Sia G un gruppo e $x, y \in G$. Provare che $o(xy) = o(yx)$.*

Esercizio 11.16 *Siano G un gruppo abeliano e $f : G \to G$ un omomorfismo di gruppo tale che $f \circ f = f$. Dimostrare che $G \cong f(G) \times \ker f$.*

Esercizio 11.17 *Siano $f : K \to G$ e $t : K \to H$ due omomorfismi. Sia $F : K \to G \times H$ l'applicazione definita da $F(x) = (f(x), t(x))$. Allora:*

(a) F è un omomorfismo e $p_1 \circ F = f$, $p_2 \circ F = t$;

(b) F è iniettivo se e solo se lo sono f e t;

(c) ogni omomorfismo $s : K \to G \times H$ si ottiene in questo modo: cioè gli omomorfismi $f : K \to G$ e $t : K \to H$ dati da $f = p_1 \circ s$, $t = p_2 \circ s$ danno luogo ad un omomorfismo $F : K \to G \times H$ come sopra che coincide con s.

Esercizio 11.18 *Sia $n > 2$ un numero intero e siano $f_1 : G \to H_1$, $f_2 : G \to H_2$, ..., $f_n : G \to H_n$ n omomorfismi. Allora esiste un unico omomorfismo $f : G \to H_1 \times H_2 \times \ldots \times H_n$ tale che $p_i \circ f = f_i$, dove $p_i : H_1 \times \ldots \times H_n \to H_i$, per $i = 1, ..., n$ sono le proiezioni.*

Esercizio 11.19 *Dato un gruppo G possiamo definire la relazione $x \sim_G y$ se e solo se esiste $g \in G$ tale che $y = x^g$. Dimostrare che $\sim$ è di equivalenza.*

Esercizio 11.20 *Dimostrare che il sottogruppo $V = \{1, (12)(34), (13)(24), (14)(23)\}$ del gruppo simmetrico S_4 è isomorfo al gruppo $Aut(\mathbb{Z}_8)$.*

Esercizio 11.21 *Descrivere tutti i sottogruppi normali del gruppo simmetrico S_4.*

Esercizio 11.22 *Nel gruppo moltiplicativo G delle matrici quadrate invertibili di ordine 3 a coefficienti reali, cioè $G = GL(3, \mathbb{R})$, si consideri il sottoinsieme H delle matrici della forma*

$$\begin{pmatrix} 1 & n & \frac{n^2-n}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}, \quad n \in \mathbb{Z}.$$

i) Si dimostri che H è un sottogruppo di G.

ii) Si provi che H è ciclico e se ne trovi un generatore.

Esercizio 11.23 *Sia G il sottogruppo additivo dei numeri complessi $G = \{x + iy | x, y \in \mathbb{Z}\}$.*

i) Si provi che la posizione $f : G \to G$ definita da $f(x + iy) = x + y$ è un endomorfismo di G;

ii) si dimostri che $\ker(f)$ è ciclico e se ne trovi un generatore;

iii) si trovi $f(G)$.

Esercizio 11.24 *Sull'insieme $G = \mathbb{Z}_4 \times \{-1, 1\}$ si definisca un' operazione "$\cdot$" ponendo per ogni $(x, u), (y, v) \in G$, $(x, u) \cdot (y, v) = (x + uy, uv)$.*

(a) Si dimostri che G con questa operazione è un gruppo non abeliano.

(b) Si trovi un sottogruppo di G che non è normale.

(c) Si dimostri che G è isomorfo al gruppo diedrale D_8 definito nell'Esercizio 11.1.

Esercizio 11.25 ** *Descrivere $Aut(\mathbb{Z}_2 \times \mathbb{Z}_4)$*

Esercizio 11.26 *Sull'insieme $G = \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ si definisca un operazione "$\cdot$" ponendo per ogni $(x, y, z), (u, v, w) \in G$ $(x, y, z) \cdot (u, v, w) = (x + (-1)^z y, y + v, z + w)$.*

(a) Si dimostri che G con questa operazione è un gruppo non abeliano.

(b) Si dimostri che il sottoinsieme $N = \mathbb{Z} \times \{0\} \times \{0\}$ di G è un sottogruppo normale di G e G/N è isomorfo al gruppo $\mathbb{Z} \times \mathbb{Z}$.

(c) Esistono sottogruppi di G che non sono normali?

(d) Calcolare il centro di G.

Esercizio 11.27 *Sia G l'insieme dei numeri complessi del tipo $a+ib$ con $a, b \in \mathbb{Q}$ non entrambi nulli.*

i) si provi che G è un gruppo rispetto alla moltiplicazione;

ii) si dica quale dei seguenti elementi sono periodici e quali aperiodici: $1 + i$, $1/2i$, -1;

iii) si provi che la posizione $f : z \mapsto z^{-2}$ definisce un endomorfismo f di G non suriettivo.

Esercizio 11.28 *Siano A e B due gruppi ciclici infiniti generati da a e da b rispettivamente e sia $G = A \times B$ il prodotto diretto di A e B. Si provi che*

i) G è senza torsione;

ii) l'applicazione $f : G \to G$ tale che $f(a^i, b^j) = (a^{-i}, b^j)$ per ogni $i, j \in \mathbb{Z}$ è un automorfismo di G;

iii) si determini il periodo di f come elemento di $Aut(G)$,

iv) indicando con π_1 la proiezione di G su A, si definisca un automorfismo φ di G tale che $(\pi_1 \circ \varphi)(a^i, b^j) = a^{i+j}$ per ogni $i, j \in \mathbb{Z}$.

v) È vero che $Aut(G)$ contiene un sottogruppo non ciclico di ordine 4?

vi)* Dimostrare che $Aut(G)$ è isomorfo al sottogruppo di $GL_2(\mathbb{R})$ formato dalle matrici con coefficienti interi.

Esercizio 11.29 *Dimostrare che ogni sottogruppo finitamente generato di $\mathbb{Q}/\mathbb{Z}$ è ciclico.*

Esercizio 11.30 *Dimostrare che il gruppo abeliano $\mathbb{Q} \times \mathbb{Q}$ non è isomorfo a $\mathbb{Q}$.*[1]

Esercizio 11.31 *Dimostrare che esiste un sottogruppo H di $\mathbb{R}$ tale che $\mathbb{R} \cong \mathbb{Q} \times H$.*

Esercizio 11.32 *Sia p un primo e sia G l'insieme delle radici p^n-esime dell'unità al variare di $n \in \mathbb{N}$. Dimostrare che*

a) $(G, \cdot)$ è un sottogruppo infinito di $(\mathbb{C}, \cdot)$;

b) ogni sottogruppo proprio di G è ciclico finito;

c) G è isomorfo al gruppo quoziente $\mathbb{Q}_p/\mathbb{Z}$, dove $\mathbb{Q}_p$ è il sottogruppo di $\mathbb{Q}$ formato di tutte le frazioni del tipo a/p^n al variare di $a, n \in \mathbb{Z}$.

Esercizio 11.33 *Sia G il gruppo $GL_2(\mathbb{R})$. Dimostrare che:*

(a) i sottoinsiemi

$$B_2^+ = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in GL_2(\mathbb{R}) : a, b \in \mathbb{R} \right\} \text{ e } B_2^- = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \in GL_2(\mathbb{R}) : a, b \in \mathbb{R} \right\}$$

di G sono sottogruppi abeliani isomorfi entrambi a $(\mathbb{R}, +) \times (\mathbb{R}^*, \cdot)$;

(b) le matrici $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, con a, b, c e d numeri razionali, formano un sottogruppo H di G (denotato solitamente anche con $GL_2(\mathbb{Q})$);

[1] Si può dimostrare invece che $\mathbb{R}\times\mathbb{R}$ è isomorfo a $\mathbb{R}$. A questo scopo bisogna provare che $\mathbb{R}$ come spazio vettoriale sopra $\mathbb{Q}$ ha dimensione infinita, cioè ha una base infinita B. Trovando una partizione $B = B_1 \cup B_2$ di B con $|B_1| = |B_2| = |B|$ si dimostra che i sottospazi V_1 e V_2 dello spazio $\mathbb{R}$ generati da B_1 e B_2 rispettivamente, sono isomorfi entrambi a $\mathbb{R}$ e quindi $\mathbb{R} \cong V_1 \times V_2 \cong \mathbb{R} \times \mathbb{R}$.

(c) per ogni numero irrazionale $r \in \mathbb{R}$ *e* $x = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$, $z = \begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ *e* $u = \begin{pmatrix} r^{-1} & 0 \\ 0 & r \end{pmatrix}$ *si ha* $H \cap H^x \leq B_2^+$, $H \cap H^y \leq B_2^-$, $H \cap H^z \leq D_2$ *e* $H \cap H^u \leq D_2$, *dove* $D_2 := \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in GL_2(\mathbb{R}) : a, b \in \mathbb{R} \right\}$.

(d) esistono matrici $x, y \in G$, *tali che* $H \cap H^x \cap H^y \leq Z(GL_2(\mathbb{R}))$.

Esercizio 11.34 *Sia* G *il sottoinsieme del gruppo* $GL_2(\mathbb{R})$ *formato da tutte le matrici della forma* $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. *Dimostrare che:*

(a) G *è un sottogruppo di* $GL_2(\mathbb{R})$;

(b) il centro di G *è dato solo dalla matrice identica;*

(c) le matrici $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$, *con* a *e* b *numeri razionali, formano un sottogruppo* H *di* G;

(d) sia N^+ *l'insieme definito nell'esercizio 11.33 e* $H_1 = H \cap N^+$. *Allora esiste una matrice* $z \in G$, *tale che* $H_1 \cap H_1^z = \{I_2\}$, *dove* I_2 *è la matrice identica di* G.

(e) esistono matrici $x, z \in G$, *tali che* $H \cap H^x \cap H^z = \{I_2\}$, *dove* I_2 *è la matrice identica di* G.

Esercizio 11.35 *Sia* G *il gruppo* $SL_2(\mathbb{R})$. *Dimostrare che:*

(a) $Z(G) = \{I_2, -I_2\}$;

(b) le matrici $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, *con* a, b, c *e* d *numeri razionali, formano un sottogruppo* H *di* G;

(c) esistono matrici $x, y \in G$, *tali che* $H \cap H^x \cap H^y = \{\pm I_2\}$, *dove* I_2 *è la matrice identica di* G.

Esercizio 11.36 *Sia* G *il gruppo* $T_2^+(\mathbb{R})$ *delle matrici triangolari superiori in* $GL_2(\mathbb{R})$. *Dimostrare che per il sottogruppo* $H = GL_2(\mathbb{Q}) \cap G$ *di* G *esistono matrici* $x, y \in G$ *tali che* $H \cap H^x \cap H^y \leq Z(G)$.

Esercizio 11.37 *Provare che il sottoinsieme* H *del gruppo* $GL_2(\mathbb{F}_3)$ *che consiste dalle matrici della forma* $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $a \in \mathbb{F}_3^*$, $b \in \mathbb{F}_3$, *è un sottogruppo isomorfo a* S_3.

Esercizio 11.38 *Provare che i gruppi* $(\mathbb{Z}_8, +)$ *e* $Aut(\mathbb{Z}_{15})$ *non sono isomorfi.*

Esercizio 11.39 *Sia* G *un gruppo abeliano di ordine* $m > 1$. *Provare che il gruppo* G *non è ciclico se e solo se esiste un divisore proprio* n *di* m *tale che* $nx = 0$ *per ogni* $x \in G$.

Esercizio 11.40 ** *Sia* p *un numero primo dispari. Provare che il gruppo* $Aut(\mathbb{Z}_p)$ *è ciclico.*

Esercizio 11.41 ** *Sia* p *un numero primo dispari. Provare che il gruppo* $Aut(\mathbb{Z}_{p^k})$ *è ciclico per ogni intero* $k > 0$.

Esercizio 11.42 * *Sia* $m = p_1^{k_1} \dots p_s^{k_s}$, *con numeri primi dispari distinti* $p_1, \dots, p_s$. *Provare che*

$$Aut(\mathbb{Z}_m) \cong \mathbb{Z}_{p_1^{k_1} - p_1^{k_1 - 1}} \times \dots \times \mathbb{Z}_{p_s^{k_s} - p_s^{k_s - 1}}.$$

Esercizio 11.43 *Descrivere i sottogruppi di:*

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2$;

(b) $\mathbb{Z}_2 \times \mathbb{Z}_3$;

(c) $\mathbb{Z}_3 \times \mathbb{Z}_3$;

(d) $\mathbb{Z}_2 \times \mathbb{Z}_4$;

(e) $\mathbb{Z}_8 \times \mathbb{Z}_9$;

(f) $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;

(g) $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$

Esercizio 11.44 *Sia* $\mathbb{R}^*$ *il gruppo moltiplicativo dei numeri reali non nulli e sia* N *il sottogruppo ciclico di* $\mathbb{R}^*$ *generato da* π.

(1) Quanti elementi di ordine 2 ha il gruppo quoziente $\mathbb{R}^*/N$?

(2) Si determinino gli elementi di ordine finito del quoziente $\mathbb{R}^*/N$.

12 Svolgimento e suggerimenti per la risoluzione di alcuni esercizi

Esercizi sui semigruppi e sui monoidi

1.5 Fissare n arbitrariamente e dimostrare per induzione su m che vale $x^{n+m} = x^n x^m$ per tutti gli m.

1.20 Supponiamo per assurdo che esistano semigruppi finiti che non hanno elementi idempotenti. Allora $\mathcal{A} = \{|\mathcal{S}| : \mathcal{S}$ è semigruppo finito e non S non ha idempotenti $\}$ è un sottoinsieme non vuoto di $\mathbb{N}^*$. Per il principio del buon ordinamento, tale insieme ammette minimo. Quindi esiste $(S, \cdot)$ semigruppo finito che non ammette idempotenti, con $|S|$ minimo. Un tale esempio si dice *controesempio minimale*. Allora ogni sottosemigruppo H di S, con $|H| < |S|$ deve contenere un idempotente a che ovviamente è anche un idempotente di S. Quindi l'unico sottosemigruppo di S è S stesso. Sia $a \in S$, e $H = \{a^{2n} : n \in \mathbb{N}^*\}$ Allora $H \neq \emptyset$ perché $a^2 \in H$ e dati $h = a^{2n}$, $k = a^{2m} \in H$, $h \cdot k = a^{2n} \cdot a^{2m} = a^{2(n+m)} \in H$. Pertanto H è un sottosemigruppo. Quindi $a \in S = H$ implica $a = a^{2n}$ per qualche $n \in N^*$. Sia $b = a^{2n-1}$, allora $b^2 = a^{2n-1} \cdot a^{2n-1} = a^{2n} \cdot a^{2n-2} = a \cdot a^{2n-2} = a^{2n-1} = b$. Quindi b è un idempotente di S, che contraddice l'ipotesi assurda. Allora $\mathcal{A} = \emptyset$.

1.21 Si applichino l'Esercizio 1.20 ed il Lemma 1.6 per dedurre che S è un monoide e si utilizzi il Teorema 1.2 per concludere.

1.22 Per l'Esercizio 1.20, S ha sempre un idempotente, quindi deve valere $a^2 = a$ oppure $b^2 = b$ in ogni tabella. Questo elimina le quattro tabelle con $a^2 = b$ e $b^2 = a$. Inoltre, se vale $a^2 = a$ e $b^2 = a$, allora il semigruppo è abeliano. Infatti, se avessimo $ab = b$ e $ba = a$, allora $(ba)b = ab = b$, mentre $b(ab) = b^2 = a$ e quindi non varrebbe la legge associativa. Allo stesso modo si dimostra che se vale $a^2 = b$ e $b^2 = a$, allora il semigruppo è abeliano. In questo modo sono state eliminate altre 4 tabelle. Visto che ci sono 16 applicazioni distinte $S \times S \to S$, restano 8 tabelle che riportiamo qui sotto. Lasciamo al lettore la verifica che esse definiscono una struttura di semigruppo su S. Ci sono essenzialmente 4 strutture diverse – la prima, la seconda, la terza, e la quarta, che risulta l'unica non abeliana. Le altre 4 strutture si ricavano scambiando semplicemente a e b. Le tabelle 1 e 5 presentano le due strutture in cui la moltiplicazione è una funzione costante (su $S \times S$).

Tabella 1

·	a	b
a	a	a
b	a	a

,

Tabella 2

·	a	b
a	b	a
b	a	b

,

Tabella 3

·	a	b
a	a	b
b	b	b

,

Tabella 4

·	a	b
a	a	a
b	b	b

,

Tabella 5

·	a	b
a	b	b
b	b	b

,

Tabella 6

·	a	b
a	a	b
b	b	a

,

Tabella 7

·	a	b
a	a	a
b	a	b

,

Tabella 8

·	a	b
a	a	b
b	a	b

. □

1.23 (a) Si verifica facilmente che | soddisfa la proprietà riflessiva e transitiva.

(b) Proviamo che | soddisfa anche la proprietà antisimmetrica. Siano $a, b \in S$ tali che $a|b$ e $b|a$. Allora eistono $x, y \in S$ tali che $a = bx$ e $b = ay$. Poichè $b1 = b = ax = (by)x = b(yx)$ e $a1 = a = by = (ax)y = a(xy)$, la legge di cancellazione valida in S implica che $yx = 1 = xy$. Per l' unicità dell' inverso si ha $y = x = 1$ e dunque $a = b$.

Poiché $a = a1$ per ogni $a \in S$, risulta $1|a$ per ogni $a \in S$ e dunque 1 è l' elemento minimo cercato.

Esercizi sui gruppi

2.19 Dimostriamo che l'ordine di ab divide mn. Per il Lemma 2.4 risulta $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n 1^m = 1$, e la tesi segue dal punto (a) del Lemma 2.6.

2.21 È facile verificare che $(\mathbb{Q} \times \mathbb{Z}^*, \cdot)$ è un monoide con elemento neutro $(0, 1)$. Un elemento $(q, m) \in \mathbb{Q} \times \mathbb{Z}^*$ è invertibile se e solo e esiste $(q', m') \in \mathbb{Q} \times \mathbb{Z}^*$ tale che

$$(q, m) \cdot (q', m') = (q + mq', mm') = (0, 1) = (q' + m'q, m'm) = (q', m') \cdot (q, m).$$

Ciò accade se e solo se $q + mq' = 0 = q' + m'q$ e $mm' = 1$ se e solo se $m = m' = 1$ e $q + q' = 0$ oppure $m = m' = -1$ e $q - q' = 0$. Quindi gli elementi invertibili di $\mathbb{Q} \times \mathbb{Z}^*$ sono tutti e soli della forma $(q, 1)$ (con inverso $(-q, 1)$) e $(q, -1)$ (con inverso $(q, -1)$).

$(\mathbb{Q} \times \mathbb{Z}^*, \cdot)$ non è abeliano perché presi $(q, m), (q', m) \in \mathbb{Q} \times \mathbb{Z}^*$ con $q \neq q'$ e $m \neq 1$, non commutano.

2.23 $(\{0\}, +)$, $(\{1, -1\}, \cdot)$ e $(\mathbb{Q}_+, \cdot)$ sono gruppi mentre $(\{0, 1\}, \cdot)$ non lo è poiché l' elemento 0 non ammette inverso.

2.25 È facile verificare che $(\mathbb{Q}^* \times \mathbb{Q}, \cdot)$ è un monoide con elemento neutro $(1, 0)$. Inoltre, per ogni $(a, b) \in \mathbb{Q}^* \times \mathbb{Q}$ l' elemento $(a^{-1}, -b)$ appartiene a $\mathbb{Q}^* \times \mathbb{Q}$ e $(a^{-1}, -b) \cdot (a, b) = (1, 0) = (a, b) \cdot (a^{-1}, -b)$. Quindi $(\mathbb{Q}^* \times \mathbb{Q}, \cdot)$ è un gruppo. Non è abeliano perché presi $(a, b), (a, b') \in \mathbb{Q}^* \times \mathbb{Q}$ con $a \neq \pm 1$ e $b \neq b'$, $(a, b) \cdot (a, b') \neq (a, b') \cdot (a, b)$.

2.27 Siano $f \in G$ e $x, y \in \mathbb{R}$. Allora $f(x) = f(y)$ se e solo se $ax + b = ay + b$ se e solo se $ax = ay$ se esolo se $x = y$ poiché $a \neq 0$. Dunque f è iniettiva. f è anche suriettiva poiché per ogni $y \in \mathbb{R}$ si ha $y = f\left(\frac{y-b}{a}\right)$. Ciò prova che $G \subseteq S_{\mathbb{R}}$. Siano $f, g \in G$ tali che $f(x) = ax + b$ e $g(x) = cx + d$ per ogni $x \in \mathbb{R}$ con $a, c \in \mathbb{R} \setminus \{0\}$ e $b, d \in \mathbb{R}$. Allora $(g \circ f)(x) = g(ax + b) = cax + cb + d$ per ogni $x \in \mathbb{R}$ e quindi $g \circ f \in G$ poiché $ac \neq 0$. È facile verificare che $(G, \circ)$ è un monoide con elemento neutro $id_{\mathbb{R}}$ e che ogni $f \in G$ è invertibile con inversa definita da $f^{-1}(x) = a^{-1}x - \frac{b}{a}$ per ogni $x \in \mathbb{R}$. Ciò prova che $(G, \circ)$ è un gruppo. G non è abeliano perché date f e g definite rispettivamente da $x \mapsto 2x + 5$ e $x \mapsto 3x + 1$, $(g \circ f) \neq (f \circ g)$.

2.28 U è non vuoto poiché $1 \in U$. Inoltre, $u^{-1} \in U$ per ogni $u \in U$. Per concludere si osservi che se $u, v \in U$, allora $(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = uu^{-1} = 1 = v^{-1}v = v^{-1}(u^{-1}u)v = (v^{-1}u^{-1})(uv)$. Quindi $uv \in U$.

2.29 Si consideri un ciclo di lunghezza pari.

2.31 $\sigma = (1512)(26911)(374108)$ è la decomposizione di σ in cicli disgiunti. Siano $\tau_1 := (1512)$, $\tau_2 := (26911)$ e $\tau_3 := (374108)$. Allora per il Lemma 2.4 risulta che $\sigma^n = \tau_1^n \tau_2^n \tau_3^n$ per ogni $n \in \mathbb{Z}$. Osserviamo che:
$\tau_1^3 = id \Longrightarrow \tau_1^2 = \tau_1^{-1}$;
$\tau_2^4 = id \Longrightarrow \tau_2^3 = \tau_2^{-1}$ e $\tau_2^5 = \tau_2$;
$\tau_3^5 = id \Longrightarrow \tau_3^3 = \tau_3^{-2}$.
Quindi $\sigma^2 = (1125)(29)(611)(348710)$; $\sigma^3 = (21196)(310784)$ e $\sigma^5 = (1125)(26911)$.

Esercizi sui sottogruppi

3.31 Come si è visto nel Lemma 3.9, $x^n, y^m \in \langle X \rangle$ per ogni $n, m \in \mathbb{Z}$. Poiché $\langle X \rangle$ è un sottogruppo, sfruttando (S1) si può dimostrare per induzione su k che $x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k} \in \langle X \rangle$, per ogni $k \in \mathbb{N}_+, n_i, m_i \in \mathbb{Z}$. Pertanto l'insieme H è contenuto in $\langle X \rangle$. Per l'altra inclusione basta vedere che H è un sottogruppo. Infatti, se $x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k}, x^{i_1}y^{j_1}x^{i_2}y^{j_2} \dots x^{i_h}y^{j_h} \in H$, allora

$$x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k}x^{i_1}y^{j_1}x^{i_2}y^{j_2} \dots x^{i_h}y^{j_h} \in H.$$

Inoltre

$$(x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k})^{-1} = y^{-m_k}x^{-n_k} \dots y^{-m_1}x^{-n_1} = x^0y^{-m_k}x^{-n_k} \dots y^{-m_1}x^{-n_1}y^0$$

che è ancora un elemento di H.

La seconda affermazione segue dal fatto che, se x, y commutano, allora

$$x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k} = x^{n_1+n_2\dots+n_k}y^{m_1+m_2\dots+m_k}.$$

3.32 Definiamo $\mathcal{H} := \{h_1k_1h_2k_2 \dots h_sk_s : s \in \mathbb{N}_+, h_i \in H, k_i \in K \text{ per } i = 1, 2, \dots, s\}$. Poiché $\langle X \rangle$ è un sottogruppo di G contenente H e K, $\langle X \rangle$ contiene anche i prodotti dei loro elementi quindi $hk \in \langle X \rangle$ per ogni $h \in H$ e $k \in K$. Sfruttando (S1) si può dimostrare per induzione su $s \in \mathbb{N}_+$ che $\mathcal{H} \subseteq \langle X \rangle$. Chiaramente, $\mathcal{H}$ contiene sia H che K poiché $h = h1$ per ogni $h \in H$ e $k = 1k$ per ogni $k \in K$.

Per dimostrare l' inclusione $\langle X \rangle \subseteq \mathcal{H}$ basta quindi verificare che $\mathcal{H}$ è un sottogruppo di G. Infatti, se $h_{i_1}k_{i_1}h_{i_2}k_{i_2} \dots h_{i_s}k_{i_s}$ e $h_{j_1}k_{j_1}h_{j_2}k_{j_2} \dots h_{j_t}k_{j_t} \in \mathcal{H}$, allora

$$h_{i_1}k_{i_1}h_{i_2}k_{i_2} \dots h_{i_s}k_{i_s}h_{j_1}k_{j_1}h_{j_2}k_{j_2} \dots h_{j_t}k_{j_t} \in \mathcal{H}.$$

Inoltre,

$$(h_{i_1}k_{i_1}h_{i_2}k_{i_2}\dots h_{i_s}k_{i_s})^{-1} = 1k_{i_s}^{-1}h_{i_s}^{-1}\dots k_{i_1}^{-1}h_{i_1}^{-1}1 \in \mathcal{H}.$$

La seconda affermazione segue dal fatto che, se G è abeliano, allora gli elementi di H e K permutano quindi $h_{i_1}k_{i_1}h_{i_2}k_{i_2}\dots h_{i_s}k_{i_s} = hk$ ove $h = h_{i_1}h_{i_2}\dots h_{i_s} \in H$ e $k = k_{i_1}k_{i_2}\dots k_{i_s} \in K$.

3.34 Sia $V = \{(12)(34), (13)(24), (14)(23), id\}$. Essendo prodotto di trasposizioni disgiunte, ogni permutazione σ di V ha periodo 2. Quindi $\sigma = \sigma^{-1}$ e V contiene dunque gli inversi di ogni suo elemento. È un facile esercizio verificare che $\sigma \circ \tau \in V$ per ogni coppia di permutazioni $\sigma, \tau \in V$.

3.36 (i) $\mathcal{C}(\mathbb{R})$ è un sottoinsieme non vuoto di G poiché $id_{\mathbb{R}} \in \mathcal{C}(\mathbb{R})$. Inoltre, poiché la differenza di funzioni continue è ancora un funzione continua, si ha che $f - g \in \mathcal{C}(\mathbb{R})$ per ogni $f, g \in \mathcal{C}(\mathbb{R})$. Per il Lemma 3.6 possiamo concludere che $\mathcal{C}(\mathbb{R})$ è un sottogruppo di G.

(ii)–(iii) Si ragioni come in (i).

3.39 Poiché V è un gruppo abeliano, le classi laterali destre e sinistre di W coincidono. Si osservi che ogni vettore $v \in V$ si rappresenta come $v = le_1 + se_2 + re_3$ ove $l, s, r \in \mathbb{R}$ quindi $W + v = W + re_3$.

3.40 Sia k la dimensione di W. Si scelga una base $e_1, \dots, e_n$ di V tale che $e_1, \dots, e_k$ sia una base di W e si ragioni come nell' Esercizio 3.39.

3.41 Poiché $(\mathbb{Z}, +)$ è un gruppo abeliano, le classi laterali destre e sinistre di un sottogruppo $H \leq \mathbb{Z}$ coincidono. Dato $n \in \mathbb{N}$, un sistema di rappresentanti delle classi laterali del sottogruppo $n\mathbb{Z}$ di $(\mathbb{Z}, +)$ è $0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $2 + n\mathbb{Z}$, $\dots$, $(n-2) + n\mathbb{Z}$, $(n-1) + n\mathbb{Z}$ quindi $[\mathbb{Z} : n\mathbb{Z}] = n$.

3.42 Ragionando come nell' Esempio 3.28, si verifica che gli unici sottogruppi di $(\mathbb{Z}_2, +)$, $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_5, +)$ e $(\mathbb{Z}_7, +)$ sono $\{0\}$ e G.

Se H è un sottogruppo di $(\mathbb{Z}_8, +)$, allora $|H|$ deve dividere 8 per il Teorema di Lagrange. Quindi le sole possibilità sono $|H| = 1, 2, 4, 8$. Si verifica che se $H = \langle [1]_8 \rangle, \langle [3]_8 \rangle, \langle [5]_8 \rangle, \langle [7]_8 \rangle$, allora $H = \mathbb{Z}_8$.

Sia $H = \langle [4]_8 \rangle$. Allora $H = \{[0]_8, [4]_8\}$ e quindi $[G : H] = 4$. Un sistema di rappresentanti per le classi laterali di H in G è $[0]_8 + H$, $[1]_8 + H = \{[1]_8, [5]_8\}$, $[2]_8 + H = \{[2]_8, [6]_8\}$ e $[3]_8 + H = \{[3]_8, [7]_8\}$.

Sia $K = \langle [2]_8 \rangle$. Allora $K = \{[0]_8, [2]_8, [4]_8, [6]_8\}$ e quindi $[G : K] = 2$. Un sistema di rappresentanti per le classi laterali di K in G è $[0]_8 + K$, $[1]_8 + K = \{[1]_8, [3]_8, [5]_8, [7]_8\}$.

Si ragioni in maniera analoga per $(\mathbb{Z}_9, +)$ e $(\mathbb{Z}_{10}, +)$.

3.46 $|S_3| = 6$ quindi un sottogruppo H di S_3 può avere ordine $1, 2, 3, 6$. Siano $\tau_1 = (23)$, $\tau_2 = (13)$, $\tau_3 = (12)$ e $\sigma = (123)$. Si verifica che $\langle \tau_i, \tau_j \rangle = S_3$ se $i \neq j$ e $\langle \tau_i, \sigma \rangle = S_3$ per ogni $i = 1, 2, 3$. Quindi gli unici sottogruppi propri di S_3 sono $\langle \tau_i \rangle$ $(i = 1, 2, 3)$ e $\langle \sigma \rangle$.

3.48 (i) L' elemento $(1, 0)$ è l' unità di G poiché $(1, 0) \cdot (a, b) = (1a, 1b + 0) = (a, b) = (a1, a0 + b) = (a, b) \cdot (1, 0)$ per ogni $(a, b) \in G$.

Se $(a, b) \in G$, allora anche $(a^{-1}, -ba^{-1})$ è un elemento ben definito di G e $(a, b) \cdot (a^{-1}, -ba^{-1}) = (1, 0) = (a^{-1}, -ba^{-1}) \cdot (a, b)$ quindi $(a^{-1}, -ba^{-1}) = (a, b)^{-1}$.

(ii) Chiaramente $H \neq \emptyset$ poiché $(1, 0) \in H$. Inoltre, se $(a, 0), (b, 0) \in H$, allora $(a, 0)^{-1} \cdot (b, 0) = (a^{-1}b, 0) \in H$, quindi H è un sottogruppo di G per il Lemma 3.6.

3.49 Sia $G = \mathbb{R} \times \mathbb{R}$, $H = \mathbb{R} \times \{0\}$, $K = \{0\} \times \mathbb{R}$ e $L = \{(r, r) : r \in \mathbb{R}\}$ il sottogruppo diagonale. Allora $H + K = G$, mentre $H \cap L = K \cap L = \{0\}$.

3.50 Basta vedere che per due sottogruppi H e K l'estremo superiore $H \vee K$ coincide con $\langle H, K \rangle$ e l'estremo inferiore $H \wedge K$ coincide con $H \cap K$.