

V - I GRUPPI

1 Operazioni

Sia A un insieme non vuoto. Una **operazione** (binaria) su A è un'applicazione

$$* : A \times A \longrightarrow A .$$

Se $*$ è una operazione su A , allora per ogni $(a, b) \in A \times A$, scriveremo $a * b$. Anzi, il più delle volte (quando non si corra il rischio di confondere) tralascieremo anche di assegnare un simbolo all'operazione e scriveremo semplicemente ab .

Esempi. 1) Sono operazioni le usuali "somma" $+$ e "prodotto" \cdot definite sugli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. La sottrazione, nel significato corrente, è una operazione su $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e \mathbb{C} , ma non è una operazione su \mathbb{N} , dato che la differenza di due numeri interi non è, in genere, un numero intero.

2) Se X è un insieme, allora $\cap, \cup, \Delta, \setminus$ sono operazioni su $A = \mathcal{P}(X)$.

3) Se X è un insieme non vuoto, allora la *composizione* \circ è una operazione sull'insieme X^X di tutte le applicazioni di X in se stesso.

(**Osservazione Importante**) La composizione è anche una operazione sull'insieme $Sym(X)$ di tutte le applicazioni biettive di X in se stesso; infatti, come sappiamo, la composizione di due applicazioni biettive è biettiva.

Dalla definizione data, risulta che su un insieme non vuoto A è possibile in genere definire moltissime operazioni. La maggior parte di esse è tuttavia scarsamente importante (secondo il punto di vista delle strutture algebriche - come si capirà meglio andando avanti). La proprietà fondamentale che, il più delle volte (ma non sempre!), esclude operazioni poco interessanti o di difficile studio è la cosiddetta *associatività*.

Definizione. Un'operazione $*$ sull'insieme A si dice **associativa** se, per ogni $a, b, c \in A$,

$$(a * b) * c = a * (b * c).$$

Definizione. Un **semigrupp** è una coppia (A, \cdot) dove A è un insieme e \cdot una operazione **associativa** su A .

Osservazione importante. Se (A, \cdot) è un semigrupp, allora, per ogni $a, b, c \in A$ possiamo scrivere senza ambiguità

$$a \cdot b \cdot c$$

intendendo con ciò l'elemento $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Questa osservazione si estende ad una stringa finita qualunque di elementi di A . Ad esempio se $a_1, a_2, a_3, a_4 \in A$, allora:

$$a_1 \cdot ((a_2 \cdot (a_3 \cdot a_4))) = a_1 \cdot ((a_2 \cdot a_3) \cdot a_4) = a_1 \cdot (a_2 \cdot a_3 \cdot a_4) = (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = (a_1 \cdot a_2 \cdot a_3) \cdot a_4 = \text{etc.}$$

elemento che scriviamo semplicemente: $a_1 \cdot a_2 \cdot a_3 \cdot a_4$.

Più in generale, per ogni $n \geq 1$ e $a_1, a_2, \dots, a_n \in A$, possiamo individuare senza ambiguità l'elemento

$$a_1 \cdot a_2 \cdot \dots \cdot a_n.$$

(anche questa affermazione, che appare ovvia, andrebbe provata con rigore, operazione non difficile ma noiosa - la cosa più delicata è enunciare correttamente in modo formale la proprietà, poi si può procedere per induzione sul numero n di elementi. Chi è interessato trova una dimostrazione sui testi di Jacobson e Artin.)

Esercizio. Su $\mathbb{Z} \times \mathbb{Z}$ si definisca l'operazione $*$ ponendo, per ogni $(x, y), (x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) * (x_1, y_1) = (x, y_1)$. Si dica se $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigrupp.

Soluzione. Siano $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$. Allora

$$(x, y) * ((x_1, y_1) * (x_2, y_2)) = (x, y) * (x_1, y_2) = (x, y_2) = (x, y_1) * (x_2, y_2) = ((x, y) * (x_1, y_1)) * (x_2, y_2),$$
 dunque l'operazione $*$ è associativa, e $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigrupp.

Definizione. Sia \cdot una operazione sull'insieme A . Un sottoinsieme B di A si dice **chiuso** (rispetto a \cdot) se, per ogni $b, b' \in B$ risulta $b \cdot b' \in B$.

Se B è un sottoinsieme chiuso, allora si può definire su B l'operazione \cdot *indotta* da A (cioè quella definita dalla restrizione della operazione $A \times A \rightarrow A$ ad una operazione $B \times B \rightarrow B$, dove la regola che determina il prodotto rimane la stessa). Ovviamente se l'operazione su A è associativa, anche l'operazione indotta su un sottoinsieme chiuso è tale. Una proprietà elementare ma importante dei sottoinsiemi chiusi è che l'intersezione di due o più di essi è ancora un sottoinsieme chiuso.

Proposizione 1.1 *Sia (A, \cdot) un insieme con operazione, e siano X, Y sottoinsiemi chiusi. Allora $X \cap Y$ è chiuso. Più in generale, se \mathcal{F} è una famiglia qualsiasi di sottoinsiemi chiusi di A , allora $\bigcap_{X \in \mathcal{F}} X$ è un sottoinsieme chiuso.*

Dimostrazione. Proviamo direttamente il caso generale. Sia \mathcal{F} una famiglia di sottoinsiemi chiusi di A , e sia $W = \bigcap_{X \in \mathcal{F}} X$. Siano $x, y \in W$, allora $x, y \in X$ per ogni $X \in \mathcal{F}$ e poichè tali X sono chiusi, si ha $x \cdot y \in X$ per ogni $X \in \mathcal{F}$, cioè $x \cdot y \in W$. Dunque W è chiuso.

Definizione. Sia (A, \cdot) un semigrupp. Un sottoinsieme chiuso di A si dice **sottosemigrupp** di A .

Esempi 1) L'insieme $2\mathbb{Z}$ dei numeri interi pari è un sottosemigrupp di $(\mathbb{Z}, +)$ e di (\mathbb{Z}, \cdot) , mentre l'insieme dei numeri dispari è un sottosemigrupp di (\mathbb{Z}, \cdot) ma non di $(\mathbb{Z}, +)$.

2) Sia X un insieme infinito e poniamo $F(X) = \{ Y \subseteq X \mid |Y| \text{ è finito} \}$. Allora $F(X)$ è un sottosemigrupp dei semigrupp $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$, $(\mathcal{P}(X), \Delta)$. Si studi per esercizio il caso $I(X) = \{ Y \subseteq X \mid |Y| = \infty \}$.

Un semigrupp (A, \cdot) ammette se stesso come sottosemigrupp. Un sottosemigrupp di un semigrupp è, con l'operazione indotta, un semigrupp.

Dalla Proposizione 1.1 segue che l'intersezione di sottosemigrupp di un semigrupp è un sottosemigrupp. Sia (A, \cdot) un semigrupp e sia X un sottoinsieme di A ; allora

l'intersezione di tutti i sottosemigruppi che contengono X (almeno uno c'è: A stesso) è un sottosemigruppo, ed è il minimo (rispetto alla relazione di inclusione) sottosemigruppo di (A, \cdot) che contiene il sottoinsieme X ; esso si chiama il **sottosemigruppo generato** da X .

Chiaramente, un sottosemigruppo che contiene un sottoinsieme X deve contenere tutti i prodotti del tipo $x_1 x_2 \cdots x_n$ con x_1, \dots, x_n elementi (non necessariamente distinti) di X . Il sottosemigruppo generato da X è proprio l'insieme di tali prodotti. Ad esempio l'insieme $D = \{2^n \mid n \geq 1\}$ è il sottosemigruppo generato da $\{2\}$ nel semigruppato (\mathbb{Z}, \cdot) . Infatti D è un sottosemigruppo e contiene $\{2\}$. Sia S un sottosemigruppo di (\mathbb{Z}, \cdot) con $2 \in S$; allora si prova per induzione su n , che $2^n \in S$. Infatti $2^1 = 2 \in S$ e se $2^n \in S$ allora $2^{n+1} = 2^n 2 \in S$ dato che S è chiuso. Quindi $D \subseteq S$ per ogni sottosemigruppo S che contiene $\{2\}$, e dunque D è il sottosemigruppo generato da $\{2\}$.

Con un altro esempio, sia X un insieme e $Y, Z, U \subseteq X$; allora il sottosemigruppo generato da $\{Y, Z, U\}$ in $(\mathcal{P}(X), \cap)$ è $\{Y, Z, U, Y \cap Z, Y \cap U, Z \cap U, Y \cap Z \cap U\}$.

Definizione. Una operazione $*$ sull'insieme A si dice **commutativa** se, per ogni $a, b \in A$ risulta:

$$a * b = b * a .$$

Esempi. 1) Sono commutative le operazioni di somma e moltiplicazione in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; mentre non è commutativa la sottrazione.

2) Sono commutative le operazioni \cap, \cup, Δ sull'insieme $\mathcal{P}(X)$.

3) Se $|X| \geq 2$ la composizione in X^X non è commutativa. Infatti siano a, b elementi distinti di X e si considerino le applicazioni $f, g: X \rightarrow X$ definite da

$$f(x) = a \text{ per ogni } x \in X \quad \text{e} \quad g(x) = b \text{ per ogni } x \in X ;$$

allora $(f \circ g)(a) = f(g(a)) = f(b) = a$, mentre $(g \circ f)(a) = g(f(a)) = g(a) = b$. Quindi $f \circ g \neq g \circ f$.

Se $|X| \geq 3$ la composizione in $Sym(X)$ non è commutativa. Infatti siano a, b, c elementi distinti di X ; si considerino le permutazioni $\sigma, \tau: X \rightarrow X$ definite da

$$\sigma(a) = b, \sigma(b) = a, \sigma(x) = x \text{ per ogni altro } x \in X$$

$$\tau(a) = c, \tau(c) = a, \tau(x) = x \text{ per ogni altro } x \in X$$

e si provi che $\sigma \circ \tau \neq \tau \circ \sigma$.

Non si dà un nome particolare ad un insieme dotato di operazione commutativa. Se (A, \cdot) è un semigruppato e l'operazione è commutativa, si dice che (A, \cdot) è un semigruppato commutativo.

Elementi identici e monoidi

Definizione. Sia (A, \cdot) un semigruppato. Un elemento $e \in A$ si dice **elemento identico** (o identità, o elemento neutro) se, per ogni $a \in A$:

$$a \cdot e = a = e \cdot a .$$

Proposizione 1.2 Sia (A, \cdot) un semigruppato, e siano e, e' elementi identici su A . Allora $e = e'$.

Dimostrazione. Se e, e' sono elementi identici, si ha:

$$e = e \cdot e' = e'$$

dove la prima uguaglianza sussiste perchè e' è un elemento identico, e la seconda perchè e è un elemento identico.

Dunque se un semigruppoo (A, \cdot) ha un elemento identico, esso è unico. Lo si denota, in generale, con 1_A .

Definizione. Un semigruppoo dotato di elemento identico si dice **monoide**.

Esempi. 1) Sono monoidi i semigruppoo $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ (l'elemento identico è 0); sono monoidi i semigruppoo $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ (l'elemento identico è 1)

2) Se X è un insieme e $A = \mathcal{P}(X)$, allora

(A, \cap) è un monoide, con identità X ;

(A, \cup) è un monoide, con identità \emptyset ;

(A, Δ) è un monoide, con identità \emptyset .

3) Se X è un insieme non vuoto, allora (X^X, \circ) e $(Sym(X), \circ)$ sono monoidi con elemento identico ι_X .

Un monoide (M, \cdot) si dice *commutativo* se l'operazione \cdot è commutativa.

Definizione. Un sottoinsieme B di un monoide (M, \cdot) si dice **sottomonoido** se

$$(1) \quad B \text{ è chiuso} \quad (2) \quad 1_M \in B .$$

Esempi. 1) Pwr $n \in \mathbb{N}$, l'insieme $\{m \in \mathbb{N} \mid m \geq n\} \cup \{0\}$ è un sottomonoido di $(\mathbb{N}, +)$.

2) Se $r \in \mathbb{R}$, allora gli insiemi $\{r^n \mid n \in \mathbb{N}\}$ e $\{r^n \mid n \in \mathbb{Z}\}$ sono sottomonoidi di (\mathbb{R}, \cdot) .

3) Sia X un insieme non vuoto e fissiamo $x \in X$. L'insieme $S_x = \{f \in X^X \mid f(x) = x\}$ è un sottomonoido del monoide (X^X, \circ) . Infatti, $\iota_X \in S_x$ (perchè $\iota_X(x) = x$), e per ogni $f, g \in S_x$, $(f \circ g)(x) = f(g(x)) = f(x) = x$ dunque $f \circ g \in S_x$.

Un monoide M ha almeno due sottomonoidi: M stesso e $\{1_M\}$. Per i sottomonoidi valgono inoltre le osservazioni fatte per i sottosemigruppoo. In particolare l'intersezione di una famiglia di sottomonoidi di un monoide M è un sottomonoido, e, se X è un sottoinsieme di M , il sottomonoido generato da X è l'intersezione di tutti i sottomonoidi che contengono X .

Ad esempio il sottomonoido di (\mathbb{Z}, \cdot) generato dall'insieme $\{2\}$ è $\{2^n \mid n \geq 0\}$ (infatti per definizione deve contenere $1 = 2^0$).

Esercizio. Si determini il sottomonoido S generato da $2, 3$ in $(\mathbb{N}, +)$.

Soluzione. Osserviamo che se un sottomonoido di $(\mathbb{N}, +)$ contiene l'elemento n , allora, per la chiusura rispetto alla somma, deve contenere tutti i multipli positivi di n , incluso 0. Quindi S che è un sottomonoido che contiene 2, contiene tutti i numeri pari positivi. Sia ora $d \geq 3$ un numero dispari, allora $d - 3$ è un numero pari positivo, quindi $d - 3 \in S$ e poichè S è chiuso, $d = 3 + (d - 3) \in S$. Dunque $S \supseteq \mathbb{N} \setminus \{1\}$. Ora, si verifica facilmente che $\mathbb{N} \setminus \{1\}$ è un sottomonoido di $(\mathbb{N}, +)$, quindi $S = \mathbb{N} \setminus \{1\}$.

Inversi e gruppi.

Proposizione 1.3 Sia (M, \cdot) un monoide con elemento identico 1_M , e sia $a \in M$. Se b, c sono elementi di M tali che $ba = 1_M = ac$, allora $b = c$.

Dimostrazione. Siano $a, b, c \in M$ come nelle ipotesi. Allora :

$$b = b \cdot 1_M = b(ac) = (ba)c = 1_M \cdot c = c .$$

Un elemento b tale che $ba = 1_M$ si dice inverso sinistro di a ; un elemento c tale che $ac = 1_M$ si dice inverso destro di a . Mentre è possibile che un elemento di un monoide abbia diversi inversi sinistri o diversi inversi destri (si pensi alle applicazioni), la proposizione precedente implica che se un elemento a di un monoide ha un inverso sinistro e un inverso destro allora questi coincidono (in tal caso a ha, quindi, un unico inverso sinistro che è anche l'unico inverso destro).

Definizione. Sia (M, \cdot) un monoide con elemento identico 1_M . Un elemento $a \in M$ si dice **invertibile** se esiste $b \in M$ tale che

$$a \cdot b = 1_M = b \cdot a .$$

in tal caso b è unico, si denota con a^{-1} e si chiama l'**elemento inverso** di a in M .

Dunque, per la Proposizione 1.3, un elemento è invertibile se e solo se ha un inverso sinistro ed un inverso destro. E' inoltre chiaro che se il monoide M è commutativo, allora la condizione $ba = 1_M$ implica $ab = 1_M$ e quindi una delle due è sufficiente a stabilire che b è inverso di a .

L'elemento identico 1_M di un monoide M è invertibile, e coincide con il proprio inverso.

Proposizione 1.4 Sia (M, \cdot) un monoide con elemento identico 1_M , e siano a, b elementi invertibili di M . Allora

- (i) a^{-1} è invertibile e $(a^{-1})^{-1} = a$;
- (ii) ab è invertibile e $(ab)^{-1} = b^{-1}a^{-1}$.

Dimostrazione. La dimostrazione è essenzialmente la stessa che abbiamo già visto per le applicazioni.

(i) Poichè

$$(a^{-1})a = 1_M = a(a^{-1})$$

si ha che a^{-1} è invertibile e, per l'unicità dell'inverso, $(a^{-1})^{-1} = a$.

(ii) Se a e b sono invertibili:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1_M b = b^{-1}b = 1_M ;$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1_M a^{-1} = aa^{-1} = 1_M$$

dunque ab è invertibile e, per l'unicità dell'inverso, $(ab)^{-1} = b^{-1}a^{-1}$.

Dalla Proposizione 4 e dall'osservazione che la precede, segue che, se M è un monoide, il sottoinsieme $U(M)$ di tutti gli elementi invertibili di M è un sottomonoido.

Esempi. 1) Gli elementi invertibili del monoide (\mathbb{Z}, \cdot) sono 1 e -1, quindi $U(\mathbb{Z}, \cdot) = \{1, -1\}$. Gli elementi invertibili del monoide (\mathbb{Q}, \cdot) sono tutti i numeri razionali diversi da 0, quindi $U(\mathbb{Q}, \cdot) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0, \}$ (e similmente per \mathbb{R} e \mathbb{C}).

2) Sia X un insieme e sia Y un elemento invertibile del monoide $(\mathcal{P}(X), \cap)$, allora esiste $Z \in \mathcal{P}(X)$ tale che $Y \cap Z = X$ (X è l'elemento neutro), e quindi deve essere $Y = X$; dunque $U(\mathcal{P}(X), \cap) = \{X\}$. Similmente si osserva che $U(\mathcal{P}(X), \cup) = \{\emptyset\}$.

3) Se X è un insieme, $U(X^X, \circ) = \text{Sym}(X)$.

Definizione. Un **gruppo** è un *monoide in cui ogni elemento è invertibile*.

Quindi un insieme con operazione (G, \cdot) è un gruppo se e solo se sono soddisfatte le seguenti condizioni:

1. Per ogni $a, b, c \in G$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. Esiste $1_G \in G$ tale che, per ogni $a \in G$: $a 1_G = a = 1_G a$.
3. Per ogni $a \in G$ esiste $b \in G$ tale che $a \cdot b = 1_G = b \cdot a$ (tale b è quindi unico e si denota con a^{-1}).

Esempi. 1) Sono gruppi i monoidi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ e (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , (\mathbb{C}^*, \cdot) , dove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

2) Se X è un insieme non vuoto, allora $(\text{Sym}(X), \circ)$ è un gruppo, detto il *Gruppo Simmetrico* su X .

3) Se X è un insieme, allora $(\mathcal{P}(X), \Delta)$ è un gruppo. Infatti, l'elemento neutro è \emptyset e, per ogni $Y \in \mathcal{P}(X)$, $Y \Delta Y = \emptyset$, quindi Y coincide con il proprio inverso. Non sono invece gruppi (tranne nel caso banale $X = \emptyset$) i monoidi $(\mathcal{P}(X), \cap)$ e $(\mathcal{P}(X), \cup)$.

4) Se (M, \cdot) è un monoide, allora l'insieme $U(M)$ degli elementi invertibili di M è un gruppo rispetto alla operazione indotta da M .

Un gruppo si dice **commutativo** (o **abeliano**) se l'operazione è commutativa. Per i gruppi (o monoidi) commutativi, a volte è conveniente utilizzare la cosiddetta *notazione additiva* in cui l'operazione si denota con il simbolo $+$ (mentre la notazione che usiamo in generale, in cui il simbolo dell'operazione è un puntino oppure viene omissa, si dice moltiplicativa). In notazione additiva il simbolo per l'elemento neutro è 0_M (o, semplicemente, 0); se $(A, +)$ è un monoide commutativo, un elemento $a \in A$ è invertibile se esiste $b \in A$ tale che $a + b = 0$, in tal caso si scrive $b = -a$ (invece di $b = a^{-1}$) e $-a$ si chiama *l'opposto* di a . L'enunciato della Proposizione 4 diventa: se a, b sono invertibili, $-(-a) = a$ e $-(a + b) = -b + (-a) = -a + (-b)$ (perchè M è commutativo). Infine, se $(A, +)$ è un gruppo, e $x, y \in A$, si adotta la convenzione di scrivere $x + (-y) = x - y$.

Esercizio. Sia G un gruppo, e sia $g^{-1} = g$ per ogni $g \in G$. Si dimostri che G è commutativo.

Soluzione. Siano $g, h \in G$. Allora $hg = h^{-1}g^{-1} = (gh)^{-1} = gh$.

Potenze. Sia G un gruppo e sia $g \in G$ e $z \in \mathbb{Z}$. La potenza z -esima g^z di g si definisce induttivamente nella maniera seguente:

$$g^0 = 1_G ;$$

$$\text{se } z \geq 0 , \quad g^{z+1} = g^z g ;$$

$$\text{se } z \leq -1 , \quad g^z = (g^{-1})^{-z} .$$

In pratica, se $z \geq 0$,

$$g^z = \underbrace{g \cdot g \cdot \dots \cdot g}_z \text{ volte}$$

Dalla definizione, tenendo conto che $(g^{-1})^{-1} = g$ segue in particolare che, per ogni $z \in \mathbb{Z}$,

$$g^1 = g, \quad g^{-z} = (g^{-1})^z.$$

Osserviamo anche che, se $n < 0$:

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

Abbiamo dato la definizione di potenze di un elemento in un gruppo, ma le stesse definizioni valgono, limitando opportunamente gli esponenti, ad elementi in un semigrupp o in un monoide. Così, in un semigrupp le potenze di un elemento sono definite come sopra per esponenti $z \geq 1$, e nel caso di un monoide per esponenti $z \geq 0$. Similmente, la seguente proposizione, che enunciamo e dimostriamo per i gruppi, sussiste, restringendo il dominio degli esponenti, anche per semigruppi e monoidi.

Proposizione 1.5 *Sia G un gruppo, $g \in G$ e siano $n, m \in \mathbb{Z}$. Allora*

$$(i) \quad g^{n+m} = g^n g^m;$$

$$(ii) \quad g^{nm} = (g^n)^m.$$

Dimostrazione. (i) Se $m = 0$, $g^{n+0} = g^n = g^n \cdot 1_G = g^n g^0$.

Sia ora $m \geq 0$ e procediamo per induzione su m ; se, per ipotesi induttiva, $g^{n+m} = g^n g^m$ allora:

$$\begin{aligned} g^{n+(m+1)} &= g^{(n+m)+1} = g^{n+m} g^1 && \text{(per definizione)} \\ &= (g^n g^m) g^1 && \text{(per ipotesi induttiva)} \\ &= g^n (g^m g^1) = g^n g^{m+1}. && \text{(per definizione)} \end{aligned}$$

Sia ora $m \leq -1$. Allora, per le osservazioni fatte sopra, e per il caso precedente :

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

(ii) Se $m = 0$ allora $g^{n0} = g^0 = 1_G = (g^n)^0$. Se $m = 1$, $g^{n1} = g^n = (g^n)^1$.

Sia ora $m \geq 1$ e procediamo per induzione su m ; se, per ipotesi induttiva, $g^{nm} = (g^n)^m$ allora, usando il punto (i) :

$$g^{n(m+1)} = g^{nm+n} = g^{nm} g^n = (g^n)^m g^n = (g^n)^m (g^n)^1 = (g^n)^{m+1}.$$

Quindi la proprietà è provata per $m \geq 1$. Ora osserviamo che per il caso (i), $g^{-n} g^n = g^{-n+n} = g^0 = 1_G$ e quindi, per ogni $n \in \mathbb{Z}$,

$$g^{-n} = (g^n)^{-1}.$$

Se $m \leq -1$, usando il caso positivo, si ha quindi

$$g^{nm} = g^{(-n)(-m)} = (g^{-n})^{-m} = ((g^n)^{-1})^{-m} = (g^n)^m.$$

Notazione additiva. In notazione additiva è preferibile adottare una diversa notazione per le potenze di un elemento, sotto forma di multipli. Se $(A, +)$ è un gruppo additivo, $a \in A$ e $n \in \mathbb{N}$, si scrive

$$\begin{aligned} 0a &= 0_A ; \\ na &= a + a + \dots + a \quad (\text{n volte}); \\ (-n)a &= n(-a) = -(na) . \end{aligned}$$

e la Proposizione 5 diventa: per ogni $a \in A$ e $m, n \in \mathbb{Z}$,

$$(n + m)a = na + ma \quad (nm)a = n(ma) .$$

In generale, se G è un gruppo, $x, y \in G$ e $z \in \mathbb{Z}$ allora $(xy)^z \neq x^z y^z$. Infatti, ad esempio:

$$(xy)^2 = x^2 y^2 \Leftrightarrow xyxy = xxyy \Leftrightarrow x^{-1}xyxy^{-1} = x^{-1}xxyyy^{-1} \Leftrightarrow yx = xy .$$

Quello che si può dire è il seguente fatto, la cui facile dimostrazione lasciamo per esercizio.

Proposizione. *Sia G un gruppo, $g, h \in G$ con $gh = hg$. Allora, per ogni $z \in \mathbb{Z}$, $(gh)^z = g^z h^z$.*

Si dice che un semigruppoo S soddisfa la legge di cancellazione se, per ogni $a, b, c \in S$, da $ab = ac$ segue $b = c$, e da $ba = ca$ segue $b = c$. Ad esempio, il monoide (\mathbb{Z}^*, \cdot) soddisfa la legge di cancellazione, mentre, in generale, il monoide (X^X, \circ) non la soddisfa (lo si verifichi con un esempio). Una proprietà elementare ma fondamentale di un gruppo è che esso soddisfa la legge di cancellazione.

Proposizione 1.6 (Legge di cancellazione). *Sia G un gruppo, e siano $a, b, c \in G$. Se $ab = ac$ allora $b = c$. Se $ba = ca$ allora $b = c$.*

Dimostrazione. Sia G un gruppo, e siano $a, b, c \in G$ tali che $ab = ac$. Allora, moltiplicando a sinistra per a^{-1} si ha

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

La dimostrazione che $ba = ca \Rightarrow b = c$ si fa allo stesso modo moltiplicando a destra per a^{-1} .

Esercizio. Sia G un gruppo, e siano $g, h \in G$ tali che $g^2 h^2 = h^2 g^2$ e $(gh)^3 = g^3 h^3$. Si provi che $gh = hg$.

Soluzione. Per le ipotesi su g, h si ha $(gh)^3 = g^3 h^3 = (gg^2)(h^2 h) = g(g^2 h^2)h = gh^2 g^2 h$; cioè $(gh)(gh)(gh) = (gh)(hg)(gh)$ e quindi, per la legge di cancellazione, $gh = hg$.

Matrici.

Un esempio molto importante di operazione, e strettamente legato alla composizione di applicazioni, è il prodotto (righe per colonne) di matrici. Lo studio delle matrici è parte del corso di Geometria. Richiamiamo qui, senza dimostrazione, solo alcuni fatti.

Sia $1 \leq n \in \mathbb{N}$. Una **Matrice quadrata di ordine n** a coefficienti reali è una tabella

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

dove i coefficienti a_{ij} sono numeri reali. Denoteremo con $M_n(\mathbb{R})$ l'insieme di tutte le matrici quadrate di ordine n a coefficienti reali.

Se $A = (a_{ij}) \in M_n(\mathbb{R})$, allora, per ogni $i = 1, 2, \dots, n$ la n-upla di numeri reali

$$(a_{i1} \ a_{i2} \ \cdots \ a_{in})$$

è detta **i-esima riga** della matrice A. Mentre la **i-esima colonna** di A è

$$(a_{1i} \ a_{2i} \ \cdots \ a_{ni}).$$

Il **prodotto** di due matrici quadrate di ordine n, $A = (a_{ij})$, $B = (b_{ij})$ è definito nella maniera seguente: $(a_{ij})(b_{ij}) = (c_{ij})$ dove, per ogni $i, j = 1, 2, \dots, n$

$$c_{ij} = \sum_{r=1}^n a_{ir} b_{rj}.$$

Cioè il coefficiente di posto ij nella matrice prodotto è

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \dots + a_{in}b_{nj}$$

ovvero il prodotto (scalare) della i-esima riga di A per la j-esima colonna di B.

Esempi:

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + (-\frac{1}{2} \cdot \frac{1}{2}) & 1 \cdot (-1) + (-\frac{1}{2}) \cdot (-2) \\ -2 \cdot 0 + 3 \cdot \frac{1}{2} & -2 \cdot (-1) + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{3}{2} & -4 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 1 \\ 3 & 0 & 1 \\ -2 & \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 5 & \frac{1}{4} & 2 \\ 3 & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Si verifica che, per ogni $n \geq 1$ il prodotto di matrici quadrate di ordine n è una operazione associativa. Inoltre la **matrice identica**

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

è l'elemento identico. Quindi $(M_n(\mathbb{R}), \cdot)$ è un monoide. Se $n \geq 2$ il prodotto di matrici non è commutativo, ad esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Ad ogni matrice quadrata reale A è associato un numero reale $|A| = \text{Det}(A)$ detto **determinante** di A . La definizione generale di determinante di una matrice e le sue proprietà sono parte del corso di Geometria. Qui ricordo solo il caso di matrici di ordine $n = 2, 3$. (Una matrice di ordine 1 è un numero reale e coincide con il suo determinante)

$$\text{Det} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$$\text{Det} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} \text{Det} \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + (-1)a_{12} \text{Det} \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} \text{Det} \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Ad esempio

$$\begin{aligned} \text{Det} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} &= 1 \cdot \text{Det} \begin{pmatrix} 2 & \frac{1}{2} \\ 1 & 0 \end{pmatrix} + (-1)0 \cdot \text{Det} \begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} + (-1) \cdot \text{Det} \begin{pmatrix} 0 & 2 \\ -\frac{1}{2} & 1 \end{pmatrix} = \\ &= 1(2 \cdot 0 - 1 \cdot \frac{1}{2}) - 0 - 1(0 \cdot 1 - 2(-\frac{1}{2})) = -\frac{1}{2} - 0 - 1 = -\frac{3}{2}. \end{aligned}$$

Una proprietà molto importante del determinante è che per ogni $A, B \in M_n(\mathbb{R})$:

$$\text{Det}(A \cdot B) = \text{Det}(A)\text{Det}(B).$$

Inoltre, per ogni $n \geq 1$, $\text{Det}(I_n) = 1$.

Un altro fatto fondamentale (che si vedrà al corso di Geometria) è che una matrice $A \in M_n(\mathbb{R})$ è **invertibile** se e solo se $\text{Det}(A) \neq 0$.

Dunque $\{ A \in M_n(\mathbb{R}) \mid \text{Det}(A) \neq 0 \}$ è l'insieme degli elementi invertibili di $M_n(\mathbb{R})$ e quindi, con l'operazione di prodotto righe per colonne, è un **gruppo** che si denota con $GL(n, \mathbb{R})$ e si chiama il gruppo Lineare Generale di ordine n su \mathbb{R} .

Rimandiamo al corso di Geometria per le regole generali per determinare la inversa di una matrice invertibile. Qui riporto, al fine di comprendere esempi ed esercizi, il caso $n = 2$.

Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R})$ (quindi $\Delta = \text{Det}(A) \neq 0$). Allora

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}.$$

Ha senso considerare matrici quadrate, prodotto di matrici, e determinanti, anche a coefficienti in \mathbb{Q} , \mathbb{C} o in \mathbb{Z} , o più in generale su ogni insieme R dotato di operazioni di somma e moltiplicazione con determinate proprietà (gli anelli commutativi, che studieremo più avanti). L'insieme di esse costituisce un monoide e si denota con $M_n(\mathbb{Q})$, $M_n(\mathbb{Z})$ etc.

Nel caso di coefficienti in \mathbb{Z} risulta che le matrici invertibili in $M_n(\mathbb{Z})$ sono quelle il cui determinante è 1 o -1, e costituiscono un gruppo denotato con $GL(n, \mathbb{Z})$.

Omomorfismi e isomorfismi

Definizione. 1) Siano (S, \cdot) e $(S', *)$ due semigrupp. Un **omomorfismo** (di semigrupp) di S in S' è una applicazione $\phi: S \rightarrow S'$ tale che, per ogni $x, y \in S$,

$$\phi(x \cdot y) = \phi(x) * \phi(y).$$

2) Siano (M, \cdot) e $(M', *)$ due monoidi. Un **omomorfismo** (di monoidi) di M in M' è una applicazione $\phi: M \rightarrow M'$ tale che, per ogni $x, y \in M$,

$$\phi(x \cdot y) = \phi(x) * \phi(y) \quad \text{e} \quad \phi(1_M) = 1_{M'} .$$

Un **isomorfismo** di semigrupperi (monoidi) è un **omomorfismo biiettivo**. Un **automorfismo** di un semigruppero (monoidi) S è un isomorfismo di S in se stesso.

Proposizione 1.7 *Siano (S, \cdot) , $(S', *)$ semigrupperi (monoidi), e sia $\phi: S \rightarrow S'$ un isomorfismo. Allora $\phi^{-1}: S' \rightarrow S$ è un isomorfismo.*

Dimostrazione. Siano $a, b \in S'$. Allora, poichè ϕ è un omomorfismo

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

e, poichè ϕ è iniettiva, si ha

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

(se S è monoidi, $\phi(1_S) = 1_{S'}$ e dunque $\phi^{-1}(1_{S'}) = 1_S$) quindi ϕ^{-1} è un omomorfismo; poichè è anche biettiva, ϕ^{-1} è un isomorfismo.

Osserviamo che se (S, \cdot) è un semigruppero (monoidi), l'applicazione identica ι_S è un isomorfismo di S in se stesso (quindi un automorfismo). Un'altra proprietà importante degli omomorfismi e isomorfismi è che la composizione di due di essi è ancora un omomorfismo.

Proposizione 1.8 *Siano (A, \cdot) , (B, \cdot) , (C, \cdot) semigrupperi (monoidi), e $\phi: A \rightarrow B$, $\psi: B \rightarrow C$ omomorfismi. Allora $\psi \circ \phi: A \rightarrow C$ è un omomorfismo. Se ϕ e ψ sono isomorfismi, $\psi \circ \phi$ è un isomorfismo.*

Dimostrazione. Siano $a, b \in A$. Allora, poichè ϕ e ψ sono omomorfismi

$$\psi \circ \phi(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi(a))(\psi \circ \phi(b))$$

dunque $\psi \circ \phi$ è un omomorfismo. Se ϕ e ψ sono isomorfismi, allora sono biettive e quindi $\psi \circ \phi$ è biettiva e pertanto è un isomorfismo.

Definizione. 1) Siano (G, \cdot) , $(G', *)$ gruppi. Un **omomorfismo** (di gruppi) di G in G' è una applicazione $\phi: G \rightarrow G'$ tale che, per ogni $x, y \in G$,

$$\phi(x \cdot y) = \phi(x) * \phi(y) .$$

2) Un **isomorfismo** tra i gruppi (G, \cdot) e $(G', *)$ è un **omomorfismo biiettivo** di G in G' .

Osserviamo che nella definizione di omomorfismo di gruppi non viene richiesto esplicitamente, come per i monoidi, che $\phi(1_G) = 1_{G'}$. La ragione è che nel caso dei gruppi ciò viene necessariamente.

Proposizione 1.9 Siano (G, \cdot) , $(G', *)$ gruppi, e sia $\phi : G \rightarrow G'$ un omomorfismo. Allora $\phi(1_G) = 1_{G'}$ e per ogni $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.

Dimostrazione. Sia $b = \phi(1_G)$. Allora

$$b * b = \phi(1_G) * \phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) = b$$

moltiplicando a destra per b^{-1} si ottiene $b = b * b * b^{-1} = b * b^{-1} = 1_{G'}$.

Sia ora $g \in G$, allora

$$\phi(g^{-1}) * \phi(g) = \phi(g^{-1} \cdot g) = \phi(1_G) = 1_{G'}$$

e quindi $\phi(g^{-1}) = (\phi(g))^{-1}$.

Due gruppi G , G' si dicono **isomorfi** se esiste un isomorfismo da G in G' . Si scrive in tal caso $G \simeq G'$. Dalle proposizioni e osservazioni precedenti segue che $G \simeq G$ (mediante l'applicazione identica), se $G \simeq G'$ allora $G' \simeq G$, e che se $G \simeq G'$ e $G' \simeq G''$ allora $G \simeq G''$. (si osservi che una applicazione tra due gruppi G, G' è un omomorfismo (isomorfismo) di gruppi se e solo se è un omomorfismo (isomorfismo) di G in G' considerati come semigrupp). Similmente si definiscono semigrupp e monoidi isomorfi e si fanno le stesse osservazioni, ma in questo corso ci occuperemo principalmente di gruppi, quindi esponiamo i concetti con particolare riferimento a questo tipo di struttura.

Come già suggerisce la Proposizione 9, se due gruppi sono isomorfi allora soddisfano le stesse proprietà strutturali come gruppi. Tutto ciò che, relativamente all'operazione, si può affermare per uno dei due gruppi vale, passando attraverso la corrispondenza biunivoca stabilita dall'isomorfismo, anche per l'altro gruppo. Parlando informalmente, si giunge a dire che due gruppi isomorfi sono "lo stesso" gruppo.

Esempi. 1) Sia P l'insieme dei numeri reali strettamente maggiori di zero. Allora P è un gruppo con l'operazione di moltiplicazione. L'applicazione logaritmo naturale $P \rightarrow \mathbb{R}$ definita da, per ogni $x \in P$, $x \mapsto \log_e(x)$ è un isomorfismo del gruppo moltiplicativo (P, \cdot) nel gruppo additivo $(\mathbb{R}, +)$. Infatti, è biettiva e per ogni $x, y \in P$, $\log_e(xy) = \log_e(x) + \log_e(y)$. L'applicazione inversa è la funzione esponenziale, ed è un isomorfismo da $(\mathbb{R}, +)$ in (P, \cdot) . (naturalmente si ottiene un isomorfismo anche considerando il logaritmo in una qualsiasi base positiva $\neq 1$ fissata)

2) Sia X un insieme. Allora l'applicazione $\mathcal{C} : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ definita da, per ogni $Y \in \mathcal{P}(X)$, $\mathcal{C}(Y) = X \setminus Y$ è un isomorfismo del monoide $(\mathcal{P}(X), \cap)$ nel monoide $(\mathcal{P}(X), \cup)$. Infatti, \mathcal{C} è biettiva (coincide con la propria inversa), e per ogni $X, Z \in \mathcal{P}(X)$ si ha, per la legge di De Morgan (Parte I, Prop. 4), $\mathcal{C}(Y \cup Z) = X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z) = \mathcal{C}(Y) \cap \mathcal{C}(Z)$.

3) L'applicazione $Det : M_2(\mathbb{R}) \rightarrow \mathbb{R}$ definita nelle pagine precedenti, è un omomorfismo del monoide $M_2(\mathbb{R})$ nel monoide (\mathbb{R}, \cdot) , e l'applicazione $Det : GL(2, \mathbb{R}) \rightarrow \mathbb{R}^*$ è un omomorfismo del gruppo $GL(2, \mathbb{R})$ nel gruppo (\mathbb{R}^*, \cdot) . Le stesse affermazioni valgono per matrici di qualsiasi ordine $n \geq 1$.

4) Sia G un gruppo, e sia $g \in G$. La proposizione 5 implica che la applicazione $\gamma : \mathbb{Z} \rightarrow G$ definita da, per ogni $z \in \mathbb{Z}$, $\gamma(z) = g^z$ è un omomorfismo del gruppo $(\mathbb{Z}, +)$ nel gruppo G .

Definizione. Un omomorfismo di un gruppo G in se stesso si dice **endomorfismo** di G ; un isomorfismo di G in se stesso si dice **automorfismo** di G .

Dalla Proposizione 8 e l'osservazione che la precede segue che l'insieme $End(G)$ di tutti gli endomorfismi di un gruppo G è un monoide rispetto all'operazione di composizione

(è un sottomonoido di (G^G, \circ)). Dalle Proposizioni 7, 8 segue inoltre il fatto importante che l'insieme $Aut(G)$ di tutti gli automorfismi di un gruppo G è un gruppo rispetto all'operazione di composizione; $(Aut(G), \circ)$ si chiama **Gruppo degli Automorfismi** di G .

Esercizio. Sia G un gruppo. Si dimostri che l'applicazione $f : G \rightarrow G$ definita da, per ogni $g \in G$, $f(g) = g^{-1}$ è un automorfismo se e solo se G è commutativo.

Soluzione. Sia G un gruppo. Supponiamo che l'applicazione f sia un omomorfismo, allora per ogni $g, h \in G$,

$$g^{-1}h^{-1} = f(g)f(h) = f(gh) = (gh)^{-1},$$

dunque $gh = ((gh)^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = (h^{-1})^{-1}(g^{-1})^{-1} = hg$, e quindi G è commutativo.

Viceversa, sia G commutativo. Allora, per ogni $g, h \in G$,

$$f(gh) = (gh)^{-1} = (hg)^{-1} = g^{-1}h^{-1} = f(g)f(h)$$

dunque f è un omomorfismo. Poichè f è una applicazione biettiva (coincide con la propria inversa), essa è un automorfismo.

Avremo più avanti ancora molte cose da dire sugli omomorfismi e isomorfismi tra gruppi, e sul gruppo degli automorfismi.

ESERCIZI

1. Sia S un insieme non vuoto. Si provi che l'operazione definita su S da $(a, b) \mapsto a$ è associativa.

2. Sia X un insieme e sia $Y \subseteq X$. Si provi che $(\mathcal{P}(Y), \cup)$ è un sottomonoido del monoido $(\mathcal{P}(X), \cup)$.

3. Sia M un monoido e X un insieme non vuoto. Sull'insieme M^X di tutte le applicazioni di X in M si definisca una operazione $(f, g) \mapsto f \cdot g$ ponendo, per ogni $f, g \in M^X$ e ogni $x \in X$: $(f \cdot g)(x) = f(x)g(x)$. Si provi che (M^X, \cdot) è un monoido.

4. Sia M un monoido e sia $a \in M$. Si provi che se, per qualche $n \geq 1$, a^n è invertibile allora a è invertibile.

5. Siano (A, \cdot) , $(B, *)$ semigrupp. Sul prodotto diretto $A \times B$ si definisca una operazione ponendo, per ogni $(a, b), (a_1, b_1) \in A \times B$:

$$(a, b)(a_1, b_1) = (a \cdot a_1, b * b_1).$$

Si dimostri che, con tale operazione, $A \times B$ è un semigrupp. Si provi che se A e B sono monoidi (gruppi), allora $A \times B$ è un monoido (gruppo).

6. Nel monoido $(\mathbb{N}^{\mathbb{N}}, \circ)$ si consideri l'elemento f definito da, per ogni $n \in \mathbb{N}$

$$f(n) = \begin{cases} n & \text{se } n \text{ è pari} \\ 2n & \text{se } n \text{ è dispari} \end{cases}$$

Si determini il sottomonoido generato da f .

7. Sia M un monoide che soddisfa la legge di cancellazione. Si provi che se M è finito allora è un gruppo. [sugg.: per ogni $a \in M$ si consideri la applicazione da M in se stesso definita da $x \mapsto ax$; usando la proprietà di cancellazione si provi che è iniettiva e quindi ...] Si dica se la stessa affermazione vale se M è infinito.

8. Si provi che nel monoide $M_2(\mathbb{R})$ non vale la legge di cancellazione.

9. Sia $\phi: G \rightarrow G'$ un omomorfismo di gruppi. Procedendo per induzione su n , si provi che, per ogni $x_1, x_2, \dots, x_n \in G$: $\phi(x_1 x_2 \cdots x_n) = \phi(x_1) \phi(x_2) \cdots \phi(x_n)$.

10. Sia (G, \cdot) un gruppo e sia $a \in G$ tale che $ag = ga$ per ogni $g \in G$. Su G si definisca una nuova operazione $*$, ponendo, per ogni $x, y \in G$: $x * y = x \cdot a \cdot y$. Si provi che $(G, *)$ è un gruppo, e che la applicazione

$$\begin{array}{ccc} G & \rightarrow & G \\ x & \mapsto & a^{-1}x \end{array}$$

è un isomorfismo del gruppo (G, \cdot) nel gruppo $(G, *)$.

2 Gruppi e sottogruppi

Sottogruppi

Definizione. Sia G un gruppo. Un sottoinsieme H di G si dice **sottogruppo** (e si scrive $H \leq G$) se soddisfa alle seguenti proprietà

- (1) H è chiuso; cioè, per ogni $x, y \in H$, $xy \in H$;
- (2) $1_G \in H$;
- (3) per ogni $x \in H$, $x^{-1} \in H$.

Un sottogruppo H di un gruppo G è un gruppo rispetto all'operazione indotta da G . Viceversa si può provare che se un sottoinsieme S di un gruppo G è un gruppo rispetto all'operazione indotta, allora è un sottogruppo di G nel senso della definizione data (lo si verifichi per esercizio, il punto essenziale è dimostrare che l'elemento identico di S rispetto all'operazione indotta è proprio 1_G).

Dalla definizione segue immediatamente che se $S \leq H$ e $H \leq G$, allora $S \leq G$. Osserviamo anche che ogni gruppo G ha almeno due sottogruppi: G stesso e $\{1_G\}$. $\{1_G\}$ è detto il *sottogruppo banale* di G , mentre un sottogruppo H si dice *proprio* se $H \neq G$.

In notazione additiva le condizioni affinché un sottoinsieme H di un gruppo additivo A sia un sottogruppo si scrivono:

- (1) $\forall x, y \in H, x + y \in H$
- (2) $0_A \in H$
- (3) $\forall x \in H, -x \in H$.

Esempi 1) (importante) Sia $n \in \mathbb{N}$ e indichiamo con $n\mathbb{Z}$ l'insieme di tutti i multipli interi di n ; cioè

$$n\mathbb{Z} = \{ nz \mid z \in \mathbb{Z} \}.$$

Allora $n\mathbb{Z}$ è un sottogruppo del gruppo $(\mathbb{Z}, +)$. Infatti,

- (1) $0 = n0 \in n\mathbb{Z}$;
- (2) se $x, y \in n\mathbb{Z}$ esistono $z, z_1 \in \mathbb{Z}$ tali che $x = nz$, $y = nz_1$; quindi $x + y = nz + nz_1 = n(z + z_1) \in n\mathbb{Z}$;
- (3) se $x = nz \in n\mathbb{Z}$ allora $-x = -(nz) = n(-z) \in n\mathbb{Z}$.

Vedremo più avanti (Teorema 1) che tutti i sottogruppi del gruppo $(\mathbb{Z}, +)$ sono di questo tipo.

2) Sia X un insieme e sia $Y \subseteq X$. Allora

$$S_Y = \{ f \in \text{Sym}(X) \mid f(Y) = Y \}$$

è un sottogruppo del gruppo $\text{Sym}(X)$. Infatti

- (1) $\iota_X \in S_Y$;
- (2) se $f, g \in S_Y$, allora $(f \circ g)(Y) = f(g(Y)) = f(Y) = Y$, dunque $(f \circ g) \in S_Y$;
- (3) se $f \in S_Y$, allora $f^{-1}(Y) = f^{-1}(f(Y)) = (f^{-1} \circ f)(Y) = \iota_X(Y) = Y$, e dunque $f^{-1} \in S_Y$.

In questi esempi, la prova che determinati sottoinsiemi sono sottogruppi è consistita nel verificare che essi soddisfano alle tre condizioni della definizione di sottogruppo. In genere però risulterà più conveniente utilizzare il criterio stabilito dal seguente Lemma.

Lemma (Criterio per sottogruppi). *Siano G un gruppo e $H \subseteq G$. Allora sono equivalenti:*

- (i) $H \leq G$;
- (ii) $H \neq \emptyset$ e, per ogni $x, y \in H$, $xy^{-1} \in H$.

Dimostrazione. (i) \Rightarrow (ii). Sia $H \leq G$. Allora $1_G \in H$, in particolare è $H \neq \emptyset$. Se $x, y \in H$, allora $y^{-1} \in H$ per il punto (3) della definizione di sottogruppo e quindi $xy^{-1} \in H$ per il punto (1) della definizione. Quindi H soddisfa la condizione (ii).

(ii) \Rightarrow (i). Sia H sottoinsieme di G che verifica la condizione (ii); proviamo che $H \leq G$. Poichè H non è vuoto, esiste $x \in H$ e quindi, per la condizione (ii) applicata alla coppia $x, x \in H$, $1_G = xx^{-1} \in H$.

Sia $h \in H$, allora per quanto visto sopra $1_G, h \in H$ e, per la condizione (ii), $h^{-1} = 1_G h^{-1} \in H$.

Rimane da verificare che H è chiuso. Siano $h, g \in H$; allora, per quanto già dimostrato, $g^{-1} \in H$ e quindi, per la condizione (ii) applicata alla coppia h, g^{-1} , si ha $hg = h(g^{-1})^{-1} \in H$.

Il criterio per sottogruppi a cui facevamo cenno è l'implicazione (ii) \Rightarrow (i) di questo Lemma.

Esempio. Sia $1 \leq n \in \mathbb{N}$. Nell'insieme \mathbb{C} dei numeri complessi, consideriamo il sottoinsieme delle radici n-esime dell'unità:

$$U_n = \{ z \in \mathbb{C}^* \mid z^n = 1 \} .$$

Allora U_n è un sottogruppo del gruppo moltiplicativo (\mathbb{C}^*, \cdot) . Infatti $U_n \neq \emptyset$ perchè $1 \in U_n$, e per ogni $z_1, z_2 \in U_n$ si ha $(z_1 z_2^{-1})^n = z_1^n (z_2^{-1})^n = z_1^n (z_2^n)^{-1} = 1 \cdot 1 = 1$; dunque $z_1 z_2^{-1} \in U_n$. Per il criterio dei sottogruppi, $U_n \leq \mathbb{C}^*$.

Sia ora g un fissato (ma generico) elemento di un gruppo G . Le proprietà delle potenze implicano che l'insieme di tutte le potenze intere di g ,

$$\langle g \rangle = \{ g^z \mid z \in \mathbb{Z} \}$$

è un sottogruppo di G . Si chiama il **sottogruppo ciclico generato** da g . Se H è un qualche sottogruppo di G che contiene g , allora, per la chiusura rispetto a prodotti ed inversi, H deve contenere tutte le potenze intere di g ; cioè $H \supseteq \langle g \rangle$. Quindi $\langle g \rangle$ è il minimo sottogruppo di G che contiene l'elemento g .

Osserviamo che un sottogruppo ciclico è commutativo. Infatti per ogni $g \in G$ e ogni $n, m \in \mathbb{Z}$, $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$.

In *notazione additiva*, il sottogruppo ciclico generato da un elemento a è l'insieme dei multipli interi di a ; ovvero $\langle a \rangle = \{ za \mid z \in \mathbb{Z} \}$. Dimostriamo ora l'importante fatto che tutti i sottogruppi del gruppo additivo $(\mathbb{Z}, +)$ sono ciclici. Per quanto appena osservato, se $a \in \mathbb{Z}$ allora il sottogruppo ciclico generato da a è $a\mathbb{Z} = \{ az \mid z \in \mathbb{Z} \}$.

Teorema 2.1 Sia H un sottogruppo del gruppo additivo \mathbb{Z} . Allora esiste $n \in \mathbb{N}$ tale che $H = n\mathbb{Z}$.

Dimostrazione. Sia $H \leq \mathbb{Z}$. Se $H = \{0\}$ allora $H = 0\mathbb{Z}$.

Supponiamo quindi che $H \neq \{0\}$. Allora esiste $0 \neq a \in H$; poichè H è un sottogruppo, si ha anche $-a \in H$. Ora, uno di questi due elementi di H è un numero positivo non nullo, quindi l'insieme

$$\mathcal{S} = \{ m \in H \mid m > 0 \}$$

è un sottoinsieme non vuoto dei numeri naturali. Sia $n = \min(\mathcal{S})$. Abbiamo osservato sopra che $n\mathbb{Z}$ è un sottogruppo di \mathbb{Z} . Proviamo che $H = n\mathbb{Z}$.

Poichè $n \in H$ ed H è un sottogruppo, H contiene tutti i multipli di n , cioè $n\mathbb{Z} \subseteq H$. Viceversa, sia $b \in H$; poichè $n \neq 0$ possiamo dividere b per n ; esistono cioè $q, r \in \mathbb{Z}$ tali che

$$b = nq + r \quad \text{e} \quad 0 \leq r < n.$$

Ora, $nq \in H$ per quanto visto sopra, e quindi

$$r = b - nq \in H;$$

se fosse $r > 0$ allora $r \in \mathcal{S}$ e quindi, per la scelta di $n = \min(\mathcal{S})$, sarebbe $n \leq r$ che contraddice la proprietà del resto. Dunque $r = 0$, cioè $b = nq \in n\mathbb{Z}$. Quindi $H \subseteq n\mathbb{Z}$ e pertanto $H = n\mathbb{Z}$.

Quindi i sottogruppi di \mathbb{Z} sono tutti e soli i sottoinsiemi del tipo $n\mathbb{Z}$. Osserviamo anche che la dimostrazione del Teorema fornisce un'indicazione, dato $\{0\} \neq H \leq \mathbb{Z}$, per trovare un generatore di H : è il minimo intero positivo non nullo che appartiene ad H .

Applichiamo questo fatto per fare una osservazione interessante. Dati $n, m \in \mathbb{N}$ poniamo

$$n\mathbb{Z} + m\mathbb{Z} = \{ x + y \mid x \in n\mathbb{Z}, y \in m\mathbb{Z} \} = \{ nz_1 + mz_2 \mid z_1, z_2 \in \mathbb{Z} \}.$$

Si dimostri per esercizio che $n\mathbb{Z} + m\mathbb{Z}$ è un sottogruppo di \mathbb{Z} . Proviamo che se $d = \text{MCD}(n, m)$ allora $d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$. Infatti, siano $r, s \in \mathbb{Z}$ tali che $n = ds$, $m = dr$; allora per ogni $z_1, z_2 \in \mathbb{Z}$, $nz_1 + mz_2 = dsz_1 + drz_2 = d(sz_1 + rz_2) \in d\mathbb{Z}$ e quindi $n\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$. Per il viceversa, siano $a, b \in \mathbb{Z}$ tali che $d = na + mb$; allora, per ogni $z \in \mathbb{Z}$, $dz = (na + mb)z = n(az) + m(bz) \in n\mathbb{Z} + m\mathbb{Z}$ e dunque $d\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$. Quindi $d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$.

Si dimostri per esercizio che $n\mathbb{Z} \leq m\mathbb{Z}$ se e solo se $m|n$ e che se $c = \text{m.c.m.}(n, m)$ allora $c\mathbb{Z} = n\mathbb{Z} \cap m\mathbb{Z}$.

Per i sottogruppi vale un analogo della Proposizione 1. La facile dimostrazione è lasciata per esercizio.

Proposizione 2.2 Sia G un gruppo, e siano H, K sottogruppi di G . Allora $H \cap K \leq G$. Più in generale, se \mathcal{F} è una famiglia qualsiasi non vuota di sottogruppi di G , allora $\bigcap_{X \in \mathcal{F}} X$ è un sottogruppo di G .

Osservazione. Dato un gruppo G , l'insieme $\mathcal{S}(G)$ di tutti i sottogruppi di G ordinato per inclusione (di insiemi) è un insieme parzialmente ordinato. La proposizione 2.2 dice, in particolare, che dati $H, K \leq G$ (cioè $H, K \in \mathcal{S}(G)$), $H \cap K$ è il massimo sottogruppo di G contenuto in H ed in K ; cioè $H \cap K$ è l'estremo inferiore di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$.

In generale (vedi esercizio sotto), l'unione insiemistica di due sottogruppi non è un sottogruppo. Tuttavia, dati due sottogruppi H, K del gruppo G , possiamo considerare la famiglia di tutti i

sottogruppi di G che contengono H e K - cioè la famiglia dei maggioranti di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$. Essa è non vuota perchè contiene almeno il sottogruppo G , quindi, per la Proposizione 2.2, ha un minimo che è l'intersezione di tutti i suoi membri. Tale sottogruppo si denota con $\langle H, K \rangle$ ed è pertanto il minimo sottogruppo di G che contiene sia H che K . In altri termini $\langle H, K \rangle$ è l'estremo superiore di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$.

Da quanto osservato, risulta quindi che $(\mathcal{S}(G), \subseteq)$ è un reticolo. Esso si chiama **reticolo dei sottogruppi** di G .

Esercizio. Siano A, B sottogruppi del gruppo G . Si provi che se $G = A \cup B$, allora $G = A$ oppure $G = B$.

Soluzione. Siano A, B sottogruppi propri del gruppo G e supponiamo per assurdo $G = A \cup B$. Ora, $B \not\subseteq A$ perchè se così fosse sarebbe $G = A \cup B = A$ (contro l'ipotesi che A sia un sottogruppo proprio); e similmente $A \not\subseteq B$. Dunque esistono $a \in A \setminus B$ e $b \in B \setminus A$. Considero ab . Se $ab \in A$ allora $b = a^{-1}(ab) \in A$ contro la scelta di b ; quindi $ab \notin A$. Similmente $ab \notin B$. Quindi $ab \notin A \cup B$, assurdo.

Il Gruppo S_3 .

Questo paragrafo è di fatto un esercizio. Illustriamo i concetti introdotti sinora per descrivere il gruppo simmetrico su un insieme di ordine 3. Più avanti studieremo i gruppi simmetrici in generale e più in dettaglio.

Sia S_3 il gruppo simmetrico sull'insieme $\{1, 2, 3\}$, cioè il gruppo di tutte le permutazioni di $\{1, 2, 3\}$. Come sappiamo, S_3 contiene 6 elementi. Ogni elemento $\sigma \in S_3$ può essere descritto mediante la tabella

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$$

(osserviamo che, essendo σ una applicazione biettiva, la seconda riga della tabella contiene tutti gli elementi $\{1, 2, 3\}$). Allora

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Poniamo quindi

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

allora

$$\gamma^2 = \gamma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

componendo ancora con γ si trova $\gamma^3 = \gamma^2 \circ \gamma = \iota$. Quindi $\gamma^2 = \gamma^{-1}$. Se consideriamo un qualunque numero intero z possiamo scrivere $z = 3q + r$ con $r \in \{0, 1, 2\}$, dunque

$$\gamma^z = \gamma^{3q+r} = \gamma^{3q} \circ \gamma^r = (\gamma^3)^q \circ \gamma^r = \iota^q \circ \gamma^r = \iota \circ \gamma^r = \gamma^r ;$$

il sottogruppo ciclico generato da γ (che denotiamo con A) è quindi composto dai tre elementi

$$\iota = \gamma^0, \quad \gamma, \quad \gamma^2.$$

γ si dice un **ciclo** di ordine 3, o un 3-ciclo (perchè permuta ciclicamente i tre elementi 1,2,3). Chiaramente, il gruppo ciclico generato da $\gamma^2 = \gamma^{-1}$ coincide con $A = \langle \gamma \rangle$.

Poniamo ora

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

queste applicazioni "scambiano" due elementi e fissano i rimanenti; si chiamano **trasposizioni**. Allora, per ogni $i = 1, 2, 3$, $\tau_i^2 = \iota$ e quindi, ragionando come abbiamo fatto con γ , il sottogruppo T_i generato da τ_i è

$$T_i = \langle \tau_i \rangle = \{ \iota, \tau_i \}.$$

Abbiamo quindi elencato tutti gli elementi di S_3 . Sono

$$\iota, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3;$$

ed abbiamo determinato tutti i sottogruppi ciclici di S_3 che sono

$$\{ \iota \}, A, T_1, T_2, T_3.$$

In particolare, S_3 non coincide con alcuno dei suoi sottogruppi ciclici; cosa che poteva essere anche stabilita osservando che S_3 non è abeliano, ad esempio

$$\tau_1 \circ \tau_2 = \gamma \neq \gamma^2 = \tau_2 \circ \tau_1$$

(vedremo in seguito che ogni gruppo non commutativo di ordine 6 è isomorfo a S_3 e che i gruppi di ordine minore o uguale a 5 sono commutativi. Quindi S_3 è il più piccolo gruppo non commutativo).

Vediamo ora che i sottogruppi elencati costituiscono l'insieme di tutti i sottogruppi propri di S_3 . Sia $H \leq S_3$ e supponiamo che H contenga due distinte trasposizioni, diciamo τ_1 e τ_2 ; allora H contiene $\tau_2 \circ \tau_1 = \gamma^2$ e $\tau_1 \circ \tau_2 = \gamma$ e quindi contiene anche $\gamma \circ \tau_1 = \tau_3$; dunque $H = S_3$. Similmente si ragiona a partire dalle altre coppie di trasposizioni.

Supponiamo allora che H contenga un'unica trasposizione τ_i ; se $H \neq \langle \tau_i \rangle = T_i$, H contiene γ o γ^2 . Se $\gamma \in H$ allora H contiene $\tau_i \circ \gamma = \tau_{\gamma(i)}$ contro l'assunzione che H contenga un'unica trasposizione. Allo stesso modo, se $\gamma^2 \in H$ allora $\tau_{\gamma(i)} = \gamma^2 \circ \tau_i \in H$ contro l'assunzione su H . Quindi $H = \langle \tau_i \rangle = T_i$.

Infine, se H non contiene trasposizioni, allora $H = \{1\}$ o $H = \langle \gamma \rangle = A$.

In conclusione, i sottogruppi di S_3 sono

$$\{ \iota \}, A, T_1, T_2, T_3, S_3.$$

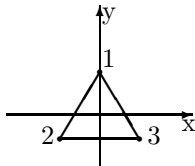
Dal controllo dei loro elementi si vede che se H, K sono sottogruppi propri e distinti di S_3 allora $H \cap K = \{1\} = \{ \iota \}$. Quindi il reticolo dei sottogruppi di S_3 è il seguente:

$$\begin{array}{c} S_3 \\ \cdot \\ A \cdot \quad \cdot T_1 \cdot T_2 \cdot T_3 \\ \cdot \\ \{ \iota \} \end{array}$$

Osserviamo che dallo studio dei sottogruppi fatto sopra segue, tra l'altro, che date due distinte trasposizioni, ad esempio τ_1, τ_2 , il più piccolo sottogruppo che le contiene è S_3 ; si dice allora che S_3 è **generato** dalle trasposizioni τ_1, τ_2 (o che $\{ \tau_1, \tau_2 \}$ è un insieme di generatori di S_3), e si scrive $S_3 = \langle \tau_1, \tau_2 \rangle$. Ogni elemento di S_3 si scrive come un prodotto i cui fattori sono τ_1, τ_2 , o loro inversi (che in questo caso coincidono con gli stessi generatori); infatti: $\iota = \tau_1 \circ \tau_2$, $\gamma = \tau_1 \circ \tau_2$, $\gamma^2 = \tau_2 \circ \tau_1$ e $\tau_3 = \tau_1 \circ \tau_2 \circ \tau_1$.

Osserviamo infine che gli ordini dei sottogruppi di S_3 sono: 1, 2, 3, 6. Ognuno divide l'ordine del gruppo S_3 . Questo fatto è una proprietà fondamentale dei gruppi finiti, che dimostreremo nel prossimo paragrafo. Per il momento abbiamo dovuto impiegare un certo lavoro per studiare il gruppo S_3 (che è un gruppo piccolo); nei paragrafi seguenti introdurremo strumenti più raffinati per lo studio dei gruppi, che alla fine faranno apparire come quasi banale questa discussione di S_3 .

Il gruppo S_3 può anche essere visto (il termine tecnico è *rappresentato*) come il **gruppo delle simmetrie** di un triangolo equilatero. Consideriamo un triangolo equilatero Δ sul piano, con i vertici numerati con 1, 2, 3; per comodità fissiamo un riferimento cartesiano con origine il centro del triangolo e asse y passante per il vertice 1:

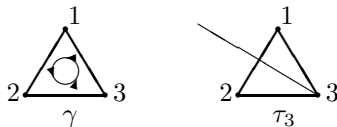


Consideriamo ora l'insieme di tutti i movimenti rigidi del piano che mutano il triangolo Δ in se stesso. Essi sono:

- l'identità;
- le rotazioni (antiorarie) intorno all'origine di $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ radianti (120 e 240 gradi);
- le tre riflessioni lungo gli assi del triangolo.

L'insieme γ di queste sei applicazioni (biettive) del piano in se costituisce un gruppo mediante la composizione, che si chiama gruppo delle simmetrie di Δ ; ad esempio la composizione della rotazione di $\frac{2\pi}{3}$ radianti con la riflessione lungo l'asse y è la riflessione lungo l'asse passante per il vertice 3, l'inversa della rotazione di $\frac{2\pi}{3}$ radianti è la rotazione di $\frac{4\pi}{3}$ radianti, etc.

Ora, si può definire un isomorfismo da Γ in S_3 associando ad ogni elemento di Γ la permutazione da esso indotta sull'insieme $\{1, 2, 3\}$ dei vertici di Δ . Ad esempio, alla rotazione di $\frac{2\pi}{3}$ radianti corrisponde il 3-ciclo γ , alla riflessione lungo l'asse passante per il vertice 3 corrisponde la trasposizione τ_3 , etc. Il sottoinsieme di Γ costituito dalle rotazioni (inclusa l'identità, che è la rotazione di un angolo nullo) è un sottogruppo ciclico, e corrisponde in S_3 al sottogruppo $\langle \gamma \rangle$.



Considerazioni simili si possono fare per un qualunque poligono (regolare) o più in generale una qualunque figura piana. Ad esempio il gruppo delle simmetrie di una circonferenza con centro l'origine è un gruppo infinito che contiene tutte le rotazioni e tutte le riflessioni lungo rette passanti per l'origine. Per **esercizio** si studi il caso di un quadrato; si provi che il suo gruppo delle simmetrie contiene 8 elementi e non è commutativo (tale gruppo si chiama *gruppo diedrale* di ordine 8)

Gruppi Ciclici

Definizione. Un gruppo G si dice **ciclico** se esiste un elemento $g \in G$ tale che G è il sottogruppo generato da g ; cioè

$$G = \langle g \rangle = \{ g^z \mid z \in \mathbb{Z} \}.$$

In tal caso, g si dice un **generatore** di G .

(In notazione additiva, un gruppo A è ciclico se esiste $a \in A$ tale che $A = \{ za \mid z \in \mathbb{Z} \}$).

Esempi. 1) $(\mathbb{Z}, +)$ è un gruppo ciclico con generatore 1 (un altro possibile generatore è -1; si verifichi che questi sono i soli possibili generatori di \mathbb{Z}).

2) S_3 non è un gruppo ciclico (si veda il paragrafo precedente).

Abbiamo già osservato che un gruppo ciclico è abeliano. Il gruppo \mathbb{Z} è il modello fondamentale per i gruppi ciclici. Vediamo ad esempio che, così come avviene per \mathbb{Z} , ogni sottogruppo di un gruppo ciclico è ciclico. La dimostrazione di questo fatto ricalca quella data per \mathbb{Z} (Teorema 2.1); ne diamo quindi una esposizione rapida. Cercate di completarla e di capire che quella per \mathbb{Z} è la "stessa" dimostrazione.

Proposizione 2.3 *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Dimostrazione. Sia $G = \langle g \rangle$ un gruppo ciclico con generatore g , e sia $H \leq G$. Se $H = \{1_G\}$ allora $H = \langle 1_G \rangle$. Sia quindi $H \neq \{1_G\}$; allora esiste $0 \neq z \in \mathbb{Z}$ tale che $g^z \in H$. Poichè H è un sottogruppo si ha anche $g^{-z} \in H$. Quindi non è vuoto l'insieme $\{0 \neq m \in \mathbb{N} \mid g^m \in H\}$. Sia n il minimo di tale insieme. Allora $g^n \in H$ e quindi $\langle g^n \rangle \leq H$. Viceversa, se $h = g^z \in H$, si divide z per n : $z = nq + r$ con $0 \leq r < n$. Quindi $g^r = g^{z-nq} = g^z (g^n)^{-q} \in H$ da cui segue, per la scelta di n , $r = 0$. Quindi $h = g^z = g^{nq} = (g^n)^q \in \langle g^n \rangle$ e dunque $H \leq \langle g^n \rangle$. Quindi $H = \langle g^n \rangle$ è ciclico.

I due esempi seguenti illustrano come la classe dei gruppi ciclici si suddivida naturalmente in due tipologie; quelli infiniti e quelli finiti. Agli esempi seguirà una proposizione che descrive in generale la differenza tra il caso finito e quello infinito.

Esempi. 1) Consideriamo la matrice

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R}).$$

e consideriamo il gruppo ciclico $G = \langle g \rangle$. L'elemento identico di tale gruppo è la matrice identica di ordine 2. Proviamo per induzione che per ogni $n \in \mathbb{N}$ si ha $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Infatti ciò è vero per $n = 0, 1$; supposto vero per n si ha

$$g^{n+1} = g^n g = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 1+n \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

dunque l'affermazione è provata. Osserviamo quindi che per $0 < z \in \mathbb{Z}$ si ha

$$g^z = (g^{|z|})^{-1} = \begin{pmatrix} 1 & |z| \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}.$$

In questo caso quindi, per ogni $0 \neq z \in \mathbb{Z}$ si ha $g^z \neq 1_G$, e $g^x = g^y$ se e solo se $x = y$. In particolare quindi $|G| = \infty$.

Provate inoltre per esercizio che i soli possibili generatori del gruppo G sono la matrice g e la sua inversa (dimostrate cioè che se $z \neq \pm 1$ allora il sottogruppo generato da g^z non contiene g), e che l'omomorfismo $\gamma: \mathbb{Z} \rightarrow G$, definito da $\gamma(z) = g^z$, è un isomorfismo.

2) Consideriamo la matrice

$$h = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in GL(2, \mathbb{R}).$$

e consideriamo il gruppo ciclico $H = \langle h \rangle$. Facendo i calcoli, si trova

$$h^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \quad h^3 = h^2 h = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

e così via :

$$h^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad h^5 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \quad h^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = 1_H.$$

Abbiamo in particolare trovato un intero strettamente positivo $n = 6$ tale che $h^6 = 1_H$ e 6 è il **più piccolo** naturale non nullo per cui avviene ciò. (Si osservi anche che $h^5 = h^{-1}$)

Ora, dato $z \in \mathbb{Z}$, lo dividiamo per 6: $z = 6q + r$ con $r \in \{0, 1, 2, 3, 4, 5\}$. Si ha allora:

$$h^z = h^{6q+r} = (h^6)^q h^r = 1^q h^r = h^r.$$

Dunque possiamo concludere che

$$H = \langle h \rangle = \{ h^r \mid 0 \leq r \leq 5 \} = \{ h^0 = 1, h, h^2, h^3, h^4, h^5 \}$$

e $|\langle h \rangle| = 6$.

Ordine di un elemento. Sia g un elemento del gruppo G . L'**ordine** di g , che si denota con $|g|$, è per definizione

il minimo numero intero $n \geq 1$ tale che $g^n = 1_G$, se esiste; ed è ∞ se un tale intero non esiste (ovvero se $g^n \neq 1_G$ per ogni $n \geq 1$).

Proposizione 2.4 *Sia $G = \langle g \rangle$ un gruppo ciclico. Si verifica uno dei casi seguenti.*

(1) *Se $|g| = n \geq 1$, allora $|G| = n$ e $G = \{ g^0 = 1_G, g, g^2, \dots, g^{n-1} \}$.*

(2) *Se $|g| = \infty$, allora $|G| = \infty$ e tutte le potenze di g sono distinte (cioè, per ogni $z, w \in \mathbb{Z}$, $g^z = g^w \Leftrightarrow z = w$).*

Dimostrazione. (1) Sia $n \geq 1$ e $|g| = n$. Per definizione, n è il minimo numero naturale non nullo tale che $g^n = 1_G$. Se $z \in \mathbb{Z}$, possiamo dividere z per n : $z = nq + r$ con $0 \leq r \leq n-1$. Allora

$$g^z = g^{nq+r} = (g^n)^q g^r = (1_G)^q g^r = g^r;$$

dunque $G = \{ g^r \mid 0 \leq r \leq n-1 \} = \{ 1_G, g, \dots, g^{n-1} \}$. Per concludere, verificiamo che gli elementi $1_G = g^0, g, g^2, \dots, g^{n-1}$ sono tutti distinti. Infatti se $0 \leq i \leq j \leq n-1$ e $g^i = g^j$, allora $j-i \geq 0$ e $g^{j-i} = g^j (g^i)^{-1} = 1_G$ e quindi, per la minimalità di n , $j-i = 0$ cioè $i = j$, come si voleva. In particolare, $|G| = n$.

(2) Sia ora $|g| = \infty$. Allora, per ogni $n \geq 1$, $g^n \neq 1_G$. Siano $z, w \in \mathbb{Z}$, $z \geq w$, con $g^z = g^w$, allora

$$g^{z-w} = g^z(g^w)^{-1} = 1_G$$

e quindi $z - w = 0$ cioè $z = w$. Dunque potenze di g con esponenti distinti sono distinte e, in particolare, $|G| = \infty$.

Esercizio. Si provi che due gruppi ciclici dello stesso ordine sono isomorfi.

Esercizio. Si provi che il gruppo additivo dei numeri razionali non è ciclico.

Consideriamo ora un gruppo ciclico $G = \langle g \rangle$ di ordine finito n . Dalla dimostrazione della proposizione 2.4 segue che, dato $z \in \mathbb{Z}$, $g^z = g^r$ dove r è il resto della divisione di z per n . In particolare

$$g^z = 1_G \Leftrightarrow |g| = n \text{ divide } z.$$

Ora, gli elementi di G sono $1_G, g, g^2, \dots, g^{n-1}$. Sia $0 \leq a \leq n-1$ e sia $d = \frac{n}{(a,n)}$; allora n divide ad e quindi $(g^a)^d = g^{ad} = 1_G$, d'altra parte, se $1_G = (g^a)^m = g^{am}$ allora $n|am$ e quindi $\frac{n}{(a,n)}$ divide m (dato che non ha fattori comuni con $\frac{a}{(a,n)}$). Dunque d è l'ordine dell'elemento g^a di G ; cioè

$$|\langle g^a \rangle| = \frac{n}{(a,n)}.$$

Da questa osservazione segue che per ogni divisore d di n , l'elemento $g^{\frac{n}{d}}$ genera un sottogruppo di $\langle g \rangle$ di ordine d ; quindi

se G è un gruppo ciclico di ordine n , allora G ha un sottogruppo di ordine d per ogni divisore d di n .

Ad esempio se $G = \langle g \rangle$ ha ordine 40, allora il sottogruppo generato da g^5 ha ordine 8. Tale sottogruppo è

$$\{1_G, g^5, (g^5)^2, (g^5)^3, \dots, (g^5)^7\} = \{1_G, g^5, g^{10}, g^{15}, g^{20}, g^{25}, g^{30}, g^{35}\}.$$

Si provi per **esercizio** che questo è l'unico sottogruppo di $\langle g \rangle$ di ordine 8. Si generalizzi quindi la cosa provando che

per ogni divisore d di n un gruppo ciclico di ordine n ha uno e un solo sottogruppo di ordine d .

Esercizio. Sia g un elemento di un gruppo e $n, m \in \mathbb{Z}$, si dimostri che $\langle g^n \rangle \leq \langle g^m \rangle$ se e solo se $m|n$.

Un'altra conseguenza della osservazione di sopra è se $\langle g \rangle$ ha ordine finito n e $0 \leq a \leq n-1$, allora $|g^a| = n$ (e quindi $\langle g^a \rangle = \langle g \rangle$) se e solo se $(a, n) = 1$. Cioè

il numero di generatori distinti di un gruppo ciclico di ordine n coincide con il numero di interi positivi strettamente minori di n e coprimi con n .

Tale numero si denota con $\phi(n)$ dove ϕ si chiama la **funzione di Eulero**. In particolare, in un gruppo ciclico di ordine primo ogni elemento non nullo è un generatore.

Non è difficile valutare $\phi(n)$:

Esercizio. 1) Si dimostri che se p è un numero primo, allora per ogni $a \geq 1$:

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).$$

- 2) Si dimostri che se $(n, m) = 1$ allora $\phi(nm) = \phi(n)\phi(m)$.
 3) Si provi che se $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ con p_1, p_2, \dots, p_s primi distinti, allora

$$\phi(n) = \prod_{i=1}^s p_i^{a_i-1} (p_i - 1).$$

Ad esempio, $\phi(40) = \phi(5)\phi(2^3) = (5-1)(2-1)2^2 = 4 \cdot 4 = 16$. Se $\langle g \rangle$ ha ordine 40, allora i suoi generatori distinti sono gli elementi g^a con $1 \leq a \leq 39$ e $(a, 40) = 1$, cioè $a = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$.

Classi laterali e Teorema di Lagrange.

Sia H un sottogruppo del gruppo G e sia $x \in G$. La **classe laterale sinistra** di x modulo H è il *sottoinsieme* di G :

$$xH = \{ xh \mid h \in H \}.$$

Esempio. Sia $G = S_3$ e H il sottogruppo generato dalla trasposizione τ_1 (cioè $H = \{ \iota, \tau_1 \}$). Allora:

$$H = \iota H = \tau_1 H,$$

$$\tau_2 H = \{ \tau_2 \circ \iota, \tau_2 \circ \tau_1 \} = \{ \tau_2, \gamma^2 \} = \gamma^2 H,$$

$$\tau_3 H = \{ \tau_3 \circ \iota, \tau_3 \circ \tau_1 \} = \{ \tau_3, \gamma \} = \gamma H.$$

Osserviamo alcuni aspetti di questo esempio. Intanto elementi diversi possono dare la stessa classe laterale; le classi trovate sono disgiunte e costituiscono una partizione di G come insieme. Infine abbiamo trovato 3 classi laterali che contengono tutte lo stesso numero di elementi del sottogruppo considerato H . Questi fatti non sono peculiari di questo esempio ma, come proveremo in questo paragrafo, valgono in generale.

Innanzitutto vediamo che l'insieme delle classi laterali sinistre modulo un sottogruppo è sempre una partizione del gruppo. Infatti, le classi laterali sono classi di equivalenza di una opportuna relazione di equivalenza che è determinata dal sottogruppo.

Sia H un sottogruppo del gruppo G . Sull'insieme G consideriamo la relazione \sim_H definita ponendo per ogni $x, y \in G$: $x \sim_H y$ se $x^{-1}y \in H$.

Verifichiamo che tale relazione è una equivalenza su G .

- E' riflessiva: infatti per ogni $x \in G$, $x^{-1}x = 1_G \in H$.

- E' simmetrica: infatti per ogni $x, y \in G$, se $x \sim_H y$ allora $x^{-1}y \in H$ e quindi $y^{-1}x = (x^{-1}y)^{-1} \in H$, cioè $y \sim_H x$.

- E' transitiva: infatti se $x, y, z \in G$ sono tali che $x \sim_H y$ e $y \sim_H z$, allora $x^{-1}y \in H$ e $y^{-1}z \in H$, quindi $x^{-1}z = x^{-1}yy^{-1}z \in H$, cioè $x \sim_H z$.

Ora, per ogni $x \in G$ la classe di equivalenza

$$[x] = \{ y \in G \mid x \sim_H y \}$$

coincide con la classe laterale xH , infatti

$$y \in xH \Leftrightarrow \text{esiste } h \in H \text{ tale che } y = xh \Leftrightarrow x^{-1}y = h \text{ con } h \in H \Leftrightarrow x \sim_H y$$

Da ciò segue la proprietà fondamentale che l'insieme delle classi laterali sinistre (distinte) modulo H

$$\{ xH \mid x \in G \}$$

è l'insieme quoziente modulo la equivalenza \sim_H e quindi è una **partizione** di G . Inoltre, poichè due classi di equivalenza coincidono se e solo se i loro rappresentanti sono in relazione, si ha il seguente fatto, che è bene avere sempre presente.

Per ogni $x, y \in G$, $xH = yH$ se e solo se $x^{-1}y \in H$ se e solo se $y \in xH$.

Esercizio. Utilizzando la definizione di classe laterale sinistra, si dimostri direttamente che classi laterali distinte, modulo lo stesso sottogruppo, sono disgiunte

In *notazione additiva* le classi laterali modulo un sottogruppo H in un gruppo additivo A sono i sottoinsiemi

$$a + H = \{ a + b \mid b \in H \}$$

con $a \in A$; e $a + H = b + H$ se e solo se $a - b \in H$ (si ricordi che la notazione additiva si applica a gruppi commutativi).

Definizione. Sia G un gruppo e $H \leq G$. L'**indice** di H in G è il numero di classi laterali (sinistre) di G modulo H . Tale numero si denota con

$$[G : H] .$$

Se il gruppo G è finito allora l'indice di ogni sottogruppo è un numero naturale; ad esempio l'indice del sottogruppo H generato dalla trasposizione τ_1 in S_3 è 3. Se il gruppo G è infinito, allora l'indice di un sottogruppo può essere sia un numero naturale che infinito, come vedremo con esempi più avanti. Osserviamo anche che le classi laterali modulo il sottogruppo banale $\{1_G\}$ contengono tutte un solo elemento e che quindi $[G : \{1_G\}] = |G|$.

Un **caso molto importante** è quello dei sottogruppi di \mathbb{Z} . Sia $n \geq 1$ e consideriamo il sottogruppo $n\mathbb{Z}$ di \mathbb{Z} . Siano $x, y \in \mathbb{Z}$, allora

$$x \sim_{n\mathbb{Z}} y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow n \mid x - y \Leftrightarrow x \equiv y \pmod{n} ,$$

quindi l'equivalenza associata al sottogruppo $n\mathbb{Z}$ coincide con la congruenza modulo n . Di conseguenza le classi laterali modulo $n\mathbb{Z}$ sono le classi di congruenza (o classi resto) modulo n . Questo si può rivedere direttamente; per ogni $a \in \mathbb{Z}$,

$$a + n\mathbb{Z} = \{ b = a + nz \mid z \in \mathbb{Z} \} = \{ b \mid b - a = nz, z \in \mathbb{Z} \} = \{ b \mid n \mid b - a \} = \{ b \mid b \equiv a \pmod{n} \} .$$

detto ancora in un altro modo: $a + n\mathbb{Z} = b + n\mathbb{Z} \Leftrightarrow a \equiv b \pmod{n}$.

Dalla teoria delle congruenze in \mathbb{Z} sappiamo che ci sono n distinte classi di congruenza modulo n : $[0], [1], [2], \dots, [n-1]$. Quindi ci sono n classi laterali di \mathbb{Z} modulo $n\mathbb{Z}$, che sono

$$n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z} ;$$

dunque

$$[\mathbb{Z} : n\mathbb{Z}] = n$$

e per ogni $z \in \mathbb{Z}$, $z + n\mathbb{Z} = r + n\mathbb{Z}$ dove r è il resto della divisione di z per n .

Il seguente Teorema stabilisce in particolare una proprietà fondamentale dei gruppi finiti: che *l'ordine di ogni sottogruppo di un gruppo finito divide l'ordine del gruppo*. Questo fatto è veramente alla base dello studio dei gruppi finiti.

Teorema di Lagrange. *Sia G un gruppo finito, e sia $H \leq G$. Allora*

$$|G| = [G : H]|H| .$$

Dimostrazione. Innanzi tutto proviamo che le classi laterali di G modulo H contengono tutte lo stesso numero $|H|$ di elementi. Infatti per ogni classe xH esiste la biezione

$$\sigma_x : H \longrightarrow xH$$

definita ponendo per ogni $h \in H$, $\sigma_x(h) = xh$. Tale applicazione è iniettiva perchè se $\sigma_x(h) = \sigma_x(h')$ allora $xh = xh'$ e quindi, per la legge di cancellazione, $h = h'$; ed è suriettiva per la definizione di classe laterale xH .

Ora, le classi laterali costituiscono una partizione di G . Quindi se $[G : H] = n$ e denotiamo con K_1, K_2, \dots, K_n le classi laterali distinte di G modulo H , G è l'unione disgiunta $G = K_1 \cup K_2 \cup \dots \cup K_n$, dunque

$$|G| = \sum_{i=1}^n |K_i| = \sum_{i=1}^n |H| = n|H| = [G : H]|H| ,$$

e la dimostrazione è completa.

Ad esempio, se $|G| = 6$ i possibili ordini dei sottogruppi di G sono 1,2,3 e 6. Studiando S_3 abbiamo visto che per ogni divisore di 6 esiste in S_3 almeno un sottogruppo di tale ordine. Tuttavia, in generale non è vero che se G è un gruppo finito allora per ogni divisore d di $|G|$ deve necessariamente esistere un sottogruppo di ordine d ; vedremo in seguito un esempio in cui ciò non avviene. Dimostreremo più avanti anche il notevole Teorema di Sylow, che afferma in particolare che se p è un primo e p^m divide $|G|$ allora G ha un sottogruppo di ordine p^m .

Una prima importante conseguenza del Teorema di Lagrange è il seguente

Corollario 2.5 *Sia G un gruppo finito. Allora l'ordine di ogni elemento di G divide l'ordine di G .*

Dimostrazione. Sia G un gruppo finito e $g \in G$. Allora, per definizione, l'ordine di g è l'ordine del sottogruppo $\langle g \rangle$ e questo, per il Teorema di Lagrange, divide $|G|$.

Osserviamo che da questo corollario segue anche che, se G è un gruppo finito, allora $g^{|G|} = 1_G$ per ogni $g \in G$.

Ecco un'altra immediata e interessante applicazione del Teorema di Lagrange.

Proposizione 2.6 *Sia p un primo. Allora ogni gruppo di ordine p è ciclico.*

Dimostrazione. Sia G un gruppo di ordine primo p e sia $1_G \neq g \in G$. Allora il sottogruppo $\langle g \rangle$ di G non è banale e il suo ordine divide $|G| = p$. Dunque deve essere $\langle g \rangle = G$.

Vediamo ora un esempio di studio delle classi laterali modulo un sottogruppo; la cosa fondamentale è individuare un opportuno *insieme di rappresentanti*, cioè un insieme di elementi del gruppo, le classi laterali dei quali siano distinte e siano tutte quelle del gruppo. Ad esempio, $\{0, 1, 2, \dots, n-1\}$ è un insieme di rappresentanti del gruppo \mathbb{Z} modulo il sottogruppo $n\mathbb{Z}$.

Esempio. Fissato un numero primo p , nel gruppo additivo \mathbb{Q} dei numeri razionali consideriamo il sottoinsieme

$$S = \left\{ \frac{m}{n} \in \mathbb{Q} \mid p \nmid n \right\}.$$

$S \leq \mathbb{Q}$; infatti $S \neq \emptyset$ e se $\frac{m}{n}, \frac{r}{s} \in S$ allora $\frac{m}{n} - \frac{r}{s} = \frac{ms - nr}{ns} \in S$ perchè p non divide ns dato che è primo e non divide n né s . Quindi $S \leq \mathbb{Q}$ per il criterio dei sottogruppi.

Studiamo ora le classi laterali di \mathbb{Q} modulo S ; proviamo che l'insieme

$$\mathcal{R} = \left\{ 0, \frac{r}{p^i} \mid i \in \mathbb{N}, 1 \leq r \leq p^i - 1 \text{ e } (r, p) = 1 \right\}$$

è un insieme di rappresentanti di \mathbb{Q} modulo S .

Sia $x = \frac{m}{n} \in \mathbb{Q}$, con $(m, n) = 1$. Se $p \nmid n$ allora $x \in S = 0 + S$. Altrimenti $p \nmid m$ e $n = ap^i$ con $i \geq 1$ e $(a, p^i) = 1$. Poichè a, p^i sono coprimi, esistono $b, r \in \mathbb{Z}$ tali che

$$ar + bp^i = m \quad (*)$$

osservo che si può prendere $1 \leq r \leq p^i - 1$, infatti posso sostituire r in $(*)$ con il suo resto della divisione per p^i che non è zero perchè p non divide m . Allora $\frac{r}{p^i} \in \mathcal{R}$ e

$$x - \frac{r}{p^i} = \frac{m}{ap^i} - \frac{r}{p^i} = \frac{m - ra}{ap^i} = \frac{bp^i}{ap^i} = \frac{b}{a} \in S$$

quindi

$$x + S = \frac{r}{p^i} + S.$$

Dunque la classi $y + S$ con $y \in \mathcal{R}$ sono tutte le classi di \mathbb{Q} modulo S . Verifichiamo che sono tutte distinte. Se $\frac{r}{p^i}, \frac{s}{p^j} \in \mathcal{R}$ con $j \geq i$, allora

$$\frac{r}{p^i} + S = \frac{s}{p^j} + S \Leftrightarrow \frac{r}{p^i} - \frac{s}{p^j} \in S \Leftrightarrow \frac{rp^{j-i} - s}{p^j} \in S$$

ora, se $j \neq i$, p non divide il numeratore (perchè non divide s) e quindi $\frac{rp^{j-i} - s}{p^j} \notin S$; dunque $i = j$ e allora $\frac{r}{p^i} - \frac{s}{p^j} = \frac{r-s}{p^i} \in S$ se e solo se p^i divide $r - s$ il che implica, dato che $r, s < p^i$, $r = s$. Dunque

$$\frac{r}{p^i} + S = \frac{s}{p^j} + S \Leftrightarrow i = j \text{ e } r = s.$$

osserviamo in particolare che $[\mathbb{Q} : S] = \infty$.

Concludiamo questo paragrafo con due osservazioni sugli indici che sono marginali per quanto riguarda gli argomenti di questo corso, ma possono essere utili nella risoluzione di qualche problema; considerate la dimostrazione come esercizio.

Proposizione 2.7 Siano H, K sottogruppi di indice finito del gruppo G , allora

1) (formula del prodotto) Se $K \leq H$ allora $[G : K] = [G : H][H : K]$;

2) (Lemma di Poincarè) $[G : H \cap K] \leq [G : H][G : K]$.

Dimostrazione 1) Sia $[G : H] = n$, $[H : K] = m$ e siano g_1H, \dots, g_nH le classi laterali distinte di G modulo H e h_1K, \dots, h_mK quelle di H modulo K . Consideriamo le classi

$$(g_i h_j)K \text{ di } G \text{ modulo } K \text{ con } i = 1, \dots, n \quad j = 1, \dots, m \quad (*)$$

di G modulo K . Se $(g_i h_j)K = (g_r h_s)K$ allora $h_s^{-1} g_r^{-1} g_i h_j = (g_r h_s)^{-1} (g_i h_j) \in K$, in particolare poichè $K \leq H$, $h_s^{-1} g_r^{-1} g_i h_j = y \in H$ e quindi $g_r^{-1} g_i = h_s y h_j^{-1} \in H$, da cui $g_r H = g_i H$ e $r = i$; dunque $h_s^{-1} h_j = h_s^{-1} g_r^{-1} g_i h_j \in K$ e quindi $h_s K = h_j K$ da cui $s = j$. Dunque tutte le classi in (*) sono distinte, quindi $[G : K] \geq nm = [G : H][G : K]$.

Sia ora $g \in G$, allora, per qualche $i = 1, \dots, n$: $g \in g_i H$ dunque esiste $y \in H$ tale che $g = g_i y$; similmente esistono un indice $j = 1, \dots, m$ ed un elemento $x \in K$ tali che $y = h_j x$. Quindi $g = g_i y = h_j g_i x \in h_j g_i K$ da cui $gK = h_j g_i K$. Dunque la classi in (*) sono tutte le classi di G modulo K e pertanto $[G : K] = nm = [G : H][G : K]$.

2) Si applichi la legge di cancellazione per dimostrare che per ogni $g \in G$: $gH \cap gK = g(H \cap K)$. Da ciò segue facilmente che il numero di classi di G modulo $H \cap K$ è al più $nm = [G : H][G : K]$.

A partire da un sottogruppo H di un gruppo G si definiscono anche le **classi laterali destre** modulo H ; per ogni $g \in G$ si pone

$$Hg = \{ hg \mid h \in H \} .$$

Le classi laterali destre sono le classi di equivalenza della relazione di equivalenza definita ponendo per ogni $x, y \in G$: $x \sim y$ se $xy^{-1} \in H$.

Quindi l'insieme $\{ Hx \mid x \in G \}$ è una partizione di G , e per ogni $x, y \in G$ si ha $Hx = Hy$ se e solo se $xy^{-1} \in H$. Inoltre valgono le stesse osservazioni fatte per le classi sinistre riguardo al loro numero e cardinalità. In particolare vale il Teorema di Lagrange e il fatto che *il numero di classi laterali destre modulo H coincide con $[G : H]$, il numero di classi laterali sinistre.*

Osserviamo che, in generale, per un $H \leq G$ e un $g \in G$ non è detto che la classe Hx coincida con la classe xH . Ad esempio, se $G = S_3$ e $H = \{ \iota, \tau_1 \}$ è il sottogruppo generato dalla trasposizione τ_1 , allora:

$$H\tau_2 = \{ \iota \circ \tau_2, \tau_1 \circ \tau_2 \} = \{ \tau_2, \gamma \} \neq \{ \tau_2, \gamma^2 \} = \tau_2 H .$$

Ovviamente, se il gruppo G è commutativo, allora $Hx = xH$ per ogni $H \leq G$ ed ogni $x \in G$.

Esercizio. Siano H e K sottogruppi del gruppo G e $x, y \in G$. Si provi che se $Hx = Ky$ allora $H = K$.

Soluzione. Sia $Hx = Ky$ e osserviamo che allora $x = 1x \in Ky$ e dunque $Kx = Ky$. Quindi, se $h \in H$, allora $hx \in Hx = Ky = Kx$ e quindi esiste $k \in K$ tale che $hx = kx$ cioè $h = k \in K$. Dunque $H \subseteq K$. Analogamente si prova che $K \subseteq H$ e quindi $H = K$.

ESERCIZI

1. Si provi che l'insieme

$$\left\{ \frac{m}{2^i} \mid m \in \mathbb{Z}, i \in \mathbb{N} \right\}$$

è un sottogruppo del gruppo $(\mathbb{Q}, +)$.

2. Si provi che l'insieme $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R}, a \neq 0 \neq d \right\}$ è un sottogruppo del gruppo $GL(2, \mathbb{R})$.

3. Sia X un insieme finito e sia $\mathcal{B} = \{ Y \mid Y \subseteq X, |Y| \text{ è pari} \}$. Si provi che \mathcal{B} è un sottogruppo del gruppo $(\mathcal{P}(X), \Delta)$.

4. Siano a, b elementi del gruppo G tali che $ab = ba$. Si provi che l'insieme $\{ a^u b^v \mid u, v \in \mathbb{Z} \}$ è un sottogruppo di G .

5. Si scriva la tavola di moltiplicazione di S_3 .

6. Sia \mathbf{R} un rettangolo i cui lati adiacenti hanno lunghezza diversa. Si provi che il gruppo delle simmetrie di \mathbf{R} è commutativo, ha ordine 4, e tutti i suoi elementi hanno ordine 2.

7. Nel gruppo moltiplicativo \mathbb{Q}^* si considerino i sottogruppi

$$A = \langle -\frac{1}{2} \rangle, \quad B = \langle \frac{1}{3} \rangle, \quad C = \langle -2 \rangle, \quad D = \langle 2 \rangle .$$

Si determinino $A \cap B, A \cap C, C \cap D,$ e $[C : C \cap D]$.

8. Sia $G = \langle g \rangle$ un gruppo ciclico di ordine 14. Si descrivano esplicitamente il sottogruppo di ordine 7, ed i generatori di G .

9. Sia $P = \{ x \in \mathbb{R} \mid x > 0 \}$. Si provi che $P \leq \mathbb{R}^*$ e si determini l'indice $[\mathbb{R}^* : P]$.

10. Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi e sia g un elemento di ordine finito di G . Si provi che $|\phi(g)|$ divide $|g|$.

11. Siano a, b elementi di un gruppo G tali che $ab = ba$ e $\langle a \rangle \cap \langle b \rangle = \{1_G\}$. Si provi che $|ab| = m.c.m.(|a|, |b|)$.

12. Per ogni intero $k \geq 1$ sia $U_k = \{ z \in \mathbb{C} \mid z^k = 1 \}$ il gruppo moltiplicativo delle radici k -esime dell'unità. Sia $n|m$, si provi che $U_n \leq U_m$ e si determini l'indice $[U_m : U_n]$.

13. Siano H, K sottogruppi di ordine finito del gruppo G . Si provi che se $(|H|, |K|) = 1$ allora $H \cap K = \{1_G\}$.

14. Sia $T = \left\{ \frac{m}{3^i} \mid m \in \mathbb{Z}, i = 0, 1 \right\}$. Si provi che $\mathbb{Z} \leq T \leq \mathbb{Q}$ (additivamente). Si calcoli quindi l'indice $[T : \mathbb{Z}]$ trovando un opportuno insieme di rappresentanti di T modulo \mathbb{Z} .

15. Sia p un primo. Si provi che se G è un gruppo di ordine p^n per qualche intero $n \geq 1$, allora G contiene un elemento di ordine p .

3 Sottogruppi normali e Quozienti

Sottogruppi normali

Definizione. Sia G un gruppo. Un sottogruppo H di G si dice sottogruppo **normale** (e si scrive $H \trianglelefteq G$) se per ogni $g \in G$:

$$Hg = gH .$$

I sottogruppi normali sono molto importanti perchè, come vedremo tra breve, sull'insieme delle classi laterali modulo un sottogruppo normale (sinistre o destre non ha rilevanza perchè coincidono) è possibile definire una operazione che lo rende un gruppo.

Dalla definizione segue immediatamente che in un qualunque gruppo G , il sottogruppo banale $\{1_G\}$ e G sono sottogruppi normali. Un gruppo G si dice *semplice* se $\{1_G\}$ e G sono i soli sottogruppi normali di G . Ad esempio ogni gruppo di ordine primo è semplice (perchè per il Teorema di Lagrange in un gruppo G di ordine primo, $\{1_G\}$ e G sono i soli sottogruppi). I gruppi semplici sono estremamente importanti nella teoria dei gruppi e in altri ambiti (la dimostrazione di Galois che non esiste una formula risolutiva per le equazioni di quinto grado, o superiore, si basa sul fatto che un certo gruppo - il cosiddetto gruppo alterno A_5 che definiremo più avanti - è semplice), tuttavia il loro studio esula dal programma di questo corso.

Osserviamo inoltre che in un gruppo commutativo ogni sottogruppo è normale. Questo, tranne che per alcune eccezioni (il gruppo dei quaternioni che anche definiremo più avanti), non è il caso dei gruppi non commutativi.

Esempio. Come osservato in precedenza il sottogruppo generato da una trasposizione di S_3 non è normale in S_3 . Consideriamo invece il sottogruppo $A = \{1, \gamma, \gamma^2\}$ generato dal ciclo γ di ordine 3. Allora $[S_3 : A] = |S_3|/|A| = 2$ e le classi laterali sinistre di S_3 modulo A sono

$$A = \gamma A = \gamma^2 A \quad \text{e} \quad \tau_1 A = \tau_2 A = \tau_3 A = S_3 \setminus A,$$

ognuna delle quali coincide con la classe laterale destra con lo stesso rappresentante; quindi $A \trianglelefteq S_3$.

Esercizio. Si dimostri che ogni sottogruppo di indice 2 di un gruppo è normale.

Anche per la proprietà di normalità è conveniente disporre di un criterio che sia più maneggevole della verifica diretta della definizione.

Lemma (Criterio di normalità). *Sia H un sottogruppo del gruppo G . Allora sono equivalenti:*

- i) $H \trianglelefteq G$.
- ii) Per ogni $h \in H$ e ogni $g \in G$: $g^{-1}hg \in H$.

Dimostrazione i) \Rightarrow ii). Sia H normale in G , e siano $h \in H, g \in G$. Allora $hg \in Hg = gH$ quindi esiste $h_1 \in H$ tale che $hg = gh_1$ da cui, moltiplicando a sinistra per g^{-1} , si ottiene $g^{-1}hg = h_1 \in H$. Quindi H soddisfa la proprietà ii).

ii) \Rightarrow i). Supponiamo che il sottogruppo H soddisfi la proprietà ii), e sia $g \in G$. Sia $x \in Hg$, allora esiste $h \in H$ tale che $x = hg$; quindi per la proprietà soddisfatta da H , $g^{-1}x = g^{-1}hg \in H$ da cui segue $x = g(g^{-1}hg) \in gH$; dunque $Hg \subseteq gH$. Viceversa sia $y = gh$ un generico elemento di gH ; allora $y = (ghg^{-1})g \in Hg$ perchè $ghg^{-1} = (g^{-1})^{-1}h(g^{-1}) \in H$. Quindi $gH \subseteq Hg$ e dunque $Hg = gH$ e $H \trianglelefteq G$.

Se G è un gruppo e $g, x \in G$, l'elemento $g^{-1}xg$ si chiama **coniugato** di x tramite g ; è importante osservare che in genere si tratta di un elemento diverso da x (infatti, $g^{-1}xg = x \Leftrightarrow xg = gx$).

Esempio. Sia G l'insieme di tutte le matrici reali

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{con} \quad ac \neq 0.$$

Si provi che G è un gruppo. Si consideri quindi il sottoinsieme

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid 0 \neq b \in \mathbb{R} \right\}.$$

Proviamo che $N \trianglelefteq G$. Innanzi tutto occorre verificare che N è un sottogruppo di G . Infatti N non è vuoto e per ogni $x = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \in N$:

$$xy^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b - b_1 \\ 0 & 1 \end{pmatrix} \in N;$$

dunque $N \leq G$.

Verifichiamo ora la normalità usando il criterio del Lemma. Siano

$$x = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in N \quad \text{e} \quad g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G,$$

allora

$$g^{-1}xg = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & \frac{cs}{a} \\ 0 & 1 \end{pmatrix} \in N;$$

quindi $N \trianglelefteq G$.

Esercizio. Si provi che se H, K sono sottogruppi normali del gruppo G allora $H \cap K \trianglelefteq G$. Più in generale, se \mathcal{F} è una famiglia di sottogruppi normali di G allora $\bigcap_{H \in \mathcal{F}} H \trianglelefteq G$.

Gruppi quoziente

Sia G un gruppo e $N \trianglelefteq G$. Denotiamo con G/N l'insieme delle classi laterali di G modulo N , cioè

$$\frac{G}{N} = \{ gN \mid g \in G \}.$$

Su tale insieme definiamo una operazione (che si denota con lo stesso simbolo dell'operazione di G (quindi in generale semplicemente accostando gli elementi), ponendo, per ogni $xN, yN \in G/N$:

$$(xN)(yN) = xyN .$$

Verifichiamo che si tratta di una **buona definizione**. Infatti se $x_1, y_1 \in G$ sono tali che

$$x_1N = xN \quad \text{e} \quad y_1N = yN ,$$

allora

$$x^{-1}x_1 \in N \quad \text{e} \quad y^{-1}y_1 \in N$$

poichè $N \trianglelefteq G$, per il Lemma precedente si ha:

$$y^{-1}(x^{-1}x_1)y \in N$$

e quindi

$$(xy)^{-1}(x_1y_1) = (y^{-1}x^{-1})x_1(yy^{-1})y_1 = (y^{-1}x^{-1}x_1y)(y^{-1}y_1) \in N ,$$

dunque

$$xyN = x_1y_1N$$

il risultato non dipende dalla scelta dei rappresentanti delle classi.

(Si provi per esercizio che se N non è normale allora non si può definire una operazione allo stesso modo.)

Teorema 3.1 *Sia N un sottogruppo normale del gruppo G , allora l'insieme G/N con l'operazione definita sopra è un gruppo, detto **Gruppo Quoziente** (di G modulo N), e si ha*

- 1) $1_{G/N} = 1_G N = N$;
- 2) per ogni $xN \in G/N$: $(xN)^{-1} = x^{-1}N$.

Dimostrazione. Siano $aN, bN, cN \in G/N$, allora:

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN)$$

dunque l'operazione su G/N è associativa.

Per ogni $xN \in G/N$ si ha $N \cdot xN = 1_G N \cdot xN = (1_G x)N = xN = xN \cdot N$ e

$$(xN)(x^{-1}N) = (xx^{-1})N = 1_G N = N ,$$

quindi G/N è un gruppo con elemento identico la classe $1_G N = N$ e tale che $(xN)^{-1} = x^{-1}N$ per ogni elemento $xN \in G/N$.

Osserviamo che se $N \trianglelefteq G$ allora $|G/N| = [G : N]$. In particolare, per il Teorema di Lagrange, se G è un gruppo finito allora *l'ordine di G/N divide l'ordine di G .*

Esempio. Consideriamo il gruppo S_3 ed il suo sottogruppo $A = \langle \gamma \rangle$ che abbiamo visto essere normale. Allora $S_3/A = \{ A, \tau_1 A \}$ è un gruppo, il cui elemento identico è A e l'operazione è data da:

$$A \circ A = A, \quad A \circ \tau_1 A = \tau_1 A, \quad \tau_1 A \circ A = \tau_1 A, \quad \tau_1 A \circ \tau_1 A = A.$$

In *notazione additiva* il simbolo che si usa per l'operazione del gruppo quoziente è ancora +; quindi se N è un sottogruppo (normale) di un gruppo additivo A allora

$$\frac{A}{N} = \{ a + N \mid a \in A \},$$

e per ogni $a, b \in A$

$$(a + N) + (b + N) = (a + b) + N;$$

inoltre $0_{A/N} = 0 + N = N$ e $-(a + N) = -a + N$.

(Si osservi che se N è un sottogruppo di un gruppo commutativo A , allora A/N è un gruppo commutativo.)

Consideriamo il **caso importante** del gruppo \mathbb{Z} . Poichè \mathbb{Z} è un gruppo commutativo, ogni suo sottogruppo è normale. Sia $n \geq 1$, allora come abbiamo visto nella sezione precedente:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{ a + n\mathbb{Z} \mid a = 0, 1, 2, \dots, n-1 \}.$$

In quanto quoziente di \mathbb{Z} esso è un gruppo additivo di ordine n che si chiama il **gruppo delle classi resto modulo n** , il cui elemento neutro è $0 + n\mathbb{Z}$. Denoteremo tale gruppo anche con \mathbb{Z}_n .

Per comodità, quando non ci siano ambiguità riguardo al modulo n , indicheremo gli elementi di \mathbb{Z}_n (cioè le classi di congruenza modulo n) semplicemente ponendo una linea sopra al rappresentante: \bar{a} invece di $a + n\mathbb{Z}$.

La somma di classi si esegue sommando i rappresentanti (e riducendo poi modulo n). Così, se $n = 7$:

$$\mathbb{Z}_7 = \frac{\mathbb{Z}}{7\mathbb{Z}} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \};$$

e si ha ad esempio

$$\begin{aligned} \bar{4} + \bar{5} &= \bar{9} = \bar{2} & -\bar{4} &= \overline{-4} = \bar{3} \\ \bar{4} - [\bar{5} - (\bar{6} + \bar{2})] &= \overline{4 - [(5 - (6 + 2))]} = \overline{4 - (-3)} = \bar{7} = \bar{0}. \end{aligned}$$

Osserviamo che i quozienti di \mathbb{Z} consentono di rispondere affermativamente alla domanda se per ogni naturale $n \geq 1$ esista un gruppo di ordine n (basta prendere \mathbb{Z}_n).

Esercizio. Si scriva la tabella di addizione del gruppo \mathbb{Z}_7 .

Esercizio. Si osservi che, per ogni $n \in \mathbb{N}$, \mathbb{Z}_n è ciclico generato dall'elemento $\bar{1}$. Più in generale, si provi che ogni quoziente di un gruppo ciclico è ciclico.

Omomorfismi

Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi. Denotiamo con $Im(\phi)$ l'immagine della applicazione ϕ , cioè

$$Im(\phi) = \phi(G) = \{ \phi(x) \mid x \in G \}.$$

La proposizione seguente completa in un certo senso la Proposizione 9 della Sezione 1.

Proposizione 3.2 Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi; allora $Im(\phi) \leq G'$.

Dimostrazione. Chiaramente $Im(\phi) \neq \emptyset$. Se $a, b \in Im(\phi)$ allora esistono $x, y \in G$ tali che $\phi(x) = a$, $\phi(y) = b$, e quindi

$$ab^{-1} = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in Im(\phi);$$

per il criterio dei sottogruppi, $Im(\phi) \leq G'$.

Esercizio. Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi; si provi che per ogni $g \in G$ e ogni $z \in \mathbb{Z}$: $\phi(g^z) = (\phi(g))^z$.

Definizione. Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi. Il **nucleo** $Ker(\phi)$ di ϕ è l'insieme degli elementi di G la cui immagine tramite ϕ è l'elemento identico; cioè

$$Ker(\phi) = \{ x \in G \mid \phi(x) = 1_{G'} \} = \phi^{-1}(1_{G'}).$$

Vediamo subito due importanti proprietà del nucleo di un omomorfismo.

Teorema 3.3 Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi; allora $Ker(\phi) \trianglelefteq G$.

Dimostrazione. Innanzi tutto $Ker(\phi) \neq \emptyset$, infatti (Proposizione 9 della sez. 1) $\phi(1_G) = 1_{G'}$ e quindi $1_G \in Ker(\phi)$. Siano $x, y \in Ker(\phi)$, allora

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} = 1_{G'}1_{G'} = 1_{G'}$$

e quindi $xy^{-1} \in Ker(\phi)$; per il criterio dei sottogruppi, $Ker(\phi) \leq G$. Siano ora $x \in Ker(\phi)$ e $g \in G$, allora

$$\phi(g^{-1}xg) = \phi(g^{-1})\phi(x)\phi(g) = (\phi(g))^{-1}1_{G'}\phi(g) = (\phi(g))^{-1}\phi(g) = 1_{G'}$$

quindi $g^{-1}xg \in Ker(\phi)$ e dunque, per il criterio di normalità, $Ker(\phi) \trianglelefteq G$.

Teorema 3.4 Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi; allora ϕ è iniettivo se e solo se $Ker(\phi) = \{1_G\}$.

Dimostrazione. (\Rightarrow) Sia ϕ un omomorfismo. Allora $\phi(1_G) = 1_{G'}$, e se ϕ è iniettivo nessun altro elemento di G ha immagine $1_{G'}$; quindi $Ker(\phi) = \{1_G\}$.

(\Leftarrow) Sia ϕ un omomorfismo tale che $Ker(\phi) = \{1_G\}$, e siano $x, y \in G$ tali che $\phi(x) = \phi(y)$. Allora

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = \phi(x)\phi(x)^{-1} = 1_{G'},$$

cioè $xy^{-1} \in Ker(\phi)$ e quindi $xy^{-1} = 1_G$ da cui $x = y$; dunque ϕ è iniettivo.

Sia N un sottogruppo normale del gruppo G . Si verifica facilmente che la applicazione

$$\pi : G \rightarrow G/N$$

$$g \mapsto gN$$

è un omomorfismo suriettivo di gruppi; si chiama la *proiezione canonica* di G su G/N .
 Notiamo che

$$g \in \ker(\pi) \Leftrightarrow \pi(g) = 1_{G/N} \Leftrightarrow gN = N \Leftrightarrow g \in N ,$$

dunque $\text{Ker}(\pi) = N$.

Quest'ultima osservazione, insieme con il Teorema 3, ci consente di affermare che *un sottoinsieme di un gruppo è un sottogruppo normale se e solo se è il nucleo di qualche omomorfismo del gruppo.*

Proveremo ora che se $\phi : G \rightarrow G'$ è un omomorfismo di gruppi; allora $G/\text{Ker}(\phi)$ è isomorfo a $\text{Im}(\phi)$. Si tratta di un fatto molto importante che dedurremo da una versione per omomorfismi del Teorema 2 della prima dispensa.

Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi, sia $K = \text{Ker}(\phi)$, e sia $\pi : G \rightarrow G/K$ la proiezione canonica. Cominciamo con l'osservare che la relazione \sim_ϕ associata alla applicazione ϕ coincide con la relazione \sim_K associata al sottogruppo K ; infatti, per ogni $x, y \in G$:

$$\begin{aligned} x \sim_K y &\Leftrightarrow x^{-1}y \in K \Leftrightarrow \phi(x^{-1}y) = 1_{G'} \Leftrightarrow \phi(x)^{-1}\phi(y) = 1_{G'} \Leftrightarrow \\ &\Leftrightarrow \phi(x) = \phi(y) \Leftrightarrow x \sim_\phi y . \end{aligned}$$

Quindi la classe di equivalenza modulo \sim_ϕ di un qualunque elemento g di G coincide con la classe laterale gK , e il quoziente G/K coincide con l'insieme quoziente G/\sim_ϕ . Applicando il Teorema citato alla applicazione ϕ , si ha che esiste un'unica applicazione $\bar{\phi} : G/K \rightarrow G'$ tale che $\bar{\phi}$ è iniettiva e $\bar{\phi} \circ \pi = \phi$. Tale $\bar{\phi}$ è definita da, per ogni $gK \in G/K$:

$$\bar{\phi}(gK) = \phi(g) ;$$

inoltre $\bar{\phi}(G/K) = \text{Im}(\phi)$.

Siano ora $xK, yK \in G/K$, allora

$$\bar{\phi}(xK \cdot yK) = \bar{\phi}(xyK) = \phi(xy) = \phi(x)\phi(y) = \bar{\phi}(xK)\bar{\phi}(yK) ,$$

quindi tale $\bar{\phi}$ è un **omomorfismo** iniettivo di gruppi. Abbiamo quindi dimostrato il

Primo Teorema di Omomorfismo per Gruppi. *Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi, $K = \text{Ker}(\phi)$, e π la proiezione canonica di G su G/K . Allora esiste un unico omomorfismo $\bar{\phi} : G/K \rightarrow G'$ tale che $\bar{\phi} \circ \pi = \phi$; inoltre $\bar{\phi}$ è iniettivo e $\text{Im}(\bar{\phi}) = \text{Im}(\phi)$.*

Corollario 3.5 *Sia $\phi : G \rightarrow G'$ un omomorfismo di gruppi. Allora $\frac{G}{\text{Ker}(\phi)} \simeq \text{Im}(\phi)$. (in particolare, se ϕ è suriettivo allora $G/\text{Ker}(\phi) \simeq G'$.)*

Il seguente esercizio è una prima applicazione di questo risultato, e ne suggerisce la forza.

Esercizio. Sia $\phi : G \rightarrow H$ un omomorfismo di gruppi finiti tali che $(|G|, |H|) = 1$. Si provi che ϕ è l'omomorfismo banale, cioè che $\phi(g) = 1_H$ per ogni $g \in G$.

Soluzione. Sia $K = \text{Ker}(\phi)$, allora per il Teorema di omomorfismo G/K è isomorfo a $\text{Im}(\phi)$; in particolare, $|G/K| = |\text{Im}(\phi)|$. Ma, per il Teorema di Lagrange, $|G/K| = [G : K]$ divide $|G|$, e $|\text{Im}(\phi)|$ divide $|H|$. Poichè $|G|$ e $|H|$ sono coprimi, deve essere $|G/K| = |\text{Im}(\phi)| = 1$, cioè $G = K$ e quindi $\phi(g) = 1_H$ per ogni $g \in G$.

Vediamo un'altra applicazione

Proposizione 3.6 *Ogni gruppo ciclico è isomorfo a un quoziente di \mathbb{Z} .*

Dimostrazione. Sia $G = \langle g \rangle$ un gruppo ciclico. Allora la applicazione $\phi : \mathbb{Z} \rightarrow G$ definita da, per ogni $z \in \mathbb{Z} : \phi(z) = g^z$ è un omomorfismo suriettivo di gruppi. Per il Teorema di omomorfismo, G è isomorfo a $\mathbb{Z}/\text{Ker}(\phi)$. (si completi il quadro, provando che $\text{Ker}(\phi) = n\mathbb{Z}$ se $|G| = n$, e $\text{Ker}(\phi) = \{0\}$ se $|G| = \infty$ - in particolare ogni gruppo ciclico infinito è isomorfo a \mathbb{Z} .)

Il primo Teorema di omomorfismo è un risultato molto importante. Da un punto di vista concettuale, esso dice che le immagini omomorfe di un gruppo si possono descrivere "all'interno" del gruppo stesso, mediante la descrizione dei suoi quozienti. In questo senso lo abbiamo utilizzato nell'esercizio di sopra. Su un piano pratico può essere utile per provare, mediante la considerazione di opportuni omomorfismi, l'esistenza di determinati quozienti in un gruppo dato. Vediamo un esempio.

Esercizio. Sia \mathbb{R}^+ il gruppo moltiplicativo dei numeri reali strettamente maggiori di zero. Si provi che il gruppo moltiplicativo \mathbb{C}^* ha un quoziente isomorfo a \mathbb{R}^+ .

Soluzione. Dato un numero complesso $z = a + ib$ ($a, b \in \mathbb{R}$), definiamo il modulo di z :

$$|z| = \sqrt{a^2 + b^2}.$$

Si verifica facilmente che, per ogni $z, z_1 \in \mathbb{C} : |zz_1| = |z||z_1|$, che per ogni $a \in \mathbb{R}^+, |a| = a$, e che $|z| = 0 \Leftrightarrow z = 0$. Quindi la applicazione $\mathbb{C}^* \rightarrow \mathbb{R}^+$ che associa ad ogni $z \in \mathbb{C}^*$ il suo modulo è un omomorfismo suriettivo di gruppi. Posto U il nucleo di tale omomorfismo, si ha, per il primo Teorema di omomorfismo, che \mathbb{C}^*/U è isomorfo a \mathbb{R}^+ .

Per completare, osserviamo che $U = \{ z \in \mathbb{C}^* \mid |z| = 1 \}$ è l'insieme dei numeri complessi che nel piano complesso stanno sulla circonferenza unitaria con centro l'origine. Gli elementi del quoziente sono le circonferenze con centro l'origine e raggio non nullo.

Esercizio. Si provi che il gruppo additivo $(\mathbb{C}, +)$ ha un quoziente isomorfo al gruppo additivo $(\mathbb{R}, +)$.

Esercizio. Si provi che il gruppo moltiplicativo \mathbb{C}^* ha un quoziente isomorfo al gruppo additivo $(\mathbb{R}, +)$.

Se H, K sono sottoinsiemi di un gruppo G , si pone

$$HK = \{ xy \mid x \in H, y \in K \}.$$

Anche nel caso, che è quello che ci interessa, in cui H e K sono sottogruppi, in generale HK non è un sottogruppo (vedi paragrafo seguente).

Ovviamente, in notazione additiva, invece di HK si scrive $H + K = \{ x + y \mid x \in H, y \in K \}$.

Lemma 3.7 *Sia G un gruppo e siano $H \leq G$ e $N \trianglelefteq G$. Allora HN è un sottogruppo di G .*

Dimostrazione. $1_G = 1_G 1_G \in HN$, quindi $HN \neq \emptyset$. Siano ora, $h, h_1 \in H$, $x, x_1 \in N$; poichè N è normale, $h_1(x x_1^{-1})h_1^{-1} \in N$ e quindi

$$(hx)(h_1 x_1)^{-1} = h x x_1^{-1} h_1^{-1} = h(h_1^{-1} h_1) x x_1^{-1} h_1^{-1} = (h h_1^{-1})(h_1 x x_1^{-1} h_1^{-1}) \in HN$$

quindi $HN \leq G$.

Lemma 3.8 *Sia $\phi : G \rightarrow G'$ un omomorfismo suriettivo di gruppi. Allora*

- 1) $H \leq G \Rightarrow \phi(H) \leq G'$;
- 2) $H \trianglelefteq G \Rightarrow \phi(H) \trianglelefteq G'$;
- 3) $T \leq G' \Rightarrow \phi^{-1}(T) \leq G$;
- 4) $T \trianglelefteq G' \Rightarrow \phi^{-1}(T) \trianglelefteq G$.

Dimostrazione. 1) È simile alla dimostrazione della Proposizione 1, e la lasciamo per esercizio.

2) Sia $H \trianglelefteq G$, allora $\phi(H) \leq G'$ per il punto 1). Siano $a \in \phi(H)$, $b \in G'$. Poichè ϕ è suriettiva, esistono $h \in H$, $g \in G$, tali che $\phi(h) = a$ e $\phi(g) = b$. Essendo $H \trianglelefteq G$ si ha $g^{-1}hg \in H$ e quindi

$$b^{-1}ab = \phi(g^{-1})\phi(h)\phi(g) = \phi(g^{-1}hg) \in \phi(H)$$

dunque $\phi(H) \trianglelefteq G'$.

3) Sia $T \leq G'$ e $\phi^{-1}(T)$ la controimmagine di T . Poichè $1_{G'} \in T$, si ha $1_G \in \phi^{-1}(T)$. Se $x, y \in \phi^{-1}(T)$ allora $\phi(x), \phi(y) \in T$ e quindi $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in T$; dunque $\phi^{-1}(T) \leq G$.

4) Sia $T \trianglelefteq G'$; allora $\phi^{-1}(T) \leq G$ per il punto 3). Siano $x \in \phi^{-1}(T)$, $g \in G$; allora $\phi(x) \in T$ e poichè T è normale in G' ,

$$\phi(g^{-1}xg) = \phi(g^{-1})\phi(x)\phi(g) = \phi(g)^{-1}\phi(x)\phi(g) \in T,$$

dunque $\phi^{-1}(T) \trianglelefteq G$.

Osservazione. Si mostri con un esempio che il punto 2) di questo Lemma non vale in generale se ϕ non è suriettiva; mentre i punti 1), 3), 4) del Lemma valgono anche senza l'ipotesi di suriettività. Tale ipotesi non è tuttavia molto restrittiva: dato un omomorfismo $\phi : G \rightarrow G'$, si può sempre definire, poichè $\phi(G)$ è un gruppo, un omomorfismo suriettivo restringendo a $\phi(G)$ il codominio originario di ϕ . Questa osservazione si applica anche al prossimo Teorema che mostra che la struttura dei sottogruppi di una immagine omomorfa (o, che è la stessa cosa, di un quoziente) di un gruppo G si legge a partire dalla struttura dei sottogruppi di G stesso.

Teorema di Corrispondenza. *Sia $\phi : G \rightarrow G'$ un omomorfismo suriettivo di gruppi e $N = \text{Ker}(\phi)$. Allora ϕ definisce una biezione tra l'insieme dei sottogruppi di G che contengono N e l'insieme di tutti i sottogruppi di G' . Tale corrispondenza conserva inclusioni e normalità.*

Dimostrazione. Poniamo

$$\mathcal{L} = \{ H \mid H \leq G \text{ e } N \leq H \}$$

$$\mathcal{S} = \{ T \mid T \leq G' \} .$$

Per il punto 1) del Lemma 2 si può definire una applicazione da \mathcal{L} in \mathcal{S} che associa ad ogni elemento di \mathcal{L} la sua immagine tramite ϕ . Definiamo cioè la applicazione

$$\Phi : \mathcal{L} \rightarrow \mathcal{S}$$

$$H \mapsto \phi(H) .$$

Chiaramente, se $H, H_1 \in \mathcal{L}$ e $H \leq H_1$, allora $\phi(H) \leq \phi(H_1)$, e per il Lemma 2, se $H \in \mathcal{L}$ è normale in G allora $\phi(H) \trianglelefteq G'$.

Rimane dunque da provare che Φ è biettiva. Sia $T \in \mathcal{S}$ e sia $H = \phi^{-1}(T)$. Allora $H \leq G$ per il Lemma 2; inoltre, poichè $1_{G'} \in T$,

$$N = \text{Ker}(\phi) = \phi^{-1}(1_{G'}) \subseteq \phi^{-1}(T) = H ,$$

quindi $H \in \mathcal{L}$ e, per definizione di controimmagine, $\phi(H) \subseteq T$. Ma poichè ϕ è suriettiva, $\phi(H) = \phi(\phi^{-1}(T)) = T$, infatti se $y \in T$, esiste $g \in G$ tale che $\phi(g) = y$; tale g appartiene a $\phi^{-1}(T) = H$. Quindi Φ è suriettiva.

Siano ora $H, K \in \mathcal{L}$ tali che $\Phi(H) = \Phi(K)$ (cioè $\phi(H) = \phi(K)$). Allora, per ogni $h \in H$ esiste $g \in K$ tale che $\phi(g) = \phi(h)$; quindi $\phi(hg^{-1}) = 1_{G'}$, cioè $hg^{-1} \in \text{Ker}(\phi) = N$. Ma $N \subseteq K$ dunque $hg^{-1} \in K$ da cui segue $h \in K$. Quindi $H \subseteq K$. Similmente si prova che $K \subseteq H$. Dunque $H = K$ e la applicazione Φ è iniettiva, concludendo la dimostrazione.

Esercizio. Sia $\phi : G \rightarrow G'$ un omomorfismo suriettivo di gruppi e $N = \text{Ker}(\phi)$. Si provi che per ogni $N \leq G$, $\phi^{-1}(\phi(H)) = HN$. Si provi che per ogni $N \leq H \leq G$, $[G : H] = [G' : \phi(H)]$.

Il Teorema di Corrispondenza dice in sostanza che, dato un omomorfismo suriettivo di gruppi, il reticolo dei sottogruppi dell'immagine coincide con il reticolo dei sottogruppi del dominio che contengono il nucleo. Una immediata e importante applicazione riguarda i sottogruppi di un gruppo quoziente.

Teorema 3.9 *Sia G un gruppo e $N \trianglelefteq G$. Allora i sottogruppi del gruppo quoziente G/N sono tutti e soli quelli del tipo H/N al variare di H nell'insieme dei sottogruppi di G che contengono N .*

Dimostrazione. Si applica il Teorema di Corrispondenza alla proiezione canonica $\pi : G \rightarrow G/N$, che è un omomorfismo suriettivo il cui nucleo è N . Quindi i sottogruppi di G/N sono le immagini tramite la proiezione dei sottogruppi H di G tali che $N \leq H$. Ora, se $N \leq H$ possiamo vedere N come sottogruppo di H ; chiaramente $N \trianglelefteq H$, e si ha

$$\pi(H) = \{ \pi(x) \mid x \in H \} = \{ xN \mid x \in H \} = \frac{H}{N} .$$

Esempio. Consideriamo il caso di un quoziente $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. I suoi sottogruppi sono in corrispondenza con i sottogruppi $m\mathbb{Z}$ di \mathbb{Z} tali che $m\mathbb{Z} \geq n\mathbb{Z}$. Si dimostri che $m\mathbb{Z} \geq n\mathbb{Z}$ se e solo se $m|n$. Quindi, i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono tutti e soli quelli del tipo

$$\frac{m\mathbb{Z}}{n\mathbb{Z}} = \{ x + n\mathbb{Z} \mid x \in m\mathbb{Z} \} = \{ mz + n\mathbb{Z} \mid z \in \mathbb{Z} \} = \{ mz + n\mathbb{Z} \mid 0 \leq mz \leq n-1 \}$$

con $m|n$.

Ad esempio, sottogruppi di $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$ sono, utilizzando la convenzione di indicare con una barra le classi resto ($a + 12\mathbb{Z} = \bar{a}$):

$$\begin{aligned}\mathbb{Z}/12\mathbb{Z} &= \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{11} \}, \\ 2\mathbb{Z}/12\mathbb{Z} &= \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10} \}, \\ 3\mathbb{Z}/12\mathbb{Z} &= \{ \bar{0}, \bar{3}, \bar{6}, \bar{9} \}, \\ 4\mathbb{Z}/12\mathbb{Z} &= \{ \bar{0}, \bar{4}, \bar{8} \}, \\ 6\mathbb{Z}/12\mathbb{Z} &= \{ \bar{0}, \bar{6} \}, \\ 12\mathbb{Z}/12\mathbb{Z} &= \{ \bar{0} \} .\end{aligned}$$

Secondo Teorema di Omomorfismo. Sia G un gruppo e siano $H \leq G$ e $N \trianglelefteq G$. Allora:

- 1) $H \cap N \trianglelefteq H$;
- 2) $\frac{HN}{N} \simeq \frac{H}{H \cap N}$.

Dimostrazione. Consideriamo la restrizione $\eta : H \rightarrow G/N$ ad H della proiezione canonica $\pi : G \rightarrow G/N$ (quindi $\eta(h) = hN$ per ogni $h \in H$). Allora η è un omomorfismo di gruppi, e

$$\text{Ker}(\eta) = \{ h \in H \mid \eta(h) = 1_{G/N} \} = \{ h \in H \mid hN = N \} = \{ h \in H \mid h \in N \} = H \cap N ,$$

in particolare, per il Teorema 3, $H \cap N \trianglelefteq H$.

Osserviamo ora che, per il Lemma 1, $HN \leq G$ e che per ogni $h \in H$, $n \in N$: $hnN = hN$, infatti $h^{-1}(hn) = n \in N$. Dunque

$$\text{Im}(\eta) = \{ \eta(h) \mid h \in H \} = \{ hN \mid h \in H \} = \{ hnN \mid hn \in HN \} = \frac{HN}{N} .$$

Quindi, per per il Primo Teorema di Omomorfismo

$$\frac{H}{H \cap N} \simeq \frac{HN}{N} .$$

Esempi. 1) Nel gruppo S_3 consideriamo il sottogruppo normale $A = \langle \gamma \rangle$ ed il sottogruppo $T = \{ \iota, \tau_1 \}$ generato dalla trasposizione τ_1 . Allora $S_3 = AT$ e $A \cap T = \{ \iota \}$; quindi, per il secondo Teorema di omomorfismo

$$\frac{S_3}{A} = \frac{AT}{A} \simeq \frac{T}{A \cap T} = T .$$

(l'isomorfismo da T a S_3/A è dato da $\iota \mapsto A$, $\tau_1 \mapsto \tau_1 A$.)

2) Abbiamo osservato in precedenza che per ogni $n, m \in \mathbb{N}$,

$$n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z} \quad \text{e} \quad n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z} .$$

Quindi per il secondo Teorema di omomorfismo

$$\frac{(n, m)\mathbb{Z}}{n\mathbb{Z}} = \frac{n\mathbb{Z} + m\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{m\mathbb{Z}}{n\mathbb{Z} \cap m\mathbb{Z}} = \frac{m\mathbb{Z}}{[n, m]\mathbb{Z}} ;$$

(si determini esplicitamente un isomorfismo tra questi due gruppi).

In particolare, se $(n, m) = 1$, $\mathbb{Z}/n\mathbb{Z} \simeq m\mathbb{Z}/nm\mathbb{Z}$; ad esempio $3\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z}$.

Esiste anche un cosiddetto **terzo** teorema di omomorfismo che enunciamo solamente, lasciando la dimostrazione per esercizio.

Teorema 3.10 Siano H, K sottogruppi normali del gruppo G e sia $K \leq H$, allora

$$\frac{H}{K} \trianglelefteq \frac{G}{K} \quad e \quad \frac{G}{H} \simeq \frac{G/K}{H/K}.$$

Ad esempio, se $m|n$ allora

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Prodotto di gruppi

Dati due sottoinsiemi A e B di un gruppo G , abbiamo definito *prodotto* di A e di B il sottoinsieme di G

$$AB = \{ab \mid a \in A, b \in B\}$$

Se A e B sono *sottogruppi* di G , il prodotto AB non è necessariamente un sottogruppo, come mostra il seguente esempio.

Esempio Consideriamo in S_3 i sottogruppi $T_1 = \langle \tau_1 \rangle$ e $T_2 = \langle \tau_2 \rangle$, dove $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ e $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{pmatrix}$. Allora $AB = \{1, \tau_1, \tau_2, \tau_1\tau_2\}$ non è un sottogruppo di G , dato che $\tau_1\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ e quindi $(\tau_1\tau_2)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \notin AB$.

Proposizione 3.11 Siano A, B sottogruppi di un gruppo G . Allora

$$AB \text{ è un sottogruppo di } G \text{ se e solo se } AB = BA.$$

Dimostrazione. \Rightarrow) Supponiamo che AB sia un sottogruppo di G . Sia $x = ba \in BA$, con $b \in B$ e $a \in A$. Allora $b = 1_G b \in AB$ e $a = a 1_G \in AB$ e quindi, siccome AB è un sottogruppo, $x \in AB$. Segue $BA \subseteq AB$. Sia, viceversa, $x \in AB$. Allora, sfruttando ancora l'ipotesi $AB \leq G$, $x^{-1} \in AB$ e quindi $x^{-1} = ab$ con $a \in A$ e $b \in B$. Dunque $x = b^{-1}a^{-1} \in BA$ e $AB \subseteq BA$.

\Leftarrow) Supponiamo $AB = BA$. Siano $x_1, x_2 \in AB$ con $x_1 = a_1 b_1$ e $x_2 = a_2 b_2$, $a_1, a_2 \in A$, $b_1, b_2 \in B$. Abbiamo $x_1 x_2^{-1} = a_1 b_1 b_2^{-1} a_2^{-1}$. Osserviamo che $b_1 b_2^{-1} a_2^{-1} \in BA = AB$ e quindi $b_1 b_2^{-1} a_2^{-1} = a_3 b_3$ per opportuni $a_3 \in A$ e $b_3 \in B$. Dunque $x_1 x_2^{-1} = a_1 a_3 b_3 \in AB$ e, dato che AB è non vuoto ($1_G = 1_G 1_G \in AB$), AB è un sottogruppo di G .

La condizione di cui sopra è sicuramente verificata se almeno uno dei due sottogruppi è normale:

Corollario 3.12 Sia $N \trianglelefteq G$. Allora per ogni $B \leq G$, $NB = BN$ e $NB \leq G$.

Esercizio. Più in generale, se $A, B \leq G$ e $b^{-1}Ab = A$ per ogni $b \in B$, allora $AB \leq G$.

Lemma 3.13 Siano A e B sottogruppi del gruppo G . Allora

a) ogni elemento $g \in AB$ si può scrivere in $|A \cap B|$ modi distinti come prodotto di un elemento di A e di un elemento di B ;

b) $|AB||A \cap B| = |A||B|$. Se G è finito,

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Dimostrazione. a) Consideriamo l'applicazione $\phi : A \times B \rightarrow G$ definita ponendo, per ogni $(a, b) \in A \times B$, $\phi((a, b)) = ab$. Osserviamo che, in generale, ϕ non è un omomorfismo. E' immediato osservare che $Im(\phi) = AB$. Sia $g \in AB$, $g = ab$ con $a \in A$ e $b \in B$, e proviamo che $\phi^{-1}(g) = \{(at, t^{-1}b) \mid t \in A \cap B\}$. Infatti $\phi((at, t^{-1}b)) = g$ e se, per $c \in A$ e $d \in B$, $\phi((c, d)) = cd = g = ab$ allora $t = a^{-1}c = bd^{-1} \in A \cap B$ e $c = at$, $b = t^{-1}d$. Quindi $|\phi^{-1}(g)| = |A \cap B|$ ovvero per $|A \cap B|$ coppie distinte $(c, d) \in A \times B$ vale $g = cd$.

b) L'insieme delle controimmagini $\{\phi^{-1}(g)\}$ è una partizione di $A \times B$ e quindi

$$|A \times B| = |A||B| = \sum_{g \in AB} |\phi^{-1}(g)| = |AB||A \cap B|.$$

Osservazione. Dal Lemma precedente segue, in particolare, che se $A, B \leq G$ e $A \cap B = \{1_G\}$ allora ogni $g \in AB$ si rappresenta in modo *unico* come prodotto di un elemento di A e di un elemento di B .

Esempio Siano $A = \langle \gamma \rangle$ e $T = \langle \tau \rangle$ sottogruppi del gruppo simmetrico S_3 , dove $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e τ è una trasposizione. Per il Corollario, AT è un sottogruppo di S_3 , dato che $A \trianglelefteq S_3$. Inoltre, poichè $A \cap T = \{1\}$,

$$|AT| = \frac{|A||T|}{|A \cap T|} = 3 \cdot 2 = |S_3|$$

e quindi $AT = S_3$.

Consideriamo ora un tipo di prodotto molto importante, il *prodotto diretto*:

Definizione. Sia G un gruppo e H, K sottogruppi di G . G si dice **prodotto diretto (interno)** di H e K se:

- 1) $G = HK$;
- 2) $H, K \trianglelefteq G$;
- 3) $H \cap K = \{1_G\}$.

In tal caso scriviamo: $G = H \times K$.

Esercizi 1) Sia $G = \{z \in \mathbb{C} \mid z^6 = 1\}$ il gruppo moltiplicativo delle radici seste dell'unità e siano $H = \{z \in \mathbb{C} \mid z^3 = 1\}$ e $K = \{z \in \mathbb{C} \mid z^2 = 1\}$ sottogruppi di G . Provare che $G = H \times K$.

2) Sia $\phi : G \rightarrow G_0$ un isomorfismo di gruppi e $H, K \leq G$. Provare che se $G = H \times K$ allora $G_0 = H_0 \times K_0$, con $H_0 = \phi(H)$ e $K_0 = \phi(K)$.

Diamo ora una descrizione alternativa del prodotto diretto di due sottogruppi:

Teorema 3.14 Sia G un gruppo e $H, K \leq G$. Allora $G = H \times K$ se e solo se:

- a) ogni elemento di G si scrive in uno ed un solo modo come prodotto di un elemento di H e di un elemento di K ;
- b) per ogni $h \in H, k \in K, hk = kh$.

Dimostrazione. Sia $G = H \times K$. Poichè $G = HK$, per ogni $g \in G$ esistono $h \in H, k \in K$ tali che $g = hk$. Ma $H \cap K = \{1_G\}$ e dunque per il Lemma 4.3 tale scrittura è unica e a) è dimostrata. Siano infine $h \in H, k \in K$ e $x = h^{-1}k^{-1}hk$. Siccome $K \trianglelefteq G, h^{-1}k^{-1}h \in K$ e quindi $x = (h^{-1}k^{-1}h)k \in K$. Analogamente, dato che $H \trianglelefteq G, k^{-1}hk \in H$ e $x = h^{-1}(k^{-1}hk) \in H$. Dunque $x \in H \cap K = \{1_G\}$. Segue $kh = kh1_G = khh^{-1}k^{-1}hk = hk$ e pertanto vale b).

Supponiamo viceversa che valgano a) e b). Se $g \in G$, per a) esistono $h \in H, k \in K$ tali che $g = hk$. Quindi $G \subseteq HK$ ovvero $HK = G$. L'unicità di scrittura, per il Lemma 4.3, equivale a $H \cap K = \{1_G\}$. Resta da provare $H, K \trianglelefteq G$. Sia $g \in G, g = hk$ con $h \in H, k \in K$, e sia $x \in K$. Allora, dato che per b) $xh = hx$, abbiamo $g^{-1}xg = k^{-1}h^{-1}xhk = k^{-1}h^{-1}hxxk = k^{-1}xk \in K$. Quindi K è un sottogruppo normale di G . Analogamente si prova che anche H è un sottogruppo normale di G .

Fino a qui abbiamo considerato il prodotto di due sottogruppi di un gruppo. Possiamo ora introdurre un concetto più generale, il prodotto diretto (esterno) di gruppi arbitrari, ovvero non necessariamente contenuti in un comune gruppo "ambiente".

Definizione. Dati i gruppi G_1, G_2 si definisce **prodotto diretto (esterno)** di G_1 e G_2 l'insieme $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ con l'operazione definita ponendo, per $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$,

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$$

Esercizio: Verificare che l'operazione data definisce una struttura di gruppo su $G_1 \times G_2$.

Proposizione 3.15 Sia $G = G_1 \times G_2$ il prodotto diretto esterno dei gruppi G_1 e G_2 e siano

$H_1 = \{(g_1, 1_{G_2}) \mid g_1 \in G_1\}$ e $H_2 = \{(1_{G_1}, g_2) \mid g_2 \in G_2\}$. Allora :

- 1) H_1 e H_2 sono sottogruppi normali di G ;
- 2) $H_1 \simeq G_1$ e $H_2 \simeq G_2$;
- 3) G è prodotto diretto interno dei sottogruppi H_1 e H_2 .

Dimostrazione. Siano $\pi_1 : G \rightarrow G_1$ e $\pi_2 : G \rightarrow G_2$ applicazioni definite ponendo, per $g = (g_1, g_2) \in G, \pi_1(g) = g_1$ e $\pi_2(g) = g_2$. Poichè π_1, π_2 sono omomorfismi (verificare per esercizio), i rispettivi nuclei $\text{Ker}(\pi_1) = H_2$ e $\text{Ker}(\pi_2) = H_1$ sono sottogruppi normali di G . Inoltre, le restrizioni $\pi_1|_{H_1} : H_1 \rightarrow G_1$ e $\pi_2|_{H_2} : H_2 \rightarrow G_2$ sono isomorfismi. La suriettività segue infatti subito dalla definizione dei π_i . Inoltre, $\text{Ker}(\pi_1|_{H_1}) = H_1 \cap H_2 = \{1_G\}$ e, analogamente, $\text{Ker}(\pi_2|_{H_2}) = \{1_G\}$ e quindi i π_1 e π_2 sono iniettivi. Dunque 1) e 2) sono provate. Per provare 3) osserviamo che, se $g = (g_1, g_2) \in G$,

$g = (g_1, 1_{G_2})(1_{G_1}, g_2) \in H_1 H_2$ e quindi $G = H_1 H_2$. Inoltre, per ogni $(g_1, 1_{G_2}) \in H_1$ e $(1_{G_1}, g_2) \in H_2$, vale $(g_1, 1_{G_2})(1_{G_1}, g_2) = (g_1, g_2) = (1_{G_1}, g_2)(g_1, 1_{G_2})$.

Osservazione: Per la Proposizione 4.4, ogni gruppo isomorfo al prodotto diretto esterno di due gruppi è prodotto diretto interno di sottogruppi isomorfi ai gruppi dati. Nel seguito, quindi, parleremo semplicemente di prodotto diretto, tralasciando la distinzione tra i casi interno ed esterno.

Esercizio Siano C_n e C_m gruppi ciclici di ordine rispettivamente n e m . Provare che il prodotto diretto $C_n \times C_m$ è ciclico se e solo se $(n, m) = 1$.

Fino a qui abbiamo considerato prodotti di due gruppi. Più in generale, se H_1, H_2, \dots, H_n sono sottogruppi di G , possiamo definire il prodotto

$$H_1 H_2 \dots H_n = \{g \in G \mid g = h_1 h_2 \dots h_n \text{ con } h_i \in H_i, i = 1, 2, \dots, n\}$$

Esercizio Provare che se H_1, H_2, \dots, H_n sono sottogruppi normali di G allora $H_1 H_2 \dots H_n$ è un sottogruppo di G .

Definiamo ora il prodotto diretto (esterno) di n gruppi, dove n è un qualunque intero positivo.

Definizione Siano G_1, G_2, \dots, G_n gruppi ($n \in \mathbb{N}_0$). Nell'insieme

$$G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i \text{ per } i = 1, 2, \dots, n\}$$

definiamo una operazione ponendo:

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n)$$

Rispetto a tale operazione $G_1 \times G_2 \times \dots \times G_n$ è un gruppo, detto **prodotto diretto (esterno)** dei gruppi G_1, G_2, \dots, G_n .

Osserviamo che, se $G = G_1 \times G_2 \times \dots \times G_n$, $1_G = (1_{G_1}, 1_{G_2}, \dots, 1_{G_n})$ e, per ogni $(g_1, g_2, \dots, g_n) \in G$, $(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$.

Analogamente a quanto visto nella Proposizione 4.4, ogni prodotto diretto esterno è prodotto di opportuni sottogruppi, isomorfi ai fattori "esterni". La dimostrazione del seguente risultato, che omettiamo, è simile a quella della Proposizione 4.4.

Proposizione 3.16 Sia $G = G_1 \times G_2 \times \dots \times G_n$ il prodotto diretto esterno dei gruppi G_i e sia, per $i = 1, 2, \dots, n$,

$$H_i = \{(1_{G_1}, 1_{G_2}, \dots, g_i, \dots, 1_{G_n}) \mid g_i \in G_i\}.$$

Allora:

- (1) $H_i \trianglelefteq G$
- (2) $G = H_1 H_2 \dots H_n$
- (3) $H_i \cap H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n = \{1_G\}$, per ogni $i \in \{1, 2, \dots, n\}$
- (4) $H_i \simeq G_i$, per ogni $i \in \{1, 2, \dots, n\}$.

Definizione. Sia G un gruppo e H_1, H_2, \dots, H_n sottogruppi di G che verificano le condizioni (1), (2) e (3) della Proposizione 4.6. Allora G si dice **prodotto diretto (interno)** dei sottogruppi H_1, H_2, \dots, H_n .

Osservazioni

- 1) Nel seguito non distingueremo tra prodotto diretto esterno ed interno e parleremo semplicemente di “prodotto diretto”.
- 2) La condizione (3) non puo’ essere indebolita richiedendo semplicemente $H_j \cap H_i = \{1\}$ per ogni $i \neq j$. Sia infatti, ad esempio, $G = C_1 \times C_2$ il prodotto diretto di due gruppi ciclici di ordine 2, $C_1 = \langle x_1 \rangle$ e $C_2 = \langle x_2 \rangle$. Il gruppo G , che è abeliano, ha tre sottogruppi normali di ordine 2, $H_1 = \langle (x_1, 1) \rangle$, $H_2 = \langle (1, x_2) \rangle$ e $H_3 = \langle (x_1, x_2) \rangle$. H_1 , H_2 e H_3 si intersecano a due a due trivialmente, ma ognuno di essi è contenuto nel prodotto degli altri due, che è G stesso.
- 3) Nel caso di gruppi in notazione additiva, si usa di solito l’espressione “somma diretta” al posto di “prodotto diretto”.

Esempio. Il gruppo additivo $(\mathbb{R}^n, +)$ dello spazio vettoriale \mathbb{R}^n di dimensione n sul campo reale è isomorfo alla somma diretta di n “copie” del gruppo additivo $(\mathbb{R}, +)$.

Automorfismi

Ricordiamo che un **automorfismo** di un gruppo G è un isomorfismo di G in se stesso. Abbiamo osservato (pagina 13) che

L’insieme degli automorfismi di G con l’operazione di composizione è un gruppo.

Tale gruppo, il cui elemento identico è l’identità 1_G , si denota con $Aut(G)$.

Particolari automorfismi di un gruppo G sono i coniugi. Dato $g \in G$, si definisce una applicazione

$$\begin{aligned} \sigma_g : G &\rightarrow G \\ x &\mapsto g^{-1}xg \end{aligned}$$

che si chiama **coniugio** tramite l’elemento g .

Proposizione 3.17 *Sia G un gruppo, allora per ogni $g \in G$, $\sigma_g \in Aut(G)$.*

Dimostrazione. Fissato $g \in G$, siano $x, y \in G$; allora

$$\sigma_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \sigma_g(x)\sigma_g(y),$$

quindi σ_g è un omomorfismo. Verifichiamo che è iniettivo; sia $x \in Ker(\sigma_g)$, allora $g^{-1}xg = 1_G$ da cui, moltiplicando a sinistra per g e a destra per g^{-1} si ottiene $x = 1_G$, quindi $Ker(\sigma_g) = \{1_G\}$ e per il Teorema 4 σ_g è iniettiva. Infine, σ_g è suriettiva perchè per ogni $y \in G$, $y = g^{-1}gyg^{-1}g = \sigma_g(gyg^{-1})$. Dunque σ_g è biettiva e quindi un automorfismo di G .

Sia $g \in G$ e $S \subseteq G$. L’immagine di S tramite l’automorfismo σ_g si chiama **coniugato** di S tramite g , e si denota con $g^{-1}Sg$ o, più comodamente, con S^g . Quindi

$$S^g = \{ g^{-1}xg \mid x \in S \}.$$

Questo concetto è particolarmente rilevante nel caso in cui S sia un sottogruppo di G . Ad esempio, si provi per esercizio la seguente importante osservazione

Proposizione 3.18 *Sia H un sottogruppo del gruppo G . Allora $H \trianglelefteq G$ se e solo se H coincide con tutti i suoi coniugati (cioè $H = H^g$ per ogni $g \in G$).*

Osserviamo che se G è commutativo, allora per ogni $x, g \in G$, $g^{-1}xg = g^{-1}gx = x$. Quindi se G è commutativo ogni coniugazione è l'identità. Le coniugazioni sono quindi rilevanti solo per i gruppi non commutativi, nel qual caso sono gli automorfismi più importanti.

Sia G un gruppo e ϕ un automorfismo di G . L'insieme degli elementi di G che sono mandati in se stessi da ϕ si dice insieme dei **punti fissi** di ϕ . Chiaramente 1_G è un punto fisso per ogni automorfismo; il prossimo Lemma asserisce che l'insieme dei punti fissi è sempre un sottogruppo di G . La dimostrazione è immediata e la lasciamo per esercizio.

Lemma 3.19 . *Sia G un gruppo e $\phi \in \text{Aut}(G)$; allora l'insieme $\{x \in G \mid \phi(x) = x\}$ è un sottogruppo di G .*

Sia G un gruppo e $g \in G$. L'insieme degli elementi di G che commutano con g si chiama **centralizzante** di g e si denota con $C_G(g)$. Quindi

$$C_G(g) = \{x \in G \mid gx = xg\}.$$

Ora, $gx = xg$ se e solo se $x = g^{-1}xg = \sigma_g(x)$. Quindi il centralizzante di g non è altro che l'insieme dei punti fissi di σ_g , dunque per il Lemma precedente,

$$\text{per ogni } g \in G, C_G(g) \leq G.$$

(Si dimostri questo fatto direttamente dalla definizione di centralizzante)

Definizione. Sia G un gruppo. Il **centro** di G è l'insieme degli elementi che commutano con tutti gli elementi di G . Esso si denota con $Z(G)$.

Quindi $Z(G) = \{x \in G \mid xg = gx \text{ per ogni } g \in G\}$, e anche

$$Z(G) = \bigcap_{g \in G} C_G(g).$$

Chiaramente $1_G \in Z(G)$, e G è commutativo se e solo se $G = Z(G)$.

Esercizio. Si provi che per ogni gruppo G si ha $Z(G) \trianglelefteq G$.

Esercizio. Sia G un gruppo e $x, y \in G$. Si provi che $\sigma_x = \sigma_y$ se e solo se $x^{-1}y \in Z(G)$.

Osserviamo che può bene verificarsi il caso che $Z(G)$ si riduca al sottogruppo banale; ad esempio, verificate che $Z(S_3) = \{e\}$.

Il resto di questa sezione è di carattere complementare, ma è una interessante e istruttiva applicazione del Teorema di omomorfismo.

Dato un gruppo G denotiamo con $\text{Inn}(G) = \{\sigma_g \mid g \in G\}$ l'insieme di tutte le coniugazioni di G .

Proposizione 3.20 *Sia G un gruppo. Allora $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.*

Dimostrazione. Innanzi tutto osserviamo che, per ogni $g, x \in G$,

$$\sigma_{g^{-1}} \circ \sigma_g(x) = \sigma_{g^{-1}}(g^{-1}xg) = gg^{-1}xgg^{-1} = x = \iota_G(x)$$

quindi $\sigma_{g^{-1}} = \sigma_g^{-1}$. Proviamo ora che $Inn(G)$ è un sottogruppo di $Aut(G)$. Abbiamo appena visto che $Inn(G)$ contiene l'inverso di ogni suo elemento. Verifichiamo quindi la chiusura: siano $\sigma_g, \sigma_h \in Inn(G)$; allora per ogni $x \in G$,

$$\sigma_g \circ \sigma_h(x) = \sigma_g(h^{-1}xh) = g^{-1}h^{-1}xhg = (hg)^{-1}x(hg)\sigma_{hg}$$

quindi $\sigma_g \circ \sigma_h = \sigma_{hg} \in Inn(G)$. Poichè $\iota_G = \sigma_{1_G} \in Inn(G)$, si ha quindi $Inn(G) \leq Aut(G)$. Verifichiamo ora la normalità. Siano $\sigma_g \in Inn(G)$ e $\phi \in Aut(G)$. Allora, per ogni $x \in G$,

$$\begin{aligned} \phi^{-1} \circ \sigma_g \circ \phi(x) &= \phi^{-1} \circ \sigma_g(\phi(x)) = \phi^{-1}(g^{-1}\phi(x)g) = \\ &= \phi^{-1}(g^{-1})\phi^{-1}(\phi(x))\phi^{-1}(g) = \phi^{-1}(g)^{-1}x\phi^{-1}(g) = \sigma_{\phi^{-1}(g)}, \end{aligned}$$

quindi $\phi^{-1} \circ \sigma_g \circ \phi = \sigma_{\phi^{-1}(g)} \in Inn(G)$. Per il criterio di normalità, $Inn(G) \trianglelefteq Aut(G)$.

Teorema 3.21 *Sia G un gruppo. Allora $Inn(G) \simeq G/Z(G)$.*

Dimostrazione. Consideriamo la applicazione

$$\begin{aligned} \Phi : G &\rightarrow Inn(G) \\ g &\mapsto \sigma_{g^{-1}} \end{aligned}$$

Φ è un omomorfismo di gruppi; infatti dalla dimostrazione della Proposizione precedente segue che, per ogni $g, h \in G$,

$$\Phi(g)\Phi(h) = \sigma_{g^{-1}} \circ \sigma_{h^{-1}} = \sigma_{h^{-1}g^{-1}} = \sigma_{(gh)^{-1}} = \Phi(gh).$$

Ora, $g \in Ker(\Phi)$, se e solo se $\sigma_{g^{-1}} = \iota_G$, se e solo se $gxg^{-1} = x$ per ogni $x \in G$, se e solo se $gx = xg$ per ogni $x \in G$, se e solo se $g \in Z(G)$. Quindi $Ker(\Phi) = Z(G)$. Poichè Φ è suriettiva per definizione di $Inn(G)$, per il primo Teorema di omomorfismo si conclude che

$$\frac{G}{Z(G)} \simeq Inn(G)$$

come si voleva dimostrare.

Esercizio. Si provi che $Aut(S_3) = Inn(S_3) \simeq S_3$.

ESERCIZI

1. Sia G un gruppo tale che $(xy)^3 = x^3y^3$ per ogni $x, y \in G$. Si provi che $\{x^3 \mid x \in G\}$ è un sottogruppo normale di G .

2. Sull'insieme $W = \mathbb{R}^* \times \mathbb{R}$ si definisca una operazione ponendo, per ogni $(a, b), (a_1, b_1) \in W$:

$$(a, b)(a_1, b_1) = (aa_1, ab_1 + b).$$

Si provi che, con tale operazione, W è un gruppo. Si dimostri che $K = \{(1, b) \mid b \in \mathbb{R}\}$ è un sottogruppo normale, e che $W/K \simeq \mathbb{R}^*$.

3. Siano N, M sottogruppi normali del gruppo G tali che $N \cap M = \{1_G\}$. Si provi che, per ogni $x \in N, y \in M$ si ha $xy = yx$.
4. Si provi che per ogni elemento x del gruppo (additivo) $G = \mathbb{Q}/\mathbb{Z}$ esiste un $n \geq 1$ tale che $nx = 0_G$.
5. Sia H un sottogruppo proprio del gruppo additivo dei razionali \mathbb{Q} . Si provi che $[\mathbb{Q} : H] = \infty$.
6. Sia $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ il gruppo moltiplicativo delle radici n -esime dell'unità. Si provi che \mathbb{C}^*/U_n è isomorfo a \mathbb{C}^* . [Si usi il fatto che per ogni $z \in \mathbb{C}^*$ esiste $a \in \mathbb{C}^*$ tale che $a^n = z$].
7. Sia G un gruppo finito e siano $H, K \leq G$ tali che $|H|^2 > |G|$ e $|K|^2 > |G|$. Si provi che $H \cap K \neq \{1_G\}$.
8. Siano G, N i gruppi definiti nell'esempio a pagina 31. Si provi che $G/N \simeq \mathbb{R}^* \times \mathbb{R}^*$. [Si cominci col trovare un omomorfismo suriettivo da G in $\mathbb{R}^* \times \mathbb{R}^*$.]
9. Sia P l'insieme dei numeri reali strettamente maggiori di 0. Si provi che $\mathbb{R}^* = \{1, -1\} \times P$.
10. Si provi che il gruppo $\mathbb{Z} \times \mathbb{Z}$ non è ciclico.
11. Si determinino tutti i coniugati in S_3 del sottogruppo $T = \langle \tau_1 \rangle$.
12. Sia G un gruppo e $H \leq G$. Il *normalizzatore* di H in G è l'insieme

$$N_G(H) = \{ g \in G \mid g^{-1}Hg = H \}$$

(si osservi che $H \trianglelefteq G$ se e solo se $N_G(H) = G$). Si dimostri che $H \leq N_G(H) \leq G$.

13. Nel gruppo $G = GL(2, \mathbb{R})$ si determini il centralizzatore $C_G(g)$ dell'elemento $g = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$. Si determini quindi $Z(GL(2, \mathbb{R}))$.
14. Sia $G = \langle g \rangle$ un gruppo ciclico.
 - i) Si provi che se α, β sono omomorfismi di G nel medesimo gruppo H , e $\alpha(g) = \beta(g)$, allora $\alpha = \beta$.
 - ii) Si provi che per ogni $\psi \in \text{Aut}(G)$, $\psi(g)$ è un generatore di G .
 - iii) Si provi che se $|G| = n$ allora $|\text{Aut}(G)| = \phi(n)$, dove ϕ è la funzione di Eulero.
15. Si determini $\text{Aut}(\mathbb{Z})$.

4 Azioni di Gruppi

Il concetto di azione di un gruppo è molto importante in matematica. Abbiamo visto nelle sezioni precedenti che l'insieme di tutte le permutazioni di un insieme è un gruppo, l'insieme di tutti gli automorfismi di un gruppo è un gruppo, e che l'insieme delle simmetrie di un sistema di punti del piano è un gruppo. Questi gruppi possono essere visti come costituiti dall'insieme delle biezioni che conservano una certa "struttura" (gli automorfismi di un gruppo G sono biezioni che conservano l'operazione, le simmetrie di una figura piana sono biezioni del piano che conservano la figura stessa - che possiamo intendere come una struttura geometrica, le permutazioni semplicemente conservano una struttura "nulla"). Questo è un fenomeno molto generale; un altro esempio è dato dall'insieme di tutti gli automorfismi di uno spazio vettoriale, che costituisce un gruppo. Detto in modo informale, una *azione* di un gruppo G significa un omomorfismo del gruppo G nel gruppo delle biezioni su una certa struttura. Ad esempio, sia V uno spazio vettoriale di dimensione n sui reali e \mathcal{B} una sua base fissata, allora ad ogni matrice quadrata reale invertibile di ordine n si associa una applicazione lineare definita rispetto alla base \mathcal{B} , e ciò definisce un isomorfismo del gruppo $GL(n, \mathbb{R})$ nel gruppo $Aut_{\mathbb{R}}(V)$ di tutte le applicazioni lineari invertibili di V in se stesso; questa è una azione di $GL(n, \mathbb{R})$ come gruppo di applicazioni lineari.

In questa sezione studieremo alcuni tipi di azione; come gruppi di permutazioni (si chiamano azioni su un insieme), come gruppi di simmetrie di una figura piana, e come gruppi di automorfismi di un gruppo. Le azioni come gruppi di permutazioni sono in un certo senso quelle fondamentali e sottendono a tutti gli altri tipi di azione; inizieremo quindi con esse. Per prima cosa introdurremo qualche strumento generale per lavorare con i gruppi simmetrici.

Permutazioni

Ricordiamo che, se I è un insieme, si dice *permutazione* su I una qualunque applicazione biunivoca di I in se e si denota con $Sym(I)$ il gruppo, rispetto alla composizione, delle permutazioni su I . Se I e J sono due insiemi della stessa cardinalità, allora $Sym(I) \simeq Sym(J)$. Se I è un insieme finito di n elementi possiamo quindi assumere che sia $I = \{1, 2, \dots, n\}$. Di solito, invece di $Sym(\{1, 2, \dots, n\})$, viene usato il simbolo S_n .

Ogni $\pi \in S_n$ può essere rappresentata nel modo seguente:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(i) & \dots & \pi(n) \end{pmatrix}$$

Esiste però una rappresentazione per molti aspetti più conveniente:

Esempio. Sia $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 7 & 6 \end{pmatrix} \in S_7$. Osserviamo che $\pi(1) = 3$, $\pi(3) = 5$ e $\pi(5) = 1$ ovvero $1 \xrightarrow{\pi} 3 \xrightarrow{\pi} 5 \xrightarrow{\pi} 1$. Inoltre, $2 \xrightarrow{\pi} 2$, $4 \xrightarrow{\pi} 4$ e $6 \xrightarrow{\pi} 7 \xrightarrow{\pi} 6$. Scriviamo allora

$$\pi = (1\ 3\ 5)(6\ 7).$$

Cominciamo introducendo il concetto di *permutazione ciclica* (o *ciclo*) :

Definizione. π : Una permutazione $\sigma \in S_n$ si dice un **ciclo di lunghezza k** (o un **k -ciclo**), per k intero, $k > 1$, se esiste un sottoinsieme di ordine k $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$ tale che

$$(a) \quad \pi(i_1) = i_2, \pi(i_2) = i_3, \dots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1 \quad ;$$

$$(b) \quad \pi(j) = j \text{ per ogni } j \in \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_k\} .$$

Scriviamo allora

$$\sigma = (i_1\ i_2\ \dots\ i_k).$$

Osservazioni. 1) Se σ è un k -ciclo, $\sigma = (i_1\ i_2\ \dots\ i_k)$, possiamo anche scrivere in modo equivalente

$$\sigma = (i_2\ i_3\ \dots\ i_k\ i_1) = (i_3\ i_4\ \dots\ i_k\ i_1\ i_2) = \dots$$

2) Se $\sigma = (i_1\ i_2\ \dots\ i_k)$ è un k -ciclo, allora $\sigma^2(i_1) = i_3, \sigma^2(i_2) = i_4, \dots, \sigma^2(i_k) = i_2$ e, più in generale, per $1 \leq r \leq k$

$$\sigma^r(i_j) = i_{j+r} \text{ se } j+r \leq k$$

$$\sigma^r(i_j) = i_{j+r-k} \text{ se } j+r > k .$$

Notazione. A differenza di quanto convenuto per le applicazioni, da questo momento scriveremo le permutazioni *a destra* degli elementi cui vengono applicate e cambieremo di conseguenza anche la notazione della composizione di due permutazioni. Se $\sigma_1, \sigma_2 \in S_n$ e $i \in \{1, 2, \dots, n\}$, denoteremo con $i\sigma_1$ l'immagine di i tramite σ_1 e con $\sigma_1\sigma_2$ la permutazione ottenuta componendo *prima* σ_1 e *poi* σ_2 . Pertanto, per ogni $i \in \{1, 2, \dots, n\}$, $i\sigma_1\sigma_2 = (i\sigma_1)\sigma_2$.

Esempio. Consideriamo in S_5 le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} \quad e \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} .$$

α è un 3-ciclo, $\alpha = (2\ 4\ 3)$, e β è un 2-ciclo, $\beta = (1\ 3)$. La composizione $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$ è un 4-ciclo: $\alpha\beta = (1\ 3\ 2\ 4)$.

Definizione. Data una permutazione $\pi \in S_n$, si dice **supporto** di π l'insieme

$$\text{supp}(\pi) = \{i \mid i \in \{1, 2, \dots, n\}, i\pi \neq i\}$$

degli elementi “mossi” dalla π .

Esempi. 1) Se $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix} \in S_7$, $\text{supp}(\pi) = \{1, 2, 4, 6\}$.

2) Se $\sigma = (i_1\ i_2\ \dots\ i_k)$ è un k -ciclo ($k > 1$), allora $\text{supp}(\sigma) = \{i_1, i_2, \dots, i_k\}$.

Se $\sigma = \iota$, $\text{supp}(\sigma) = \emptyset$.

Osserviamo che, come segue subito dalla definizione, per ogni permutazione π vale

$$\text{supp}(\pi^{-1}) = \text{supp}(\pi) .$$

Definizione. Due cicli $\sigma_1, \sigma_2 \in S_n$ si dicono **disgiunti** se $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset$.

Proposizione 4.1 1) Se $\sigma = (i_1 i_2 \dots i_k)$ allora $\sigma^{-1} = (i_k i_{k-1} \dots i_1)$.

2) Se σ e' un k -ciclo, allora $|\sigma| = k$.

3) Se σ_1, σ_2 sono cicli disgiunti, allora sono permutabili : $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Dimostrazione. 1) Sia $\tau = (i_k i_{k-1} \dots i_1)$. Se $j \notin \{i_1, i_2, \dots, i_k\}$ chiaramente $j\sigma\tau = j = j\tau\sigma$. Se $j \in \{i_1, i_2, \dots, i_k\}$, si verifica immediatamente che vale ancora $j\sigma\tau = j = j\tau\sigma$.

2) Se σ e' un k -ciclo, allora $\sigma^k = \iota$. D'altra parte, se h e' un intero positivo, $h < k$, abbiamo $i_1\sigma^h = i_{h+1}$, dato che $h+1 \leq k$. Quindi $i_1\sigma \neq i_1$ e $\sigma^h \neq \iota$.

3) Siano $\sigma_1, \sigma_2 \in S_n$ tali che $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset$ e sia $j \in \{1, 2, \dots, n\}$. Se $j \notin \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$, allora $j\sigma_1\sigma_2 = j = j\sigma_2\sigma_1$. Se $j \in \text{supp}(\sigma_1)$ e $i = j\sigma_1$, allora $i \in \text{supp}(\sigma_1)$ e dunque $i, j \notin \text{supp}(\sigma_2)$. Quindi $j\sigma_1\sigma_2 = i\sigma_2 = i = j\sigma_1 = j\sigma_2\sigma_1$. Se $j \in \text{supp}(\sigma_2)$ si procede analogamente. Dunque $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Teorema 4.2 Ogni permutazione $\pi \in S_n$, $\pi \neq \iota$, si può esprimere come prodotto

$$\pi = \sigma_1\sigma_2 \dots \sigma_t$$

di cicli disgiunti $\sigma_1, \sigma_2, \dots, \sigma_t \in S_n$. Tale decomposizione è unica, a meno dell'ordine dei fattori.

Dimostrazione. Procediamo per induzione sull'ordine di $\text{supp}(\pi)$. Scegliamo $i \in \text{supp}(\pi)$ e sia $J = \{i\pi^m \mid m \text{ intero positivo}\}$. Poichè $J \subseteq \{1, 2, \dots, n\}$, esistono sicuramente due interi positivi a e b , $b > a$, tali che $i\pi^b = i\pi^a$ e quindi $i\pi^{b-a} = i$. Denotiamo con k il minimo dell'insieme $\{h \mid h \in \mathbb{N}_0, i\pi^h = i\}$, non vuoto per quanto appena osservato, e siano $i_1 = i, i_2 = i\pi, \dots, i_k = i\pi^{k-1}$. Dunque $J = \{i_1, i_2, \dots, i_k\}$ e, considerando il k -ciclo $\sigma = (i_1 i_2 \dots i_k)$, abbiamo $j\sigma^{-1}\pi = j$ per ogni $j \in J$. Quindi $\text{supp}(\sigma^{-1}\pi) = \text{supp}(\pi) \setminus J$. Se $\sigma^{-1}\pi = \iota$ allora $\pi = \sigma$ è un ciclo. Altrimenti, applicando l'ipotesi di induzione, abbiamo $\sigma^{-1}\pi = \sigma_2\sigma_3 \dots \sigma_t$ con $\sigma_2, \sigma_3, \dots, \sigma_t \in S_n$ cicli disgiunti. Dunque $\pi = \sigma\sigma_2 \dots \sigma_t$ è prodotto di cicli disgiunti, dato che $\text{supp}(\sigma) = J$ e $\text{supp}(\sigma_u) \subseteq \text{supp}(\pi) \setminus J$ per ogni $2 \leq u \leq t$. Supponiamo infine che $\pi = \sigma_1\sigma_2 \dots \sigma_t$ e $\pi = \tau_1\tau_2 \dots \tau_u$ siano due decomposizioni di π in prodotto di cicli disgiunti e sia $i \in \text{supp}(\sigma_1)$. Poichè, in particolare, $i \in \text{supp}(\pi)$, esiste un τ_j per cui $i \in \text{supp}(\tau_j)$. Dato che le τ_j sono permutabili, possiamo supporre $i \in \text{supp}(\tau_1)$. Allora, come si verifica facilmente, deve essere $\sigma_1 = \tau_1$. Dunque, procedendo per induzione come sopra, segue $t = u$ e $\sigma_j = \tau_j$ per ogni $1 \leq j \leq t$.

Esercizio. Sia $\pi = \sigma_1\sigma_2 \dots \sigma_t$ con σ_i k_i -cicli disgiunti, per $1 \leq i \leq t$.

Provare che $\text{supp}(\pi) = \bigcup_{i=1}^t \text{supp}(\sigma_i)$ e che $|\pi| = \text{m.c.m.}(k_1, k_2, \dots, k_t)$.

Vediamo ora come la decomposizione in cicli fornisca un semplice criterio per stabilire se due permutazioni in S_n sono coniugate. Premettiamo una definizione:

Definizione. Siano $\pi, \rho \in S_n$. Diciamo che π e ρ hanno lo stesso **tipo ciclico** se, date le decomposizioni $\pi = \sigma_1 \sigma_2 \dots \sigma_t$ e $\rho = \tau_1 \tau_2 \dots \tau_u$ in prodotto di cicli disgiunti, vale $t = u$ e, a meno di rinumerazione, σ_i e τ_i sono cicli della stessa lunghezza, per ogni $1 \leq i \leq t$.

Ad esempio, le permutazioni $(1\ 2)(3\ 5\ 4)(6\ 7)$ e $(1\ 3\ 2)(4\ 6)(5\ 7)$ hanno lo stesso tipo ciclico.

Lemma 4.3 1) Sia $\sigma = (i_1\ i_2\ \dots\ i_k)$ un k -ciclo in S_n e $\pi \in S_n$. Allora $\pi^{-1}\sigma\pi = (i_1\pi\ i_2\pi\ \dots\ i_k\pi)$.

2) Se $\gamma, \pi \in S_n$ e $\gamma = \sigma_1 \sigma_2 \dots \sigma_t$ è la decomposizione in prodotto di cicli disgiunti di γ , allora $\pi^{-1}\gamma\pi = (\pi^{-1}\sigma_1\pi)(\pi^{-1}\sigma_2\pi) \dots (\pi^{-1}\sigma_t\pi)$ è la decomposizione in prodotto di cicli disgiunti della coniugata $\pi^{-1}\gamma\pi$.

Dimostrazione. 1) Osserviamo che $\text{supp}(\pi^{-1}\sigma\pi) = \text{supp}(\sigma)\pi$. Infatti, per $j \in \{1, 2, \dots, n\}$, vale $j = j(\pi^{-1}\sigma\pi)$ se e solo se $j\pi^{-1} = j\pi^{-1}\sigma$ ovvero $j\pi^{-1} \notin \text{supp}(\sigma)$ cioè $j \notin \text{supp}(\sigma)\pi$. Per $j < k$, $(i_j\pi)(\pi^{-1}\sigma\pi) = i_j\sigma\pi = i_{j+1}\pi$. Inoltre, $(i_k\pi)(\pi^{-1}\sigma\pi) = i_k\sigma\pi = i_1\pi$. Dunque $\pi^{-1}\sigma\pi$ è il k -ciclo $(i_1\pi\ i_2\pi\ \dots\ i_k\pi)$. La 2) segue da 1), osservando che la $\text{supp}(\pi^{-1}\sigma_i\pi) \cap \text{supp}(\pi^{-1}\sigma_j\pi) = \text{supp}(\sigma_i)\pi \cap \text{supp}(\sigma_j)\pi = \emptyset$ per ogni $i \neq j$, $1 \leq i, j \leq t$.

Esempio. Consideriamo in S_6 gli elementi $\pi = (1\ 2\ 3\ 4\ 5)$ e $\gamma = (1\ 3)(2\ 5\ 4\ 6)$. Allora $\pi^{-1}\gamma\pi = (2\ 4)(3\ 1\ 5\ 6)$.

Proposizione 4.4 Due permutazioni γ e δ sono coniugate in S_n se e solo se hanno lo stesso tipo ciclico.

Dimostrazione. Supponiamo che, per $\pi \in S_n$, sia $\delta = \pi^{-1}\gamma\pi$. Allora per il Lemma 4.3, γ e δ hanno lo stesso tipo ciclico.

Supponiamo viceversa che γ e δ abbiano lo stesso tipo ciclico. Sia $\gamma = (a_1\ a_2\ \dots\ a_h)(b_1\ b_2\ \dots\ b_k) \dots$ e $\delta = (\hat{a}_1\ \hat{a}_2\ \dots\ \hat{a}_h)(\hat{b}_1\ \hat{b}_2\ \dots\ \hat{b}_k) \dots$ e siano $\{f_1, f_2, \dots, f_m\} = \{1, 2, \dots, n\} \setminus \text{supp}(\gamma)$ e $\{\hat{f}_1, \hat{f}_2, \dots, \hat{f}_m\} = \{1, 2, \dots, n\} \setminus \text{supp}(\delta)$ gli insiemi degli elementi fissati γ e δ rispettivamente. Osserviamo che $m = \hat{m}$, poiché $|\text{supp}(\gamma)| = |\text{supp}(\delta)|$. Consideriamo quindi la permutazione

$$\pi = \begin{pmatrix} a_1 & a_2 & \dots & a_h & b_1 & b_2 & \dots & b_k & \dots & f_1 & f_2 & \dots & f_m \\ \hat{a}_1 & \hat{a}_2 & \dots & \hat{a}_h & \hat{b}_1 & \hat{b}_2 & \dots & \hat{b}_k & \dots & \hat{f}_1 & \hat{f}_2 & \dots & \hat{f}_m \end{pmatrix}.$$

Per il Lemma 4.3 segue allora $\delta = \pi^{-1}\gamma\pi$.

Prendiamo ora in considerazione un altro modo di decomporre una permutazione in prodotto di cicli. Questa volta i fattori ciclici avranno tutti lunghezza 2, ma non più, in generale, supporti disgiunti.

Definizione. Un ciclo di lunghezza 2 si dice **trasposizione**.

Lemma 4.5 Ogni ciclo di lunghezza k si può esprimere come prodotto di $k - 1$ trasposizioni.

Dimostrazione. Vale infatti $(i_1 i_2 \dots i_k) = (i_1 i_2)(i_1 i_3) \dots (i_1 i_k)$, come si verifica facilmente per induzione su k .

Osserviamo come la decomposizione in prodotto di cicli di lunghezza due del lemma precedente *non* sia più però costituita da cicli *disgiunti*. Anche l'unicità di decomposizione viene a cadere: in S_4 , ad esempio $(1 2 3) = (1 2)(1 3) = (1 2)(4 3)(1 3)(1 4)$. Inoltre, $(1 2)(1 3) \neq (1 3)(1 2)$.

Corollario. Ogni permutazione $\pi \in S_n$, $\pi \neq \iota$, si può scrivere come prodotto di trasposizioni. Dunque

$$S_n = \langle \{ \tau \mid \tau \in S_n, \tau \text{ trasposizione} \} \rangle .$$

Esercizio. Provare che, dati $a, b, c \in \{1, 2, \dots, n\}$, vale $(b c) = (a b)(a c)(a b)$ in S_n . Provare quindi che

$$S_n = \langle (1 2), (1 3), \dots, (1 n) \rangle .$$

Tutte le decomposizioni di una data permutazione in prodotto di trasposizioni hanno una proprietà in comune, la *parità* del numero di fattori:

Proposizione 4.6 Sia $\pi \in S_n$ e siano

$$\pi = \tau_1 \tau_2 \dots \tau_n = \theta_1 \theta_2 \dots \theta_m$$

due decomposizioni di π come prodotto di trasposizioni $\tau_i, \theta_j \in S_n$.

Allora $n \equiv m \pmod{2}$, ovvero n è pari (risp. dispari) se e solo se m è pari (risp. dispari).

Dimostrazione. Supponiamo, per assurdo, che sia $\pi = \tau_1 \tau_2 \dots \tau_n = \theta_1 \theta_2 \dots \theta_m$ con τ_i, θ_j trasposizioni e n pari, m dispari. Allora $\iota = \tau_1 \dots \tau_n \theta_m^{-1} \dots \theta_1^{-1} = \tau_1 \dots \tau_n \theta_m \dots \theta_1$ ovvero l'identità ι di S_n si decompone nel prodotto di un numero dispari di trasposizioni. Sia d il minimo intero positivo dispari per cui valga

$$\iota = \gamma_1 \gamma_2 \dots \gamma_d \tag{1}$$

con γ_i trasposizioni e sia $a \in \{1, 2, \dots, n\}$ un elemento "mosso" da almeno una γ_i . Chiaramente γ_i commuta con ogni γ_j tale che $|\text{supp}(\gamma_i) \cap \text{supp}(\gamma_j)| = 0, 2$ e inoltre, come è facile verificare, per ogni $b, c \in \{1, 2, \dots, n\}$ vale $(a b)(b c) = (b c)(a c)$.

Possiamo dunque trasformare la decomposizione (1) in

$$\iota = \delta_1 \delta_2 \dots \delta_t \beta_1 \beta_2 \dots \beta_v \tag{2}$$

con $t + v = d$, $a \notin \text{supp}(\delta_i)$ e $\beta_j = (a b_j)$, $b_j \in \{1, 2, \dots, n\}$, per ogni $1 \leq i \leq t$, $1 \leq j \leq v$. Osserviamo ora che se gli elementi b_j sono tutti distinti, allora $\beta_1 \beta_2 \dots \beta_v = (a b_1)(a b_2) \dots (a b_v) = (a b_1 b_2 \dots b_v)$ e quindi $a \beta_1 \beta_2 \dots \beta_v = b_1 \neq a$. Ma $\beta_1 \beta_2 \dots \beta_v = (\delta_1 \delta_2 \dots \delta_t)^{-1} = \delta_t \delta_{t-1} \dots \delta_1$ e $a \delta_t \delta_{t-1} \dots \delta_1 = a$, contraddizione. Esistono quindi $1 \leq$

$r, s \leq v$, $r \neq s$, tali che $b_r = b_s = b$. Poichè, per ogni $c \in \{1, 2, \dots, n\}$, $(a b)(a c) = (b c)(a b)$ possiamo trasformare la (2) in

$$\iota = \delta_1 \delta_2 \dots \delta_t \delta_{t+1} \dots \delta_{d-2} (a b)(a b) = \delta_1 \delta_2 \dots \delta_{d-2}$$

contraddicendo la minimalità di d .

In virtù del risultato precedente è ben posta la seguente

Definizione. Una permutazione si dice **pari** (risp. **dispari**) se si può scrivere come prodotto di un numero pari (risp. dispari) di trasposizioni.

Proposizione 4.7 *L'applicazione $\text{sgn} : S_n \rightarrow \{+1, -1\}$ definita ponendo, per ogni $\pi \in S_n$,*

$$\text{sgn}(\pi) = \begin{cases} +1 & \text{se } \pi \text{ è pari} \\ -1 & \text{se } \pi \text{ è dispari} \end{cases}$$

è, per ogni $n > 1$, un omomorfismo suriettivo del gruppo simmetrico S_n nel gruppo moltiplicativo $\{+1, -1\}$. ($\text{sgn}(\pi)$ si dice **segno** della permutazione π).

Dimostrazione. Date $\pi_1, \pi_2 \in S_n$, scriviamo $\pi_1 = \alpha_1 \alpha_2 \dots \alpha_{n_1}$, $\pi_2 = \beta_1 \beta_2 \dots \beta_{n_2}$ con α_i, β_j trasposizioni. Allora $\text{sgn}(\pi_1) = (-1)^{n_1}$, $\text{sgn}(\pi_2) = (-1)^{n_2}$ e

$$\text{sgn}(\pi_1 \pi_2) = \text{sgn}(\alpha_1 \alpha_2 \dots \alpha_{n_1} \beta_1 \beta_2 \dots \beta_{n_2}) = (-1)^{n_1 + n_2} = \text{sgn}(\pi_1) \text{sgn}(\pi_2).$$

La suriettività segue osservando, ad esempio, che $\text{sgn}(\iota) = 1$ e $\text{sgn}((1\ 2)) = -1$.

Definizione. Denotiamo con

$$A_n = \{\pi \in S_n \mid \pi \text{ è pari}\}$$

l'insieme delle permutazioni pari di S_n . Per la Proposizione 4.7, A_n è un sottogruppo normale di S_n , detto **gruppo alterno** su n oggetti.

Enunciamo, senza dimostrazione, il seguente fondamentale risultato:

Teorema 4.8 *Il gruppo alterno A_n è semplice per ogni $n \geq 5$.*

Concludiamo mostrando che ogni gruppo finito si può immergere in un gruppo simmetrico :

Teorema (Cayley). *Sia G un gruppo finito di ordine n . Allora G è isomorfo ad un sottogruppo del gruppo simmetrico S_n .*

Dimostrazione. Siano, tramite opportuna numerazione, g_1, g_2, \dots, g_n gli elementi del gruppo G . Fissato un elemento $g \in G$, consideriamo l'applicazione $\phi_g : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ definita ponendo, per ogni $i \in \{1, 2, \dots, n\}$, $\phi(i) = j$ se vale $gg_i = g_j$.

Dato che, per ogni $j \in \{1, 2, \dots, n\}$, $gg_i = g_j$ se e solo se $g_i = g^{-1}g_j$, l'applicazione ϕ_g è biettiva ovvero $\phi_g \in S_n$. Sia quindi $\omega : G \rightarrow S_n$ definita, per ogni $g \in G$, da $\omega(g) = \phi_g$. Verifichiamo che ω è un omomorfismo: per $g, h \in G$, $i \in \{1, 2, \dots, n\}$,

$$g\phi_{gh}(i) = (gh)g_i = g(hg_i) = g(g\phi_h(i)) = g\phi_g(\phi_h(i))$$

e quindi $\phi_{gh} = \phi_g \circ \phi_h$.

Infine, ω è iniettiva: se $\phi_g = \phi_h$ allora, per ogni $i \in \{1, 2, \dots, n\}$, $gg_i = hg_i$ e quindi $g = h$. Dunque G è isomorfo al sottogruppo $\omega(G)$ di S_n .

Abbiamo dimostrato questo Teorema per un gruppo finito, perchè in questo caso il legame con le permutazioni è particolarmente trasparente. Tuttavia il teorema di Cayley vale per qualunque gruppo. Se il gruppo G in questione è infinito, non si può in generale "enumerare" gli elementi di G , come abbiamo fatto nel caso finito; allora si prende come insieme su cui definire le permutazioni, il gruppo G stesso. La dimostrazione la suggeriamo mediante una coppia di esercizi.

Teorema di Cayley. *Sia G un gruppo. Allora G è isomorfo ad un sottogruppo del gruppo simmetrico $Sym(G)$.*

Dimostrazione. Sia G un gruppo.

1) Si provi che per ogni $g \in G$ la applicazione

$$\begin{aligned} \rho_g : G &\rightarrow G \\ x &\mapsto gx \end{aligned}$$

è una permutazione di G .

2) Si provi che la applicazione

$$\begin{aligned} \Phi : G &\rightarrow Sym(G) \\ x &\mapsto \rho_x \end{aligned}$$

è un omomorfismo iniettivo del gruppo G nel gruppo $Sym(G)$. Da ciò si conclude che $G \simeq \Phi(G) \leq Sym(G)$.

ESERCIZI

1. Siano I, J insiemi tali che $|I| = |J|$. Provare che $Sym(I) \simeq Sym(J)$.

2. Date le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 2 & 6 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$$

scrivere $\alpha, \beta, \alpha\beta, \beta\alpha, \beta^{-1}\alpha\beta$ e $\alpha^{-1}\beta\alpha$ come prodotto di cicli disgiunti.

3. Scrivere la permutazione $\pi = (1 \ 2 \ 3)(2 \ 4 \ 5)(3 \ 2 \ 4)(1 \ 2 \ 5)$ come prodotto di cicli disgiunti e come prodotto di trasposizioni. Dire se π appartiene al gruppo alterno A_5 .

4. Determinare il numero dei coniugati della permutazione

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

nel gruppo simmetrico S_5 .

5. Determinare il massimo ordine di un elemento nei seguenti gruppi:

a) S_7 ; b) S_{10} ; c) A_{10} .

6. Scrivere gli elementi del gruppo alterno A_4 .

7. Determinare un sottogruppo del gruppo simmetrico S_8 isomorfo al gruppo Q dei quaternioni.

Azioni di un gruppo su un insieme

Definizione. Sia G un gruppo e S un insieme non vuoto. Una **azione** di G su S è un omomorfismo

$$\Phi : G \rightarrow \text{Sym}(S)$$

di G nel gruppo delle permutazioni di S (e si dice che G opera su S).

Se un tale omomorfismo è iniettivo l'azione si dice *fedele*. In tal caso l'immagine $\Phi(G)$ è un sottogruppo di $\text{Sym}(S)$ isomorfo a G ; si dice in questo caso che G è un *gruppo di permutazioni* su S (e si identifica G con $\Phi(G)$).

Ad esempio, il Teorema di Cayley descrive una azione fedele di un gruppo G su se stesso.

Se $\Phi : G \rightarrow \text{Sym}(X)$ è una azione di G su S , allora, per ogni $g \in G$ e ogni $s \in S$ si scrive

$$g \cdot s = \phi(g)(s).$$

Si hanno quindi le seguenti proprietà, per ogni $g, h \in G$ e ogni $s \in S$:

$$(gh) \cdot s = g \cdot (h \cdot s), \quad 1_G \cdot s = s.$$

Questa notazione suggerisce un altro modo per definire il concetto di azione di un gruppo su un insieme. Se G è un gruppo e S un insieme, una azione di G su S è una applicazione

$$\begin{aligned} G \times S &\rightarrow S \\ (g, s) &\mapsto g \cdot s \end{aligned}$$

tale che per ogni per ogni $g, h \in G$ e ogni $s \in S$, $(gh) \cdot s = g \cdot (h \cdot s)$ e $1_G \cdot s = s$. Allora, per ogni $g \in G$ la applicazione

$$\begin{aligned} \phi(g) : S &\rightarrow S \\ s &\mapsto g \cdot s \end{aligned}$$

è una biezione di S , e (lo si verifichi per esercizio) la applicazione che associa ad ogni $g \in G$ la permutazione $\phi(g)$ è un omomorfismo di G in $\text{Sym}(S)$.

Esempio. Su $G = \mathbb{R}^* \times \mathbb{R}$ si definisca una operazione ponendo, per ogni $(a, b), (c, d) \in G$

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

Si verifichi che, rispetto a tale operazione, G è un gruppo con elemento identico $(1, 0)$. Ora, la regola

$$(a, b) \cdot s = as + b$$

per ogni $(a, b) \in G$ e ogni $s \in \mathbb{R}$, definisce una azione del gruppo G sull'insieme \mathbb{R} . Infatti, per ogni $s \in \mathbb{R}$:

$$1_G \cdot s = (1, 0) \cdot s = 1s + 0 = s$$

e, per ogni $(a, b), (c, d) \in G$:

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

Supponiamo di avere data una azione del gruppo G sull'insieme S . Per ogni $s \in S$ si definiscono:

- l'**orbita** $O_G(s)$ di s (rispetto alla azione di G)

$$O_G(s) = \{ g \cdot s \mid g \in G \} ,$$

ovvero l'insieme dei trasformati di s tramite tutti gli elementi di G .

- lo **stabilizzatore** G_s (o anche $Stab_G(s)$) di s in G :

$$G_s = \{ g \in G \mid g \cdot s = s \}$$

ovvero l'insieme degli elementi di G la cui corrispondente permutazione fissa s .

Definizione. Una azione si dice **transitiva** se esiste $s \in S$ tale che $O_G(s) = S$; ciò avviene se per ogni $t \in S$ esiste $g \in G$ tale che $g \cdot s = t$.

Ad esempio, l'azione descritta nell'esempio di sopra è transitiva: infatti, per ogni $a \in \mathbb{R}$: $(a, 0) \cdot 1 = a1 + 0 = a$ se $a \neq 0$, e $(1, -1) \cdot 1 = 1 \cdot 1 + (-1) = 0$; quindi $O_G(1) = \mathbb{R}$. Calcoliamo lo stabilizzatore di un punto $s \in \mathbb{R}$. Sia $(a, b) \in G$; allora $(a, b) \in G_s$ se e solo se $s = (a, b) \cdot s = as + b$, se e solo se $b = s - as$; quindi $G_s = \{ (a, s - as) \mid a \in \mathbb{R}^* \}$ (ad esempio, $G_1 = \{ (a, 1 - a) \mid a \in \mathbb{R}^* \}$).

Esercizio Si provi che una azione di un gruppo G su un insieme S è transitiva se e solo se $O_G(x) = S$ per ogni $x \in S$.

Proposizione 4.9 *Sia data una azione del gruppo G sull'insieme S . Allora l'insieme delle orbite è una partizione di S .*

Dimostrazione. Poichè, per ogni $s \in S$, $s = 1_G \cdot s \in O_G(s)$, si ha che le orbite sono non vuote e che la loro unione è tutto S .

Siano ora $s, t \in S$ tali che $O_G(s) \cap O_G(t) \neq \emptyset$; allora esiste $u \in O_G(s) \cap O_G(t)$ e quindi esistono $g, h \in G$ tali che $u = g \cdot s = h \cdot t$. Allora, per ogni $x \in G$,

$$x \cdot s = (xg^{-1}g) \cdot s = (xg^{-1}) \cdot (g \cdot s) = (xg^{-1}) \cdot (h \cdot t) = (xg^{-1}h) \cdot t \in O_G(t) .$$

Dunque $O_G(s) \subseteq O_G(t)$. Allo stesso modo si prova che $O_G(t) \subseteq O_G(s)$, e quindi $O_G(s) = O_G(t)$; il che dimostra che orbite distinte sono disgiunte e completa la dimostrazione. (Per esercizio si verifichi che la partizione in orbite è l'insieme quoziente rispetto alla equivalenza \sim_G definita su S da $s \sim_G t \Leftrightarrow \exists g \in G : g \cdot s = t$).

Teorema 4.10 *Sia data una azione del gruppo G sull'insieme S , e sia $s \in S$. Allora:*

- 1) G_s è un sottogruppo di G .
- 2) $|O_G(s)| = [G : G_s]$.

Dimostrazione. 1) Poichè $1_G \cdot s = s$, si ha $1_G \in G_s$ per qualunque $s \in S$. Fissato ora un tale punto s , siano $g, h \in G_s$. Allora $g \cdot s = s = h \cdot s$ e quindi

$$(gh^{-1}) \cdot s = (gh^{-1}) \cdot (h \cdot s) = (gh^{-1}h) \cdot s = g \cdot s = s,$$

dunque $gh^{-1} \in G_s$ e, per il criterio dei sottogruppi, $G_s \leq G$.

2) Sia $\mathcal{C} = \{ xG_s \mid x \in G \}$ l'insieme delle classi laterali sinistre di G modulo G_s e consideriamo la applicazione

$$\begin{aligned} \eta : \mathcal{C} &\rightarrow O_G(s) \\ xG_s &\mapsto x \cdot s \end{aligned}$$

essa è ben definita, infatti se $x, y \in G$ sono tali che $xG_s = yG_s$ allora $y^{-1}x \in G_s$, cioè $(y^{-1}x) \cdot s = s$ e quindi $y \cdot s = y \cdot ((y^{-1}x) \cdot s) = (yy^{-1}x) \cdot s = x \cdot s$. Dunque η è ben definita.

Proviamo ora che η è biettiva. Essa è suriettiva per definizione di orbita di s . Siano ora $xG_s, yG_s \in \mathcal{C}$ tali che $\eta(xG_s) = \eta(yG_s)$; allora $x \cdot s = y \cdot s$, e quindi

$$(y^{-1}x) \cdot s = y^{-1} \cdot (x \cdot s) = y^{-1} \cdot (y \cdot s) = (y^{-1}y) \cdot s = 1_G \cdot s = s ;$$

dunque $y^{-1}x \in G_s$, cioè $xG_s = yG_s$. Quindi η è iniettiva e pertanto è una biezione. In particolare si ha $[G : G_s] = |\mathcal{C}| = |O_G(s)|$, come si voleva.

Se il gruppo G è finito allora, in congiunzione con il Teorema di Lagrange, segue dal Teorema precedente la seguente importante osservazione.

Corollario. *Se il gruppo finito G opera sull'insieme S , allora per ogni $s \in S$, $|O_G(s)|$ divide $|G|$. In particolare, se l'azione è transitiva, allora $|S|$ divide $|G|$.*

Consideriamo ora il caso in cui sia G che S sono finiti, ed è data una azione di G su S . Siano $O_G(s_1), O_G(s_2), \dots, O_G(s_n)$ le orbite distinte di G su S (l'insieme $\{s_1, s_2, \dots, s_n\}$ si dice un insieme di rappresentanti per le orbite di G su S). Per la Proposizione 4.9 esse costituiscono una partizione di S , quindi

$$|S| = |O_G(s_1)| + |O_G(s_2)| + \dots + |O_G(s_n)| .$$

Ora, per il Teorema 4.10, per ogni $i = 1, \dots, n$ si ha $|O_G(s_i)| = [G : G_{s_i}]$; quindi si ricava l'importante:

Equazione delle orbite. *Sia $\{s_1, s_2, \dots, s_n\}$ un insieme di rappresentanti per le orbite di G su S . Allora*

$$|S| = \sum_{i=1}^n [G : G_{s_i}] .$$

Definizione. Se G opera sull'insieme S ed $s \in S$ è tale che $O_G(s) = \{s\}$, allora s si dice un **punto fisso** l'azione di G su S . In altri termini, $s \in S$ è un punto fisso se e solo se $g \cdot s = s$ per ogni $g \in G$, ovvero se e solo se $G_s = G$.

Come applicazione dell'equazione delle orbite, vediamo un criterio sufficiente all'esistenza di un punto fisso. Sia p un numero primo e sia P un gruppo di ordine p^m (si dice che P è un p -gruppo finito), e sia data una azione di P su un insieme finito S . Sia $\{s_1, s_2, \dots, s_n\}$ un insieme di rappresentanti per le orbite di G su S . Per il teorema di Lagrange, per ogni $i = 1, \dots, n$, l'indice $[G : G_{s_i}]$ divide $|P| = p^m$. Assumiamo che non vi siano punti fissi per l'azione di P su S ; allora, per ogni $i = 1, \dots, n$, G_{s_i} è un sottogruppo proprio di P , quindi $[G : G_{s_i}] = p^{k(i)}$ con $k(i) \geq 1$; in particolare p divide $[G : G_{s_i}]$. Applicando la formula delle orbite si ha che p divide $\sum_{i=1}^n [G : G_{s_i}] = |S|$. Abbiamo quindi dimostrato

Teorema 4.11 *Sia P un p -gruppo finito che opera su un insieme S . Se $(|S|, p) = 1$ allora esiste almeno un punto fisso di P su S .*

Esercizio. Sia data una azione del gruppo G su un insieme S . Siano $s \in S$, $g \in G$ e poniamo $t = g \cdot s$. Si provi che $G_s = g^{-1}(G_t)g$.

Vediamo ora un esempio interessante di azione transitiva di un gruppo G . Sia H un sottogruppo fissato di G e denotiamo con $G \setminus H$ l'insieme delle classi laterali sinistre di G modulo H ; su questo insieme definiamo una azione di G ponendo, per ogni $g \in G$ e ogni $xH \in G \setminus H$,

$$g \cdot xH = gxH .$$

Si verifica immediatamente che ciò definisce una azione, e che tale azione è transitiva. Infatti, per ogni $xH, yH \in G \setminus H$ si ha

$$(yx^{-1}) \cdot xH = yx^{-1}xH = yH .$$

Supponiamo ora che l'indice $[G : H] = n$ sia finito. Allora $|G \setminus H| = [G : H] = n$, e l'azione di G su $G \setminus H$ sopra descritta da luogo ad un omomorfismo $G \rightarrow \text{Sym}(G \setminus H) = S_n$. Sia N il nucleo di questo omomorfismo, allora

$$\begin{aligned} N &= \{ g \in G \mid g \cdot xH = xH \ \forall xH \in G \setminus H \} = \{ g \in G \mid gxH = xH \ \forall x \in G \} = \\ &= \{ g \in G \mid x^{-1}gxH = H \ \forall x \in G \} \end{aligned}$$

osservando che

$$x^{-1}gxH = H \Leftrightarrow x^{-1}gx \in H \Leftrightarrow \exists h \in H : x^{-1}gx = h \Leftrightarrow g \in xHx^{-1} = H^{x^{-1}}$$

possiamo concludere che

$$N = \{ g \in G \mid g \in H^{x^{-1}} \ \forall x \in G \} = \bigcap_{x \in G} H^x .$$

Questo sottogruppo normale di G si denota con H_G . Chiaramente $H_G \leq H$. Inoltre, per il Teorema di omomorfismo, G/H_G è isomorfo ad un sottogruppo di S_n ; in particolare $[G : H_G]$ divide $n!$.

Questo tipo di azioni di G è importante perchè si può dimostrare che ogni azione transitiva di G è equivalente (secondo una naturale definizione di equivalenza di azioni, vedi gli esercizi 5 e 6) ad una azione di G sulle classi laterali di un suo opportuno sottogruppo.

ESERCIZI

1. Sia data una azione transitiva del gruppo S_3 su un insieme S . Quanti elementi può avere S ?
2. Sia G un gruppo di ordine 1998 e S un insieme di ordine 14. Si provi che ogni azione di G su S ha almeno tre orbite.
3. Sia $I_n = \{1, 2, \dots, n\}$ (con $n \geq 2$) e sia X l'insieme costituito dai sottoinsiemi di ordine 2 di I_n . Allora il gruppo simmetrico S_n opera su X in modo naturale: per ogni $\sigma \in S_n$ e ogni $\{i, j\} \in X$, $\sigma \cdot \{i, j\} = \{i\sigma, j\sigma\}$.
 - a) Si provi che tale azione è transitiva, e si calcoli l'ordine dello stabilizzatore di $\{1, 2\}$.
 - b) Posto $n = 5$, si determini $Stab_{S_5}(\{1, 2\}) \cap A_5$.
4. Sia $G = GL(2, \mathbb{R})$ e consideriamo l'azione di G sull'insieme dei vettori colonna reali non nulli $S = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{R} \ (a, b) \neq (0, 0) \right\}$ definita da

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Si dica se tale azione è transitiva, e si determini lo stabilizzatore del punto $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

5. Sia G un gruppo. Due azioni di G su insiemi S e S' si dicono *equivalenti* se esiste una biezione $f: S \rightarrow S'$ tale che, per ogni $g \in G$, $s \in S$

$$g \cdot (f(s)) = f(g \cdot s)$$

Si provi che se due azioni di G su S e S' sono equivalenti, allora per ogni $s \in S$ si ha $O_G(f(s)) = f(O_G(s))$ e $G_{f(s)} = G_s$.

6. Sia data una azione transitiva del gruppo G sull'insieme S ; fissato un $s \in S$, si ponga $H = G_s$. Si provi che l'azione di G su S è equivalente all'azione di G sull'insieme delle classi laterali sinistre modulo H .
7. Sia G un gruppo finito, e sia p il minimo numero primo che divide $|G|$. Si provi che se $H \leq G$ e $[G : H] = p$, allora $H \trianglelefteq G$.
8. Sia G un gruppo e $H \leq G$. Si provi che H_G è il massimo sottogruppo normale di G contenuto in H .

Classi di coniugio

In questo paragrafo applicheremo i risultati del paragrafo precedente al caso dell'azione di un gruppo G su se stesso mediante coniugio. Ricordiamo che se x, g sono elementi di un gruppo G , il *coniugato* di x tramite g è l'elemento $g^{-1}xg$, che si denota con x^g . Il coniugio definisce una azione di G su G ponendo, per ogni $g, x \in G$: $g \cdot x = x^{g^{-1}}$. Infatti, per ogni $x \in G$, $x^{1_G} = x$, e per ogni $x, g, h \in G$:

$$(gh) \cdot x = x^{(gh)^{-1}} = (gh)x(h^{-1}g^{-1}) = g(hxh^{-1})g^{-1} = (x^{h^{-1}})^{g^{-1}} = (h \cdot x)^{g^{-1}} = g \cdot (h \cdot x).$$

In questo caso, la notazione "a destra" risulta più conveniente. Infatti per ogni $x, g, h \in G$ si ha

$$x^{gh} = (x^g)^h .$$

(La permutazione di G associata ad ogni elemento $g \in G$ rispetto a questa azione è - come abbiamo visto nell'ultimo paragrafo della sezione precedente - l'automorfismo σ_g di G . Quindi l'omomorfismo da G in $Sym(G)$ associato all'azione per coniugio è di fatto un omomorfismo da G in $Aut(G)$. Potremo dire che l'azione per coniugio è una azione di G come gruppo di automorfismi su se stesso. Da questo punto di vista è stata trattata nell'ultimo paragrafo della sezione precedente; ora ci interessa piuttosto il punto di vista delle permutazioni, in modo da applicare i concetti che abbiamo esposto su questo tipo di azioni.)

L'orbita di un elemento $x \in G$ rispetto all'azione per coniugio si chiama **classe di coniugio** di x ed è

$$\{ x^g \mid g \in G \} .$$

Lo stabilizzatore in G di x si denota con $C_G(x)$ e si chiama **centralizzante** di x in G :

$$C_G(x) = \{ g \in G \mid x^g = x \} = \{ g \in G \mid g^{-1}xg = x \} = \{ g \in G \mid xg = gx \} .$$

Il centralizzante di un elemento x è quindi l'insieme degli elementi di G che commutano con x . Se G è un gruppo finito si ha, per il Teorema 4.10

$$|\{ x^g \mid g \in G \}| = [G : C_G(x)] .$$

Inoltre G (come insieme) si ripartisce nelle sue classi di coniugio distinte (che sono le orbite dell'azione per coniugio).

Dopo aver ricordato la definizione di **centro** di G :

$$Z(G) = \{ x \in G \mid xg = gx \text{ per ogni } g \in G \} ,$$

osserviamo che un elemento $x \in G$ appartiene al centro $Z(G)$ se e solo se $gx = xg$ per ogni $g \in G$, ovvero se e solo se $x^g = g^{-1}xg = x$ per ogni $g \in G$, cioè se e solo se la classe di coniugio di x consiste del solo elemento x .

Prima di andare avanti con la teoria delle classi di coniugio, vediamo una interessante applicazione del Teorema 4.11

Teorema 4.12 *Sia p un numero primo e G un p -gruppo finito. Allora $Z(G) \neq \{1_G\}$.*

Dimostrazione. Sia G un gruppo di ordine p^n , dove p è un numero primo. Poniamo $S = G \setminus \{1_G\}$; chiaramente l'azione per coniugio di G su se stesso induce una azione per coniugio su S . Ora $|S| = p^n - 1$, quindi per il Teorema 4.11, G ha punto fisso su S , cioè esiste un elemento $1_G \neq x \in G$ tale che la sua classe di coniugio è $\{x\}$. Per quanto osservato sopra, $x \in Z(G)$ e quindi $Z(G) \neq \{1_G\}$.

Sia ora G un gruppo finito, denotiamo con K_1, K_2, \dots, K_n le sue classi di coniugio distinte e, per ogni $i = 1, 2, \dots, n$ fissiamo un elemento $x_i \in K_i$ (l'insieme $\{x_1, x_2, \dots, x_n\}$

è detto allora un insieme di rappresentanti delle classi di coniugio di G). Allora la formula delle orbite si scrive

$$|G| = \sum_{i=1}^n |K_i| = \sum_{i=1}^n [G : C_G(x_i)] .$$

Una classe di coniugio si dice *centrale* se consiste di un solo elemento; per quanto abbiamo osservato prima, una classe è centrale se e solo se è la classe di un elemento appartenente al centro di G . Il numero di classi centrali è dunque $|Z(G)|$. Se, nella somma di sopra, raccogliamo gli addendi corrispondenti alle classi centrali, il loro contributo alla somma è ancora $|Z(G)|$, a cui va sommato il contributo delle classi non centrali. Possiamo enunciare questa importante osservazione con la seguente

Formula delle Classi. *Sia G un gruppo finito, e siano y_1, y_2, \dots, y_m rappresentanti delle classi non centrali di G . Allora*

$$|G| = |Z(G)| + \sum_{i=1}^m [G : C_G(y_i)] .$$

Come esempio, consideriamo il gruppo S_4 . Per la Proposizione 4.4, due elementi di S_4 sono coniugati se e solo se hanno lo stesso tipo ciclico. Per ottenere un insieme di rappresentanti delle classi di coniugio di S_4 è quindi sufficiente considerare un elemento per ciascun tipo ciclico; ad esempio possiamo prendere $\{ x_1 = \iota, x_2 = (12), x_3 = (12)(34), x_4 = (123), x_5 = (1234) \}$. Indichiamo con n_i il numero di elementi coniugati a x_i (ovvero $n_i = [S_4 : C_{S_4}(x_i)]$). Allora, $n_1 = 1$, $n_2 = \binom{4}{2} = 6$ (infatti ogni coppia di elementi di $\{1, 2, 3, 4\}$ dà luogo ad una trasposizione), $n_3 = 3$, $n_4 = 2 \binom{4}{3} = 8$ (infatti ogni terna di elementi di $\{1, 2, 3, 4\}$ dà luogo a due 3-cicli). Possiamo ora calcolare n_5 usando la formula delle classi:

$$n_5 = |S_4| - (n_1 + n_2 + n_3 + n_4) = 24 - 18 = 6 .$$

Esercizio. Si dimostri il Teorema 4.12 utilizzando la Formula delle Classi.

La serie di esercizi svolti che segue tratta alcune interessanti applicazioni dei concetti e delle formule introdotte in questo paragrafo. Naturalmente, cercate di discuterli da voi prima di controllarne la soluzione. Ricordiamo che il centro di un gruppo è sempre un sottogruppo normale.

Esercizio A. Sia G un gruppo. Dimostrare che se $G/Z(G)$ è ciclico allora G è commutativo (quindi $Z(G) = G$).

Soluzione. Sia $G/Z(G)$ un gruppo ciclico. Allora esiste un elemento $gZ(G) \in G/Z(G)$ tale che

$$G/Z(G) = \langle gZ(G) \rangle = \{ (gZ(G))^z \mid z \in \mathbb{Z} \} = \{ g^z Z(G) \mid z \in \mathbb{Z} \} .$$

Quindi, se $x, y \in G$, esistono $a, b \in \mathbb{Z}$ tali che $xZ(G) = g^a Z(G)$ e $yZ(G) = g^b Z(G)$; cioè esistono $h, k \in Z(G)$ tali che $x = g^a h$ e $y = g^b k$. Poichè h, k commutano con ogni elemento di G , abbiamo

$$xy = g^a h g^b k = g^a g^b h k = g^{a+b} h k = g^b g^a k h = g^b k g^a h = yx .$$

Dunque G è commutativo.

Esercizio B. Sia p un numero primo. Dimostrare che ogni gruppo di ordine p^2 è commutativo.

Soluzione. Sia G un gruppo con $|G| = p^2$. Allora, per il Teorema 4.12, $Z(G) \neq \{1_G\}$, e quindi, per il Teorema di Lagrange, $|Z(G)| = p, p^2$. Se $|Z(G)| = p^2$, allora $G = Z(G)$ è commutativo. Se invece $|Z(G)| = p$, allora $|G/Z(G)| = p$; ma allora, per la Proposizione 13 della sezione precedente, $G/Z(G)$ è ciclico, e quindi, per Esercizio A, G è commutativo (quindi, a posteriori, possiamo dire che il caso $|Z(G)| = p$ non si verifica se $|G| = p^2$).

Esercizio C. Sia G un gruppo di ordine 6. Si dimostri che se G non è commutativo allora G è isomorfo a S_3 .

Soluzione. Sia G un gruppo non commutativo di ordine 6. Allora $G \neq Z(G)$. Poichè $Z(G)$ è un sottogruppo di G , il suo ordine è un divisore di 6. Se fosse $|Z(G)| = 2$, allora $|G/Z(G)| = 3$ e quindi $G/Z(G)$ sarebbe ciclico e pertanto, per l'esercizio A, G sarebbe commutativo. Similmente si esclude il caso $|Z(G)| = 3$. Quindi si ha $|Z(G)| = 1$.

Ora, se $y \in G \setminus Z(G)$ allora $[G : C_G(y_i)]$ non è uguale ad 1, e quindi, sempre per il Teorema di Lagrange, deve essere 2 o 3. Se y_1, \dots, y_m sono rappresentanti delle classi non centrali di G , abbiamo, per la Formula delle Classi,

$$6 = |Z(G)| + [G : C_G(y_1)] + \dots + [G : C_G(y_m)] = 1 + [G : C_G(y_1)] + \dots + [G : C_G(y_m)] ,$$

dove gli addendi $[G : C_G(y_i)]$ appartengono tutti all'insieme $\{2, 3\}$. La sola possibilità è: $6 = 1 + 2 + 3$.

In particolare, segue che G ha una classe di coniugio K di ordine 3. Ora, G opera per coniugio, transitivamente, su K , e tale azione determina un omomorfismo $\phi : G \rightarrow S_K$. Sia $N = \text{Ker}(\phi)$. Non può essere $|N| = 2$, perchè un sottogruppo normale di ordine 2 è sempre contenuto nel centro (questo è facile e lo lasciamo), contro il fatto che $Z(G) = \{1_G\}$. Quindi (poichè l'azione è transitiva) si ha $N = \{1_G\}$. Dunque ϕ è un omomorfismo iniettivo; siccome $|G| = 6 = |S_K|$, ϕ è allora un isomorfismo. Dunque G è isomorfo a S_K che è isomorfo a S_3 .

L'idea di azione per coniugio si può estendere in modo naturale considerando l'azione, invece che sugli elementi, su sottoinsiemi del gruppo G .

Se G è un gruppo, $\emptyset \neq S \subseteq G$ e $g \in G$, il coniugato di S tramite g è l'insieme

$$S^g = \{ x^g \mid x \in S \} .$$

Si verifica facilmente che $S^{1_G} = S$ e che $S^{gh} = (S^g)^h$ per ogni $g, h \in G$. Lo stabilizzatore di S è (il sottogruppo) $\{ g \in G \mid S^g = S \}$.

Se $H \leq G$ allora $H^g \leq G$ per ogni $g \in G$, e lo stabilizzatore di H rispetto alla azione di coniugio si chiama **normalizzatore** di H in G , e si denota con $N_G(H)$. Allora $H \leq N_G(H) \leq G$ (vedi esercizio 13 alla fine della sezione precedente), ed il numero di coniugati distinti di H in G è uguale all'indice

$$[G : N_G(H)]$$

in particolare, $H \trianglelefteq G$ se e soltanto se $N_G(H) = G$.

Naturalmente, non è necessario considerare l'azione per coniugio di un gruppo G sulla famiglia di tutti i suoi sottoinsiemi non vuoti. L'azione per coniugio si può definire su una particolare famiglia di sottoinsiemi, purchè essa contenga tutti i coniugati di ogni suo elemento. Ad esempio, si può considerare l'azione sulla famiglia dei sottogruppi di G , oppure sulla famiglia dei sottogruppi di un ordine fissato.

Utilizzeremo l'azione per coniugio su sottogruppi nel prossimo paragrafo, per dimostrare gli importanti Teoremi di Sylow.

Concludiamo con una osservazione che sarà anch'essa utilizzata nel prossimo paragrafo. La dimostrazione è lasciata per esercizio, perchè ricalca quella del Lemma 1 della sezione precedente.

Lemma 4.13 *Siano G un gruppo, e $H, K \leq G$. Se $K \subseteq N_G(H)$ allora $HK \leq G$.*

ESERCIZI

1. Sia G un gruppo di ordine 21. Si provi che se $Z(G) \neq \{1_G\}$ allora G è commutativo.
2. Si provi che un gruppo di ordine p^2 (p un numero primo) è ciclico oppure è il prodotto diretto di due gruppi ciclici di ordine p .
3. Si scriva la formula delle classi per il gruppo S_5 .
4. Si provi che il gruppo S_6 ha un sottogruppo di indice 90 (sugg.: si consideri la classe dell'elemento $(1\ 2\ 3\ 4)$).
5. Si provi che ogni gruppo di ordine 6 è ciclico oppure isomorfo a S_3 .
6. Sia G un gruppo di ordine dispari. Si provi che G ha un numero dispari di classi di coniugio.
7. Sia G un gruppo di ordine dispari, e sia $x \in G$. Si provi che se x è coniugato a x^{-1} allora $x = 1_G$.
8. Sia G un gruppo di ordine 15. Si provi che G è commutativo.
9. Sia H un sottogruppo del gruppo G e sia

$$C_G(H) = \{ g \in G \mid gx = xg \ \forall x \in H \} .$$

Si provi che $C_G(H) \leq G$ e che $C_G(H) \trianglelefteq N_G(H)$.

Teoremi di Sylow

Insieme al Teorema di Lagrange, i Teoremi di Sylow sono lo strumento fondamentale per lo studio dei gruppi finiti. La dimostrazione che daremo non è quella originaria di L. Sylow (1832 - 1918), ma è ispirata a quella scoperta molti anni più tardi (1959) da H. Wielandt, ed è una ingegnosa applicazione della azione su sottoinsiemi.

Primo Teorema di Sylow. *Sia p un numero primo, e sia G un gruppo finito tale che p^k divide $|G|$. Allora esistono sottogruppi di G di ordine p^k .*

Se G è un gruppo di ordine $p^m a$, con p un numero primo e $(p, a) = 1$, allora il Primo Teorema di Sylow assicura l'esistenza di sottogruppi di G di ordine p^k per ogni $1 \leq k \leq m$ (per il Teorema di Lagrange, G non ha certo sottogruppi di ordine p^s con $s \geq m+1$). I sottogruppi di G di ordine p^m si chiamano *p-sottogruppi di Sylow* di G .

Dimostreremo il Primo Teorema di Sylow procedendo per induzione su $|G|$. Per comodità, isoliamo in un Lemma un caso molto particolare (e già noto a Cauchy).

Lemma 4.14 *Sia G un gruppo finito commutativo, e p un primo che divide l'ordine di G . Allora G ha un elemento di ordine p .*

Dimostrazione. Sia G un gruppo commutativo il cui ordine è diviso da p . Allora $|G| = pr$, e procediamo per induzione su r . Se $r = 1$, G è ciclico ed è generato da un elemento di ordine p .

Sia quindi $|G| = pr > p$ e supponiamo l'affermazione vera per ogni gruppo il cui ordine è diviso da p ed è strettamente minore dell'ordine di G . Sia $1_G \neq a \in G$, e sia $A = \langle a \rangle$. Se p divide l'ordine di a allora A contiene un elemento di ordine p (se n è l'ordine di a , $a^{n/p}$ ha ordine p).

Supponiamo quindi che p non divida $|a| = |A|$. Poichè G è commutativo, $A \trianglelefteq G$ ed il quoziente G/A ha ordine $|G/A| = |G|/|A|$ diviso da p e minore dell'ordine di G . Per ipotesi induttiva G/A contiene un elemento bA di ordine p , cioè tale che $bA \neq 1_{G/A} = A$ e $A = (bA)^p = b^p A$. Ora, se s è l'ordine di b , si ha $(bA)^s = b^s A = A = 1_{G/A}$, quindi $p = |bA|$ divide s ; e quindi $\langle b \rangle$ ha un elemento di ordine p , completando la dimostrazione.

Dimostrazione (del Primo Teorema di Sylow). Procediamo per induzione sull'ordine di G . Se $|G| = 1$ non c'è nulla da provare. Sia $|G| > 1$ e supponiamo il Teorema vero per ogni gruppo di ordine strettamente minore di $|G|$, e sia p^k (con $k \geq 1$) un divisore di $|G|$. Consideriamo l'equazione delle classi per G :

$$|G| = |Z(G)| + \sum_{i=1}^m [G : C_G(y_i)] .$$

Supponiamo che per un indice $i \in \{1, 2, \dots, m\}$, p non divida $[G : C_G(y_i)]$, allora per il Teorema di Lagrange, p^k divide $|C_G(y_i)| = |G|/[G : C_G(y_i)]$. Poichè y_i è un elemento non centrale di G , $C_G(y_i)$ è un sottogruppo proprio di G , e quindi, per ipotesi induttiva, contiene un sottogruppo di ordine p^k , e siamo a posto.

Supponiamo quindi che p divida ogni indice $[G : C_G(y_i)]$; allora p divide anche $|Z(G)|$. Per il Lemma precedente, $Z(G)$ ha un elemento a di ordine p . Sia $A = \langle a \rangle$. Poichè $A \leq Z(G)$ si ha $A \trianglelefteq G$. Ora $|G/A| = |G|/p$; quindi p^{k-1} divide $|G/A|$ e, per ipotesi induttiva, G/A ha un sottogruppo H/A (ove, per il Teorema di Corrispondenza, $A \leq H \leq G$) di ordine p^{k-1} . Ma allora H è il sottogruppo di G cercato; infatti $|H| = [H : A]|A| = |H/A||A| = p^{k-1}p = p^k$.

Secondo Teorema di Sylow. *Sia G un gruppo finito, e $|G| = p^m a$, dove p è un numero primo e $(p, a) = 1$. Allora i p -sottogruppi di Sylow G sono tra loro coniugati, e se n_p denota il numero di p -sottogruppi di Sylow di G si ha*

$$n_p \equiv 1 \pmod{p} \quad e \quad n_p | a .$$

Dimostrazione. Sia Σ l'insieme di tutti i p -sottogruppi di Sylow di G (quindi $n_p = |\Sigma|$). Osserviamo che, se $U \in \Sigma$ allora, per ogni $x \in G$, $U^x \in \Sigma$; quindi G opera per coniugio sull'insieme Σ . Sia P un fissato p -sottogruppo di Sylow di G , e consideriamo l'azione di

P per coniugio su Σ . Poichè $P \in \Sigma$ e $P^x = P$ per ogni $x \in P$, P è (come elemento di Σ) un punto fisso per l'azione di P . Vediamo che non ci sono altri punti fissi. Infatti, se $Q \in \Sigma$ è un punto fisso, allora $Q^x = Q$ per ogni $x \in P$, cioè $P \subseteq N_G(Q)$; quindi, per il Lemma 4.13, $PQ \leq G$. Ora, $P \leq PQ$ e, per il Lemma 3(b) della sezione precedente

$$|PQ| = \frac{|P||Q|}{|P \cap Q|}$$

è una potenza di p , da cui segue $P = Q$ perchè P è un p -sottogruppo di Sylow e quindi il suo ordine è la massima potenza di p che divide G . Quindi P è l'unico punto fisso nella azione di P su Σ . Ciò significa che $\{P\}$ è un orbita di P su Σ , e che se \mathcal{O} è un'altra orbita diversa da $\{P\}$, allora $1 \neq |\mathcal{O}|$; poichè $|\mathcal{O}|$ è uguale all'indice dello stabilizzatore in P di un elemento di \mathcal{O} , e P è un p -gruppo, si ha che p divide $|\mathcal{O}|$. La formula delle orbite si scrive quindi

$$n_p = |\Sigma| = |\{P\}| + \sum_{\mathcal{O} \neq \{P\}} |\mathcal{O}| = 1 + \sum_{\mathcal{O} \neq \{P\}} |\mathcal{O}| \equiv 1 \pmod{p}$$

dimostrando una delle affermazioni dell'enunciato.

Proviamo ora che tutti i p -sottogruppi di Sylow sono tra loro coniugati in G ; ovvero che Σ è una classe di coniugio di sottogruppi di G . Considerando l'azione per coniugio di tutto il gruppo G su Σ , si tratta di verificare che c'è una sola orbita. Fissiamo un p -sottogruppo di Sylow P e sia $\mathcal{A} = O_G(P)$ la sua orbita. Considerando, l'azione di P su \mathcal{A} e ragionando come sopra, si ha $|\mathcal{A}| \equiv 1 \pmod{p}$. Supponiamo, per assurdo, che esista $Q \in \Sigma$ tale che $Q \notin \mathcal{A}$, e consideriamo l'azione di Q su \mathcal{A} . Ora, Q ha un solo punto fisso nella sua azione su Σ , che è Q stesso. Poichè Q non appartiene ad \mathcal{A} , ne segue che Q non ha punti fissi su \mathcal{A} , e quindi, per il Teorema 4.11, p divide $|\mathcal{A}|$, una contraddizione. Dunque $\mathcal{A} = \Sigma$, e quindi, per ogni coppia di p -sottogruppi di Sylow P, Q di G , esiste $x \in G$ tale che $Q = P^x$.

Infine, stabilito che l'azione di G per coniugio su Σ è transitiva, abbiamo che il numero di elementi di Σ coincide con l'indice dello stabilizzatore in G di un suo elemento. Quindi, per quanto osservato nel paragrafo precedente, se P è un p -sottogruppo di Sylow di G , allora

$$n_p = |\Sigma| = [G : N_G(P)].$$

Ora, $P \leq N_G(P) \leq G$, e quindi

$$a = [G : P] = [G : N_G(P)][N_G(P) : P] = n_p[N_G(P) : P]$$

in particolare, n_p divide $a = [G : P]$, e questo completa la dimostrazione del Teorema.

Terzo Teorema di Sylow. *Sia G un gruppo finito, e sia p un numero primo che divide $|G|$. Allora ogni sottogruppo di G il cui ordine è una potenza di p è contenuto in almeno un p -sottogruppo di Sylow di G .*

Dimostrazione. Sia $H \leq G$ tale che $|H| = p^k$ per qualche $k \geq 1$. Sia Σ l'insieme di tutti i p -sottogruppi di Sylow di G e consideriamo l'azione per coniugio di H su Σ . Poichè $(|\Sigma|, |H|) = (n_p, p^k) = 1$, per il Teorema 4.11, H ha almeno un punto fisso su Σ ; cioè esiste un $P \in \Sigma$ tale che $P^x = P$ per ogni $x \in H$, ovvero $H \subseteq N_G(P)$. Allora,

ragionando come nella dimostrazione del Secondo Teorema di Sylow, $PH \leq G$ e, di conseguenza, $H \leq P$, che è quello che si voleva dimostrare.

Concludiamo questo paragrafo illustrando con alcuni esempi come i teoremi di Sylow possano fornire molte informazioni su un gruppo finito. Gli esempi che considereremo sono molto specifici, ma danno un'idea dei metodi che si possono applicare in molte circostanze. Negli esercizi verranno suggeriti anche alcuni casi più generali, non complicati, che si possono affrontare mediante queste tecniche. Un fatto banale ma fondamentale da tener presente è che se $H \leq G$ allora per ogni $g \in G$ il coniugato H^g è un sottogruppo dello stesso ordine di H ; quindi se avviene che H è il solo sottogruppo di un certo ordine, allora $H \trianglelefteq G$. In particolare, se per qualche primo p il numero di p -sottogruppi di Sylow di G è 1, l'unico p -sottogruppo di Sylow è normale.

Esempio 1. Sia G un gruppo di ordine $45 = 3^2 \cdot 5$; proviamo che G è commutativo. Ora, i 3-sottogruppi di Sylow di G hanno ordine $3^2 = 9$ ed i 5-sottogruppi di Sylow hanno ordine 5. Indichiamo con n_3 , n_5 , rispettivamente il numero di 3-sottogruppi di Sylow e di 5-sottogruppi di Sylow di G . Allora, per il secondo Teorema di Sylow, $n_3 \equiv 1 \pmod{3}$ e $n_3 | 5$; quindi $n_3 = 1$ e dunque G ha un solo 3-sottogruppo di Sylow T ed è $T \trianglelefteq G$. Similmente, $n_5 \equiv 1 \pmod{5}$ e $n_5 | 9$; quindi $n_5 = 1$ e G ha un solo 5-sottogruppo di Sylow Q che è normale in G . Ora, $T \cap Q$ è sottogruppo sia di T che di Q e dunque il suo ordine deve dividere sia $|T| = 9$ che $|Q| = 5$; quindi $T \cap Q = \{1_G\}$. Si ha quindi

$$|TQ| = \frac{|T||Q|}{|T \cap Q|} = \frac{9 \cdot 5}{1} = 45$$

quindi $TQ = G$. Dunque $G = T \times Q$. Poichè T e Q sono commutativi (perchè il loro ordine è una potenza di esponente al più 2 di un numero primo), concludiamo che G è commutativo.

Ricordiamo che un gruppo G si dice *semplice* se i soli suoi sottogruppi normali son $\{1_G\}$ e G .

Esempio 2. Sia G un gruppo di ordine $72 = 2^3 \cdot 3^2$; proviamo che G non è semplice. Sia n_3 il numero di 3-sottogruppi di Sylow di G . Se $n_3 = 1$ allora G ha un 3-sottogruppo di Sylow normale e quindi G non è semplice. Supponiamo quindi $n_3 \neq 1$. Allora, per il secondo Teorema di Sylow, si ha $n_3 = 4$. Siano P, Q due distinti 3-sottogruppi di Sylow di G . Poichè $|P| = |Q| = 9 = 3^2$, P e Q sono commutativi. Consideriamo il loro prodotto $PQ \subseteq G$, e sia $H = P \cap Q$, si ha

$$72 = |G| \geq |PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{81}{|H|}$$

e quindi $H \neq \{1_G\}$. Poichè $P \neq Q$, deve essere, per il Teorema di Lagrange, $|H| = 3$, e $|PQ| = 27$. Sia ora $1 \neq x \in H$. Poichè P e Q sono commutativi, $C_G(x)$ contiene sia P che Q ; quindi $PQ \subseteq C_G(x)$. In particolare $|C_G(x)| \geq |PQ| = 27$. Poichè $|C_G(x)|$ divide $|G|$, deve essere $|C_G(x)| = 36, 72$. Se $|C_G(x)| = 72$ allora $C_G(x) = G$, e quindi $x \in Z(G)$, cioè $Z(G) \neq \{1_G\}$ e quindi G non è semplice. Sia quindi $|C_G(x)| = 36 = 2^2 \cdot 3^2$; poichè $C_G(x)$ contiene almeno due distinti 3-sottogruppi di Sylow (i nostri P e Q), applicando il secondo Teorema di Sylow al gruppo $C_G(x)$ si ha che esso contiene quattro 3-sottogruppi di Sylow; questi sono necessariamente anche tutti i 3-sottogruppi di Sylow di G . Da ciò segue che $H = \langle x \rangle$ è contenuto in ogni 3-sottogruppo di Sylow di G . Allora, se $g \in G$, $H^g = (P \cap Q)^g = P^g \cap Q^g = H$ e quindi $H \trianglelefteq G$, e G non è semplice.

Esempio 3. Sia G un gruppo di ordine 408; proviamo che G contiene un sottogruppo di indice 3. Abbiamo $408 = 2^3 \cdot 3 \cdot 17$. Per il secondo teorema di Sylow, il numero n_{17} di 17-sottogruppi di Sylow di G è congruo ad 1 modulo 17, e divide $2^3 \cdot 3 = 24$; quindi $n_{17} = 1$, G ha un unico 17-sottogruppo di Sylow N e $N \trianglelefteq G$. Consideriamo ora il gruppo quoziente G/N . Ora, $|G/N| = |G|/|N| = 24$ e quindi G/N ha un sottogruppo di ordine 2^3 ; per il Teorema di Corrispondenza, esiste un sottogruppo H di G tale che $N \leq H$ e $|H/N| = 2^3$. Quindi $|H| = |H/N||N| = 2^3 \cdot 17$ e dunque $[G : H] = |G|/|H| = 3$ e H è il sottogruppo cercato.

ESERCIZI

1. Si determinino tutti i sottogruppi di Sylow (per ogni primo che divide l'ordine del gruppo) dei gruppi S_3 e S_4 .
2. Sia G un gruppo finito, $N \trianglelefteq G$ e p un divisore primo dell'ordine di G . Sia P un p -sottogruppo di Sylow di G . Si provi che NP/N è un p -sottogruppo di Sylow di G/N , e che $P \cap N$ è un p -sottogruppo di Sylow di N .
Si faccia un esempio di un gruppo finito G , un p -sottogruppo di Sylow P di G , e di un sottogruppo (non normale) H di G , tali che $P \cap H$ non è un p -sottogruppo di Sylow di H .
3. Sia G un gruppo finito, e p un divisore primo dell'ordine di G . Sia $N \trianglelefteq G$ tale che $|N| = p^k$. Si provi che il numero di p -sottogruppi di Sylow di G è uguale al numero di p -sottogruppi di Sylow di G/N .
4. Sia G un gruppo di ordine pq , con p e q numeri primi. Si provi che G non è semplice. Si provi quindi che se $p < q$ e $p \nmid q - 1$ allora G è commutativo (anzi ciclico).
5. Siano p, q primi distinti. Si provi che un gruppo di ordine p^2q non è semplice.
6. Si provi che un gruppo di ordine 120 ha almeno 6 classi di coniugio.
7. Sia G un gruppo di ordine 224. Si provi che G non è semplice.
8. Sia G un gruppo di ordine 1998. Si provi che G ha un unico sottogruppo di indice 2.
9. Sia G un gruppo di ordine 63. Si provi che $Z(G) \neq \{1_G\}$.
10. Sia G un gruppo di ordine pq^2 , con p, q primi distinti. Si provi che se $|Z(G)| = p$ allora G è commutativo.
11. Sia G un gruppo di ordine 12. Si provi che si verifica uno dei casi seguenti.
 - a) G è commutativo; in tal caso G è ciclico oppure isomorfo al prodotto diretto di un gruppo non ciclico di ordine 4 per un gruppo ciclico di ordine 3.
 - b) $|Z(G)| = 3$ e $G/Z(G)$ è isomorfo a S_3 .
 - c) $|Z(G)| = 1$ e G è isomorfo a A_4 .