NOZIONI ELEMENTARI SUI GRUPPI

Si presentano qui alcune nozioni sui gruppi. Molte di queste si ritrovano in ogni tipo di struttura algebrica, perciò lo studio dei gruppi ha anche valore di modello per comprendere poi gli anelli, gli spazi vettoriali, le algebre.

Con un piccolo abuso di linguaggio e come è consuetudine quando non vi siano ambiguità, i gruppi saranno identificati mediante i loro sostegni; ossia, un gruppo $(G,\cdot)$ sarà sovente denotato solo con G.

Prerequisiti[1]**:** insiemi, funzioni, relazioni d'equivalenza e d'ordine, operazioni e loro proprietà, strutture algebriche, insiemi numerici e calcolo combinatorio.

Contenuto:

Lo studio dei gruppi è incominciato in Francia all'inizio dell'800, in relazione alla ricerca di formule risolutive per le equazioni algebriche, e ha riguardato inizialmente i gruppi finiti di permutazioni. E' stato successivamente esteso ai gruppi lineari, anche in vista della classificazione delle varie geometrie, ed ai gruppi topologici.

[1] Per ciascuno dei prerequisiti si vedano i capitoli precedenti.

§ 1 – GRUPPI

Un gruppo è una struttura algebrica $(G, \cdot)$ sull'insieme sostegno G, in cui l'operazione $\cdot$ è associativa, 1_G è l'elemento neutro (che è unico, come sempre) e ogni elemento x ha l'inverso x', che per ogni x è unico. Infatti, sia x" un altro inverso di x, allora:

$$\begin{cases} x \cdot x' = x' \cdot x = 1_G \\ x \cdot x'' = x'' \cdot x = 1_G \end{cases} \Rightarrow x'' = x'' \cdot 1_G = x'' \cdot (x \cdot x') = (x'' \cdot x) \cdot x' = 1_G \cdot x' = x'$$

Vedremo poi che l'inverso di x sarà denotato generalmente con x^{-1}.

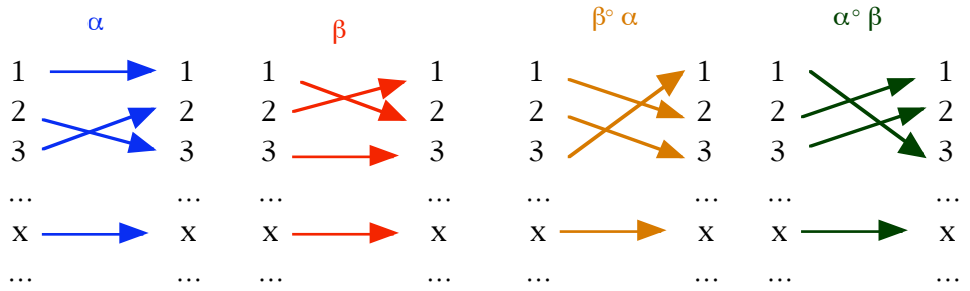
Se l'operazione $\cdot$ possiede anche la proprietà commutativa il gruppo si dice *abeliano*. Sovente, soprattutto nel caso di gruppi abeliani, l'operazione è denotata col simbolo +. In questo caso, l'elemento neutro è denotato con 0_G e ogni x ha l'*opposto* –x.

Col simbolo |G| denoteremo l'*ordine* di G, ossia il numero di elementi del suo insieme sostegno.

Esempi di gruppi abeliani sono: $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{Q}^*, \cdot)$ dove con $\mathbf{Q}^*$ indichiamo l'insieme dei numeri razionali non nulli e con $\cdot$ l'usuale moltiplicazione. Vediamo ora altri esempi, in particolare di gruppi finiti.

ESEMPI 1.1.

1.1.A. - I gruppi simmetrici. Sia X un insieme non vuoto e sia S_X l'insieme delle biiezioni dell'insieme X su di sé e che chiameremo *permutazioni* di X. L'operazione $\circ$ è la composizione di funzioni, che è una operazione in S_X, poiché componendo due permutazioni si ottiene come risultato una permutazione. L'elemento neutro è l'identità su X ed ogni permutazione α possiede come inverso la *permutazione inversa* α^{-1}, tale che se $\alpha(x) = y$ allora $\alpha^{-1}(y) = x$.
Se come X scegliamo l'insieme $\{1, ..., n\}$, il suo gruppo simmetrico si denota con S_n. Dal calcolo combinatorio sappiamo che S_n possiede $n! = 1 \cdot 2 \cdot ... \cdot n$ elementi. Non è difficile verificare che, se n è maggiore di 2, il gruppo $(S_n, \circ)$ non è abeliano. Infatti, sia $X = \{1, 2, 3, \ldots, x, \ldots\}$, dove x è un generico elemento > 3:

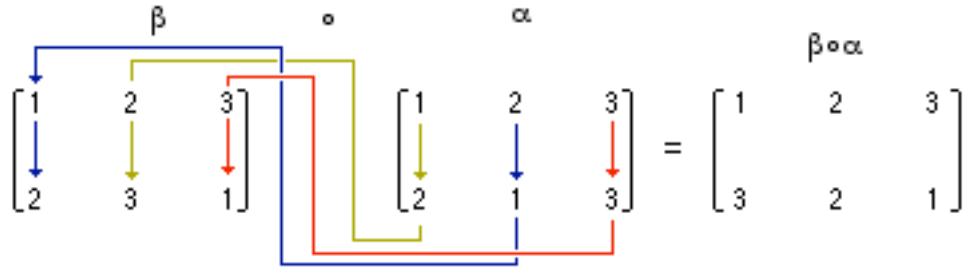


Si ha quindi $\alpha \circ \beta \neq \beta \circ \alpha$ ed il gruppo simmetrico S_n non è abeliano per $n \geq 3$.

La scrittura consueta per rappresentare una permutazione in S_n è la seguente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}$$

Per eseguire la composizione di due permutazioni si procede come nell'esempio seguente: siano $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e calcoliamo $\beta \circ \alpha$.



Per calcolare l'inversa di $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ basta "capovolgerla" e riordinare le colonne: $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \rho^{-1}$

Calcoliamo ora la tavola di composizione del gruppo simmetrico S_2. Esso ha due soli elementi, $\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Poiché id è l'elemento neutro, la tavola è necessariamente la seguente:

$\circ$	id	τ
id	id	τ
τ	τ	id

Il gruppo $(S_2, \circ)$ è abeliano ed è il "prototipo" dei gruppi con due soli elementi.

Un po' più complicata è la tavola di composizione del gruppo S_3. I suoi $6 = 3!$ elementi sono:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

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

Dobbiamo calcolare $6^2 = 36$ prodotti, che riempiono una tabella 6×6. Poiché id è l'elemento neutro, 11 di questi sono immediati: per ogni α si ha $\mathrm{id} \circ \alpha = \alpha$, $\alpha \circ \mathrm{id} = \alpha$, quindi restano 25 prodotti. Anche gli inversi sono immediati, quindi collochiamo subito le altre cinque caselle contenenti l'identità id. Restano 20 prodotti. Calcolandoli pazientemente, otteniamo:

$\circ$	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	id	τ_3	τ_1	τ_2
ρ_2	ρ_2	id	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	id	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	id

Si può risparmiare tempo? Osservando la tavola, vediamo che in ogni riga ed in ogni colonna ogni elemento del gruppo compare una ed una sola volta. Vale cioè la *legge di cancellazione*. Sarà un caso, oppure è una proprietà che hanno tutti i gruppi? Sapendolo prima, avremmo potuto calcolare solo qualche prodotto e riempire le caselle rimanenti in modo automatico. Vedremo poi che la legge di cancellazione è una proprietà di tutti i gruppi.

Tenendo presente questa proprietà, nella seconda riga, dove ci sono già $\rho_1 \circ \mathrm{id} = \rho_1$, $\rho_1 \circ \rho_2 = \mathrm{id}$, si calcolano $\rho_1 \circ \rho_1 = \rho_2$, $\rho_1 \circ \tau_1 = \tau_3$, dopo di ché restano da collocare τ_1 e τ_2. Quest'ultimo non può occupare la penultima casella, cioè la casella (2,5), perché è già presente nella penultima colonna, al I posto, quindi deve andare nella (2,6). Allora nella casella (2,5) ci va τ_1. E così via...

Più oltre vedremo altri modi di scrivere le permutazioni.

1.1.B. - I gruppi diedrali. Dato un poligono regolare $\wp$ con n lati ($n \geq 3$), come sappiamo dalla geometria ci sono 2n *isometrie* del piano che lo

trasformano in sé e precisamente: le n *rotazioni* di ampiezza $\frac{2\pi k}{n}$, k = 0, 1,..., n-1, intorno al centro O del poligono, e le n *simmetrie assiali* rispetto agli n assi di simmetria del poligono (tutti passanti per O). L'insieme di tali isometrie si indica con D_n. Siano α, β due di tali isometrie, allora

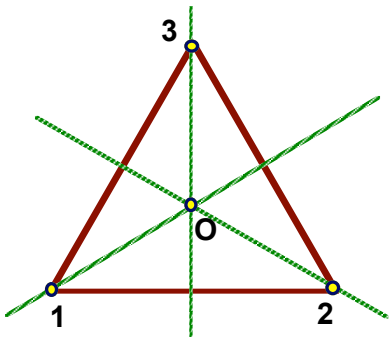
$$\begin{cases}\alpha(\wp) = \wp \\ \beta(\wp) = \wp\end{cases} \Rightarrow \alpha \circ \beta(\wp) = \alpha(\beta(\wp)) = \alpha(\wp) = \wp$$

e quindi la composizione di due elementi di D_n è ancora un elemento di D_n. L'elemento neutro è la funzione identità del piano, identificabile come la rotazione di ampiezza nulla intorno ad O, e che ovviamente lascia fisso il poligono $\wp$. E' noto che se per i = 1, 2, r_i è una rotazione di centro O ed ampiezza α_i, allora $r_1 \circ r_2$ ha ampiezza $\begin{cases}\alpha_1+\alpha_2 & \text{se } \alpha_1+\alpha_2 < 2\pi \\ \alpha_1+\alpha_2-2\pi & \text{se } \alpha_1+\alpha_2 \geq 2\pi\end{cases}$. Allora l'inversa della rotazione di ampiezza $\frac{2\pi k}{n}$ è la rotazione di ampiezza $\frac{2\pi(n-k)}{n}$. Ogni simmetria assiale ha per inversa se stessa. Perciò D_n è un gruppo rispetto alla composizione, ha 2n elementi e non è abeliano, dato che se σ è una simmetria e ρ è la rotazione di ampiezza $\frac{2\pi}{n}$, allora $\sigma \circ \rho = \rho^{-1} \circ \sigma$.

Nella figura seguente c'è il caso del triangolo equilatero. Per semplicità, le isometrie sono numerate da 1 a 6. Qui r è la rotazione di 120° in senso antiorario ed s_i è la simmetria di asse passante per il vertice numerato con i, i = 1, 2, 3.

isom.	id	r	r^2	s_1	s_2	s_3
cod.	1	2	3	4	5	6

r = rotazione di 120° intorno ad O



∘	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
6	6	4	5	2	3	1

PROPOSIZIONE 1.2. - L'operazione · di un gruppo (G, ·) possiede le proprietà seguenti. Per ogni a, b, c∈G:

a) *Leggi di cancellazione*

a sinistra: da a·b = a·c segue b = c.

a destra: da a·b = c·b segue a = c;

b) Esistenza di *operazioni inverse*

destra: esiste uno ed un solo x∈G tale che a·x = b;

sinistra: esiste uno ed un solo y∈G tale che y·a = b.

Dimostrazione. Denotiamo con a' l'inverso di a. Allora:

a) $a \cdot b = a \cdot c \Rightarrow a' \cdot (a \cdot b) = a' \cdot (a \cdot c) \Rightarrow (a' \cdot a) \cdot b = (a' \cdot a) \cdot c \Rightarrow 1_G \cdot b = 1_G \cdot c \Rightarrow b = c$

Quindi la legge di cancellazione a sinistra è vera in ogni gruppo. Analogamente si dimostra la legge di cancellazione a destra.

b) Data ora l'equazione a·x = b, si ha a'·(a·x) = a'·b, da cui segue (a'·a)·x = a'·b, ossia x = a'·b, e questa è l'unica soluzione. Analogamente, l'unica soluzione della equazione y·a = b è y = b·a'.

OSSERVAZIONI 1.3.

1.3.a) Se il gruppo è abeliano, le due equazioni hanno la stessa soluzione, che si potrebbe scrivere nella forma b:a. Altrimenti no.

Qualora poi l'operazione binaria di G sia denotata col +, allora l'equazione diventa a+x = b e la soluzione si potrebbe denotare con b-a.

1.3.b) Sia X = {1, 2, 3, 4, 5, 6}. Le tavole seguenti definiscono quattro operazioni in X, ma solo la prima costituisce un gruppo.

°	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	5	6	3	4
3	3	4	6	5	2	1
4	4	3	2	1	6	5
5	5	6	4	3	1	2
6	6	5	1	2	4	3

^	1	2	3	4	5	6
1	1	1	1	1	1	1
2	1	2	2	2	2	2
3	1	2	3	3	3	3
4	1	2	3	4	4	4
5	1	2	3	4	5	5
6	1	2	3	4	5	6

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	5	6	3
3	3	4	1	6	2	5
4	4	5	6	1	3	2
5	5	6	2	3	1	4
6	6	3	5	2	4	1

•	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	5	6	3	1	2
5	5	6	4	2	3	1
6	6	4	5	1	2	3

La seconda è associativa, commutativa, ha elemento neutro (e quindi costituisce un *monoide* commutativo), ma è *idempotente* e non ha gli inversi; la terza è commutativa, ha elemento neutro, gli inversi e la legge di cancellazione, ma non

è associativa $(2*3)*4 = 4*4=1 \neq 3 = 2*6 = 2*(3*4)$; l'ultima ha elemento neutro, gli inversi e la legge di cancellazione, ma non è associativa: $(2\bullet2)\bullet3 = 3\bullet3=2 \neq 1 = 2\bullet2 = 2\bullet(2\bullet3)$. Le ultime due costituiscono la struttura di *cappio* (o *loop*). Monoidi e cappi sono generalizzazioni dei gruppi in due direzioni differenti.

In un gruppo $(G, \cdot)$ si possono definire le *potenze* con esponente intero: siano $x\in G$ e x' il suo simmetrico. Poniamo innanzi tutto $x^0 = 1_G$. Poi, per ogni $n\in\mathbf{N}$, $n > 0$, poniamo $x^n = x^{n-1}\cdot x$, ed infine $x^{-n} = (x')^n$.

In tal modo $x^{-1} = x'$ e per questo il simmetrico di x è usualmente denotato con x^{-1}. Inoltre valgono le seguenti proprietà.

PROPOSIZIONE 1.4. Siano $(G, \cdot)$ un gruppo, $x,y\in G$, $m, n\in\mathbf{Z}$. Allora:

a) $x^m \cdot x^n = x^{m+n}$

b) $(x^m)^n = x^{mn}$

c) Se $x\cdot y = y\cdot x$ allora per ogni $n\in\mathbf{Z}$ si ha $(x\cdot y)^n = x^n\cdot y^n$. Inversamente, se $(x\cdot y)^2 = x^2\cdot y^2$ allora $x\cdot y = y\cdot x$ e quindi $(x\cdot y)^n = x^n\cdot y^n$ per ogni $n\in\mathbf{Z}$.

Dimostrazione. a) Sia $n \geq 0$. Allora:

$\begin{cases} x^m \cdot x^0 = x^m \cdot 1_G = x^m \\ x^{m+0} = x^m \end{cases}$, quindi la proprietà vale per $n = 0$. Per induzione:

$$x^m \cdot x^{n+1} = x^m \cdot \left(x^n \cdot x\right) = \left(x^m \cdot x^n\right)\cdot x = x^{m+n} \cdot x = x^{\left(m+n\right)+1} = x^{m+\left(n+1\right)}$$

Dunque, la proprietà vale se il secondo esponente, n, è ≥ 0 e per ogni $m\in\mathbf{Z}$. In particolare, si ha: $x^{-n} \cdot x^n = x^{-n+n} = x^0 = 1_G \Rightarrow \begin{cases} x^{-n} = \left(x^n\right)^{-1} \\ x^n = \left(x^{-n}\right)^{-1} \end{cases}$ (*)

Applichiamo[2] le ultime due formule trovate e la definizione di potenza per dimostrare che per ogni $n \geq 0$ si ha $x^m \cdot x^{-n} = x^{m+(-n)}$. Distinguiamo due casi:

- Se $m < 0$ allora $m' = -m > 0$, quindi:

$$x^m \cdot x^{-n} = \left(x^{-1}\right)^{m'} \cdot \left(x^{-1}\right)^n = \left(x^{-1}\right)^{m'+n} = x^{-\left(m'+n\right)} = x^{m-n} = x^{m+\left(-n\right)}$$

[2] Questa parte della dimostrazione, in carattere diverso, può essere omessa.

- Se m ≥ 0 allora poniamo $x' = x^{-1}$. Per le formule (*) si ha $x^m = \left(x^{-m}\right)^{-1} = \left(x'^m\right)^{-1} = x'^{-m}$.

Inoltre, $x^{-n} = x'^n$. Allora:

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

b) Qualunque sia m, la formula si dimostra per induzione su n nel caso n ≥ 0. Infine, mediante le formule (*) segue: $\left(x^m\right)^{-n} = \left(\left(x^m\right)^{-1}\right)^n = \left(x^{-m}\right)^n = x^{(-m)n}$.

c) Per n ≥ 0 si dimostra per induzione: è vero se n = 0, ovviamente. Inoltre:

$$(x \cdot y)^{n+1} = (x \cdot y)^n \cdot (x \cdot y) = x^n \cdot \underleftrightarrow{y^n \cdot x} \cdot y = \left(x^n \cdot x\right) \cdot \left(y^n \cdot y\right) = x^{n+1} \cdot y^{n+1}$$

Infine: $(x \cdot y)^{-n} = \left((x \cdot y)^n\right)^{-1} = \left(\underleftrightarrow{x^n \cdot y^n}\right)^{-1} = \left(y^n \cdot x^n\right)^{-1} = x^{-n} \cdot y^{-n}$.

Inversamente, se $(x \cdot y)^2 = x^2 \cdot y^2$, allora, per la legge di cancellazione:

$$x \cdot y \cdot x \cdot y = x \cdot x \cdot y \cdot y \Rightarrow y \cdot x = x \cdot y$$

Di conseguenza, se $(x \cdot y)^2 = x^2 \cdot y^2$, per la prima parte di questa dimostrazione si ha $(x \cdot y)^n = x^n \cdot y^n$ per ogni $n \in \mathbf{Z}$.

L'insieme delle potenze ad esponente intero relativo di un elemento x si denota con $\langle x \rangle$. Il numero di elementi di questo insieme si chiama *periodo* di x e si denota con $|x|$.

ESEMPI 1.5.

1.5.A. - Nel gruppo $(\mathbf{Z}, +)$ ogni elemento non nullo ha periodo infinito; si ha inoltre $\langle 1 \rangle = \mathbf{Z}$ (se l'operazione è indicata con + si parla di *multipli* anziché di potenze).

1.5.B. - Nel gruppo $\left(\mathbf{Q}^*, \cdot\right)$ oltre ad 1, che ha periodo 1, l'unico altro elemento di periodo finito è -1, dato che $\langle -1 \rangle = \{1, -1\}$.

1.5.C. - Nel gruppo $(D_n, \circ)$ ogni simmetria assiale ha periodo 2, perché composta con se stessa dà l'identità. La rotazione ρ di ampiezza $\frac{2\pi}{n}$ ha periodo n, perché eseguita n volte dà l'identità. Le altre rotazioni sono le sue potenze: infatti la rotazione ρ_k di ampiezza $\frac{2\pi k}{n}$ è uguale a ρ^k.

L'esempio precedente suggerisce l'idea che ci sia una relazione tra il numero di potenze distinte e il minimo esponente per il quale si ottiene l'elemento neutro. E infatti si ha:

TEOREMA 1.6. Sia G un gruppo e sia $x \in G$.

a) Il periodo di x è infinito se e solo se per ogni $m, n \in \mathbf{Z}$, da $m \neq n$ segue $x^n \neq x^m$.

b) Se $|x| = n$, si ha $n = \min\{h \in \mathbf{N} \mid h > 0 \text{ e } x^h = 1_G\}$. In tal caso si ha:

$$\langle x \rangle = \{x^0, x^1, ..., x^{n-1}\}.$$

c) Se $|x| = n$, si ha $x^k = 1 \Leftrightarrow$ n divide k;

Dimostrazione. a) Se per ogni $m, n \in \mathbf{Z}$, da $m \neq n$ segue $x^n \neq x^m$, la funzione $f: \mathbf{Z} \to \langle x \rangle$ definita da $f(n) = x^n$ è una biiezione, quindi x ha periodo infinito. Inversamente, se $x^n = x^m$ con $n > m$, allora $x^{n-m} = 1_G$. Poiché per ogni $k \in \mathbf{Z}$ esistono q, r tali che $k = (n-m)q+r$, con $0 \leq r < (n-m)$, si ha:

$$x^k = (x^{n-m})^q x^r = x^r \in \{x^0, x^1, ..., x^{(n-m)-1}\},$$

quindi $\langle x \rangle \subseteq \{x^0, x^1, ..., x^{(n-m)-1}\}$, e vale ovviamente anche l'altra inclusione, per cui i due insiemi coincidono. Dunque, $\langle x \rangle$ è finito.

b) Da a) segue che le potenze x^k di x non sono tutte distinte e quindi esistono esponenti $h > 0$ per i quali $x^h = 1_G$. Detto m il minimo di essi, si ha, come sopra, $\langle x \rangle = \{x^0, x^1, ..., x^{m-1}\}$. Inoltre, se $0 < h < k < m$, si ha necessariamente $x^h \neq x^k$, altrimenti si avrebbe $x^{k-h} = 1_G$ con $0 < k-h < m$, assurdo. Perciò:

$$n = |\langle x \rangle| = |\{x^0, x^1, ..., x^{m-1}\}| = m.$$

c) Posto $k = nq+r$, con $0 \leq r < n$, si ha $1_G = x^k = x^r$, da cui segue $r = 0$, per la minimalità di n.

Quando in un gruppo (G, ·) c'è un elemento x tale che $\langle x \rangle = G$ allora il gruppo si dice *ciclico* ed x si chiama *generatore* di G. Ovviamente, un gruppo ciclico è abeliano, perché le potenze di x commutano: per ogni h,k∈**Z**, per 1.4.a) si ha $x^h \cdot x^k = x^{h+k} = x^{k+h} = x^k \cdot x^h$.

ESEMPI 1.7.

1.7.A. – (**Z**, +) è ciclico infinito, generato da 1, ma anche da -1.

1.7.B. – Sia n ≥ 1. Per ogni x∈**Z** poniamo

$$\mathrm{mod}(x,n) = \text{resto della divisione di x per n}$$

Sia ora $\mathbf{Z}_n = \{0,1,\ldots,n-1\}$. Definiamo in questo insieme la seguente operazione:

$$x +_n y = \mathrm{mod}(x+y, n) = \text{resto della divisione di x+y per n.}$$

E' immediato provare che è commutativa ed ha elemento neutro 0. Ogni elemento x ha per opposto n-x: infatti, $x +_n (n-x) = \mathrm{mod}(n,n) = 0$. Occorre ora dimostrare la proprietà associativa, ma lo faremo più avanti, nel § 3, con metodi meno diretti, ma più potenti. Osserviamo ora che per ogni x∈$\mathbf{Z}_n$, x > 1, si ha $x = \underbrace{1+1+\ldots+1}_{\text{x volte}}$, quindi $\mathbf{Z}_n = \langle 1 \rangle$. Pertanto, per ogni n ≥ 1 c'è un gruppo ciclico, quindi abeliano, di ordine n.

Qui di seguito vediamo le tavole per n = 2, 3, 4,5.

$+_2$	0	1
0	0	1
1	1	0

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Oltre ad 1, ci sono altri generatori di $\mathbf{Z}_n$? Vedremo la risposta nel § 3, ma si può anticipare che un elemento a∈$\mathbf{Z}_n$ genera $\mathbf{Z}_n$ se e solo se MCD(a,n) = 1. Pertanto, ci sono $\varphi(n)$ elementi atti a generare $\mathbf{Z}_n$, dove φ è la *funzione di Eulero*.

Per n = 12 si ha il *gruppo dell'orologio*: se ora sono le 10, che ora segnerà l'orologio tra 5 ore? Segnerà le 3, tutti sappiamo rispondere, e si ha proprio:

$$3 = \mathrm{mod}(15,12) = \mathrm{mod}(10+5,12) = 10 +_{12} 5.$$

Se due elementi di un gruppo G hanno periodi rispettivamente m ed n, che cosa si può dire del periodo del prodotto? In generale non si può dire nulla.

ESEMPI 1.8.

1.8.A. – Siano $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ due matrici reali. Si verifica facilmente che $A^2 = B^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, e quest'ultima matrice ha il quadrato uguale all'identità, quindi $|A| = 4$, $|B| = 6$. Si ha però $A \times B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, e

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \ \ldots, \ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ per ogni } n \in \mathbf{N},$$

quindi $|A \times B|$ è infinito.

1.8.B. - Se $a, b \in G$ commutano ed hanno periodi finiti, allora $|a \cdot b|$ divide $m = \mathrm{mcm}(|a|, |b|)$. Infatti, $(a \cdot b)^m = a^m \cdot b^m = 1_G \cdot 1_G = 1_G$. Però in generale non vale l'uguaglianza. Infatti, se $|a| = k > 1$, preso $b = a^{-1}$, anche $|b| = k$, quindi il mcm dei periodi è k, mentre $|a \cdot b| = 1$.

PROPOSIZIONE 1.9. Siano G un gruppo ed $a, b \in G$ tali che $\begin{cases} a \cdot b = b \cdot a \\ \langle a \rangle \cap \langle b \rangle = \{1_G\} \end{cases}$. Siano $\begin{cases} h = |a| \\ k = |b| \end{cases}$, $\begin{cases} m = \mathrm{mcm}(h,k) \\ n = |a \cdot b| \end{cases}$. Allora $m = n$.

Dimostrazione. Abbiamo già visto che n divide m. Dimostriamo che m divide n.

$1_G = (a \cdot b)^n = a^n \cdot b^n \Rightarrow \underbrace{a^n}_{\in \langle a \rangle} = \underbrace{(b^n)^{-1}}_{\in \langle b \rangle}$. Ma $\langle a \rangle \cap \langle b \rangle = \{1_G\}$, dunque $\begin{cases} a^n = 1_G \\ b^n = 1_G \end{cases}$ quindi

$\begin{cases} h \text{ divide } n \\ k \text{ divide } n \end{cases}$ e di conseguenza anche m = mcm(h,k) divide n. Ne segue n = m.

Torniamo ora al gruppo simmetrico S_n, $n \geq 2$, e cerchiamo altre sue proprietà, tra cui i periodi dei suoi elementi.

Due permutazioni si dicono *disgiunte* se gli oggetti spostati dalla prima sono fissati dalla seconda e viceversa.

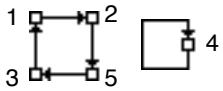
LEMMA 1.10. Siano $\alpha,\beta \in S_n$ disgiunte, allora $\alpha \circ \beta = \beta \circ \alpha$

Dimostrazione. Dimostriamo che per ogni $i \in \{1,2,\dots,n\}$ si ha $\alpha \circ \beta(i) = \beta \circ \alpha(i)$. Esaminiamo i soli tre casi possibili.

- Se $\alpha(i) = i = \beta(i)$ allora $\begin{cases} \alpha \circ \beta(i) = \alpha(\beta(i)) = \alpha(i) = i \\ \beta \circ \alpha(i) = \beta(\alpha(i)) = \beta(i) = i \end{cases} \Rightarrow \alpha \circ \beta(i) = \beta \circ \alpha(i).$
- Se $\alpha(i) = j \neq i$ allora β li fissa entrambi, essendo disgiunta da α, pertanto:
$$\begin{cases} \alpha \circ \beta(i) = \alpha(\beta(i)) = \alpha(i) = j \\ \beta \circ \alpha(i) = \beta(\alpha(i)) = \beta(j) = j \end{cases} \Rightarrow \alpha \circ \beta(i) = \beta \circ \alpha(i)$$
- Se $\beta(i) = j \neq i$ allora α li fissa entrambi, e si procede allo stesso modo.

Sia r un intero positivo, $2 \leq r \leq n$ e siano dati r elementi distinti $i_1,\dots,i_r \in \{1,2,\dots,n\}$. Col simbolo $(i_1,\dots,i_r)$ denoteremo la permutazione γ che per ogni k, $1 \leq k \leq n\text{-}1$ porta i_k in i_{k+1}, mentre porta i_r in i_1 e lascia fisso ogni altro oggetto diverso da questi. Questa permutazione si chiama *ciclo* di lunghezza r. Vediamo un ciclo di lunghezza 4 in S_5, con accanto una possibile traduzione grafica:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} = (1253)$$



Lo stesso ciclo si può scrivere in più modi: $(1253) = (2531) = (5312) = (3125)$, ma se ci accordiamo di cominciare dall'oggetto più piccolo tra quelli spostati, ossia, in questo caso, da 1, abbiamo l'unicità della rappresentazione.

I cicli hanno un ruolo importante nel gruppo simmetrico, simile a quello che hanno i numeri primi in **N**. Si ha infatti:

TEOREMA 1.11. Ogni permutazione diversa dall'identità in S_n o è un ciclo oppure si esprime come prodotto di cicli disgiunti, e questa fattorizzazione è unica a meno dell'ordine dei fattori.

Dimostrazione. Per illustrare la dimostrazione è utile premettere un esempio, che inoltre spiega come ottenere praticamente la fattorizzazione. Sia $\alpha \in S_9$,

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

Il primo elemento spostato da α è il 2. Abbiamo così:

$$2 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 5 \xrightarrow{\alpha} 6 \xrightarrow{\alpha} 2$$

che ci fornisce il primo fattore $\gamma_1 = (2356)$, ciclo di lunghezza quattro.

Dopo l'1, fissato ed il 2 e il 3, che fanno parte del ciclo γ_1, c'è il 4:

$$4 \xrightarrow{\alpha} 8 \xrightarrow{\alpha} 9 \xrightarrow{\alpha} 4$$

ed otteniamo un secondo ciclo $\gamma_2 = (489)$, di lunghezza tre.

Gli elementi 5, 6 fanno parte di cicli già considerati. Il primo elemento non ancora trattato è il 7, che è fissato da α, poi l'8 ed il 9 già considerati. Allora diciamo che $\alpha = \gamma_1 \circ \gamma_2$, (che è uguale a $\gamma_2 \circ \gamma_1$ perché i due cicli sono disgiunti).

Infatti, i due elementi 1, 7 fissati da α sono fissati anche dai due cicli. Quindi anche da $\gamma_1 \circ \gamma_2$. Si ha poi: $\begin{cases} \alpha(2) = 3 \\ \gamma_1 \circ \gamma_2(2) = \gamma_1(\gamma_2(2)) = \gamma_1(2) = 3 \end{cases}$, e più in generale per ogni i = 2, 3, 5, 6 si ha $\gamma_1 \circ \gamma_2(i) = \gamma_1(\gamma_2(i)) = \gamma_1(i) = \alpha(i)$. Infine, per ogni i = 4, 8, 9 si ha $\gamma_1 \circ \gamma_2(i) = \gamma_1(\gamma_2(i)) = \gamma_1(\alpha(i)) = \alpha(i)$. Allora si ha proprio $\alpha = \gamma_1 \circ \gamma_2$.

Tra le due possibilità $\alpha = \gamma_1 \circ \gamma_2 = \gamma_2 \circ \gamma_1$ scegliamo la prima, in cui il primo oggetto spostato dal I fattore è minore del primo oggetto spostato dal II.

Una possibile dimostrazione del teorema procede per induzione sul numero di oggetti spostati da α. Se α = id, il teorema è vero. Altrimenti, sia i_1 il più piccolo oggetto spostato da α. Abbiamo la seguente successione:

$$i_1 \xrightarrow{\alpha} i_2 \xrightarrow{\alpha} \dots \xrightarrow{\alpha} i_k \xrightarrow{\alpha} \dots$$

Poiché il numero totale n di oggetti è finito, la successione non può proseguire all'infinito trovando oggetti sempre diversi. Pertanto esiste un minimo $m \geq 2$ tale che $i_m = \alpha(i_{m-1})$ coincide con uno degli oggetti già trovati: $i_m = i_k$, $k < m$.

Se per assurdo fosse k > 1 allora $\alpha(i_{m-1}) = i_k = \alpha(i_{k-1})$, che essendo α iniettiva implicherebbe $i_{m-1} = i_{k-1}$, contro la minimalità di m. Pertanto, k = 1. Allora consideriamo il ciclo $\gamma_1 = (i_1 i_2 \dots i_{m-1})$. Per ciascuno di questi m oggetti si ha $\gamma_1(i_k) = \alpha(i_k)$. Ogni altro oggetto, anche se spostato da α, è fissato da γ_1. L'inverso ${\gamma_1}^{-1}$ del ciclo γ_1 agisce sugli oggetti i_k come α^{-1} e fissa gli altri oggetti. Poniamo allora $\beta = \gamma_1^{-1} \circ \alpha$. Ogni oggetto fissato da α è fissato anche da ${\gamma_1}^{-1}$, ma inoltre $\beta(i_k) = \gamma_1^{-1} \circ \alpha(i_k) = \gamma_1^{-1}(\alpha(i_k)) = \alpha^{-1}(\alpha(i_k)) = i_k$, quindi β fissa anche tutti gli m oggetti i_k. Dunque, β sposta meno oggetti di α, e quindi a β si può applicare l'ipotesi induttiva: esistono $\gamma_2, \dots, \gamma_r$, cicli disgiunti, tali che $\gamma_1^{-1} \circ \alpha = \beta = \gamma_2 \circ \dots \circ \gamma_r$. Ordiniamo i fattori in modo che i primi elementi spostati dai vari cicli siano in ordine crescente. Allora abbiamo anche l'unicità della fattorizzazione di β.

Di qui segue $\gamma_1^{-1} \circ \alpha = \beta = \gamma_2 \circ \dots \circ \gamma_r$. Questi cicli operano sugli oggetti spostati da β, quindi fissano a loro volta gli oggetti i_k. Ne segue che sono disgiunti da γ_1. Allora $\gamma_1^{-1} \circ \alpha = \gamma_2 \circ \dots \circ \gamma_r \Rightarrow \alpha = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_r$, prodotto di cicli disgiunti. Inoltre, il più piccolo oggetto spostato da α è in γ_1, quindi gli r fattori sono nell'ordine giusto. Per dimostrare l'unicità della fattorizzazione di α, consideriamo un ciclo γ che faccia parte di una scomposizione alternativa di α. In particolare, γ sia quello che sposta l'oggetto più piccolo, che necessariamente è il più piccolo spostato da α, ossia è i_1. Allora $\gamma(i_1) = \alpha(i_1) = i_2 = \gamma_1(i_1)$. Più in generale, per ogni k, $1 \le k \le m-1$, si deve quindi avere $\gamma(i_k) = \alpha(i_k) = \gamma_1(i_k)$ ed in particolare $\gamma(i_{m-1}) = \alpha(i_{m-1}) = i_1 = \gamma_1(i_{m-1})$. Dunque, $\gamma = \gamma_1$. Gli altri cicli fanno parte della scomposizione di β, che ha l'unicità per ipotesi induttiva. Perciò anche per α vale l'unicità.

Applichiamo ora il risultato precedente per ottenere informazioni sul periodo di una permutazione. Il primo caso è quello di un ciclo, per il quale si ha un semplice risultato: il periodo di un ciclo è uguale alla sua lunghezza. Si ha infatti:

LEMMA 1.12. Sia $\gamma = (i_1, \dots, i_m) \in S_n$, allora $|\gamma| = m$.

Dimostrazione. Per ogni $k \in \mathbf{N}$, $1 \le k \le m-1$ si ha $i_{k+1} = \gamma^k(i_1)$, quindi $\gamma^k \ne \mathrm{id}$. Ma $\gamma^m(i_1) = \gamma(\gamma^{m-1}(i_1)) = \gamma(i_m) = i_1$. Ne segue $\gamma^m(i_2) = \gamma^m(\gamma(i_1)) = \gamma(\gamma^m(i_1)) = \gamma(i_1) = i_2$, e

così via. Ogni altro oggetto fissato da γ lo è anche dalle sue potenze, quindi anche da γ^m, perciò $\gamma^m = id$. Allora $|\gamma| = m$.

COROLLARIO 1.13. Sia $\alpha \in S_n$, $\alpha = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_r$ prodotto di cicli disgiunti. Allora $|\alpha| = mcm(|\gamma_1|, |\gamma_2|, \ldots, |\gamma_r|)$

Dimostrazione. Procediamo per induzione rispetto ad r. Se $r = 1$ è ovviamente vero. Sia $r > 1$ e poniamo $\beta = \gamma_2 \circ \ldots \circ \gamma_r$. Le due permutazioni β e γ_1 sono disgiunte, quindi commutano ed inoltre, operando su oggetti distinti, non hanno potenze uguali se non l'identità. Pertanto, sono soddisfatte le condizioni della Proposizione 1.8. e si ha: $|\alpha| = mcm(|\gamma_1|, |\beta|)$. Poiché $\beta = \gamma_2 \circ \ldots \circ \gamma_r$ è prodotto di r-1 cicli disgiunti, per ipotesi induttiva si ha $|\beta| = mcm(|\gamma_2|, \ldots, |\gamma_r|)$, quindi $|\alpha| = mcm(|\gamma_1|, |\beta|) = mcm(|\gamma_1|, |\gamma_2|, \ldots, |\gamma_r|)$.

Due problemi interessanti, ma difficili e in un certo senso inversi l'uno dell'altro, sono:

I. Qual è il massimo periodo m degli elementi di S_n?

II. Dato un intero positivo $m \geq 2$, qual è il minimo intero positivo n tale che in S_n ci sia un elemento di periodo m?

Nel primo problema si tratta di esprimere n come somma di interi positivi aventi il minimo comune multiplo massimo possibile. Nel secondo, si tratta alla fine di scomporre m in fattori la cui somma sia minima.

Per esempio, se n = 10 si può scrivere 10 = 5+3+2, quindi c'è un elemento $\alpha = (12345) \circ (678) \circ (9\ 10)$ di periodo $mcm(5,3,2) = 30$. Si può fare di meglio?

Sia m = 42. Allora $\underbrace{42}_{42} = \underbrace{2 \cdot \underbrace{21}_{23}}_{17} = \underbrace{3 \cdot \underbrace{14}_{13}}_{12} = \underbrace{6 \cdot 7}_{12} = \underbrace{2 \cdot 3 \cdot 7}_{12}$, pertanto in S_{12} c'è un elemento di periodo 42, $\alpha = (1234567) \circ (8\ 9\ 10) \circ (11\ 12)$. E per n < 12 esiste?

Siano date due strutture algebriche, che denoteremo con $(H, *)$ e $(K, \bullet)$. Sul loro prodotto cartesiano $H \times K$ definiamo la seguente operazione:

$\forall h_1, h_2 \in H, k_1, k_2 \in K, (h_1, k_1) \cdot (h_2, k_2) = (h_1 * h_2, k_1 \bullet k_2)$.

La struttura $(H \times K, \cdot)$ è detta *prodotto diretto (esterno)* delle due strutture date.

La stessa nozione si può dare per due strutture qualunque, purché dello stesso tipo, e si può estendere ad un numero $n \geq 2$ di strutture dello stesso tipo.

LEMMA 1.14. Siano $(H, *)$ e $(K, \bullet)$ due gruppi, allora:

a) il prodotto diretto $(H \times K, \cdot)$ è un gruppo;

b) $(H \times K, \cdot)$ è abeliano se e solo se i due gruppi $(H, *)$ e $(K, \bullet)$ lo sono.

Dimostrazione. a) $\forall h_1, h_2, h_3 \in H$, $k_1, k_2, k_3 \in K$, per la proprietà associativa dei due fattori:

$$\left((h_1,k_1)\cdot(h_2,k_2)\right)\cdot(h_3,k_3) = (h_1 * h_2, k_1 \bullet k_2)\cdot(h_3,k_3) = \left((h_1 * h_2) * h_3, (k_1 \bullet k_2) \bullet k_3\right) =$$
$$= \left(h_1 * (h_2 * h_3), k_1 \bullet (k_2 \bullet k_3)\right) = (h_1,k_1)\cdot(h_2 * h_3, k_2 \bullet k_3) = (h_1,k_1)\cdot\left((h_2,k_2)\cdot(h_3,k_3)\right)$$

Si ha poi: $1_{H\times K} = (1_H, 1_K)$, poiché, per ogni $(h,k) \in H \times K$ si ha:

$$(1_H,1_K)\cdot(h,k) = (1_H * h, 1_K \bullet k) = (h,k), \quad (h,k)\cdot(1_H,1_K) = (h * 1_H, k \bullet 1_K) = (h,k)$$

Infine, $(h,k)^{-1} = (h^{-1}, k^{-1})$ e la verifica è lasciata per esercizio. Pertanto, $(H \times K, \cdot)$ è un gruppo.

b) $(H \times K, \cdot)$ è abeliano $\Leftrightarrow \forall h_1, h_2 \in H$, $k_1, k_2 \in K$,

$$(h_1,k_1)\cdot(h_2,k_2) = (h_2,k_2)\cdot(h_1,k_1) \Leftrightarrow (h_1 * h_2, k_1 \bullet k_2) = (h_2 * h_1, k_2 \bullet k_1) \Leftrightarrow$$
$$\Leftrightarrow \begin{cases} h_1 * h_2 = h_2 * h_1 \\ k_1 \bullet k_2 = k_2 \bullet k_1 \end{cases} \Leftrightarrow (H, *) \text{ e } (K, \bullet) \text{ sono abeliani.}$$

OSSERVAZIONE 1.15. La verifica delle proprietà è indipendente dall'essere gruppi i due fattori, ma vale per tutte le strutture algebriche che abbiano una o più delle proprietà: associativa, commutativa, idempotenza, assorbimento, legge di cancellazione, elemento neutro, inversi; il prodotto diretto ha le ha se e solo se le hanno entrambi i fattori, e lo stesso vale per le proprietà distributive. In particolare, se G ed H sono strutture algebriche dello stesso tipo (semigruppi, monoidi, gruppi, anelli, reticoli) anche il prodotto diretto lo è. Altre proprietà invece non si conservano, come vediamo subito col caso dei gruppi ciclici finiti

PROPOSIZIONE 1.16. Si consideri il prodotto diretto $G = H \times K$ di due gruppi ciclici H e K di ordini rispettivamente h e k.

a) Il massimo periodo degli elementi di G è $m = \text{mcm}(h, k)$

b) G è ciclico se e solo se MCD(h, k) = 1.

Dimostrazione. a) Poiché m è un multiplo di h e di k, per ogni g = (x, y)∈H×K si ha: $(x,y)^m = (x^m, y^m) = (1_H, 1_K) = 1_G$. D'altra parte, se in particolare a e b sono generatori di H e K, allora posto $\bar{a} = (a, 1_K)$, $\bar{b} = (1_H, b)$, si ha:

$$\begin{cases} \bar{a}\cdot\bar{b} = (a,b) = \bar{b}\cdot\bar{a} \\ \langle\bar{a}\rangle \cap \langle\bar{b}\rangle = \{(1_H, 1_k)\} = \{1_G\} \end{cases} \Rightarrow |\bar{a}\cdot\bar{b}| = \text{mcm}(|\bar{a}|, |\bar{b}|) = \text{mcm}(h,k) = m$$

Quindi il massimo è proprio m.

b) Affinché G sia ciclico occorre che ci sia un elemento di periodo $|G| = |H|\cdot|K| = h\cdot k$, quindi $h\cdot k = \text{mcm}(h,k)$ e ciò è come dire MCD(h, k) = 1.

ESEMPIO 1.17. - Il gruppo $(\mathbf{Z}_2, +)$ è ciclico d'ordine 2. Il prodotto diretto G di $\mathbf{Z}_2$ con se stesso è un gruppo abeliano di ordine 4, non ciclico, in cui gli elementi diversi da $1_G = (0,0)$ hanno tutti periodo 2. Per calcolarne la tavola di moltiplicazione, poniamo: $a = (0,1)$, $b = (1,0)$, $c = (1,1)$. Allora la tavola di G è:

·	1_G	a	b	c
1_G	1_G	a	b	c
a	a	1_G	c	b
b	b	c	1_G	a
c	c	b	a	1_G

.

Per induzione, possiamo iterare l'esempio precedente, ponendo:

$$G_1 = (\mathbf{Z}_2, +),\ G_n = G_{n-1}\times\mathbf{Z}_2\ \forall n \geq 2$$

Tutti questi gruppi sono abeliani ed i loro elementi diversi dall'elemento neutro hanno periodo 2. Un gruppo come questo è detto *2-gruppo abeliano elementare* di ordine 2^n.

Lo stesso si può ripetere a partire da $(\mathbf{Z}_p, +)$, p primo. Per ogni n ≥ 1 si costruisce un gruppo G di ordine p^n, in cui tutti gli elementi $\neq 1_G$ hanno periodo p, e che è chiamato *p-gruppo abeliano elementare* di ordine p^n.

§2 - Sottogruppi

Riprendiamo la tavola di moltiplicazione del gruppo simmetrico S_3:

$\circ$	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	id	τ_3	τ_1	τ_2
ρ_2	ρ_2	id	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	id	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	id

I tre elementi id, ρ_1, ρ_2, composti fra loro, danno ancora loro stessi come risultati. Essi danno luogo ad una tavola di composizione in cui si ritrovano le stesse caratteristiche di quella dei gruppi: c'è l'identità, ogni elemento ha l'inverso, ed inoltre vale la proprietà associativa, perché l'operazione è quella di S_3, ossia la composizione di funzioni.

$\circ$	id	ρ_1	ρ_2
id	id	ρ_1	ρ_2
ρ_1	ρ_1	ρ_2	id
ρ_2	ρ_2	id	ρ_1

Si tratta cioè di un gruppo con tre elementi, costituito dal sottoinsieme $H = \{\text{id}, \rho_1, \rho_2\}$ di S_3 e dalla restrizione ad H della operazione di S_3. Tale gruppo è detto *sottogruppo* di S_3.

Se (G, ·) è un gruppo, un **sottogruppo** è una struttura $(H, \cdot)$, dove H è un sottoinsieme di G, *chiuso* rispetto alla moltiplicazione di G e contenente 1_G e l'inverso di ogni suo elemento. Si ha così che $(H, \cdot)$ è un gruppo e $1_H = 1_G$. Si scrive $H \leq G$.

ESEMPI 2.1.

2.1.A. - L'insieme degli interi pari $2\mathbf{Z}$ dà luogo ad un sottogruppo di $(\mathbf{Z}, +)$, perché la somma di due numeri pari è pari, lo zero è pari e l'opposto di un numero pari è pari.

2.1.B. - Più in generale, dato un gruppo $(G, \cdot)$ ed un elemento $a \in G$, l'insieme $\langle a \rangle$ delle potenze di a costituisce un sottogruppo, detto *sottogruppo ciclico* generato da a. Infatti, il prodotto e l'inverso di a sono potenze di a (per la proposizione 1.4), ed anche $1_G = a^0 \in \langle a \rangle$.

2.1.C. - Nel gruppo diedrale D_n, la rotazione ρ di ampiezza $\frac{2\pi}{n}$ ha periodo n, perché il poligono ritorna nella posizione iniziale solo dopo avere compiuto un angolo giro $2\pi = n\frac{2\pi}{n}$, ciè dopo avergli applicato n volte la rotazione ρ. Dunque $\langle \rho \rangle$ è un sottogruppo con n elementi.

2.1.D. - Troviamo tutti i sottogruppi di $(\mathbf{Z}, +)$. Sia H un sottogruppo. Allora $0 \in H$. Può accadere che sia $H = \{0\}$, allora H è il *sottogruppo banale*. Altrimenti, H possiede almeno un elemento x non nullo, quindi contiene anche l'opposto –x, e tra x e –x uno è positivo. Allora H contiene numeri positivi, quindi possiamo scegliere il minimo intero positivo m appartenente ad H. Intanto, ogni multiplo di m appartiene ad H, quindi il sottogruppo $m\mathbf{Z} = \langle m \rangle$ è incluso in H. Inversamente, sia $x \in H$; diviso per m dà un quoziente q ed un resto r tali che $x = mq+r$, con $0 \le r < m$. Ora, $r = x-mq = x+(-q)m$ è somma di due elementi di H, quindi appartiene ad H. Ma m è il minimo intero positivo in H, quindi deve essere $r = 0$ e quindi $x = mq \in m\mathbf{Z}$. Dunque, $H = m\mathbf{Z}$. Se teniamo conto che anche il sottogruppo banale si può scrivere nella forma $0\mathbf{Z}$, possiamo concludere che ogni sottogruppo di $\mathbf{Z}$ è ciclico, cioè della forma $m\mathbf{Z}$, con $m \ge 0$. In particolare, $\mathbf{Z} = 1\mathbf{Z}$.

Per ogni sottogruppo H di un gruppo G e per ogni $g \in G$ poniamo $Hx = \{h \cdot x \mid h \in H\}$. E' un sottoinsieme di G detto *laterale destro* di H in G, individuato da x. Analogamente si definisce il *laterale sinistro* xH. Il numero dei laterali destri distinti di H in G si denota con [G:H] e si chiama *indice* di H in G. Si ha il seguente risultato:

TEOREMA 2.2. (Lagrange). Per ogni sottogruppo H del gruppo finito G si ha $|G| = |H| \cdot [G:H]$. In particolare, $|H|$ e $[G:H]$ dividono $|G|$.

Dimostrazione. Per ogni x, y∈G, poniamo:

$$x \sim_H y \text{ se esiste } h \in H \text{ tale che } y = h \cdot x.$$

Questa è una relazione d'equivalenza in G. Infatti:

a) proprietà riflessiva: per ogni x∈G si ha $x \sim_H x$, poiché $x = 1_G \cdot x$ e $1_G \in H$, dato che $H \leq G$.

b) proprietà simmetrica: siano x, y∈G tali che $x \sim_H y$, allora esiste h∈H tale che $y = h \cdot x$. Di qui segue $x = h^{-1} \cdot y$, con $h^{-1} \in H$ dato che $H \leq G$. Pertanto, $y \sim_H x$.

c) proprietà transitiva: siano x, y, z∈G tali che $\begin{cases} x \sim_H y \\ y \sim_H z \end{cases}$. Ciò significa che esistono h', h" ∈H tali che $\begin{cases} y = h' \cdot x \\ z = h'' \cdot y \end{cases}$. Allora, sostituendo, per la proprietà associativa si ha: $z = h'' \cdot (h' \cdot x) = (h'' \cdot h') \cdot x$, con $(h'' \cdot h') \in H$, dato che $H \leq G$. Allora $x \sim_H z$.

Per ogni x∈G, la classe di equivalenza $[x]_{\sim_H}$ coincide col laterale destro Hx. Infatti, per cominciare, ogni elemento h·x∈Hx è equivalente ad x per definizione di $\sim_H$. Dunque, $Hx \subseteq [x]_{\sim_H}$. Inversamente, per ogni $y \in [x]_{\sim_H}$ esiste h∈H tale che $y = h \cdot x \in Hx$, quindi $[x]_{\sim_H} \subseteq Hx$. Allora $[x]_{\sim_H} = Hx$.

Di conseguenza, i laterali destri di H in G formano una partizione di G.

Proviamo ora che ogni laterale destro Hx di H in G è equipotente ad H. Per fare ciò dobbiamo trovare una biiezione da H ad Hx. Proviamo con la funzione seguente: $f : H \to Hx,\ f : h \mapsto h \cdot x$. Il codominio è davvero Hx perché per ogni h∈H, $f(h) = h \cdot x \in Hx$. Inoltre è suriettiva, perché ogni elemento y di Hx è della forma h··x, con h∈H, quindi $y = f(h)$. Infine, è iniettiva perché ∀ h, h'∈H, se $f(h) = f(h')$, ossia se $h \cdot x = h' \cdot x$, allora, per la legge di cancellazione, segue h = h'.

Poiché G è finito, allora H ha un numero finito r = [G:H] di laterali destri. Siano Hx_i, $1 \leq i \leq r$, i laterali destri distinti. Dato che essi formano una partizione di G e sono tutti equipotenti ad H, allora, dal "principio di addizione" segue:

$$|G| = \sum_{i=1}^{r} |Hx_i| = \sum_{i=1}^{r} |H| = r \cdot |H| = [G : H] \cdot |H|$$

Dunque, |H| e [G:H] dividono |G|.

OSSERVAZIONI 2.3

a) La prima parte della dimostrazione non usa il fatto che G sia un gruppo finito. In altre parole, anche se G è infinito l'insieme dei laterali destri di H in G è una sua partizione e ciascun laterale destro è equipotente ad H.

b) Lo stesso risultato vale anche per i laterali sinistri di H in G: formano una partizione di G, sono tutti equipotenti ad H e ce ne sono [G:H].

c) Il teorema di Lagrange è tipico dei gruppi. Nei monoidi in generale non vale, o perché i laterali destri di un sottomonoide non formano una partizione o perché non sono equipotenti fra loro.

d) Se G è un gruppo finito d'ordine n e k è un divisore di n, non è detto che ci sia un sottogruppo d'ordine k. Un controesempio è costituito dal *gruppo alterno* A_4 su 4 oggetti, che vedremo poi: ha ordine 12, ma non ha sottogruppi di ordine 6. Un gruppo finito d'ordine n nel quale per ogni divisore k di n esiste un sottogruppo d'ordine k è detto *lagrangiano*. Si può dimostrare che i gruppi abeliani finiti sono lagrangiani.

Alcune conseguenze del teorema di Lagrange sono le seguenti:

COROLLARIO 2.4. **a)** In un gruppo finito G, il periodo di ogni suo elemento x, uguale all'ordine di $\langle x \rangle$, divide l'ordine di G.

b) Se G ha ordine primo p, è necessariamente ciclico.

Dimostrazione. b) Preso un elemento $x \neq 1_G$, il sottogruppo $\langle x \rangle$ ha ordine > 1 e divisore di p, quindi coincidente con p. Allora $\langle x \rangle = G$.

ESEMPI 2.5.

2.5.A. - Sia $G = S_3$ il gruppo simmetrico su tre oggetti. Sia H il sottogruppo $\{id, \tau\}$, dove $\tau = (12)$ è la trasposizione che scambia 1 con 2 e lascia fisso il 3. Troviamo i laterali destri di H in G.

- Il primo di essi è $H = H \circ id$, ma si ha anche $H = H \circ \tau$, perché $\tau \in H$.

- Moltiplichiamo ora H per una permutazione diversa da id e da τ. Sia $\alpha = (13)$. Allora $H\alpha = \{id \circ \alpha,\ \tau \circ \alpha\} = \{\alpha,\ \rho\}$, dove $\rho = \tau \circ \alpha = (12) \circ (13) = (132)$. Naturalmente si ha anche $H\rho = H\alpha$.

- Un elemento non ancora trovato è $\beta = (23)$. Allora $H\beta = \{id \circ \beta,\ \tau \circ \beta\} = \{\beta,\ \rho^{-1}\}$, essendo $\tau \circ \beta = (12) \circ (23) = (123) = (132)^{-1} = \rho^{-1}$.

Abbiamo così trovato i tre laterali destri di H in G.

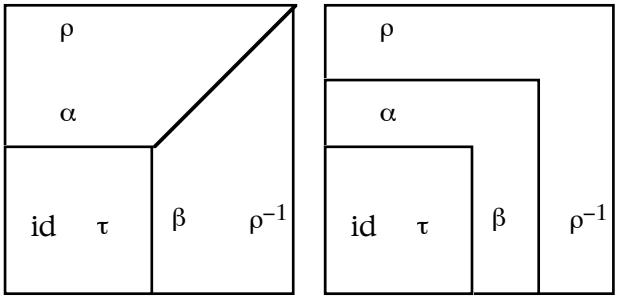
Ripetiamo ora con i laterali sinistri.

- Il primo di essi è naturalmente $H = id \circ H = \tau \circ H$.

- Sia $\alpha = (13)$. Allora $\alpha H = \{\alpha \circ id,\ \alpha \circ \tau\} = \{\alpha,\ \rho^{-1}\}$. Si osservi che $\alpha H \neq H\alpha$.

- Sia $\beta = (23)$. Allora $\beta H = \{\beta \circ id,\ \beta \circ \tau\} = \{\beta,\ \rho\}$. Si osservi che $\beta H \neq H\beta$.

Abbiamo così le due partizioni di G determinate da H e costituite rispettivamente dai tre laterali destri e dai tre laterali sinistri. Le due partizioni sono distinte.



Prendiamo ora il sottogruppo $K = \langle \rho \rangle = \{id,\ \rho,\ \rho^{-1}\}$, formato dalle tre potenze di $\rho = (132)$ e troviamo i suoi due laterali destri.

- Il primo è ovviamente $K = K \circ id = K\rho = K\rho^{-1}$.

- Sia $\alpha = (13)$. Allora $K\alpha = \{id \circ \alpha,\ \rho \circ \alpha,\ \rho^{-1} \circ \alpha\} = \{\alpha,\ \tau,\ \beta\}$ contiene le tre trasposizioni. Ma si ha anche $\alpha K = \{\alpha \circ id,\ \alpha \circ \rho,\ \alpha \circ \rho^{-1}\} = \{\alpha,\ \beta,\ \tau\} = K\alpha$.

Pertanto, in questo caso le due partizioni $\{K,\ K\alpha\}$ e $\{K,\ \alpha K\}$ coincidono.

Se per un sottogruppo K di un gruppo G e per ogni $x \in G$ si ha $Kx = xK$ allora K si dice sottogruppo *normale* di G. Per un gruppo abeliano tutti i sottogruppi sono normali. Per un gruppo non abeliano, invece, sono normali il sottogruppo banale $\{1_G\}$ e G stesso, ma per un sottogruppo proprio l'essere normale è una proprietà rara. Per indicare che K è un sottogruppo normale in G si scrive $K \triangleleft G$. Sui sottogruppi normali torneremo a fine capitolo.

2.5.B. - Sia $G = \left(\mathbf{Q}^*, \cdot\right)$, $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ e sia $H = \{1, -1\}$, che è un sottogruppo di G. Poiché G è abeliano, i laterali destri e sinistri di H coincidono. Troviamoli.

Per ogni $x \in \mathbf{Q}^*$ si ha $Hx = \{1 \cdot x, -1 \cdot x\} = \{x, -x\}$. Allora H ha infiniti laterali in G.

Sia $K = \mathbf{Q}^+ = \left\{x \in \mathbf{Q} \mid x > 0\right\}$. Anch'esso è un sottogruppo di G. Troviamo i suoi laterali. Naturalmente, $K \cdot 1 = K$. Un elemento non in K è -1, e si ha

$$K \cdot (-1) = \left\{x \cdot (-1) \mid x > 0\right\} = \left\{y \in \mathbf{Q}^* \mid y < 0\right\} = \mathbf{Q}^-$$

Dunque, $K = \mathbf{Q}^+$ ha due soli laterali in G, ossia $[G:K] = 2$.

Come detto, per indicare che H è un sottogruppo di G si scrive usualmente $H \leq G$. Si osservi che se H e K sono sottogruppi di G, con $H \subseteq K$, si ha anche $H \leq K$; inversamente, se $K \leq G$ e $H \leq K$, si ha $H \subseteq K$ e $H \leq G$.

LEMMA 2.6. Sia $(G, \cdot)$ un gruppo e sia Ω un insieme di sottogruppi. Allora $K = \bigcap_{H \in \Omega} H$ è un sottogruppo.

Dimostrazione. Siano $x_1, x_2 \in K$ e proviamo che $x_1 \cdot x_2 \in K$. Poiché $x_1, x_2 \in K$, allora essi appartengono ad ogni $H \in \Omega$ e quindi, essendo H un sottogruppo di G, si ha $x_1 \cdot x_2 \in H$. Ma allora $x_1 \cdot x_2 \in \bigcap_{H \in \Omega} H = K$.

Inoltre, $\forall H \in \Omega,\ x_1 \in H, \Rightarrow x_1^{-1} \in H \Rightarrow x_1^{-1} \in K$.

Infine, poiché ogni H è un sottogruppo, per ogni $H \in \Omega$ si ha $1_G \in H$, quindi $1_G \in K$. Pertanto, K è un sottogruppo di G.

Dal lemma precedente segue che l'insieme $\mathcal{L}(G)$ dei sottogruppi di un gruppo G è chiuso rispetto alla intersezione. Non è vero in generale per l'unione: nel gruppo $(\mathbf{Z}, +)$ consideriamo i due sottogruppi $2\mathbf{Z}$ e $3\mathbf{Z}$ costituiti dai numeri pari e dai multipli di 3: l'intersezione è l'insieme $6\mathbf{Z}$ dei multipli di 6 ed è un sottogruppo, mentre l'unione è $\{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \ldots\}$ che non è chiuso rispetto all'addizione.

Dato un sottoinsieme Y del gruppo G, consideriamo l'intersezione $\langle Y \rangle$ di tutti i sottogruppi di G che contengono Y, e lo chiamiamo *sottogruppo generato* da Y. Se in particolare si ha $\langle Y \rangle = G$, allora Y si chiama *insieme di generatori* di G

Dati ora due sottogruppi H e K di G, definiamo *sottogruppo unione* di H e K il sottogruppo $\langle H \cup K \rangle$ generato dall'unione insiemistica di H e K. Ne segue che $\mathcal{L}(G)$, ordinato rispetto alla inclusione, è un reticolo, in cui $\begin{cases} \inf\{H,K\} = H \cap K \\ \sup\{H,K\} = \langle H \cup K \rangle \end{cases}$, ed è *completo*, nel senso che ogni sottoinsieme non vuoto di $\mathcal{L}(G)$ possiede estremi superiore ed inferiore. In particolare, questo reticolo ha per massimo G e per minimo l'intersezione di tutti i suoi sottogruppi, ossia $\{1_G\}$. A partire quindi da ogni gruppo G è possibile costruire un reticolo, *il reticolo* $\mathcal{L}(G)$ *dei sottogruppi*. Esso non è in generale un sottoreticolo di $(\wp(G), \cup, \cap)$, poiché, come già detto, se H, K$\in \mathcal{L}(G)$, di solito si ha $H \cup K \neq \langle H \cup K \rangle$.

Vediamo ora la costruzione dei *gruppi alterni*, che sono importanti sottogruppi dei gruppi simmetrici. Chiamiamo *trasposizione* un ciclo di lunghezza 2. Abbiamo dapprima un lemma:

LEMMA 2.7. a) Ogni ciclo di lunghezza m > 2 è prodotto di m-1 trasposizioni.

b) Ogni permutazione è prodotto di trasposizioni.

Dimostrazione. a) Si ha $\gamma = (i_1 i_2 \dots i_m) = (i_1 i_m) \circ (i_1 i_{m-1}) \circ \cdots \circ (i_1 i_2)$

b) Si ha innanzi tutto $id = (12) \circ (12)$ e $(ij) = (ij) \circ (ij) \circ (ij)$. Sia $\alpha \neq id$ una permutazione che non sia una trasposizione. Si scomponga α in prodotto di cicli disgiunti: ciascun ciclo o è una trasposizione oppure è prodotto di trasposizioni, da cui l'asserto.

ESEMPIO 2.8.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 5 & 8 & 6 & 2 & 7 & 9 & 4 \end{pmatrix} = (2356) \circ (489) = (26) \circ (25) \circ (23) \circ (49) \circ (48)$$

Ma si ha anche $\alpha = (17) \circ (26) \circ (25) \circ (23) \circ (17) \circ (49) \circ (48)$, ossia il numero dei fattori non è univocamente determinato da α.

OSSERVAZIONE 2.9. Il lemma precedente dice che il gruppo simmetrico S_n, oltre ad essere generato dall'insieme dei cicli, lo è anche dall'insieme delle trasposizioni.

Sia $\alpha \in S_n$, che scomposto in cicli disgiunti dia $\alpha = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r$, con $r \geq 1$, $|\gamma_k| = m_k$, $1 \leq k \leq r$. Poniamo $N(\alpha) = \sum_{k=1}^{r}(m_k - 1) = \sum_{k=1}^{r} m_k - r$ = differenza tra il numero degli elementi spostati da α e il numero dei suoi cicli. Questo è anche il numero di trasposizioni che fattorizzano α mediante la tecnica del Lemma 2.7. Poniamo poi per completezza $N(id) = 0$.

Consideriamo ora $\alpha \in S_n$ nella forma consueta $\alpha = \begin{pmatrix} 1 & \dots & i & \dots & n \\ \alpha(1) & \dots & \alpha(i) & \dots & \alpha(n) \end{pmatrix}$. Chiamiamo *segno di* α il numero $\operatorname{sign}(\alpha) = \prod_{1 \leq i < j \leq n} \operatorname{sign}(\alpha(j) - \alpha(i)) \in \{-1, 1\}$. Poiché il segno di un prodotto è uguale al prodotto dei segni, si ha anche $\operatorname{sign}(\alpha) = \operatorname{sign}\left(\prod_{1 \leq i < j \leq n} (\alpha(j) - \alpha(i)) \right)$. Un fattore $(\alpha(j) - \alpha(i))$ è negativo se rispetto ad $i < j$ si ha $\alpha(i) > \alpha(j)$, ossia α ha prodotto nella seconda riga una "inversione" rispetto alla prima riga. Il prodotto $\prod_{1 \leq i < j \leq n} (\alpha(j) - \alpha(i))$ misura il numero di inversioni, ed il suo segno dice se questo numero è pari o dispari.

ESEMPI 2.10.

2.10.A. – L'identità non produce inversioni, quindi deve avere segno 1. Infatti:

$$\operatorname{sign}(id) = \prod_{1 \leq i < j \leq n} \operatorname{sign}\underbrace{(j - i)}_{>0} = \prod_{1 \leq i < j \leq n} 1 = 1.$$

2.10.B. – Sia $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (124)$. Allora $N(\alpha) = 2$. Calcoliamo il segno:

$$\operatorname{sign}(\alpha) = \operatorname{sign}((4-2)(3-2)(3-4)(1-2)(1-4)(1-3)) =$$
$$= \operatorname{sign}(2 \cdot 1 \cdot (-1) \cdot (-1) \cdot (-3) \cdot (-2)) = \operatorname{sign}(12) = +1$$

2.10.C. – Sia $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$. Allora $N(\beta) = 3$. Calcoliamo il segno:

$$\operatorname{sign}(\beta) = \operatorname{sign}((3-2)(4-2)(4-3)(1-2)(1-3)(1-4)) =$$
$$= \operatorname{sign}(1 \cdot 2 \cdot 1 \cdot (-1) \cdot (-2) \cdot (-3)) = \operatorname{sign}(-12) = -1.$$

Negli esempi precedenti $N(\alpha)$ è pari se e solo se $\text{sign}(\alpha) = 1$. Sarà un caso? Vediamo dapprima che cosa accade al segno se componiamo α con una trasposizione τ:

LEMMA 2.11. Sia $\alpha \in S_n$ e sia τ una trasposizione, allora $\text{sign}(\alpha \circ \tau) = -\text{sign}(\alpha)$.

Dimostrazione. Sia $\tau = (rs)$, con $r < s$. Confrontiamo il segno di $\alpha \circ \tau$ col segno di α. Si ha: $\text{sign}(\alpha \circ \tau) = \prod_{1 \le i < j \le n} \text{sign}(\alpha \circ \tau(j) - \alpha \circ \tau(i))$. Se $i \neq r$ e $j \neq s$ allora i e j sono fissati da τ, quindi $\text{sign}(\alpha \circ \tau(j) - \alpha \circ \tau(i)) = \text{sign}(\alpha(j) - \alpha(i))$.

Sia $i = r$. Se $j > s$, va tutto bene: $\text{sign}(\alpha \circ \tau(j) - \alpha \circ \tau(r)) = \text{sign}(\alpha(j) - \alpha(s))$, e questo fattore compare nell'espressione di $\text{sign}(\alpha)$. Se invece $r+1 \le j < s$, allora qui c'è il fattore $\text{sign}(\alpha \circ \tau(j) - \alpha \circ \tau(r)) = \text{sign}(\alpha(j) - \alpha(s))$, mentre nell'espressione di $\text{sign}(\alpha)$ c'è il fattore opposto $\text{sign}(\alpha(s) - \alpha(j))$. Abbiamo quindi s-r-1 inversioni, cioè segni opposti a quelli di $\text{sign}(\alpha)$.

Sia $j = s$. Ragionando come sopra, se $i < r$, non cambia nulla; se $r \le i < j$ abbiamo di nuovo s-r-1 inversioni, cioè segni opposti a quelli di $\text{sign}(\alpha)$.

Infine, se $j = s$ ed $i = r$ abbiamo un'inversione rispetto a $\text{sign}(\alpha)$.

Riassumendo, nel calcolo di $\text{sign}(\alpha \circ \tau)$ ci sono $(s-r-1)+(s-r-1)+1 = 2(s-r)-1$ inversioni di segno, un numero dispari, quindi $\text{sign}(\alpha \circ \tau) = -\text{sign}(\alpha)$.

LEMMA 2.12. Sia $\alpha \in S_n$.

a) Se α è prodotto di r trasposizioni, allora $\text{sign}(\alpha) = (-1)^r$

b) $\text{sign}(\alpha) = (-1)^{N(\alpha)}$.

c) Se α si scompone in due modi diversi come prodotto rispettivamente di r e di s trasposizioni, allora r ed s sono entrambi pari o entrambi dispari.

Dimostrazione. a) Sia $\alpha = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$. Allora $\alpha = \text{id} \circ \alpha = (((\text{id} \circ \tau_1) \circ \tau_2) \circ \ldots \circ \tau_r)$.

Per il lemma 2.11, da $\text{sign}(\text{id}) = 1$ segue:

$\text{sign}(\text{id} \circ \tau_1) = -1$, $\text{sign}((\text{id} \circ \tau_1) \circ \tau_2) = -1 \cdot (-1) = 1 = (-1)^2$, ... e per induzione su n si dimostra l'asserto.

b) Il numero $N(\alpha)$ è il numero di trasposizioni che fattorizzano α col metodo indicato nella sua definizione, perciò l'asserto segue da a).

c) Per a) si ha $(-1)^r = \text{sign}(\alpha) = (-1)^s$, quindi r ed s hanno la stessa parità.

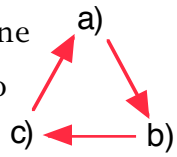
COROLLARIO 2.13. Sia $\alpha \in S_n$. Sono equivalenti:

a) $N(\alpha)$ è pari

b) $\text{sign}(\alpha) = 1$

c) α è prodotto di un numero pari di trasposizioni.

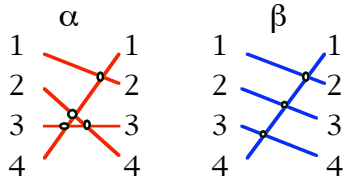
Dimostrazione. Si tratta di dimostrare che ciascuna affermazione implica le altre due. Per farlo si usa il *metodo del girotondo*, illustrato nella figura a lato.



Che a) implichi b) segue dal Lemma 2.12 b). Che b) implichi c) segue dal Lemma 2.12.a). Che c) implichi a) segue dallo stesso Lemma 2.12.a).

Una permutazione $\alpha \in S_n$ si dice *pari* se soddisfa una qualunque delle tre condizioni precedenti, *dispari* se non è pari.

ESEMPIO 2.14. La permutazione α dell'Esempio 2.10.b) è pari, essendo $N(\alpha) = 2$, mentre la permutazione β dell'Esempio 2.10.b) è dispari, essendo $N(\beta) = 3$. C'è anche un metodo grafico per stabilire la parità di una permutazione: si conta il numero delle intersezioni (purché si abbia l'avvertenza di non far passare più di due linee nello stesso incrocio). Nella figura abbiamo 4 incroci per α, che è pari, e 3 incroci per β, che è dispari.



Denotiamo con A_n l'insieme delle permutazioni pari di S_n. Si ha:

TEOREMA 2.12. a) A_n costituisce un sottogruppo di S_n,

b) $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$

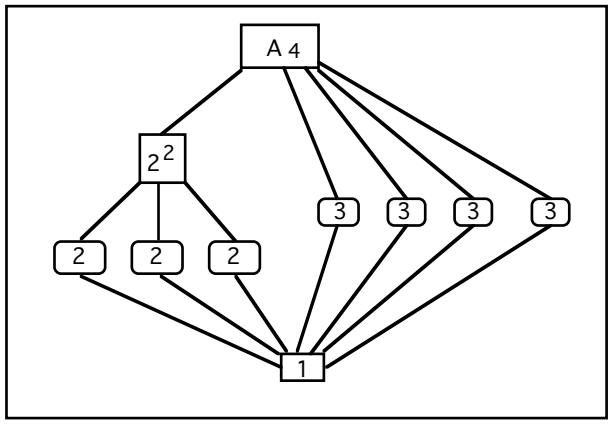
c) $A_n \triangleleft S_n$

Dimostrazione. a) L'identità è pari, quindi $\in A_n$. Date $\alpha,\beta \in A_n$, esistono trasposizioni τ_i, t_j, $1 \le i \le 2h$, $1 \le j \le 2k$, tali che $\begin{cases} \alpha = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2h} \\ \beta = t_1 \circ t_2 \circ \cdots \circ t_{2k} \end{cases}$. Allora, $\alpha \circ \beta = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2h} \circ t_1 \circ t_2 \circ \cdots \circ t_{2k}$ è prodotto di 2h+2k trasposizioni, quindi è pari. Infine, $\alpha^{-1} = \tau_{2h} \circ \tau_{2h-1} \circ \cdots \circ \tau_1$ è pari. Pertanto, $A_n \le S_n$.

b) Poniamo $\tau = (12)$, che è dispari. Allora ogni $\beta \in A_n \circ \tau$ è dispari perché prodotto di 2h+1 trasposizioni. Dunque ci sono almeno $|A_n \circ \tau| = |A_n|$ permutazioni dispari. D'altra parte, se β è una permutazione dispari, prodotto di 2k+1 trasposizioni, allora $\alpha = \beta \circ \tau$ è pari, perché prodotto di 2k+2 trasposizioni; pertanto $\beta = \alpha \circ \tau \in A_n \circ \tau$ e quindi le permutazioni dispari appartengono tutte al laterale $A_n \circ \tau$. Ne segue che tutti gli elementi fuori di A_n, ossia quelli di $S_n \setminus A_n$, costituiscono il laterale $A_n \circ \tau$. Ma allora $[S_n : A_n] = 2 \Rightarrow |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

c) Come sopra, anche il laterale sinistro $\tau \circ A_n$ è costituito da permutazioni dispari, quindi essendo equipotente ad A_n, le contiene tutte. Ma allora $\tau \circ A_n = A_n \circ \tau$. Il solo altro laterale di A_n è se stesso, dunque tutti i suoi (due) laterali destri coincidono con i corrispondenti laterali sinistri ed A_n è normale in S_n.

Nel caso di un gruppo finito, il reticolo dei sottogruppi si può rappresentare con un *diagramma di Hasse*. A titolo d'esempio, ecco il reticolo dei sottogruppi del gruppo alterno A_4. I numeri 1, 2, 3 denotano sottogruppi ciclici di quell'ordine, mentre 2^2 denota un gruppo non ciclico d'ordine 4. Le tre caselle con gli spigoli vivi denotano sottogruppi normali, nei quali ogni laterale destro coincide col corrispondente laterale sinistro. Si noti che non c'è un sottogruppo di ordine 6. Dimostriamolo. I 12 elementi di A_4 sono: l'identità; i tre doppi scambi $(12)(34)$, $(13)(24)$, $(14)(23)$, di periodo 2; otto cicli di lunghezza (e periodo) 3. I doppi scambi commutano a due a due, per cui due di essi generano un sottogruppo Q d'ordine 4, che contiene anche il terzo.



LEMMA 2.13. Sia G un gruppo d'ordine 6.

a) G possiede almeno un elemento di periodo 2.

b) Se G ha un solo elemento di periodo 2 allora G è ciclico.

Dimostrazione. a) Per il teorema di Lagrange, gli elementi di G hanno periodi 1, 2, 3 o 6. Se $x \in G$ ha periodo 3 o 6 allora anche x^{-1} ha lo stesso periodo, per cui gli elementi di periodo 3 e 6 sono in numero pari; 1_G ha periodo 1, quindi dei sei elementi di G ne abbiamo finora contato un numero dispari; dunque, ce ne deve essere uno di periodo 2, che coincide col suo inverso.

b) Sia u l'unico elemento di periodo 2. Per ogni $x \in G$ si ha $\left(x^{-1}ux\right)^{-1} = x^{-1}u^{-1}x = x^{-1}ux$, quindi $\left|x^{-1}ux\right| = 2$, da cui segue $x^{-1}ux = u$. Ciò significa che $xu = ux$. Ciò posto, se x ha periodo 6, G è ciclico. Se x ha periodo 3, allora essendo MCD(2,3) = 1, allora $\langle x\rangle \cap \langle u\rangle = \{1_G\}$ e quindi $|xu| = \mathrm{mcm}(|x|,|u|) = \mathrm{mcm}(3,2) = 6$ e G è ciclico.

Sia ora $G = A_4$, il gruppo alterno su quattro oggetti. Per assurdo esista un sottogruppo M d'ordine 6 di A_4. Innanzitutto, M non è ciclico perché, come visto, A_4 non ha elementi di periodo 6. Pertanto, per il Lemma precedente, M deve contenere almeno due elementi di periodo 2, quindi contiene il sottogruppo Q da essi generato. Ma si ha |Q| = 4, non divisore di 6 = |M|, assurdo. Pertanto, un tal M non esiste.

Il gruppo alterno A_4 è quindi un controesempio all'inverso del teorema di Lagrange.

Concludiamo il capitolo con una caratterizzazione dei sottogruppi normali. Ricordiamo che K è un sottogruppo normale in un gruppo G (ossia, in simboli, $K \triangleleft G$) se per ogni $x \in G$ si ha $Kx = xK$.

TEOREMA 2.14. Siano G un gruppo e K un suo sottogruppo. Si ha $K \triangleleft G$ se e solo se per ogni $x \in G$, per ogni $k \in K$, $x^{-1} \cdot k \cdot x \in K$.

Dimostrazione. Sia $K \triangleleft G$, allora $k \cdot x \in Kx = xK \Rightarrow \exists k' \in K \mid k \cdot x = x \cdot k'$. Ne segue: $x^{-1} \cdot k \cdot x = x^{-1} \cdot x \cdot k' = k' \in K$. Inversamente, $\forall x \in G$ e $\forall k \in K$ sia $x^{-1} \cdot k \cdot x \in K$. $\forall y \in Kx$ $\exists k \in K$ tale che $y = k \cdot x = x \cdot \underbrace{\left(x^{-1} \cdot k \cdot x\right)}_{\in K} \in xK$, quindi $Kx \subseteq xK$. Inversamente, $\forall z \in xK$ $\exists k \in K$ tale che $z = x \cdot k$. Poniamo $x' = x^{-1}$. Allora $z = x \cdot k = \underbrace{x'^{-1} \cdot k \cdot x'}_{\in K} \cdot x \in Kx$, dunque $xK \subseteq Kx$ e i due laterali sono uguali.

§3 – Omomorfismi, isomorfismi e congruenze

Riprendiamo le tavole dei due gruppi S_3 e D_3:

$\circ$	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	id	τ_3	τ_1	τ_2
ρ_2	ρ_2	id	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	id	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	id

$\circ$	id	r	r^2	s_1	s_2	s_3
id	id	r	r^2	s_1	s_2	s_3
r	r	ρ_2	id	s_3	s_1	s_2
r^2	r^2	id	r	s_2	s_3	s_1
τ_1	s_1	s_2	s_3	id	r	r^2
s_2	s_2	s_3	s_1	r^2	id	r
s_3	s_3	s_1	s_2	r	r^2	id

Appare evidente che se effettuiamo la seguente sostituzione:

id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	r	r^2	s_1	s_2	s_3

la prima tavola si muta nella seconda. I due gruppi differiscono perciò solo per i simboli usati per rappresentarne gli elementi. Diremo che i due gruppi sono *isomorfi*. La sostituzione che abbiamo effettuato è in realtà una biiezione f tra i due insiemi sostegno, tale che per ogni coppia di permutazioni α, β, posto $\gamma = \alpha \circ \beta$, $\alpha' = f(\alpha)$, $\beta' = f(\beta)$, $\gamma' = f(\gamma)$, si ha $\alpha' \circ \beta' = \gamma'$.

Un altro esempio:

$\cdot$	1	–1
1	1	–1
–1	–1	1

+	pari	dispari
pari	pari	dispari
dispari	dispari	pari

$\circ$	id	τ
id	id	τ
τ	τ	id

Il terzo è il gruppo simmetrico S_2. Anche in questo caso abbiamo tre tavole che si mutano l'una nell'altra semplicemente cambiando i simboli usati per descrivere gli elementi o l'operazione. Si tratta quindi di tre gruppi isomorfi.
Formalizziamo ora questa nozione:

Dati due gruppi $(G, \cdot)$ e $(H, *)$, si chiama *omomorfismo* una funzione $f : G \to H$ tale che per ogni coppia a, b di elementi di X sia $f(a \cdot b) = f(a) * f(b)$.

Terminologia:

a) Un omomorfismo iniettivo si chiama *monomorfismo.* In tal caso, H si dice *estensione* o *ampliamento* di G.

b) Un omomorfismo suriettivo si chiama *epimorfismo.* In tal caso, H si dice *immagine omomorfa* di G

c) Un omomorfismo biiettivo si chiama *isomorfismo*. In tal caso, anche l'inversa f^{-1} di f è un isomorfismo e i due gruppi differiscono solo per il nome degli oggetti ed i simboli usati per descriverli, ma sono essenzialmente coincidenti.

ESEMPI 3.1

3.1.A. - Un esempio di monomorfismo dal gruppo $(\mathbf{Z}, +)$ al gruppo $(\mathbf{Q}, +)$ è la funzione i che associa ad ogni $x\in\mathbf{Z}$ il numero razionale $\frac{x}{1}$ (i è l'iniziale di "immersione"). Poiché per ogni x, $\in\mathbf{Z}$ si ha $\frac{x}{1}+\frac{y}{1}=\frac{x+y}{1}$, allora $i(x+y)=i(x)+i(y)$. Inoltre, se si ha $i(x) = i(y)$ allora $\frac{x}{1}=\frac{y}{1}\Rightarrow x = y$ e quindi la funzione i è iniettiva. Pertanto, la funzione i è un monomorfismo.

3.1.B. - Un esempio di epimorfismo dal gruppo $\left(\mathbf{R}^*,\cdot\right)$ al gruppo $(\{1, -1\}, \cdot)$ è quello che associa ad ogni $x\in\mathbf{R}^*$ il suo segno: $\text{sign}:\mathbf{R}^*\to\{1,-1\}$, $\text{sign}(x)=\begin{cases}1 & \text{se } x>0\\ -1 & \text{se } x<0\end{cases}$. Il segno del prodotto è il prodotto dei segni: $\text{sign}(x\cdot y) = \text{sign}(x)\cdot\text{sign}(y)$, che è come dire che la funzione segno è un omomorfismo. La suriettività è ovvia: $1 = \text{sign}(1)$, $-1 = \text{sign}(-1)$. Pertanto, la funzione segno è un epimorfismo.

3.1.C. - Un esempio di isomorfismo tra i gruppi $\left(\mathbf{R},+\right)$ e $\left(\mathbf{R}^+,\cdot\right)$ è la funzione esponenziale $f_a(x) = a^x$, dove la base a è un numero reale positivo diverso da 1.

Dal corso di Analisi Matematica si sa che è definita per ogni $x\in\mathbf{R}$ ed i suoi valori sono tutti numeri positivi. Inoltre, è strettamente monotona (crescente se $a > 0$, decrescente se $0 < a < 1$), quindi è iniettiva, e la sua immagine è tutto $\mathbf{R}^+$. Dunque, è biiettiva. Infine, dalle proprietà delle potenze ad esponente reale segue che per ogni $x_1, x_2 \in \mathbf{R}$, $f_a(x_1 + x_2) = a^{x_1+x_2} = a^{x_1}\cdot a^{x_2} = f_a(x_1)\cdot f_a(x_2)$, quindi è anche un omomorfismo. La sua inversa, $\ln_a : \mathbf{R}^+ \to \mathbf{R}$, è a sua volta un isomorfismo.

3.1.D. – Gli omomorfismi tra un gruppo G e se stesso prendono il nome di *endomorfismi* di G. Vediamo il caso del gruppo (**Z**, +). Sia f un endomorfismo e poniamo m = f(1). Allora

$$f(2) = f(1+1) = f(1)+f(1) = m+m = 2m$$

Per induzione su $k > 0$ si ottiene $f(k) = km$. Inoltre,

$$f(0) = f(0+0) = f(0)+f(0) = 2f(0) \Rightarrow f(0) = 0.$$

Chi è f(-1)? Poiché -1+1 = 0, allora $0 = f(0) = f(-1+1) = f(-1)+f(1) = f(-1)+m$, quindi $f(-1) = -m$ e, più in generale, $f(-k) = -km$.

Pertanto, f è determinata da m ed ha per immagine l'insieme m**Z** dei multipli di m, che è un sottogruppo di **Z**. Inoltre, f è iniettiva, perché per ogni $h, k \in \mathbf{Z}$ si ha $f(h) = f(k) \Leftrightarrow hm = km \Leftrightarrow h = k$. Pertanto, ogni endomorfismo di **Z** è un monomorfismo. Per essere un isomorfismo deve essere suriettivo, e ciò avviene quando l'immagine m**Z** coincide con **Z** e ciò accade se e solo se $m = \pm 1$. Per m = 1 si ha f(k) = k per ogni k, ossia f è l'identità. Per m = -1 si ha f(k) = -k, ossia f è la funzione "opposto". Allora **Z** ha due automorfismi: l'identità id e l'opposto. Si osservi che essi formano un gruppo rispetto alla composizione.

3.1.E. – Più in generale, gli endomomorfismi di un gruppo $(G,\cdot)$ formano il monoide $(\mathrm{End}(G),\circ,\mathrm{id}_G)$. Gli isomorfismi tra il gruppo G e se stesso si chiamano *automorfismi*, e formano un gruppo denotato con Aut(G) e chiamato *automorfo* di G.

3.1.F. – Sia $G = H \times K$ il gruppo prodotto diretto dei due gruppi $(H,*)$ e $(K,\bullet)$. Siano $f: H \to G$ definita da $f : h \mapsto (h, 1_K)$, $g: K \to G$ definita da $g : k \mapsto (1_H, k)$.

Allora $\forall h_1, h_2 \in H$, $f(h_1 * h_2) = (h_1, 1_K)\cdot(h_2, 1_K) = f(h_1)\cdot f(h_2)$, quindi f è un omomorfismo. Inoltre, $f(h_1) = f(h_2) \Leftrightarrow (h_1, 1_K) = (h_2, 1_K) \Leftrightarrow h_1 = h_2$, quindi f è un monomorfismo. L'immagine di f è $\overline{H} = \{(h, 1_K) \in G \mid h \in H\}$ e non è difficile dimostrare che è un sottogruppo di G. Pertanto, f produce un isomorfismo da H ad $\overline{H}$. Analogamente, g è un monomorfismo da K a G, avente per immagine $\overline{K} = \{(1_H, k) \in G \mid k \in K\}$, che risulta essere un sottogruppo di G isomorfo a K.

Consideriamo ora l'applicazione $p_H : G \to H$, definita da $p_H : (h,k) \mapsto h$. Allora p_H è un epimorfismo da G su H. Analogamente, $p_K : G \to K$, $p_K : (h,k) \mapsto k$, è un epimorfismo da G su K. Le dimostrazioni sono lasciate per esercizio.

Per mostrare che due gruppi $(G, \cdot)$ e $(H, *)$ sono isomorfi **occorre esibire una funzione** $f:G\to H$ che abbia le proprietà richieste per essere un isomorfismo.
Per mostrare che i due gruppi non sono isomorfi **occorre dimostrare che non può esistere una funzione** $f:G\to H$ che abbia tutte le proprietà richieste.

Per esempio, se i due insiemi sostegno non sono equipotenti, allora non può esserci isomorfismo, perché ogni isomorfismo è innanzi tutto una biiezione. Se sono equipotenti, ma un gruppo ha una proprietà che l'altro non possiede, (per esempio, se uno dei due è abeliano e l'altro no), non può esservi isomorfismo. Entrambi i procedimenti possono essere assai difficili, se non impossibili. Vediamo alcuni esempi.

ESEMPI 3.2.

3.2.A. – I gruppi $(\mathbf{Z}, +)$ e $(\mathbf{Q}, +)$ non sono isomorfi, perché il primo è ciclico ed il secondo non lo è. Infatti, per ogni numero razionale $\frac{m}{n}$, preso un primo p che non divida n, la frazione $\frac{1}{p}$ non si può ottenere in nessun modo come un multiplo intero di $\frac{m}{n}$, quindi $\frac{m}{n}$ non genera $\mathbf{Q}$ perché $\frac{1}{p} \notin \left\langle \frac{m}{n} \right\rangle$.

3.2.B. – Il gruppo delle rotazioni di un esagono regolare è ciclico con 6 elementi, pertanto non è isomorfo al gruppo simmetrico S_3, che ha a sua volta 6 elementi, ma non è abeliano.

3.2.C. – I gruppi $(\mathbf{Q}, +)$ e $(\mathbf{R}, +)$ non sono isomorfi, poiché $\mathbf{Q}$ è numerabile, ossia è equipotente ad $\mathbf{N}$, mentre, per un teorema di Cantor, $\mathbf{R}$ non è numerabile.

3.2.D. – I gruppi $(D_6, \circ)$ ed $(A_4, \circ)$, entrambi di ordine 12, non sono isomorfi poiché il primo dei due ha un sottogruppo con 6 elementi, costituito dalle 6 rotazioni, mentre il secondo non ha sottogruppi con 6 elementi.

3.2.E. - I gruppi $(Q, +)$ e $(Q^+, \cdot)$ non sono isomorfi: infatti nel primo gruppo, per ogni $x\in Q$, $x \neq 0$, ed $n\in N$, $n > 0$, esiste sempre $y\in Q$ tale che $ny = x$. Invece $(Q^+, \cdot)$ non possiede questa proprietà, che tradotta in notazione moltiplicativa diviene:

per ogni $x\in Q^+$, $x \neq 1$, ed $n\in N$, $n > 0$, esiste $y\in Q^+$, tale che $y^n = x$.

Pertanto questi due gruppi, a differenza di $(R, +)$ ed $(R^+, \cdot)$, non sono isomorfi.

3.2.F. – Sia $(G,\cdot)$ un gruppo con due sottogruppi normali H, K tali che $\begin{cases} H \cap K = \{1_G\} \\ H \cdot K = G \end{cases}$. Allora G è isomorfo al prodotto diretto H×K. Per dimostrarlo ricordiamo che gli elementi di H×K sono le coppie (h,k). D'altra parte, l'ipotesi G = H·K significa che per ogni g∈G esistono h∈H, k∈K, tali che g = h·k. Allora consideriamo l'applicazione f:H×K→G, tale che f(h,k) = h·k. Per quanto appena detto, f è suriettiva. Dimostriamo che è iniettiva: siano $(h_1,k_1),(h_2,k_2) \in H \times K$ tali che $f(h_1,k_1) = f(h_2,k_2)$. Allora $h_1 \cdot k_1 = h_2 \cdot k_2 \Rightarrow \underbrace{h_2^{-1} \cdot h_1}_{\in H} = \underbrace{k_2 \cdot k_1^{-1}}_{\in K}$, e poiché $H \cap K = \{1_G\}$, allora $\begin{cases} h_2^{-1} \cdot h_1 = 1_G \\ k_2 \cdot k_1^{-1} = 1_G \end{cases} \Rightarrow \begin{cases} h_1 = h_2 \\ k_1 = k_2 \end{cases}$ ed f è iniettiva. Sarà un omomorfismo? Non è così semplice. Infatti,

$$\begin{cases} f((h_1,k_1)\cdot(h_2,k_2)) = f(h_1 \cdot h_2, k_1 \cdot k_2) = (h_1 \cdot h_2)\cdot(k_1 \cdot k_2) \\ f(h_1,k_1)\cdot f(h_2,k_2) = (h_1 \cdot k_1)\cdot(h_2 \cdot k_2) \end{cases},$$

quindi f è omomorfismo $\Leftrightarrow (h_1 \cdot h_2)\cdot(k_1 \cdot k_2) = (h_1 \cdot k_1)\cdot(h_2 \cdot k_2) \Leftrightarrow h_2 \cdot k_1 = k_1 \cdot h_2$, avendo semplificato i primi e gli ultimi fattori. Dunque, f è un omomorfismo se ogni elemento di H commuta con ogni elemento di K. Vediamo se è vero: siano h∈H, k∈K, allora per la Proposizione 1.2.a), esiste x∈G tale che $(h \cdot k) = (k \cdot h) \cdot x$. Ricordiamo che H e K sono sottogruppi normali di G. Allora, dal Teorema 2.14 segue:

$$x = (k \cdot h)^{-1} \cdot (h \cdot k) = \underbrace{h^{-1} \cdot \underbrace{k^{-1} \cdot h \cdot k}_{\in H}}_{\in H} = \underbrace{\underbrace{h^{-1} \cdot k^{-1} \cdot h}_{\in K} \cdot k}_{\in K},$$

quindi $x \in H \cap K = \{1_G\}$ e $h \cdot k = k \cdot h$. Ma allora, tornando ad f, poiché è vero che $h_2 \cdot k_1 = k_1 \cdot h_2$, oltre ad essere biiettiva f è anche un omomorfismo. Ne segue che $H \times K$ e G sono isomorfi.

Il gruppo G si dice *prodotto diretto interno* dei due sottogruppi normali H e K.

Una *rappresentazione fedele* di un gruppo "astratto" G è un monomorfismo da G ad un gruppo "concreto", nel quale cioè esiste un procedimento standard per eseguire l'operazione e trovare gli inversi. I gruppi "concreti" più usati sono i gruppi simmetrici ed i gruppi di applicazioni lineari invertibili di uno spazio vettoriale in sé. Queste ultime, come noto dal corso di Geometria, nel caso della dimensione finita n si rappresentano mediante matrici

a determinante non nullo, che costituiscono il *gruppo generale lineare* $\mathrm{GL}_n(K)$. Nel primo caso si parla di *rappresentazioni di permutazione*, nel secondo di *rappresentazioni lineari*. In effetti, ogni gruppo finito si può rappresentare fedelmente ed in molti modi come gruppo di permutazioni e come gruppo lineare. Il teorema seguente mostra un tipo di rappresentazione fedele di permutazione di un gruppo finito qualsiasi.

TEOREMA 3.3. (Cayley). Sia G un gruppo e sia S_G il gruppo simmetrico sull'insieme sostegno di G. Esiste un monomorfismo da G ad S_G.

Dimostrazione. Associamo ad ogni elemento a∈G la funzione $\tau_a : G \to G$, $\tau_a : x \mapsto a \cdot x$. Si prova subito che $\tau_a \in S_G$. Infatti, per ogni y∈G l'equazione a·x = y ha una ed una sola soluzione $x = a^{-1} \cdot y$, e ciò prova che τ_a è biiettiva. La funzione $\rho : G \to S_G$, $\rho : a \mapsto \tau_a$, è un monomorfismo di gruppi. Infatti, per ogni a, b∈G ed x∈G si ha:

$$\rho(ab)(x) = \tau_{ab}(x) = (ab)x = a(bx) = \tau_a(\tau_b(x)) = (\tau_a \circ \tau_b)(x) = (\rho(a) \circ \rho(b))(x)$$

da cui segue $\rho(ab) = \rho(a) \circ \rho(b)$. Inoltre, per ogni a, b, x∈G, se $\rho(a) = \rho(b)$ si ha:

$$\rho(a) = \rho(b) \Rightarrow \rho(a)(1_G) = \rho(b)(1_G) \Rightarrow a \cdot 1_G = b \cdot 1_G \Rightarrow a = b,$$

quindi ρ è iniettiva.

OSSERVAZIONE 3.4. Si può trasformare fedelmente ogni gruppo finito in un gruppo di permutazioni ed in un gruppo lineare di matrici su un campo qualsiasi. Sia $\alpha \in S_n$ e consideriamo la matrice identità I_n: trasformiamo tale matrice in una matrice T_α applicando alle colonne di I_n la permutazione α. Otteniamo così un insieme di n! matrici aventi in ogni riga e colonna un solo 1 ed n-1 zeri. Queste matrici formano, rispetto al prodotto righe per colonne, un gruppo isomorfo ad S_n, dove l'isomorfismo è la funzione che ad ogni $\alpha \in S_n$ associa la matrice T_α. In definitiva, combinando il teorema di Cayley e questa osservazione, si deduce che ogni gruppo finito con n elementi si rappresenta fedelmente come gruppo di matrici quadrate d'ordine n (su un campo qualsiasi). Talvolta però si può fare di meglio. Vediamo il caso del gruppo diedrale D_3, che ha 6 elementi. Il teorema di Cayley fornisce per G = D_3 una rappresentazione di permutazioni di grado 6, e di conseguenza, una rappresentazione lineare di grado 6 su un campo qualsiasi. Per esempio, detta r la rotazione di ampiezza 2π/3,

$$r \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix} \to \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Lo stesso per gli altri elementi di G.

Ogni isometria del piano è individuata dall'azione su tre punti non allineati, dunque ogni elemento di G si può identificare con una permutazione sui 3 vertici, contrassegnati coi numeri da 1 a 3. Per esempio: $r \to \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \to \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

Ed allora, come sappiamo, $D_3 \cong S_3$ si rappresenta come gruppo di permutazioni e di matrici, entrambi di grado 3.

Come gruppo di permutazioni non si può fare di meglio. Come gruppo lineare invece si può.

Nel piano cartesiano reale le isometrie si possono rappresentare algebricamente, e quelle che trasformano in sé l'origine sono applicazioni lineari. In tal modo, se collochiamo l'origine in O e l'asse y coincidente con l'asse s_3, G diviene un gruppo di matrici di ordine 2 sul campo reale, generato dalle due matrici $r \to \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$, $s_3 \to \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$.

Se in luogo di **R** scegliamo un altro campo K, non è detto si possa: occorre che esista in K una soluzione dell'equazione $4x^2 = 3$.

PROPOSIZIONE 3.5. (*proprietà elementari degli omomorfismi*). Siano $(G,\cdot)$, $(H,*)$ due gruppi e sia $f:G \to H$ un omomorfismo. Allora:

a) $f(1_G) = 1_H$

b) Per ogni $x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

Dimostrazione. a) L'uguaglianza $1_H * f(1_G) = f(1_G) = f(1_G \cdot 1_G) = f(1_G) * f(1_G)$ per la legge di cancellazione implica $f(1_G) = 1_H$.

b) $1_H = f(1_G) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$ implica che $f(x^{-1})$ è l'inverso di $f(x)$.

Data una struttura con una operazione binaria $(X, \cdot)$, una relazione d'equivalenza $\sim$ in X si dice *congruenza* rispetto a $\cdot$ se dati a, b, a', b'$\in$X, dall'essere $a \sim a'$, $b \sim b'$ segue $a \cdot b \sim a' \cdot b'$. Indichiamo con $[x]_\sim$ la classe di equivalenza di x, ossia $[x]_\sim = \{y \in X \mid y \sim x\}$ e consideriamo l'insieme quoziente $X/\sim$ costituito dalle classi di equivalenza. Definiamo tra le classi l'operazione seguente: per ogni a,b$\in$X, $[a]_\sim \cdot [b]_\sim = [a \cdot b]_\sim$.

Questa è una definizione corretta di una operazione, in quanto ogni coppia di classi ha un risultato ed un solo. Infatti se $[a]_\sim = [a']_\sim$ e $[b]_\sim = [b']_\sim$ allora $a \sim a'$, $b \sim b'$, quindi $a \cdot b \sim a' \cdot b'$ ed allora $[a \cdot b]_\sim = [a' \cdot b']_\sim$.

Otteniamo così una nuova struttura $(X/\sim, \cdot)$, detta *struttura quoziente* di X rispetto alla congruenza $\sim$. Che proprietà possiede?

LEMMA 3.6. Confrontiamo le strutture $(X, \cdot)$ e $(X/\sim, \cdot)$, dove $\sim$ è una congruenza in $(X, \cdot)$.

a) Se $(X, \cdot)$ possiede la proprietà associativa [commutativa] [di idempotenza] anche $(X/\sim, \cdot)$ la possiede.

b) Se $(X, \cdot)$ possiede l'elemento neutro 1_X anche $(X/\sim, \cdot)$ lo possiede: è $\left[1_X\right]_\sim$ [stesso discorso se $(X, \cdot)$ possiede l'elemento assorbente].

c) In tal caso, se in $(X, \cdot)$ un elemento x ha l'inverso x^{-1}, allora $\left(\left[x\right]_\sim\right)^{-1} = \left[x^{-1}\right]_\sim$.

d) La funzione $\pi : X \to X/\sim$ definita da $\pi(x) = [x]_\sim$ per ogni x$\in$X, è un epimorfismo tra $(X, \cdot)$ e $(X/\sim, \cdot)$.

Dimostrazione. a) Valga in X la proprietà associativa. Allora per ogni a, b, c$\in$X si ha: $\left(\left[a\right]_\sim \cdot \left[b\right]_\sim\right) \cdot \left[c\right]_\sim = \left[a \cdot b\right]_\sim \cdot \left[c\right]_\sim = \left[\left(a \cdot b\right) \cdot c\right]_\sim =$

$$= \left[a \cdot \left(b \cdot c\right)\right]_\sim = \left[a\right]_\sim \cdot \left[b \cdot c\right]_\sim = \left[a\right]_\sim \cdot \left(\left[b\right]_\sim \cdot \left[c\right]_\sim\right).$$

Le altre proprietà si dimostrano allo stesso modo.

COROLLARIO 3.7. Se $(G, \cdot)$ è un gruppo ed $\sim$ è una congruenza in G, anche $(G/\sim, \cdot)$ è un gruppo. Se $(G, \cdot)$ è abeliano, anche $(G/\sim, \cdot)$ lo è.

ESEMPIO 3.8. Ricordiamo la ben nota *congruenza mod m* in $\mathbf{Z}$. Nel gruppo $(\mathbf{Z},+)$ si fissi un numero m. Si definisca poi la seguente relazione: $x \equiv y \pmod m$ se $\exists q \in \mathbf{Z} \mid x - y = m \cdot q$, ossia x-y è multiplo di m. E' una relazione d'equivalenza:

a) $x \equiv x \pmod m$ perché $x-x = 0 = m\cdot 0$.

b) $x \equiv y \pmod m \Rightarrow \exists q \in \mathbf{Z} \mid x - y = m \cdot q \Rightarrow y - x = m \cdot (-q) \Rightarrow y \equiv x \pmod m$

c) $\begin{cases} x \equiv y \pmod m \\ y \equiv z \pmod m \end{cases} \Rightarrow \exists q, p \in \mathbf{Z} \mid \begin{cases} x - y = m \cdot q \\ y - z = m \cdot p \end{cases} \Rightarrow x - z = m \cdot (q + p) \Rightarrow x \equiv z \pmod m$

Denotiamo con $[x]_m$ la classe d'equivalenza di $x \in \mathbf{Z}$.

Osserviamo ora che la congruenza mod 0 è l'identità su $\mathbf{Z}$, in quanto $x \equiv y \pmod 0 \Leftrightarrow x - y = 0 \cdot q = 0 \Leftrightarrow x = y$. Pertanto, $[x]_0 = \{x\}$.

Sia $m \neq 0$. Allora si ha :

$$x \equiv y \pmod m \Leftrightarrow \exists q \in \mathbf{Z} \mid x - y = m \cdot q \Leftrightarrow x - y = (-m) \cdot (-q) \Leftrightarrow x \equiv y \pmod{(-m)}$$

Possiamo quindi supporre sempre $m > 0$.

La congruenza mod 1 è il prodotto cartesiano $\mathbf{Z}\times\mathbf{Z}$, dato che per ogni $x, y \in \mathbf{Z}$, x-y è multiplo di 1. I casi interessanti si hanno per $m \geq 2$.

Per ogni $x \in \mathbf{Z}$, la divisione per m dà $x = m\cdot q + r$, $0 \leq r < m$, dunque $x - r = m \cdot q \Rightarrow x \equiv r \pmod m$. D'altra parte, se $0 \leq r < s < m$, allora $0 < s-r < m$, quindi s-r non può essere multiplo di m. Perciò $r \not\equiv s \pmod m$. Allora le classi si possono rappresentare mediante i resti 0, 1, ..., m-1 delle divisioni per m. Si hanno quindi m classi $[0]_m, [1]_m, \ldots, [m-1]_m$, dette *classi di resti modulo m.*

La congruenza mod m è compatibile con +, infatti:

$$\begin{cases} x \equiv x' \pmod m \\ y \equiv y' \pmod m \end{cases} \Rightarrow \begin{cases} x - x' = m \cdot q \\ y - y' = m \cdot p \end{cases} \Rightarrow (x + y) - (x' + y') = m \cdot (q + p) \Rightarrow$$

$$\Rightarrow (x + y) \equiv (x' + y') \pmod m.$$

Nell'esempio precedente si ha che la classe $[0]_m$ è costituita dai multipli di m, ossia è il sottogruppo m**Z**. E' un caso? Che cosa accade in un gruppo qualsiasi?

TEOREMA 3.9. Data una congruenza $\sim$ in un gruppo G,

a) la classe K contenente l'elemento neutro 1_G è un sottogruppo normale di G, detto *nucleo della congruenza*.
b) La congruenza $\sim$ coincide con la relazione $\sim_K$ definita da: $x \sim_K y \Leftrightarrow x \cdot y^{-1} \in K$.

Dimostrazione. a) $K = [1_G]_\sim \Rightarrow 1_G \in K$. Inoltre,

$$\forall x, y \in K, \begin{cases} x \sim 1_G \\ y \sim 1_G \end{cases} \Rightarrow x \cdot y \sim 1_G \cdot 1_G = 1_G \Rightarrow x \cdot y \in K.$$

Infine, $\begin{cases} x^{-1} \sim x^{-1} \\ 1_G \sim x \end{cases} \Rightarrow x^{-1} \cdot 1_G \sim x^{-1} \cdot x \Rightarrow x^{-1} \sim 1_G \Rightarrow x^{-1} \in K$. Perciò K ≤ G.

Per ogni x∈G, per ogni $y \in [x]_\sim$ si ha:

$$\begin{cases} y \sim x \\ x^{-1} \sim x^{-1} \end{cases} \Rightarrow y \cdot x^{-1} \sim x \cdot x^{-1} = 1_G \Rightarrow y \cdot x^{-1} \in K \Rightarrow y \in Kx$$

quindi $[x]_\sim \subseteq Kx$. Inversamente, per ogni z∈Kx si ha $z \cdot x^{-1} \in K = [1_G]_\sim$, per cui:

$$\begin{cases} z \cdot x^{-1} \sim 1_G \\ x \sim x \end{cases} \Rightarrow (z \cdot x^{-1}) \cdot x \sim 1_G \cdot x \Rightarrow z \sim x \Rightarrow z \in [x]_\sim,$$

quindi $Kx \subseteq [x]_\sim$. Ne segue $Kx = [x]_\sim$. In modo simile si dimostra che $xK = [x]_\sim$, quindi xK = Kx e K è normale in G.

b) I laterali destri Kx sono le classi d'equivalenza sia della relazione ~ sia della relazione $\sim_K$, dunque le due relazioni coincidono.

Inversamente, per ogni sottogruppo $K \triangleleft G$ si può dimostrare che la relazione: $x \sim_K y \Leftrightarrow x \cdot y^{-1} \in K$ è una congruenza, di cui K è la classe contenente l'elemento neutro e, come sappiamo, per ogni x si ha $[x]_{\sim_K} = Kx$.

Pertanto, le congruenze nei gruppi sono completamente descritte dai sottogruppi normali. Il gruppo quoziente di G rispetto alla congruenza associata al sottogruppo normale K si denota con G/K.

Nel caso abeliano, tutti i sottogruppi sono normali, per cui si può determinare il gruppo quoziente rispetto ad ogni sottogruppo.

ESEMPI 3.10.

3.10.A. - Nel gruppo $(\mathbf{Z}, +)$ per la congruenza modulo m si ha $x \equiv y \pmod m$ se x-y è multiplo di m, ossia se $x-y \in m\mathbf{Z}$. L'insieme quoziente $\mathbf{Z}/m\mathbf{Z}$ è un gruppo rispetto all'addizione quoziente. Si osservi che si ha $-[x]_m = [m-x]_m$. Tale gruppo è spesso denotato con $(\mathbf{Z}_n, +)$, ed è ciclico, generato da $[1]_m$.

3.10.B. - Nel gruppo $(\mathbf{R},+)$ si consideri il sottogruppo ciclico $\langle 2\pi \rangle \leq (\mathbf{R}, +)$, generato da $2\pi = 6{,}28....$ Gli elementi del gruppo quoziente sono le classi $\alpha + \langle 2\pi \rangle$, $\alpha \in [0, 2\pi[$; in particolare, $[0] = [2\pi] = [4\pi] = ...$. In qualche testo è usato questo procedimento per definire gli angoli o le rotazioni, poiché l'operazione quoziente corrisponde alla somma di angoli o alla composizione di rotazioni con lo stesso centro.

Una struttura algebrica si dice *semplice* se le sole congruenze che possiede sono quelle banali, ossia l'identità, nella quale ogni elemento è in relazione solo con se stesso, ed il prodotto cartesiano, nel quale ogni elemento è in relazione con ogni altro. La determinazione delle strutture semplici è solitamente un problema assai complesso e di grande importanza.

Nel caso dei gruppi, come detto, le congruenze sono determinate dai sottogruppi normali. In particolare, l'identità è associata al sottogruppo $\{1_G\}$, mentre il prodotto cartesiano è associato a G. Pertanto, il gruppo G è semplice se e solo se i soli suoi sottogruppi normali sono $\{1_G\}$ e G. Un esempio è costituito dai gruppi d'ordine primo (i soli gruppi abeliani semplici) e dai gruppi alterni A_n, $n \geq 5$ (teorema di **E. Galois**). Nel caso dei gruppi finiti semplici, la classificazione è stata completata nel 1981 per opera di **M. Aschbacher**, che ha concluso così una ricerca iniziata nella prima metà dell'800 da Galois e che ha visto impegnati studiosi francesi, tedeschi, inglesi, giapponesi e statunitensi per circa 150 anni.

C'è una connessione tra omomorfismi e congruenze, come prova il seguente teorema, detto *teorema fondamentale d'omomorfismo,* che qui vediamo nella sua formulazione "universale" (nel senso che alla parola "gruppo" si può sostituire ovunque "struttura algebrica" ed il teorema resta vero):

TEOREMA 3.11. Siano $(G,\cdot)$ ed $(H,*)$ due gruppi ed f un omomorfismo tra di essi.

a) L'immagine Im f è un sottogruppo di H

b) La relazione $\sim_f$ in G così definita, per ogni $a, a' \in G$:

$$a \sim_f a' \text{ se } f(a) = f(a')$$

è una congruenza in G.

c) Detta $[x]_f$ la classe d'equivalenza di x, la funzione $\pi : G \to G/\sim_f$ tale che $\pi(x) = [x]_f$, è un epimorfismo.

d) Ponendo: $F([x]_f) = f(x)$, è ben definita la funzione F da $G/\sim_f$ ad H, la cui immagine coincide con quella di f e che risulta un monomorfismo.

e) Risulta: $f = F\circ\pi$, ed F è la sola funzione da $G/\sim_f$ ad H che ha questa proprietà.

f) Se f è un epimorfismo, F è un isomorfismo tra $G/\sim_f$ ed H.

Dimostrazione. a) Poiché $f(1_G) = 1_H$, allora $1_H \in \operatorname{Im} f$. Siano $y_1, y_2 \in \operatorname{Im} f$, allora esistono $x_1, x_2 \in G$ tali che $f(x_1) = y_1$, $f(x_2) = y_2$. Allora (si veda anche 3.5.b)):

$$y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \cdot x_2) \in \operatorname{Im} f,\ y_1^{-1} = (f(x_1))^{-1} = f\left(x_1^{-1}\right) \in \operatorname{Im} f,$$

quindi Im f è un sottogruppo di H.

b) Per ogni funzione f tra due insiemi la relazione $\sim_f$ è sempre una relazione d'equivalenza, come noto. Nel nostro caso mostriamo che è compatibile con l'operazione di G. Siano $a, a', b, b' \in G$ tali che $a \sim_f a'$, $b \sim_f b'$. Allora:

$$\begin{cases} f(a) = f(a') \\ f(b) = f(b') \end{cases} \Rightarrow f(a \cdot b) = f(a) * f(b) = f(a') * f(b') = f(a' \cdot b')$$

quindi $a \cdot b \sim_f a' \cdot b'$.

c) La funzione π è suriettiva. Proviamo che è un omomorfismo. Per ogni $x_1, x_2 \in G$ si ha $\pi(x_1 \cdot x_2) = [x_1 \cdot x_2]_f = [x_1]_f \cdot [x_2]_f = \pi(x_1) \cdot \pi(x_2)$.

d) Sia $[x]_f = [x']_f$, allora $x \sim_f x'$, quindi $f(x) = f(x')$. Ne segue $F([x]_f) = F([x']_f)$ ed F è una funzione. Inversamente, se $F([x]_f) = F([x']_f)$ allora $f(x) = f(x')$, quindi $x \sim_f x'$ e di conseguenza $[x]_f = [x']_f$, per cui F è iniettiva. Si ha infine:

$$F([x_1 \cdot x_2]_f) = f(x_1 \cdot x_2) = f(x_1) * f(x_2) = F([x_1]_f) * F([x_2]_f)$$

quindi F è anche un omomorfismo. Banalmente, essendo per ogni $x \in G$, $F([x]_f) = f(x)$, allora Im F = Im f.

e) Per ogni $x \in G$, $f(x) = F([x]_f) = F(\pi(x)) = F \circ \pi(x)$, quindi $f = F \circ \pi$. Sia ora $\Phi : G/\sim_f \to H$ tale che $f = \Phi \circ \pi$. Allora, per ogni $x \in G$ si ha

$$F([x]_\sim) = f(x) = \Phi \circ \pi(x) = \Phi([x]_\sim)$$

quindi $F = \Phi$.

f) Poiché $F: G/\sim_f \to H$ è un momomorfismo, allora è un isomorfismo se e solo se è suriettiva, ossia se e solo se Im F = Im f = H.

Una formulazione più "gruppale" del teorema fondamentale di omomorfismo si ottiene ricordando che la congruenza $\sim_f$ dà luogo in G ad un sottogruppo normale K = Ker f, detto *nucleo* di f, che costituisce la classe dell'elemento neutro. Più esplicitamente, si ha $\operatorname{Ker} f = \{x \in G \mid f(x) = 1_H\}$. Le altre classi sono i suoi laterali, così che il Teorema 3.11 si riformula in modo riassuntivo come segue, con una piccola aggiunta:

TEOREMA 3.12. Siano G ed H due gruppi e sia $f : G \to H$ un omomorfismo tra di essi. Sia poi K = Ker f il nucleo di f.

a) l'immagine Im f è un sottogruppo di H;

b) il nucleo K è un sottogruppo normale in G;

c) G/K è isomorfo ad Im f. (L'isomorfismo è definito da: $F : xK \mapsto f(x)$;

d) f è un monomorfismo se e solo se Ker f = $\{1_G\}$.

Dimostrazione. I primi tre punti sono solo riformulazioni del teorema fondamentale di omomorfismo. Per la d) si ha che se f è 1-1 allora certamente solo 1_G ha per corrispondente 1_H, quindi K = Ker f = $\{1_G\}$.

Viceversa, sia $K = \{1_G\}$, allora per ogni x, x'∈G si ha:

$$f(x) = f(x') \Rightarrow f(x' \cdot x^{-1}) = f(x') \cdot (f(x))^{-1} = 1_H \Rightarrow x' \cdot x^{-1} \in \operatorname{Ker} f = K = \{1_G\},$$

quindi x' = x ed f è iniettiva.

Il teorema precedente ha una conseguenza immediata:

TEOREMA 3.13. (Primo teorema d'isomorfismo). Siano G ed H due gruppi e sia $f:G \to H$ un epimorfismo. Allora $G/\mathrm{Ker}\, F = H$.

Dimostrazione. Segue immediatamente dal teorema fondamentale di omomorfismo.

ESEMPIO 3.14. Sia K un campo e sia $SL_n(K)$ l'insieme delle matrici quadrate di ordine n con determinante 1. Per il teorema di Binét, il determinante di un prodotto è il prodotto dei determinanti, per cui la funzione det è un omomorfismo dal gruppo $GL_n(K)$ al gruppo moltiplicativo K^* del campo K. Il suo nucleo è proprio $SL_n(K)$, che è pertanto un sottogruppo normale di $GL_n(K)$.

Poiché per ogni $k \in K^*$ si ha $\det\begin{pmatrix}\begin{bmatrix}1 & \dots & 0 & 0\\ \dots & \dots & \dots & \dots\\ 0 & \dots & 1 & 0\\ 0 & \dots & 0 & k\end{bmatrix}\end{pmatrix} = k$, allora l'immagine della funzione det è tutto K^*, per cui $GL_n(K)/SL_n(K)$ è isomorfo a K^*.

TEOREMA 3.15. (Teorema di struttura dei gruppi ciclici). Sia G un gruppo ciclico. Se è infinito, è isomorfo a $(\mathbf{Z}, +)$. Se è finito d'ordine n è isomorfo a $(\mathbf{Z}_n, +)$.

Dimostrazione. Sia a un generatore di G. Allora la funzione $f:\mathbf{Z}\to G$, $f : k \mapsto a^k$, è suriettiva, perché G è generato da a, ed è un omomorfismo per le proprietà delle potenze. Il suo nucleo è un sottogruppo di $\mathbf{Z}$, quindi è della forma $m\mathbf{Z}$, con $m \geq 0$. Se $m > 0$ il quoziente $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$ ha m elementi, quindi se G è infinito allora $m = 0$ e G è isomorfo a $\mathbf{Z}$. Se invece G è finito con n elementi, allora $m = n$ e G è isomorfo a $(\mathbf{Z}_n, +)$.

A partire dai gruppi ciclici additivi $\mathbf{Z}_m$, mediante prodotti diretti, si costruiscono nuovi gruppi finiti, ma sempre abeliani. In particolare, se m ed n non sono coprimi, allora $\mathbf{Z}_m \times \mathbf{Z}_n$ non è ciclico. Se invece sono coprimi, allora $\mathbf{Z}_m \times \mathbf{Z}_n$ è isomorfo a $\mathbf{Z}_{mn}$. Vediamo alcuni esempi.

ESEMPI 3.16.

3.16.A. – Nell'esempio 1.17.A abbiamo visto il gruppo $\mathbf{Z}_2\times\mathbf{Z}_2$: non è ciclico ed ha ordine 4. Quindi, oltre a $\mathbf{Z}_4$ c'è un altro gruppo abeliano d'ordine 4. Lo abbiamo anche incontrato come sottogruppo del gruppo alterno A_4.

3.16.B. – I gruppi $(\mathbf{Z}_2\times\mathbf{Z}_2)\times\mathbf{Z}_2$, $\mathbf{Z}_4\times\mathbf{Z}_2$, $\mathbf{Z}_8$ sono abeliani d'ordine 8, ma non sono isomorfi, perché il massimo dei periodi dei loro elementi è rispettivamente 2, 4, 8. Si può dimostrare che, a meno di isomorfismi, sono i soli gruppi abeliani di ordine 8. Il primo si ritrova come sottogruppo del gruppo simmetrico S_6, generato dalle tre trasposizioni disgiunte $(12),(34),(56)$. Anche il secondo si ritrova come sottogruppo di S_6, generato dai due cicli disgiunti $(1234),(56)$. Il terzo si ritrova in S_8, generato dal ciclo (12345678).

Di ordine 8 c'è anche il gruppo diedrale D_4, (il gruppo del quadrato), che si ritrova anche come sottogruppo di S_4. Ci sono altri gruppi di ordine 8? Sì, ce n'è un altro, il *gruppo* Q_8 *dei quaternioni*. Siano $A=\begin{bmatrix}0 & 1\\ 2 & 0\end{bmatrix}$, $B=\begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}$, ad elementi sul campo Z_3 = {0, 1, 2}. Hanno entrambe periodo 4; inoltre $A^2=B^2=\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}=2I_2$; infine, $B\times A=(A\times B)^3$, anch'essa di periodo 4. Posto C = $A\times B$, si ha $Q_8=\{I_2,\ A,\ B,\ A^2,\ C^3,\ A^3,\ C,\ B^3\}$; si può calcolarne la tavola di moltiplicazione e verificare che è un gruppo. Non è abeliano e non è isomorfo a D_4, perché Q_8 ha un solo elemento di periodo 2, mentre D_4 ne ha cinque.

3.16.C. – Sia G = $\mathbf{Z}_6\times\mathbf{Z}_{20}\times\mathbf{Z}_4$. Scomponiamo i primi due fattori: $\begin{cases}\mathbf{Z}_6=\mathbf{Z}_3\times\mathbf{Z}_2\\ \mathbf{Z}_{20}=\mathbf{Z}_5\times\mathbf{Z}_4\end{cases}$.

Ricomponiamo: $G=\mathbf{Z}_3\times\mathbf{Z}_2\times\mathbf{Z}_5\times\mathbf{Z}_4\times\mathbf{Z}_4=(\mathbf{Z}_5\times\mathbf{Z}_4\times\mathbf{Z}_3)\times\mathbf{Z}_4\times\mathbf{Z}_2=\mathbf{Z}_{60}\times\mathbf{Z}_4\times\mathbf{Z}_2$.

Alla fine, l'ordine di ciascun fattore è multiplo dell'ordine di chi lo segue. Questo è il modo canonico di riscrivere un prodotto diretto di gruppi ciclici finiti.