1

Capitolo T22
teoria dei gruppi

Contenuti delle sezioni

a. definizioni di gruppo p. 2
b. sottogruppi e omomorfismi tra gruppi p. 6
c. laterali, coniugio, automorfismi p. 12
d. sottogruppi normali, gruppi quoziente, prodotti di gruppi p. 15
e. esempi di gruppi [2] p. 17
f. teoremi di isomorfismo p. 21
g. azioni di un gruppo su un insieme p. 25
h. teoremi di Sylow p. 27
i. serie normali di un gruppo p. 31
j. gruppi liberi e presentazione dei gruppi p. 32

35 pagine

T22 0.01 Questo capitolo vuole raccogliere tutte le proprietà dei gruppi che si ritengono utili per l'*esposizione* e alcuni altri risultati che si giudicano necessari per un quadro più completo delle molteplici applicazioni delle teorie algebrichea nel suo complesso.

In queste pagine si riprendono argomentazioni e risultati sui gruppi già trovati in sviluppi precedenti [B20f, B32c06, B41b] in modo da avere un testo leggibile in modo più autonomo.
Tuttavia alcuni esempi toccati in precedenza sono solo oggetto di citazione.

T22 a. definizioni di gruppo

T22 a.01 Definiamo gruppo ogni struttura della forma $\boldsymbol{G} = \langle G, \odot, \mathcal{I}, e \rangle$ dove:

G è un insieme che chiamiamo terreno del gruppo $\boldsymbol{G}$;

$\odot$ un'operazione binaria del genere $\lceil G \times G \longmapsto G \rceil$ che gode della proprietà associativa, cioè tale che $\forall g, h, k \in G \ : \ (g \odot h) \odot k = g \odot (h \odot k))$;

e è un elemento di G tale che $\forall g \in G \ : \ e \odot g = g$;

$\mathcal{I}$ è una endofunzione di G tale che

$$\forall g \in G \ : \ g^{\mathcal{I}} \odot g = e \ \ \wedge \ \ g \odot g^{\mathcal{I}} = e \ . \tag{1}$$

Il cardinale del terreno G di un gruppo $\boldsymbol{G}$, cioè $|G|$, si usa prevalentemente chiamare **ordine del gruppo**.

Denotiamo con **Grp** la classe dei gruppi.

Ricordando le definizioni in T15b, abbiamo che $\langle G, \odot \rangle$ è un semigruppo e che $\langle G, \odot, e \rangle$ è un monoide.

T22 a.02 Ricaviamo le prime proprietà del generico gruppo $\boldsymbol{G} = \langle G, \odot, \mathcal{I}, e \rangle$.

All'elemento e è stato assegnato il ruolo di elemento neutro a sinistra del gruppo, ma esso in effetti svolge il ruolo più prestante di elemento neutro bilatero.

(1) Prop.: Se $u \in G$ tale che $u \odot u = u$, allora $u = e$;

Dim.: Consideriamo $u^{\mathcal{I}}$; si hanno le due uguaglianze $u^{\mathcal{I}} \odot (u \odot u) = u^{\mathcal{I}} \odot u = e$ e $(u^{\mathcal{I}} \odot u) \odot u = e \odot u = u$; dunque per l'associatività della operazione $\odot$ si ottiene $u = e$.

(2) Prop.: In ogni gruppo l'elemento neutro a sinistra è unico.

Se esistesse un'altro elemento neutro a sinistra e' sarebbe $e' \odot e' = e'$ e (1) implica $e' = e$. ∎

(3) Prop.: L'elemento e è l'unico elemento neutro bilatero per il gruppo e l'endofunzione $\mathcal{I}$ associa a ogni elemento del gruppo il suo unico inverso bilatero nel gruppo; in formula

$$\forall u \in G \ \ : \ \ u \odot e = u \qquad , \qquad (u^{\mathcal{I}}) \odot u = u \odot (u^{\mathcal{I}}) = e \ . \tag{4}$$

Dim.: Consideriamo un generico $g \in G$ ed $g^{\mathcal{I}}$: si ha quindi $g^{\mathcal{I}} \odot g = e$; inoltre accade che $(g \odot g^{\mathcal{I}}) \odot (g \odot g^{\mathcal{I}}) = g \odot (g^{\mathcal{I}} \odot g) \odot g^{\mathcal{I}} = g \odot (e \odot g^{\mathcal{I}}) = g \odot g^{\mathcal{I}}$. Grazie a (1) $g \odot g^{\mathcal{I}} = e$ e quindi $g^{\mathcal{I}}$ è inverso bilatero di g.

Si ha per ogni $g \in G$: $g \odot e = g \odot (g^{\mathcal{I}} \odot g) = (g \odot g^{\mathcal{I}}) \odot g = e \odot g = g$.

Inoltre se si trovasse g' tale che $g' \odot g = e$, sarebbe $g' = g' \odot e = g' \odot (g \odot g^{\mathcal{I}}) = (g' \odot g) \odot g^{\mathcal{I}} = e \odot g^{\mathcal{I}} = g^{\mathcal{I}}$

∎

T22 a.03 Le proprietà di unicità rendono lecito chiamare e **elemento neutro del gruppo** e $g^{\mathcal{I}}$ **elemento inverso nel gruppo**.

In genere l'operazione binaria di un gruppo viene chiamata prodotto e denotata con il segno "$\cdot$"; peraltro questo segno spesso per concisione viene trascurato. Quando si adotta questo modo di esprimersi "moltiplicativo" l'elemento neutro viene chiamato unità del gruppo e l'elemento inverso di $g \in G$ viene denotato con g^{-1}. Nel seguito seguiremo preferibilmente questo modo di scrivere.

Occorre tuttavia aggiungere che quando si tratta un gruppo abeliano, cioè un gruppo la cui operazione binaria gode della proprietà commutativa, in genere si preferisce adottare un modo di esprimersi "additivo": la legge di composizione viene chiamata somma e viene denotata con il segno "+", mentre

l'elemento inverso di g si denota con $-g$ e si dice elemento opposto di g e l'elemento neutro si chiama zero e si denota con 0.

T22 a.04 **(1) Prop.**: Il passaggio all'elemento inverso in un gruppo $\boldsymbol{G}$ è un'involuzione, ossia

$$\forall g \in G \ : \ (g^{-1})^{-1} = g \ .$$

Dim.: Per definizione $(g^{-1})^{-1} \cdot (g^{-1}) = e$, ma $g \cdot (g^{-1}) = e$ e l'unicità dell'inverso implica l'asserto ∎

Per ogni gruppo $\boldsymbol{G}$ vale la **legge di cancellazione** che segue.

(2) Prop.: $\forall g, h, k \in G \ : \ g \odot h = g \odot k \implies h = k \ \wedge \ h \odot g = k \odot g \implies h = k \ .$

Dim.: $g \odot h = g \odot k \implies g^{-1} \odot g \odot h = g^{-1} g \odot k \implies h = k \ .$
$h \odot g = k \odot g \implies h \odot g \odot g^{-1} = k \odot g \odot g^{-1} \implies h = k$ ∎

Ad ogni elemento h di un gruppo $\boldsymbol{G}$ sono associate le due funzioni chiamate **traslazione a sinistra** e **traslazione a destra** definite, risp., come segue

$$h^{\mathsf{trslL}} \ := \ \lceil\!\lceil \, g \in G \mapsto h \cdot g \, \rceil\!\rceil \qquad \text{e} \qquad h^{\mathsf{trslR}} \ := \ \lceil\!\lceil \, g \in G \mapsto g \cdot h \, \rceil\!\rceil \ . \tag{3}$$

(4) Prop.: Le traslazioni a sinistra e a destra sono permutazioni del terreno G.

Dim.: Ci proponiamo di dimostrare che h^{trslL} è una endofunzione entro G iniettiva e suriettiva.
Consideriamo $g_1, g_2 \in G$, $k_1 := h^{trslLt}(g_1) = h \cdot g_1$ e $k_2 := h^{trslLt}(g_2) = h \cdot g_2$; se $k_1 = k_2$, allora $h^{-1} \cdot (h \cdot g_1) = h^{-1} \cdot (h \cdot g_2)$, cioè $g_1 = g_2$. Abbiamo quindi che h^{trslL} è una endofunzione entro G iniettiva.
Per qualsiasi $k \in G$ si trova un $g \in G$ tale che $h^{trslL}(g) = k$: infatti basta assumere $g := h^{-1} \cdot k$.
Quindi h^{trslLt} è una endofunzione entro G suriettiva e di conseguenza è una biiezione.
Similmente si dimostra che h^{trslRt} è una biiezione ∎

Si osserva che le traslazioni a sinitra sono le costruzioni duali-LR delle traslazioni a destra.

Si definiscono le potenze intere di ciascuno degli elementi di un gruppo $\boldsymbol{G}$ ponendo, per ogni $g \in G$:

$$g^0 \ := \ e \quad , \quad g^1 \ := \ g \quad , \quad \forall n = 2, 3, ... : g^n \ := \ g^{n-1} \cdot g \quad , \quad \forall n \in \mathbb{P} \ : \ g^{-n} \ := \ (g^n)^{-1} \ . \tag{5}$$

(6) Prop.: $\forall g \in G \ , \ y, z \in \mathbb{Z} \ : \ g^{-z} \ = \ (g^z)^{-1} \quad , \quad g^{y+z} = g^y \cdot g^z = g^{y+z} \quad , \quad (g^y)^z = g^{y \cdot z}$ ∎

T22 a.05 Per la specie di struttura dei gruppi si possono dare varie altre definizioni.
Una definizione ridondante dalla quale spesso si trova conveniente partire è la seguente.

Si dice **gruppo** ogni struttura della forma $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e \rangle$ dove

(1) G è un insieme, che diciamo terreno del gruppo;
(2) $\odot$ è un'operazione binaria su G che gode della proprietà associativa: $\forall a, b, c \in R : a \odot (b \odot c) = (a \odot b) \odot c$;
(3) e è elemento neutro per l'operazione di prodotto, cioè $\forall a \in G \ : \ a \odot e = e \odot a = a$;
(4) ${}^{-1}$ è l'operazione unaria che a ogni $a \in G$ associa l'elemento che denotiamo con a^{-1} tale che $a \odot a^{-1} = a^{-1} \odot a = e$.

Altre definizioni fanno riferimento ad alcune specie di strutture facenti parte dei magmi come semigruppi, monoidi e quasigruppi [T15b, T15c].

In particolare si può definire gruppo un monoide avente tutti gli elementi invertibili, oppure un quasigruppo associativo.

T22 a.06 Vengono studiati proficuamente gruppi di svariati generi con ogni genere di terreno: rivestono importanza particolare i gruppi finiti, cioè gruppi con il terreno finito, vari gruppi numerabili aventi

come terreno insiemi come $\mathbb{Z}$, $\mathbb{Z}^d$, $\mathbb{Q}$ e $\mathbb{Z}^d$ (con $d = 2, 3, ...$), e vari gruppi con il terreno costituito da un insieme continuo.

Denoteremo con **GrpF** l'insieme dei gruppi finiti e più in particolare per ogni $n \in \mathbb{P}$ denoteremo con $\mathbf{Grp}_n$ l'insieme dei gruppi di ordine n.

Denoteremo inoltre con **GrpI** l'insieme dei gruppi infiniti e, se ν denota un qualsiasi numero transfinito denoteremo con $\mathbf{Grp}_\nu$ l'insieme dei gruppi il cui terreno ha cardinale ν.

Un'altra rilevante distinzione tra i gruppi riguarda gli abeliani o commutativi e i nonabeliani o non-commutativi. La struttura dei primi è tendenzialmente molto meno elaborata di quella dei nonabeliani e lo studio degli abeliani si serve di procedimenti specifici e raggiunge risultati piuttosto compatti.

Denoteremo con **GrpAb** l'insieme dei gruppi abeliani e con **GrpNab** l'insieme dei gruppi rimanenti.
Più avanti incontreremo tra i gruppi abeliani i gruppi ciclici e i gruppi numerici additivi moltiplicativi segnalati in b11.
È abeliano il gruppo delle rotazioni del piano $\mathbb{R} \times \mathbb{R}$ intorno a un suo punto, mentre è nonabeliano il gruppo delle rotazioni nello spazio $\mathbb{R}^{\times 3}$.

T22 a.07 In linea di principio ogni gruppo $\boldsymbol{G} = \langle G, \odot, ^{-1}, e \rangle$ può venire individuato dalla sua cosiddetta **tavola di Cayley** o **tavola di moltiplicazione**, cioè dalla funzione bivariata $\lceil\ \langle g, h \rangle \in G \times G \mapsto g \odot h\ \rceil$.
Ad un livello più pratico occorre distinguere il caso dei gruppi di ordine finito, per i quali la tavola di Cayley è una matrice finita, il caso dei gruppi numerabili per i quali la tavola costituisce una successione a due indici di un genere che potrebbe essere $\lceil \mathbb{N} \times \mathbb{N} \longmapsto \mathbb{N} \rceil$ o $\lceil \mathbb{Z} \times \mathbb{Z} \longmapsto \mathbb{Z} \rceil$, il caso dei gruppi di ordine continuo per i quali una tavola costituisce una funzione di due variabili di un genere che potrebbe essere $\lceil \mathbb{R} \times \mathbb{R} \longmapsto \mathbb{R} \rceil$, $\lceil [0,1] \times [0,1] \longmapsto [0,1] \rceil$, $\mathbb{R}^{\times d} \times \mathbb{R}^{\times d} \longmapsto \mathbb{R}^{\times d}$ e altro ancora.
Le tavole di Cayley sono indubbiamente utili per la comprensione dei gruppi finiti degli ordini più piccoli. In molti dei casi rimanenti le caratteristiche del gruppo non si riescono a ottenere agevolmente dalla tavola di Cayley e per determinare con buona effettività le suddette caratteristiche si devono individuare altri procedimenti.
Data la grande varietà dei gruppi effettivamente utilizzati nell'ambito della matematica e delle sue applicazioni, per lo sviluppo del loro studio, come è naturale aspettarsi, si devono adottare i più svariati metodi e procedimenti.

In ogni caso nella tavola di Cayley di un o specifico gruppo $\boldsymbol{G}$, grazie ad a04(4), si individuano righe e colonne (finite, numerabili, continue, ...) che forniscono permutazioni di G.

La tavola di moltiplicazione di un gruppo finito di ordine n è un quadrato latino di ordine n [D63].
Va osservato che vi sono quadrati latini di un ordine n che non esprimono la tavola di moltiplicazione di alcun gruppo di ordine n, in quanto esprimono una legge di composizione nonassociativa.

T22 a.08 Cominciamo a prendere in considerazione alcuni dei molti esempi di strutture costruite su nozioni consolidate dalle applicazioni che si avvalgono delle proprietà dimostrabili con procedimenti unitari e generali al livello dei gruppi astratti, basati solo sugli assunti formali.

Ricordiamo per primi i gruppi presentati in B41b : i gruppi delle permutazioni (b.01), i gruppi di 2 e 3 elementi e Sym_3 (b.03), il Viergruppe V_K o gruppo di Klein (b.04), il gruppo dell'esagono (b.07), il gruppo delle permutazioni circolari di un insieme di 5 elementi (b.08), i vari gruppi numerici additivi $\mathbb{Z}_{ag}$, $\mathbb{Q}_{ag}$, $\mathbb{R}_{ag}$ e $\mathbb{C}_{ag}$, i gruppi numerici moltiplicativi $\mathbb{Q}_{nz:mg}$, $\mathbb{R}_{mg}$ e $\mathbb{C}_{mg}$.

T22 a.09 Ricordiamo che per ogni insieme U si ha il corrispondente **gruppo simmetrico** costituito da tutte le permutazioni di tale insieme; esso viene denotato con Sym_U e si chiama anche **gruppo totale delle permutazioni** dell'insieme U.

Diciamo **gruppo di permutazioni** ogni struttura della forma $\langle G, \circ, {}^{-\mathbf{1}}, \mathsf{Id}_U \rangle$ con G sottoinsieme di $\mathbf{Perm}_U$, ossia della totalità delle permutazioni di un dato insieme U, sottoinsieme chiuso rispetto alla composizione di tali permutazioni e rispetto al passaggio alla permutazione inversa (e di conseguenza contenente Id_U).

Come vedremo sono di grande interesse molti altri gruppi formati da permutazioni che soddisfano vari tipi di vincoli. permutazioni.

L'insieme U può essere finito, infinito numerabile o infinito più che numerabile: a seconda dei casi i corrispondenti gruppi di permutazioni sono da trattare con tecniche e metodi diversi.

T22 a.10 Consideriamo un campo $\mathbb{F}$, un intero $d \in \{2, 3, 4, ...\}$, l'insieme delle matrici su $\mathbb{F}$ di profilo $d \times d$ e in particolare l'insieme delle matrici invertibili $\mathbf{MatInv}_{d;\mathbb{F}}$, matrici tutte aventi il determinante diverso da 0.

Si constata facilmente che questo insieme costituisce il terreno per un gruppo che viene chiamato **gruppo lineare generale** su $\mathbb{F}$ di d dimensioni, cioè:

$$\mathsf{GLFyRm\ Grp}_{d,\mathbb{F}} := \langle \mathbf{MatInv}_{d;\mathbb{F}}, \boldsymbol{+}, {}^{-1}, \mathbf{1}_d \rangle \ .$$

Ad un livello di maggiore astrazione si tratta il gruppo generale delle trasformazioni dello spazio vettoriale sopra il campo $\mathbb{F}$ a d dimensioni.

Anche tra i gruppi GLFyRm Grp è utile distinguere varie riduzioni costituite da insiemi di matrici invertibili che posseggono determinati requisiti. Per esempio incontreremo i gruppi delle matrici di dato ordine sopra un campo il cui determinante vale 1.
Questi insiemi di matrici costituiscono un sottogruppo di elementi di GLFyRm Grp.
Più in generale ogni insieme S di elementi di un gruppo con il ruolo di ambiente (come GLFyRm Grp) caratterizzati dal rispettare una qualche proprietà (come il valere 1 del determinante) costituisce un sottogruppo del gruppo ambiente: infatti il prodotto di due elementi di S sta in S, l'inverso di ogni elemento di S sta in S e l'elemento neutro dell'ambiente sta in S.

T22 b. sottogruppi e omomorfismi tra gruppi

T22 b.01 Un sottoinsieme nonvuoto di G $^{\searrow}$ S si dice (terreno di) **sottogruppo** di G sse $\forall g, h \in S \ : \ g\,h^{-1} \in S$.
In modo più sintetico si dice che $S \subseteq G$ è sottogruppo di G sse $S\,S^{-1} \subset S$.

Equivalentemente si può definire terreno di sottogruppo di G ogni $S \subseteq G$ nonvuoto tale che $\forall g \in G : g^{-1} \in S \ \wedge \ \forall g, h \in S : g\,h \in S$, ovvero tale che $S^{-1} \subseteq S \ \wedge \ S\,S \subseteq S$.

Due evidenti sottogruppi di ogni gruppo $\boldsymbol{G}$ sono $\{e\}$ e lo stesso $\boldsymbol{G}$; Un sottogruppo di $\boldsymbol{G}$ diverso da $\boldsymbol{G}$ si dice **sottogruppo proprio**.

(1) Prop.: Un terreno di sottogruppo S di un gruppo G è terreno di un gruppo.

Dim.: Sia s un arbitrario elemento di S; essendo S terreno di sottogruppo, a esso devono appartenere anche s^{-1} ed $e = s \odot s^{-1}$.
Muniamo S dell'operazione binaria $\odot|_{S\times S}$ ottenuta riducendo $\odot$ ad $S \times S$. Dato che $\forall g, h, k \in G : (gh)k = g(hk)$, ovviamente, si ha anche $\forall g, h, k \in S : (gh)k = g(hk)$. Quindi $\langle S, \odot|_{S\times S}, {}^{-1}|_{S\times S}, e\rangle$ soddisfa le richieste in a01 ed è un gruppo ∎

T22 b.02 Per affermare che $\boldsymbol{S}$ è sottogruppo di $\boldsymbol{G}$ scriviamo $\boldsymbol{S} \leq_{Grp} \boldsymbol{G}$; Per affermare che $\boldsymbol{S}$ è sottogruppo proprio di $\boldsymbol{G}$ scriviamo $\boldsymbol{S} <_{Grp} \boldsymbol{G}$.

In questo capitolo per le due precedenti relazioni useremo anche le notazioni più concise "$\leq_G$" e "$<_G$" . Inoltre denotiamo con $\boldsymbol{SbGrp}(G)$ l'insieme dei sottogruppi di G.

Facciamo riferimento a un gruppo $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e\rangle$ e adottiamo le semplificazioni consistenti nel sostituire $g \odot h$ con $g \cdot h$ o con $g\,h$ per ogni $g, h \in G$ e nel non distinguere $\boldsymbol{G}$ dal suo terreno G.

(1) Prop.: La relazione $\leq_{Grp}$ costituisce una relazione d'ordine. In altra forma $T \leq_{Grp} S \leq_{Grp} G \implies T \leq_{Grp} G$ ∎

T22 b.03 Accenniamo ad alcuni esempi di sottogruppi.

Il gruppo delle permutazioni degli interi 1, 2, ..., $n-1$ è sottogruppo del gruppo delle permutazioni degli interi 1, 2, ..., n.
Più in generale, consideriamo due insiemi S_1 e S_2; $S_1 \subset S_2 \implies \mathbf{Perm}_{S_1} \leq_{Grp} \mathbf{Perm}_{S_2}$.

Consideriamo le matrici di ordine d sopra un dato campo $\mathbb{F}$ e chiamiamole semplicemente matrici.
Il gruppo delle matrici aventi gli elementi della diagonale e solo essi diversi da 0 è sottogruppo del gruppo delle matrici triangolari superiori senza elementi nulli sulla diagonale principale e questo è sottogruppo del gruppo delle matrici invertibili.

Se m ed n sono interi maggiori o uguali a 2, il gruppo delle rotazioni del piano intorno all'origine per angoli multipli di $2\,\pi/n$ è sottogruppo del gruppo delle rotazioni del piano intorno all'origine per angoli multipli di $2\,\pi/(m\,n)$. Questo a sua volta è sottogruppo del gruppo di tutte le rotazioni del piano intorno all'origine.

Osserviamo che per affermare che un S è sottogruppo di un gruppo G non basta che S costituisca un gruppo e sia contenuto in G: si richiede anche che l'operazione binaria per S sia la restrizione di quella per G.
Per esempio il gruppo moltiplicativo dei numeri razionali positivi non è un sottogruppo del gruppo additivo dei numeri reali.

T22 b.04
Insieme al gruppo $\boldsymbol{G}=\langle G,\odot,^{-1},e\rangle$ consideriamo il gruppo $\boldsymbol{H}=\langle H,*,\mathcal{J},e_H\rangle$.
Una funzione $\omega\in\lceil G\longrightarrow H\rceil$ si dice **omomorfismo** dal gruppo $\boldsymbol{G}$ nel gruppo $\boldsymbol{H}$ sse

$$\forall g_1,g_2\in\mathsf{dom}(\omega)\ :\ \omega(g_1\odot g_2)\ =\ \omega(g_1)*\omega(g_2)\ . \tag{1}$$

L'insieme degli omomorfismi di gruppo da $\boldsymbol{G}$ in $\boldsymbol{H}$ verrà denotato con $\lceil \boldsymbol{G}\longrightarrow_{Grp}\boldsymbol{H}\rceil$ e quindi per affermare che ω è omomorfismo da $\boldsymbol{G}$ in $\boldsymbol{H}$ scriviamo $\omega\in\lceil \boldsymbol{G}\longrightarrow_{Grp}\boldsymbol{H}\rceil$.

Si osserva che la definizione precedente suppone che sia $\mathsf{dom}(\omega)\leq_{Grp}G$ e $\mathrm{img}(\omega)\leq_{Grp}H$.

In effetti interessano in particolare i casi in cui $\mathsf{dom}(\omega)=G$ ed $\mathrm{img}(\omega)=H$.

Un omomorfismo $\omega\in\lceil G\longrightarrow_{Grp}H\rceil$:
se $\mathsf{dom}(\omega)=G$ si dice omomorfismo di gruppo di G in H;
se $\mathrm{img}(\omega)=H$ si dice **epimorfismo di gruppo** di G in H;
se $\mathsf{dom}(\omega)=G$ e $\mathrm{img}(\omega)=H$ si dice epimorfismo di gruppo di G su H.

Denotiamo gli insiemi di questi omomorfismi, risp., con $\lceil G\longmapsto_{Grp}H\rceil$, con $\lceil G\longrightarrow\!\triangleright_{Grp}H\rceil$ e con $\lceil G\longmapsto\!\triangleright_{Grp}H\rceil$.

T22 b.05 Tra gli omomorfismo tra gruppi hanno particolare interesse quelli biiettivi, cioè quelli costituiti da funzioni invertibili.

Una funzione $\omega\in\lceil G\longleftrightarrow H\rceil$ si dice **isomorfismo** dal gruppo G nel gruppo H oppure **monomorfismo di gruppo** da G in H sse è biunivoca ed è un omomorfismo da G in H.

L'insieme degli isomorfismi di gruppo da G in H, chiamato anche insieme dei **monomorfismi di gruppo**, verrà denotato con $\lceil G\longleftrightarrow_{Grp}H\rceil$.
Quindi per affermare che ω è un isomorfismo da G in H scriviamo $\omega\in\lceil G\longleftrightarrow_{Grp}H\rceil$.

In particolare l'isomorfismo ω:
se $\mathsf{dom}(\omega)=G$ si dice isomorfismo di gruppo di G in H;
se $\mathrm{img}(\omega)=H$ si dice **isomorfismo di gruppo** di G su H;
se $\mathsf{dom}(\omega)=G$ e $\mathrm{img}(\omega)=H$ si dice **isomorfismo tra gruppi**, G e H.

Denotiamo gli insiemi di questi isomorfismi, risp., con $\lceil G\triangleleft\!\longrightarrow_{Grp}H\rceil$, con $\lceil G\longleftarrow\!\triangleright_{Grp}H\rceil$ e con $\lceil G\triangleleft\!\longrightarrow\!\triangleright_{Grp}H\rceil$.

Complessivamente i vari tipi di omomorfismi (epimorfismi, isomorfismi) di gruppo sono chiamati **morfismi di gruppo**.

In questo capitolo adotteremo anche la semplificazione secondo la quale parleremo di morfismi invece che di morfismi di gruppo.
Spesso potremo anche semplificare le notazioni sostituendo un enunciato come $\exists\omega\in\lceil G\longleftrightarrow_{Grp}H\rceil$ con il più conciso $G\longleftrightarrow_{Grp}H$.
Inoltre in opportuni contesti una scrittura come $G\triangleleft\!\longrightarrow\!\triangleright_{Grp}H$ si può abbreviare con la più generica $G\cong H$.

T22 b.06 La individuazione di un omomorfismo come $\omega\in\lceil G\longleftrightarrow H\rceil$ e più in particolare l'individuazione di un isomorfismo può essere di grande utilità.
Infatti dalla conoscenza di determinate caratteristiche di un gruppo di partenza G ci si aspetta di ottenere informazioni sulle caratteristiche di un gruppo poco noto H con un lavoro più contenuto di quello richiesto da un esame sopra il solo H.
Si parla per questo metodo di indagine di **trasporto di strutture**.

Bisogna poi tenere presenti i vantaggi provenienti dalla determinazione di omomorfismi tra gruppi (come per ogni altra specie di strutture) per la conoscenza complessiva della teoria di gruppi, ovvero della conoscenza della rete costituita dalle strutture gruppo e dalle relazioni che li riguardano.
Gli omomorfismi e le altre relazioni a esse connesse che vedremo più avanti saranno applicati a molte altre importanti specie di strutture algebriche (e non solo) e consentono di giungere a enunciati di vasta portata.

Si dimostra facilmente che l'isomorfismo tra gruppi è una relazione di equivalenza. In effetti questo vale per ogni genere di struttura.

La individuazione di isomorfismi tra strutture di una qualsiasi specie, ed in particolare tra gruppi, porta sempre a vantaggi di rilievo.
Due gruppi per i quali si possa scrivere una relazione come $G \cong H$ si possono considerare "essenzialmente identici".
Una classe di isomorfismo di gruppi si può identificare con un cosiddetto **gruppo astratto**, entità alla quale risulta conveniente fare riferimento per gestire le proprietà rinvenibili in tutti i gruppi della classe.

T22 b.07 Le proprietà che seguono riguardano i gruppi $\boldsymbol{G}$, $\boldsymbol{G'}$, $\boldsymbol{H}$, $\boldsymbol{H'}$ e $\boldsymbol{K}$; esse si possono dimostrare facilmente.

(1) Prop.: $\boldsymbol{G} \longrightarrow_{Grp} \boldsymbol{H}\ ,\ \boldsymbol{G'} \lhd\!\!\longrightarrow\!\!\rhd_{Grp} \boldsymbol{G}\ ,\ \boldsymbol{H'} \lhd\!\!\longrightarrow\!\!\rhd_{Grp} \boldsymbol{H} \implies \boldsymbol{G'} \longrightarrow_{Grp} \boldsymbol{H'}$ ∎

(2) Prop.: $\omega \in \lceil\, \boldsymbol{G} \longrightarrow_{Grp} \boldsymbol{H} \,\rceil\ ,\ \zeta \in \lceil\, \boldsymbol{H} \longrightarrow_{Grp} \boldsymbol{K} \,\rceil \implies \omega \circ_{lr} \zeta \in \lceil\, \boldsymbol{G} \longrightarrow_{Grp} \boldsymbol{K} \,\rceil$ ∎

(3) Prop.: $\omega \in \lceil\, \boldsymbol{G} \lhd\!\!\longrightarrow_{Grp} \boldsymbol{H} \,\rceil\ ,\ \zeta \in \lceil\, \boldsymbol{H} \lhd\!\!\longrightarrow_{Grp} \boldsymbol{K} \,\rceil \implies \omega \circ_{lr} \zeta \in \lceil\, \boldsymbol{G} \lhd\!\!\longrightarrow_{Grp} \boldsymbol{K} \,\rceil$ ∎

(4) Prop.: $\omega \in \lceil\, \boldsymbol{G} \longrightarrow_{Grp} \boldsymbol{H} \,\rceil\ ,\ \zeta \in \lceil\, \boldsymbol{H} \longrightarrow_{Grp} \boldsymbol{K} \,\rceil \implies \omega \circ_{lr} \zeta \in \lceil\, \boldsymbol{G} \longrightarrow_{Grp} \boldsymbol{K} \,\rceil$ ∎

(5) Prop.: $\omega \in \lceil\, \boldsymbol{G} \lhd\!\!\longrightarrow\!\!\rhd_{Grp} \boldsymbol{H} \,\rceil\ ,\ \zeta \in \lceil\, \boldsymbol{H} \lhd\!\!\longrightarrow\!\!\rhd_{Grp} \boldsymbol{K} \,\rceil \implies \omega \circ_{lr} \zeta \in \lceil\, \boldsymbol{G} \lhd\!\!\longrightarrow\!\!\rhd_{Grp} \boldsymbol{K} \,\rceil$ ∎

T22 b.08 Riprendiamo le considerazioni sulla relazione tra un gruppo e un suo sottogruppo.

(1) Prop.: Dato un sottogruppo S di un gruppo G, l'inclusione Id_S considerata come funzione di $\lceil\, S \lhd\!\!\longrightarrow G \,\rceil$ è un omomorfismo di gruppi.

Dim.: Per l'inclusione, evidentemente, $\forall s \in S : \mathsf{Id}_S(s)$.
Dunque $\forall s,t \in S : \mathsf{Id}_S(s \cdot t) = s \cdot t = \mathsf{Id}_S(s) \cdot \mathsf{Id}_S(t)$ ∎

(2) Prop.: Consideriamo i gruppi $\langle S, *, \mathcal{J}, e_S \rangle$ e $\langle G, \odot, {}^{-1}, e_G \rangle$. Se $S \subseteq G$ e se l'inclusione $\mathsf{Id}_S \in \lceil\, S \lhd\!\!\longrightarrow G \,\rceil$ è un omomorfismo, allora $S \leq_{Grp} G$.

Dim.: Per le proprietà degli omomorfismi deve essere $e_S = e_G$ e $\forall s,t \in S : \mathsf{Id}_S(s*t) = \mathsf{Id}_S(s) \odot \mathsf{Id}_S(t)$, ossia $s * t = s \odot t$. Di conseguenza $\forall s,t \in S : s * t \in S$.
Inoltre $\mathsf{Id}_S(s^{\mathcal{J}}) = \mathsf{Id}_S(s)^{-1}$, cioè l'inversione in S è la restrizione a S dell'inversione in G: quindi $\forall s \in S : s^{-1} \in S$. In conclusione $S \leq_{Grp} G$ ∎

(3) Prop.: Sia S un sottoinsieme nonvuoto di un gruppo $\langle G, \odot, {}^{-1}, e_G \rangle$; $S <_{Grp} G \iff \forall s,t \in S : g \odot h^{-1} \in S$.

Dim.: "$\Longrightarrow$" Segue dalla semplice definizione di sottogruppo.

"$\Longleftarrow$" Sia s un qualsiasi elemento di S; $s \cdot s^{-1} = e \in S$. Per ogni $h \in S$ si ha $e \cdot h^{-1} = h^{-1} \in S$.

Siano g ed h elementi di S: $g \cdot (h^{-1})^{-1} = g \cdot h \in S$. In conclusione $S <_{Grp} G$ ∎

T22 b.09 Consideriamo i gruppi $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e_G \rangle$/" e $\boldsymbol{H} = \langle H, *, \mathcal{J}, e_H \rangle$ e un omomorfismo $\omega \in \lceil\, G \longmapsto_{Grp} H \,\rceil$.

Si dice **nucleo di omomorfismo** o **kernel di omomorfismo**, ω, il sottoinsieme di G

$$\boldsymbol{ker}(\omega) \ := \ \{k \in G \,\P\, \omega(k) = e_H\} = \omega^{-1}(e_H) \ . \tag{1}$$

(2) Prop.: $\boldsymbol{ker}(\omega) \in \boldsymbol{SbGrp}(G)$

Dim.: Dato che $\omega(e_G) = e_H$, $e_H \in \boldsymbol{ker}(\omega)$; $\omega(k) = e_H$ implica $\omega(k^{-1}) = {e_H}^{\mathcal{J}} = e_H$, cioè $k^{-1} \in \boldsymbol{ker}(\omega)$; inoltre $\omega(k) = \omega(k') = e_H$ implica $\omega(k * k') = e_H$, cioè $k \odot k' \in \boldsymbol{ker}(\omega)$ ∎

(3) Prop.: $\mathrm{img}(\omega) \in \boldsymbol{SbGrp}(H)$.

Dim.: $\forall g, g' \in G : \ g \cdot {g'}^{-1} \in G$ implica $\omega(g \cdot {g'}^{-1}) = \omega(g) \odot \mathcal{J}(\omega(g')) \in \mathrm{img}(\omega$ e quindi l'asserto ∎

T22 b.10 Consideriamo l'insieme delle potenze positive e negative di un elemento a di un gruppo $\boldsymbol{G}$,

$$P \ := \ \{z \in \mathbb{Z} :| \ a^z\} \ . \tag{1}$$

Esso costituisce un sottogruppo di $\boldsymbol{G}$. Infatti per due elementi generici di questo sottoinsieme P $g := a^q$ ed $h := a^r$ si ottiene $g \cdot h^{-1} = a^{q-r}$, cioè un altro elemento di P.

Questo sottogruppo delle potenze di a viene chiamato **sottogruppo ciclico generato da** a . Esso si identifica con la notazione $\langle a \rangle_G$ o con la sua abbreviazione $\langle a \rangle$ giustificabile dove si trattano solo gruppi.

Se il gruppo $\boldsymbol{G}$ è infinito si possono avere elementi con un numero finito di potenze diverse ed elementi b con infinite potenze diverse, della forma b^z con $z \in \mathbb{Z}$.
Se $\boldsymbol{G}$ è finito le potenze positive di a diverse sono ovviamente in numero finito.
A ogni sottogruppo ciclico finito $\langle a \rangle$ si può dare la forma semplificata $\langle a \rangle = \{e, a, a^2, ..., a^{p-1}\}$ con $p := |\langle a \rangle|$.
L'intero positivo p è detto **periodo dell'elemento di gruppo** a e viene denotato con $\mathrm{prd}(a)$.
Si osserva che le potenze a^i per $i = 0, 1, 2, ..., p-1$ e comprendono anche le potenze negative dell'elemento generatore, ossia i rispettivi inversi: in effetti ${a^i}^{-1} - = a^{p-i}$, in quanto $a^i \cdot a^{p-i} = e$.

T22 b.11 Consideriamo il caso di un elemento a con un numero finito di potenze positive diverse. Scorrendole si incontra un intero naturale p, il più piccolo, per il quale $a^p = e$; da questa segue che $a^{-1} = a^{p-1}$; non serve quindi considerare separatamente le potenze negative di a.
Si osserva anche che per ogni numero intero positivo m si può scrivere $mb = qp + r$ con $r \in [p)$ e $q \in \mathbb{Z}$; di conseguenza $a^m = a^r$.

Si dice **periodo** dell'elemento a del gruppo G e si denota $\mathrm{prd}(a)$ il minimo intero positivo p, se esiste, per il quale $a^p = e$, mentre in caso contrario si pone $\mathrm{prd}(a) := +\infty$.

Ogni gruppo esprimibile nella forma $\langle {}_{Grp}a \rangle$ si dice **gruppo ciclico**. Evidentemente ogni gruppo ciclico è abeliano.

Sono ben distinti i gruppi ciclici finiti della forma $\{a, a^2, a^3, ..., a^{\mathrm{prd}(a)} = e\}$ generati da elementi di periodo finito coincidente con l'ordine del gruppo, e gruppi ciclici infiniti come $\mathbb{Z}_{ag}$, struttura che si può considerare individuata dall'espressione che è la versione additiva della (1) $\{z \in \mathbb{Z} :| \ 1 \cdot z\}$.

In ogni gruppo l'unità è l'unico elemento di periodo 1.
Gli elementi di periodo 2 di un gruppo, cioè gli elementi a caratterizzati dall'equazione $a^2 = e$, sono tutti e soli gli elementi che coincidono con il proprio inverso: infatti $a^2 = e$ sse $a = a^{-1}$. Essi sono chiamati **involuzioni nel gruppo**.

La scelta del termine involuzione, nel caso di un gruppo di permutazioni è coerente con il termine usato per le particolari permutazioni di un generico insieme ambiente che applicate due volte danno l'identità, o, equivalentemente, con le permutazioni coincidenti con la propria inversa.

T22 b.12 Accanto ai gruppi ciclici generati da un unico generatore, per ogni sottoinsieme S di un qualsiasi gruppo G si può considerare l'insieme di tutti gli elementi di G ottenibili come prodotto di un numero finito di elementi di S e dei loro elementi inversi. Tale insieme contiene l'unità ed è chiuso rispetto al passaggio all'elemento inverso e rispetto al prodotto. Quindi costituisce un sottogruppo di G il quale viene chiamato **sottogruppo generato dal sottoinsieme** S.
Esso viene denotato con $\langle_G S\rangle$, notazione che in vari contesti può essere abbreviata nella $\langle S\rangle$.
Gli elementi di un tale gruppo sono chiamati **generatori del gruppo** stesso.

Conviene segnalare esplicitamente che la composizione di un gruppo individuato da un insieme costituito da pochi generatori, anche solo due, può essere assai complessa, molto di più dei gruppi ciclici, cioè dei gruppi ottenuti da un solo generatore.

T22 b.13 Nei gruppi additivi $\mathbb{Z}_{ag}$, $\mathbb{Q}_{ag}$, $\mathbb{R}_{ag}$ e $\mathbb{C}_{ag}$ tutti gli elementi diversi dall'elemento neutro, cioè da 0, hanno periodo infinito.

Nel gruppo moltiplicativo dei reali $\mathbb{R}_{nz:mg} := \langle \mathbb{R}_{nz}, \cdot, {}^{-1}, 1\rangle$ l'elemento -1 ha periodo 2 e tutti gli elementi diversi da 1 e -1 hanno periodo infinito. Stessa conclusione per il suo sottogruppo $\mathbb{Q}_{nz:mg}$.

Nel gruppo moltiplicativo dei complessi $\mathbb{C}_{nz:mg} := \langle \mathbb{C}_{nz}, \cdot, {}^{-1}, 1\rangle$ l'elemento -1, come tra gli interi, ha periodo 2, gli elementi i e $-i$ hanno periodo 4; per ogni $r \in \mathbb{P}$ le radici r-esime dell'unità hanno periodo r. Tutti i numeri complessi diversi da questi hanno periodo infinito.

T22 b.14 Consideriamo il gruppo i cui elementi sono le successioni infinite le cui componenti sono 1 o -1 e la cui operazione binaria è la moltiplicazione componente a componente; l'unità di questo gruppo è la successione costante $1^{\mathbb{Z}} = \langle z \in \mathbb{Z} :| \ 1\rangle$ avente tutte le componenti uguali ad 1. Tutti gli elementi di questo gruppo diversi dall'unità hanno periodo 2.

Un gruppo si dice **gruppo di torsione** sse tutti i suoi elementi hanno periodo finito; ovviamente tutti i gruppi finiti sono gruppi di torsione ed i gruppi di torsione interessanti sono solo gli infiniti; il gruppo precedente è un gruppo di torsione infinito.

Un gruppo si dice **gruppo privo di torsione** sse tutti i suoi elementi diversi dall'unità hanno periodo infinito; Sono gruppi privi di torsione $\mathbb{Z}_{ag}$, $\mathbb{Q}_{ag}$, $\mathbb{R}_{ag}$, $\mathbb{C}_{ag}$ e tutti i gruppi additivi ottenuti dagli spazi vettoriali trascurando la moltiplicazione per gli scalari.

Un gruppo (infinito) si dice **gruppo misto** sse possiede sia elementi diversi dall'unità di periodo finito, che elementi di periodo infinito. I diversi gruppi moltiplicativi considerati in precedenza ($\mathbb{Q}_{nz,mg}$, $\mathbb{R}_{nz,mg}$, $\mathbb{C}_{nz,mg}$) sono gruppi misti.

Un gruppo misto che presenta un'infinità (numerabile) di elementi di periodo finito e un'infinità continua di elementi di periodo infinito è il gruppo moltiplicativo dei complessi $\mathbb{C}_{nz,mg}$.

T22 b.15 Eserc. Consideriamo il gruppo G, due suoi elementi diversi dall'unità a e b e un intero positivo k. Dimostrare che:
(a) $a^k = e \implies \lceil k \in \mathrm{prd}(a) \cdot \mathbb{P} \ \wedge \ a^{-1} = a^{k-1} \rceil$.
(b) $\mathrm{prd}(a) = \mathrm{prd}(a^{-1})$.
(3) $\mathrm{prd}(a), \mathrm{prd}(b) \in \mathbb{P} \ \wedge \ a\,b = b\,a \implies \mathrm{prd}(a\,b) = \mathrm{prd}(b\,a) \ \preceq_: \ \mathrm{mcm}(\mathrm{prd}(a), \mathrm{prd}(b))$.

T22 b.16 Vediamo altri modi di individuare sottogruppi di un dato gruppo.

(1) Prop.: L'intersezione di una qualsiasi famiglia di sottogruppi di un gruppo G è sottogruppo di G.

Dim.: Sia $\lceil \lambda \in \Lambda \ \natural \ H_\lambda \rceil$ una famiglia di elementi di $\boldsymbol{SbGrp}(G)$ e consideriamo $H := \cap_{\lambda\in\Lambda} H_\lambda$.

Dato che $\forall \lambda \in \Lambda : e \in H_\lambda$, $e \in H$; $\forall h, h' \in H$ questi elementi appartengono a tutti gli H_λ; quindi $\forall \lambda \in \Lambda : h \cdot h'^{-1} \in H_\lambda$ e di conseguenza $h \cdot h'^{-1} \in H$ ∎

(2) Prop.: Consideriamo un qualsiasi sottoinsieme S di un gruppo G. In $\boldsymbol{SbGrp}(G)$ esiste un H minimamente esteso che contiene S, cioè tale che $\forall K \in \boldsymbol{SbGrp}(G) \llbracket S \subseteq K \ : \ H \leq_{Grp} K$.

Dim.: Sia H l'intersezione di tutti i sottogruppi di G che contengono S; grazie a (1) H è sottogruppo di G e ovviamente contiene S. Ogni altro sottogruppo K che contiene S deve essere contenuto nell'intersezione suddetta ∎

T22 c. laterali, coniugio, automorfismi

T22 c.01 Consideriamo un gruppo $\boldsymbol{G} = \langle \boldsymbol{G}, \cdot, ^{-1}, e \rangle$, un suo sottogruppo H e un suo elemento a.
Si dice laterale destro o coset destro di H in G rappresentato da a l'insieme $H\,a \;:=\; \{h \in H :|\; h\,a\}$.
Per dualità-LR si definisce laterale sinistro o coset sinistro di H in G rappresentato da a l'insieme $a\,H \;:=\; \{h \in H :|\; a\,h\}$.

È possibile descrivere ogni laterale sinistro come una classe d'equivalenza rispetto alla relazione d'equivalenza $\sim_{*H}$ definita in G ponendo per $a, b \in G$:

$$(1) \qquad a \sim_{*H} b \iff b \in a\,H \iff a^{-1}\,b \in H \iff (a^{-1}\,b)^{-1} = b^{-1}\,a \in H \iff a \in b\,H \;.$$

La classe di equivalenza della $\sim_{*H}$ contenente l'elemento g è proprio $g\,H$: infatti $g = ge$ e, dato che e appartiene al sottogruppo H, $g \in gH$.
Dualmente-LR ogni laterale destro può essere definito come classe d'equivalenza per una relazione di equivalenza $\sim_{H*}$ analoga:

$$(2) \qquad a \sim_{H*} b \iff b \in Ha \iff b\,a^{-1} \in H \iff (b\,a^{-1})^{-1} = a\,b^{-1} \in H \iff a \in H\,b \;.$$

Evidentemente per un gruppo abeliano i laterali sinistri di un sottogruppo coincidono con i suoi laterali destri; nel caso di un gruppo nonabeliano si possono avere sottogruppi con questa coincidenza e sottogruppi privi della coincidenza tra laterali sinistri e laterali destri.

Consideriamo un intero $m = 2, 3, ...$, il gruppo additivo degli interi $\mathbb{Z}$ e il suo sottogruppo $m \cdot \mathbb{Z}$. I laterali (sinistri e destri) di tale sottogruppo sono gli insiemi numerici $m\mathbb{Z}$, $m\mathbb{Z} + 1$, $m\mathbb{Z} + 2$, ..., $m\mathbb{Z} + m - 1$; il loro numero è m.

T22 c.02 Osserviamo che, a causa delle due equivalenze $\sim_{H*}$ e $\sim_{*H}$, sia i laterali sinistri che i laterali destri del gruppo G sono sottoinsiemi mutuamente disgiunti del terreno del gruppo, ossia costituiscono due sue partizioni.

Per ogni gruppo G, ogni $H \leq_{Grp} G$ e ogni $g \in G$ accade che la funzione $\lceil\, h \in H \mapsto g\,h \,\rceil$ è una biiezione tra H e il laterale sinistro gH e dualmente-LR accade che la funzione $\lceil\, h \in H \mapsto hg \,\rceil \in \lceil\, H \leftrightarrow Hg \,\rceil$ è una biiezione tra H e il laterale destro $H\,g$.

Questo implica che tutti i laterali sinistri e tutti i laterali destri del sottogruppo H nel gruppo G hanno lo stesso cardinale $|H|$.

Si osserva anche che la permutazione di un gruppo G che a ogni suo elemento fa corrispondere l'inverso stabilisce una biiezione tra i laterali destri e i laterali sinistri di un suo sottogruppo H. Questo conferma che il cardinale dei laterali sinistri e quello dei laterali sinistri coincidono.

Tale cardinale è detto **indice del sottogruppo** H nel gruppo G e in genere si denota con $[G : H]$. Ricordiamo esplicitamente che tale notazione esprime un numero che può essere sia finito che transfinito [B19].

T22 c.03 Se in particolare G è un gruppo finito, denotato con n il suo ordine e con k quello di H, si ha $n = k \cdot [G : H]$, ossia $|G| = |H| \cdot [G : H]$.
Questo corrisponde ad un classico risultato.

(1) Teorema (**teorema di Lagrange**) Il cardinale di ogni sottogruppo H di un gruppo finito G e il suo indice $(G : H)$ sono divisori del cardinale di G.

Da questo teorema si ricavano con facilità varie proprietà dei gruppi finiti.

Innanzi tutto si ha che i sottogruppi di ogni gruppo finito G vanno ricercati esaminando i suoi sottoinsiemi il cui cardinale è un divisore di $|G|$.

Si può anche affermare che ogni gruppo finito il cui ordine è un numero primo non possiede sottogruppi propri e non banali, cioè è un gruppo semplice.

Inoltre ogni gruppo di ordine primo è un gruppo ciclico: infatti se g è un suo elemento diverso dalla sua unità, il sottogruppo delle potenze di g deve avere $|G|$ elementi e quindi deve coincidere con l'intero G.

T22 c.04 Due elementi g ed h di un gruppo G si dicono **elementi coniugati** sse esiste (almeno) un altro elemento x del gruppo tale che $x\,g\,x^{-1} = h$.
Questa relazione non ha interesse per i gruppi abeliani, in quanto ogni loro elemento x è coniugato solo di se stesso: $x\,g\,x^{-1} = x\,x^{-1}\,g = g$.

(1) Prop.: La relazione di coniugio tra gli elementi di un gruppo è una equivalenza.

Dim.: Infatti $e\,g\,e^{-1} = g$, quindi la relazione di coniugio è riflessiva; da $x\,g\,x^{-1} = h$ segue $x^{-1}\,h\,x = g$, cioè si ha che il coniugio è una relazione simmetrica; da $x\,g\,x^{-1} = h$ e $y\,h\,y^{-1} = k$ segue $y\,x\,g\,x^{-1}\,y^{-1}\,c = c(y\,x)g(y\,x)^{-1}\,c = c\,k$, cioè che il coniugio è una relazione transitiva ∎

La partizione del terreno di un gruppo (nonabeliano) in classi di coniugio spesso presenta aspetti interessanti.
In particolare per ogni gruppo finito di permutazioni gli elementi di una classe di coniugio sono caratterizzati da un tipo di fattorizzazione in cicli.

T22 c.05 Si dice **automorfismo di un gruppo** una permutazione del suo terreno che è un isomorfismo del gruppo con se stesso.
Formalmente α è automorfismo di un gruppo $\boldsymbol{G} = \langle G, \cdot, {}^{-1}, e\rangle$ sse $\forall a, b, x \in G : \alpha(a)\cdot\alpha(b) = \alpha(a\cdot b)$.
Denotiamo con $\mathrm{Aut}(\boldsymbol{G})$ l'insieme degli automorfismi del gruppo $\boldsymbol{G}$.
Se $\alpha, \beta \in \mathrm{Aut}(\boldsymbol{G})$, anche la composizione $\alpha \circ \beta$ è automorfismo di $\boldsymbol{G}$.
L'insieme degli automorfismi di un gruppo $\boldsymbol{G}$ munito del prodotto di composizione costituisce quindi un gruppo associato a $\boldsymbol{G}$ chiamato **gruppo degli automorfismi** di $\boldsymbol{G}$.
In genere questo gruppo si può denotare con la stessa notazione $\mathrm{Aut}(\boldsymbol{G})$.

T22 c.06 **(1) Eserc.** Dimostrare che, per ogni elemento g di un gruppo G l'endofunzione di G

$$\alpha_g \;:=\; \lceil\, g \in G \mapsto x\,g\,x^{-1} \,\rceil$$

è un automorfismo di G.

(2) Eserc. Dimostrare che tutti gli elementi di una classe di coniugio di un gruppo hanno lo stesso periodo.
Più in generale dimostrare che due elementi di un gruppo collegati da un automorfismo hanno lo stesso periodo.

T22 c.07 Si dice **gruppo trasposto** del gruppo $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e\rangle$ il gruppo

$$\boldsymbol{G}^{\mathsf{T}} \;:=\; \langle G \;,\; \lceil\, g, h \in G \mapsto h \odot g \,\rceil \;,\; {}^{-1}, e\rangle \;. \tag{1}$$

Per tale gruppo si usano anche i termini gruppo opposto, gruppo duale e gruppo riflesso di $\boldsymbol{G}$.

Evidentemente un gruppo e il suo riflesso sono isomorfi (sostanzialmente coincidono) sse il gruppo è abeliano.

Si dice **antiisomorfismo** tra un gruppo $\boldsymbol{G} = \langle G, \odot, ^{-1}, e_G \rangle$ ed un gruppo $\boldsymbol{H} = \langle H, *, \mathcal{J}, e_H \rangle$ ogni isomorfismo tra $\boldsymbol{G}$ e $\boldsymbol{H}^{\mathsf{T}}$. Se α denota una tale relazione, $\alpha^{-\mathbf{1}}$ costituisce un isomorfismo tra $\boldsymbol{G}^{\mathsf{T}}$ e $\boldsymbol{H}$.

Si dice **antiautomorfismo** di un gruppo $\boldsymbol{G} = \langle G, \odot, ^{-1}, e \rangle$ ogni permutazione di G che costituisce un isomorfismo con il suo gruppo trasposto.

Per ogni gruppo $\boldsymbol{G}$ la sua permutazione $\lceil\, g \in G \nmapsto g^{-1} \,\rceil$ è un antiautomorfismo di G.

T22 d. sottogruppi normali, gruppi quoziente, prodotti di gruppi

T22 d.01 Per ogni gruppo abeliano ciascuno dei sottogruppi ha le due partizioni dei laterali sinistri e dei laterali destri che coincidono. Per un gruppo nonabeliano si possono avere sottogruppi con le due partizioni di laterali coincidenti e sottogruppi con le due partizioni diverse.

Un sottogruppo N di un gruppo G per il quale le due partizioni di G in laterali sinistri e destri coincidono, cioè tale che $\forall g \in G : gN = Ng$, si dice **sottogruppo normale** di G.
Equivalentemente un sottogruppo di G si definisce normale sse $\forall g \in G \ : \ gNg^{-1} = N$.
Evidentemente tutti i sottogruppi di un gruppo abeliano sono normali.

Per affermare che N è sottogruppo normale di G scriviamo $N \leq_{GrpN} G$; per stabilire che N è sottogruppo normale proprio di G scriviamo $N <_{GrpN} G$. Queste due relazioni più concisamente si denotano, risp., con $\lhd_=$ e con $\lhd$.
Inoltre denotiamo con $\boldsymbol{SbGrpN}(G)$ l'insieme dei sottogruppi normali del gruppo G.

T22 d.02 Si osserva che il prodotto di due laterali (bilateri) di un sottogruppo normale N è anch'esso un laterale di N: infatti se $g, h \in G$ si ha $(gN)(hN) = ghNN = ghN$.

Questo permette di definire come **gruppo quoziente** di un gruppo G e di un suo sottogruppo normale N il gruppo avente come terreno l'insieme dei laterali di N e avente come prodotto l'estensione booleana del prodotto di G.

Questo nuovo gruppo si denota con G/N.

T22 d.03 Conviene segnalare che la relazione "essere sottogruppo normale di" non è una relazione d'ordine. Essa infatti, contrariamente alla relazione "essere sottogruppo di" non è transitiva.

Controesempi . . . . . .

T22 d.04 Consideriamo due gruppi $\boldsymbol{G}_i = \langle G_i, \odot_i, j_i, e_i \rangle$ per $i = 1, 2$.

Si dice **prodotto diretto di due gruppi** il gruppo

$$\boldsymbol{G}_1 \times \boldsymbol{G}_2 \ := \ \Big\langle G_1 \times G_2, \odot_1 \times \odot_2, j_1 \times j_2, \langle e_1, e_2 \rangle \Big\rangle \ . \tag{1}$$

Conviene esplicitare le operazioni di questo gruppo riferendole a due elementi generici di $\boldsymbol{G}_1$ $^{\searrow}$ g_1 e h_1 e a due elementi generici di $\boldsymbol{G}_2$ $^{\searrow}$ g_2 e h_2:

Per l'operazione binaria abbiamo $\quad \langle g_1, g_2 \rangle (\odot_1 \times \odot_2) \langle h_1, h_2 \rangle \ := \langle g_1 \odot_1 h_1, g_2 \odot_2 h_2 \rangle$,

Per l'operazione unaria la definizione è' $\quad \langle g_1, g_2 \rangle (j_1 \times j_2) \ := \langle g_1 j_1, g_2 j_2 \rangle$,

Osserviamo anche che $\quad \langle g_1, g_2 \rangle (\odot_1 \times \odot_2) \langle g_1 j_1, g_2 j_2 \rangle = \langle e_1, e_2 \rangle$.

T22 d.05 La costruzione prodotto si può reiterare, ovvero si possono definire i prodotti diretti di tre o più gruppi.

Più in generale, data una qualsiasi famiglia di gruppi

$$\lceil \lambda \in \Lambda \mapsto \boldsymbol{G}_\lambda \rceil \quad \text{con} \quad G_\lambda := \langle G_\lambda, \odot_\lambda, j_\lambda, e_\lambda \rangle \ , \tag{1}$$

si definisce **prodotto diretto di tale famiglia**

$$\prod_{\lambda \in \Lambda} \boldsymbol{G}_\lambda \ := \ \Big\langle \prod_{\lambda \in \Lambda} G_\lambda \ , \ \prod_{\lambda \in \Lambda} \odot_\lambda \ , \ \prod_{\lambda \in \Lambda} j_\lambda \ , \ \langle \lambda \in \Lambda :| \ e_\lambda \rangle \Big\rangle \ . \tag{2}$$

T22 d.06 Queste costruzioni consentono di definire molti gruppi di grande interesse per la matematica e le sue applicazioni. Esempi piuttosto semplici sono costituiti dagli insiemi delle coppie, oppure delle terne, o in generale delle sequenze di data lunghezza d di elementi di un campo $\mathbb{F}$ (in particolare del campo dei razionali, del campo dei reali e del campo dei complessi).

I prodotti diretti che hanno come terreni i suddetti prodotti cartesiani e come operazione la somma termine a termine degli elementi dei rispettivi campi sono i gruppi additivi e abeliani dei vettori del piano, dello spazio tridimensionale e più in generale dello spazio d-dimensionale sopra il dato campo. Per questi ambienti rinviamo a B30, B43, G30, G36 e G40 .

T22 e. esempi di gruppi [2]

T22 e.01 Per $n = 1, 2, 3, ...$ e $j \in \mathbb{Z}$ consideriamo i numeri complessi

$$\zeta_{n,j} \;:=\; \mathsf{e}^{\mathsf{i}\,\frac{2\,\pi}{n}\,j} \;=\; \cos\left(\frac{2\,\pi}{n}j\right) + \mathsf{i}\,\cos\left(\frac{2\,\pi}{n}j\right)\;. \tag{1}$$

Chiaramente $\zeta_{n,n} = 1$ e per ogni $k \in \mathbb{Z}$ abbiamo $\zeta_{n,j+k\,n} \;=\; \zeta_{n,j}$.
Dunque la precedente formula per ciascun n intero positivo individua l'insieme di n numeri complessi

$$\mathsf{rou}_n := \{j = 0, 1, ..., n-1 :|\; \zeta_{n,j}\}\;. \tag{2}$$

Evidentemente per ogni j intero $\zeta_{n,j} = {\zeta_{n,1}}^j$ e quindi gli n numeri complessi $\zeta_{n,j}$ per $j = 0, 1, ..., n-1$ sono le n radici n-esime complesse dell'unità, cioè le n soluzioni dell'equazione $z^n - 1 = 0$.

Si ottengono anche le uguaglianze

$$\forall j, k \in \mathbb{Z} \;:\; \zeta_{n,j}\,\zeta_{n,k} = \zeta_{n,j+k} \quad \text{e} \quad zet_{n,-j} = {\zeta_{n,j}}^{-1} = (\zeta_{n,j})^* \;. \tag{3}$$

Inoltre per ogni $n \in \mathbb{P}$ possiamo prendere in considerazione il **gruppo delle radici n dell'unità**

$$Rou_n \;:=\; \Big\langle \{j = 0, 1, ..., n-1 :|\; \zeta_{n,j}\}\;,\; \cdot\;,\; {}^{-1}\;,\; 1 \Big\rangle\;. \tag{4}$$

Si tratta di un gruppo finito di ordine n, abeliano e isomorfo al gruppo additivo delle classi di resti modulo n.

Osserviamo che gli indici j delle radici $\zeta_{n,j}$ potrebbero considerarsi classi di resti modulo n, oppure per tutte le relazioni precedenti i secondi indici si potrebbero far correre in $\mathbb{Z}$.

Si vede facilmente che se d è un intero positivo divisore di n e poniamo $r := n/d$, le radici r-esime dell'unità individuano un sottogruppo di Rou_n. Se invece n è un numero primo Rou_n è un gruppo semplice.

Un generatore di Rou_n è $\zeta_{n,1}$; se $n \geq 2$ è generatore anche $\zeta_{n,n-1}$. Altri generatori di Rou_n sono tutte le radici $\zeta n, h$ con h coprimo di n.

Per un tale intero h la funzione $\left\lceil\; j = 0, 1, ..., n-1 :|\; \zeta_{n,j} \;\mapsto\; \zeta_{n,hj} \;\right\rceil$ è una permutazione di Rou_n e più precisamente è un automorfismo di tale gruppo.

T22 e.02 Si dice **gruppo dei quaternioni** il gruppo

$$\mathsf{Qtrn} \;:=\; \big\langle \{1, -1, i, j, k, -i, -j, -k\}, *, 1 \big\rangle$$

con l'operazione binaria determinata dalla tavola di Cayley

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

.

Si verifica senza difficoltà che questa operazione è associativa.

In accordo con il teorema di Lagrange i sottogruppi di **Qtrn**, oltre al sottogruppo banale $\{1\}$ e al sottogruppo improprio **Qtrn**, sono il sottogruppo di ordine 2 $\{1, -1\}$ e i tre sottogruppi di ordine 4 generati, rispettivamente, da i, j e k.
Non vi possono essere altri sottogruppi $S <_{Grp}$ **Qtrn**: infatti se $|S| = 2$ deve contenere un'involuzione e solo -1 è tale; se invece $|S| = 4$ deve contenere un elemento di periodo 4; in particolare $i^2 = 1$ e quindi si ha il sottogruppo costituito da i, $-i$, 1 e -1; sottogruppi analoghi sono generati da j e k, rispettivamente.

Il gruppo dei quaternioni è evidentemente nonabeliano (e nonciclico), mentre tutti i suoi sottogruppi di 2 e 4 elementi sono ciclici (ed abeliani).

T22 e.03 Per $n = 3, 4, 5, ...$ denotiamo con plgnR_n il poligono regolare di n lati. Volendo collocare precisamente $\mathsf{P}_n := \mathsf{plgnR}_n$ in $\mathbb{R} \times \mathbb{R}$, scegliamo che abbia centro nell'origine O e un vertice nel punto $\langle 1, 0 \rangle$.
Questo n-agono regolare ha tutti i vertici sulla circonferenza di raggio 1 e decidiamo di etichettarli con V_0, V_1, V_2, ... V_{n-1} procedendo nel verso antiorario; gli indici di queste etichette conviene considerarle elementi di $\mathbb{Z}_n$, ossia interi modulo n.

Ci proponiamo di esaminare le isometrie del piano che trasformano P_n in se stesso.

A queste trasformazioni si possono associare alcune delle permutazioni dei vertici V_j per $j = 0, 1, 2, ..., n-1$.

Evidentemente le isometrie da esaminare mantengono le distanze tra i vertici e tengono fisso il centro O.

Quindi tra queste isometrie vi sono le n rotazioni del piano intorno ad O per un angolo multiplo di $2\,\pi/n$; Se denotiamo con r la rotazione intorno ad O dell'angolo $2\,\pi/n$ le n rotazioni sono l'identità $r^0 = e$, $r^1 = r$, r^2, ..., $r^{n-1} = r^{-1}$. Queste permutazioni dei vertici V_j non cambiano il loro ordine ciclico.

Vi sono inoltre altre isometrie che cambiano l'ordine ciclico nel suo opposto; tutte queste si possono ottenere ciascuna delle precedenti con una qualsiasi riflessione del poligono.

Per precisare le riflessioni di P_n è necessario distinguere i poligoni con un numero pari di lati da quelli con un numero dispari.

Se $n = 2\,k$ è pari gli assi di simmetria sono le k rette passanti per il centro ed uno dei vertici V_j (l'asse $\overline{O\,V_j}$ passa anche per il vertice V_{j+k}) e i k assi di simmetria dei lati che riguardano i vertici V_0, V_1, ..., V_{k-1} e V_k (l'asse del lato $V_j\,V_{j+1}$ coincide con l'asse del lato $V_{j+k}\,V_{j+1+k}$.
Le riflessioni rispetto ai k assi passanti per due vertici le denotiamo con m_0, m_1, ..., m_{k-1}; le riflessioni rispetto agli assi ortogonali a coppie di lati opposti le denotiamo con $m_{1/2}$, $m_{3/2}$, ..., $m_{k-1/2}$.
Per semplificare le scritture ci riserviamo di scrivere m invece di m_0.

Se $n = 2\,k+1$ è dispari gli assi di simmetria sono gli n passanti per il centro e uno dei vertici; si osserva che l'asse passante per il vertice V_j è anche l'asse del lato $V_{j+k}\,V_{j+k+1}$.

input pT22e03

Non vi può essere nessun'altra isometria che conserva P_n: infatti ogni isometria deve trasformare l'ordine ciclico dei vertici in un altro ordine ciclico o in uno degli ordini opposti.

T22 e.04 Diciamo gruppo del poligono regolare di n lati $\mathsf{P}_n = \mathsf{plgnR}_n$ e denotiamo con $\mathsf{Sym}[\mathsf{plgnR}_n]$ il gruppo costituito dalle $2\,n$ simmetrie dell'n-agono regolare munito del prodotto di composizione $\circ_{lr}$ tra tali permutazioni del piano $\mathbb{R} \times \mathbb{R}$.
Di ciascuno dei gruppi $\mathsf{Sym}[\mathsf{plgnR}_n]$ si può costruire senza difficoltà la tavola di Cayley. Per questo è utile osservare le seguenti proprietà delle rotazioni e delle riflessioni.

$$r^i \circ_{lr} r^j = r^{i+j} \quad , \quad \left(r^j\right)^{-1} = r^{-j} \quad , \quad {m_h}^2 = e = r^0 \quad , \quad m_i \circ_{lr} m_j = r^{2(j-i)}$$

Presentiamo in particolare le tavole di composizione per i gruppi delle simmetrie del pentagono e dell'esagono regolari.

	e	r	r^2	r^3	r^4	m_0	m_1	m_2	m_3	m_4
e	e	r	r^2	r^3	r^4	m_0	m_1	m_2	m_3	m_4
r	r	r^2	r^3	r^4	e	m_2	m_3	m_4	m_0	m_1
r^2	r^2	r^3	r^4	e	r	m_4	m_0	m_1	m_2	m_3
r^3	r^3	r^4	e	r	r^2	m_1	m_2	m_3	m_4	m_0
r^4	r^4	e	r	r^2	r^3	m_3	m_4	m_0	m_1	m_2
m_0	m_0	m_3	m_1	m_4	m_2	e	r^2	r^4	r	r^3
m_1	m_1	m_4	m_2	m_0	m_3	r^3	e	r^2	r^4	r^1
m_2	m_2	m_0	m_3	m_1	m_4	r	r^3	e	r^1	r^4
m_3	m_3	m_1	m_4	m_2	m_0	r^4	r^1	r^3	e	r^2
m_4	m_4	m_2	m_0	m_3	m_1	r^2	r^4	r	r^3	e

.

	e	r	r^2	r^3	r^4	r^5	m_0	$m_{1/2}$	m_1	$m_{3/2}$	m_2	$m_{5/2}$
e	e	r	r^2	r^3	r^4	r^5	m_0	$m_{1/2}$	m_1	$m_{3/2}$	m_2	$m_{5/2}$
r	r	r^2	r^3	r^4	r^5	e	$m_{5/2}$	m_0	$m_{1/2}$	m_1	$m_{3/2}$	m_2
r^2	r^2	r^3	r^4	r^5	e	r	m_2	$m_{5/2}$	m_0	$m_{1/2}$	m_1	$m_{3/2}$
r^3	r^3	r^4	r^5	e	r	r^2	$m_{3/2}$	m_2	$m_{5/2}$	m_0	$m_{1/2}$	m_1
r^4	r^4	r^5	e	r	r^2	r^3	m_1	$m_{3/2}$	m_2	$m_{5/2}$	m_0	$m_{1/2}$
r^5	r^5	e	r	r^2	r^3	r^4	$m_{1/2}$	m_1	$m_{3/2}$	m_2	$m_{5/2}$	m_3
m_0	m_0	$m_{1/2}$	m_1	$m_{3/2}$	m_2	$m_{5/2}$	e	r	r^2	r^3	r^4	r^5
$m_{1/2}$	$m_{1/2}$	m_1	$m_{3/2}$	m_2	$m_{5/2}$	m_0	r^5	e	r	r^2	r^3	r^4
m_1	m_1	$m_{3/2}$	m_2	$m_{5/2}$	m_0	$m_{1/2}$	r^4	r^5	e	r	r^2	r^3
$m_{3/2}$	$m_{3/2}$	m_2	$m_{5/2}$	m_0	$m_{1/2}$	m_1	r^3	r^4	r^5	e	r	r^2
m_2	m_2	$m_{5/2}$	m_0	$m_{1/2}$	m_1	$m_{3/2}$	r^2	r^3	r^4	r^5	e	r
$m_{5/2}$	$m_{5/2}$	m_0	$m_{1/2}$	m_1	$m_{3/2}$	m_2	r	r^2	r^3	r^4	r^5	e

.

T22 e.05 Come vedremo in T40, si dice **gruppo diedrale** ogni gruppo generato da due involuzioni.
Si dimostra che per ogni $n \in \mathbb{P}$ vi è un gruppo diedrale finito di ordine $2\,n$ che si denota con $\mathrm{D}ih_n$ e che tale gruppo è isomorfo a $\mathsf{Sym}(\mathsf{plgnR}_n)$. Spesso questi due gruppi possono essere identificati.

Per $j = 0, 1, 2, ..., n-1$ denotiamo con mr^j le isometrie ottenute con una rotazione intorno ad O per l'angolo $\dfrac{2\,\pi}{n}\,j$ seguita dalla riflessione rispetto alla retta passante per j e C.
Quindi l'insieme delle isometrie di plgnR_n è costituito dalle trasformazioni

$$\left\{e, r, r^2, ..., r^{n-1}, m, mr, mr^2, ..., mr^{n-1}\right\} .$$

Queste permutazioni del piano costituiscono un gruppo che viene chiamato **gruppo diedrale** di $2\,n$ elementi, struttura che si denota con $\mathrm{D}ih_n$.

Il gruppo diedrale si può considerare costituito da permutazioni degli interi 0,1,2,...,$n-1$ che etichettano i vertici di plgnR_n. Evidentemente le permutazioni corrispondenti a r e ad m sono, rispettivamente

$$\left|\begin{matrix}0 & 1 & 2 & 3 & \cdots & n-2 & n-1\\ 1 & 2 & 3 & 4 & \cdots & n-1 & 0\end{matrix}\right| \quad \text{e} \quad \left|\begin{matrix}0 & 1 & 2 & 3 & \cdots & n-2 & n-1\\ 0 & n-1 & n-2 & n-3 & \cdots & 2 & 1\end{matrix}\right| .$$

Dei generatori di Dih_n r ha periodo n ed m periodo 2.
Il gruppo può essere presentato aggiungendo alle due relazioni $r^n = e$ e $m^2 = e$ che esprimono la considerazione precedente l'uguaglianza $m\,r\,m = r^{-1}$.
Da queste uguaglianze, osservando che per ogni $j = 1, 2, ..., n-1$ $(m\,r\,m)^j = m\,r^j\,m$, si ricava

$$\forall j = 0, 1, 2, ..., n-1 \;:\; m\,r^j\,m = r^{-j} .$$

T22 e.06 Analizziamo le simmetrie del cubo e il gruppo che esse costituiscono.

Ogni simmetria è una isometria per l'insieme degli 8 vertici del cubo. Conviene distinguere le isometrie ottenibili con rotazioni in $\mathbb{R}^{\times 3}$ dalle isometrie che richiedono una riflessione dello spazio; cominciamo dalle prime.

L'insieme delle simmetrie conviene vederlo come insieme degli spostamenti che si possono avere per l'insieme degli 8 verttici del cubo.
Ciascuno di questi spostamenti di vertici conviene considerarlo dipendere da tre scelte che chiamiamo "scelte primarie".
La prima scelta consiste nello stabilire il vertice V' viene trasformato un vertice fissato V, la cui scelta grazie alla regolarità del poliedro in esame, è indifferente. Non si esclude che V rimanga invariato, ossia che sia $V' = V$.
Questa scelta corrisponde a ripartire in 8 parti l'insieme delle trasformazioni del complesso dei vertici.

La seconda scelta consiste nello stabilire in quale dei 3 vertici adiacenti a V' viene mandato un dato vertice V_1 adiacente a V.

Per completare la individuazione della trasformazione va precisato in quale vertice V'_2 viene mandato un secondo fissato vertice V_2 adiacente a V e diverso da V_1. Per questo vi sono due possibilità; per la prima il tetraedro determinato da V' e dai suoi tre vertici adiacenti si ottiene con una semplice rotazione dal tetraedro determinato da V e dai suoi tre vertici adiacenti; la seconda possibilità si ottiene aggiungendo alla precedente la riflessione rispetto al piano contenente V', V'_1 e il centro del cubo.

Tutti gli spostamenti degli altri vertici sono determinati dalle scelte primarie.
Quindi il gruppo delle simmetrie del cubo è costituito da $8 \cdot 3 \cdot 24 = 48$ elementi, ossia trasformazioni isometriche; 24 di quali queste sono ottenibili, anche materialmente, con rotazioni, mentre 24 richiedono anche una riflessione e quindi non conservante l'orientazione del cubo.

Le prime 24 isometrie costituiscono evidentemente un sottogruppo.
Anche questo gruppo può risultare utile rappresentarlo come sottogruppo del gruppo delle 40 320 permutazioni di 8 oggetti (i vertici del cubo) o come sottogruppo del gruppo delle 720 permutazioni di 6 oggetti (le facce); è meno pratico fare riferimento alle permutazioni dell'insieme dei 12 spigoli, in quanto si tratterebbe di individuare un sottogruppo di un gruppo di $12! = 479\,001\,600$ elementi.

T22 f. teoremi di isomorfismo

T22 f.01 I teoremi di isomorfismo per i gruppi che seguono sono dovuti essenzialmente ad Emmy Noether ed esprimono proprietà fondamentali che sono da associare a proprietà omologhe che valgono per molte altre specie di strutture algebriche.

Gran parte di queste accennate proprietà possono essere unificate a un maggiore livello di astrazione nell'ambito della teoria delle categorie [T50].

T22 f.02 (1) Teorema (**primo teorema di isomorfismo**) Consideriamo i gruppi G ed H, l'omomorfismo $h \in \lceil G \longmapsto_{Grp} H \rceil$ ed il nucleo $K := \boldsymbol{ker}(h)$. Allora $K \leq_{GrpN} G$ e $G/K \lhd\!\!\rightarrow_{Grp} \mathrm{img}(h)$.

Dim.: Si è trovato in b09 che $K \leq_{Grp} G$; innanzi tutto si tratta quindi di dimostrare il carattere normale di tale sottogruppo, cioè che $\forall a \in G : aKa^{-1} \subseteq K$. In effetti $\forall k \in K : h(aka^{-1}) = h(a)h(k)h(a^{-1}) = e_H$ e quindi $aka^{-1} \in K$.

Se $k_1, k_2 \in K$ ed $a \in G$, abbiamo $h(k_i a) = e_H\, h(a) = h(a)$; questo rende lecita la definizione $\overline{h} := \lceil \forall a \in G : Ka \mapsto h(a) \rceil$.

Questa funzione fa parte di $\lceil G/K \longmapsto\!\!\triangleright H \rceil$ ed è un omomorfismo di gruppo, in quanto $\overline{h}(Ka\,Kb) = \overline{h}(KK\,ab) = \overline{h}(Kab) = h(ab) = h(a)h(b) = \overline{h}(Ka)\,\overline{h}(Kb)$. Inoltre è una biiezione in quanto abbiamo

$$\overline{h}(Ka) = \overline{h}(Kb) \text{ implica } h(a) = h(b), \text{ cioè } h(a\,b^{-1}) = e_H, \text{ ossia } ab^{-1} \in K\ .$$

L'osservazione che $\mathrm{img}(\overline{h}) = \mathrm{img}(h)$ permette di concludere che $\overline{h}$ è l'isomorfismo richiesto ∎

T22 f.03 Il precedente enunciato dice che la conoscenza di un gruppo quoziente equivale alla conoscenza di un'immagine per omomorfismo. Dato un omomorfismo di un gruppo in un altro, se si individuano il suo nucleo e la sua immagine, il teorema dimostrato conduce a un isomorfismo.

Come si è detto, un gruppo privo di sottogruppi normali viene chiamato **gruppo semplice** e particolari gruppi semplici sono i gruppi ciclici il cui ordine è un numero primo.
Per un gruppo abeliano si può affermare che è semplice sse non possiede sottogruppi diversi da quello banale e da se stesso.

Il comportamento di un gruppo G dotato di un sottogruppo normale N, come precisato in f01 si può esprimere riconducendosi al comportamento di N e di G/N. Quindi i comportamenti dei gruppi finiti si possono ricondurre ai comportamenti dei gruppi semplici. Questi si possono considerare come i gruppi più essenziali.

Segnaliamo che un importante filone della ricerca sui gruppi ha condotto ad una completa determinazione dei gruppi semplici finiti [`Gruppi finiti semplici (wi)`].

Possiamo quindi sostenere che conosciamo gli strumenti basilari che ci consentono di esaminare le simmetrie fondamentali di tutte le configurazioni finite.

T22 f.04 (1) Prop.: Consideriamo un gruppo G e un $H \leq_{Grp} G$; H è normale sse è il nucleo di qualche omomorfismo.

Dim.: Il teorema f01(1) dice che ogni nucleo di omomorfimo di G è sottogruppo normale. Supponiamo allora $H \leq_{GrpN} G$ e introduciamo $h' := \lceil a \in G \mapsto Ha \rceil \in \lceil G \lhd\!\!\rightarrow G/H \rceil$. evidentemente $\mathrm{img}(h') = G/H$ e inoltre $\forall a, b \in G : h'(ab) = Hab = HaHb = h'(a)h'(b)$, cioè h' è un omomorfismo. Per ogni $a \in G$ abbiamo $a \in \boldsymbol{ker}(h') \iff Ha = H \iff a \in H$.
Si può quindi affermare $\boldsymbol{ker}(h') = H$ ∎

La proprietà dimostrata evidenzia l'importanza dei sottogruppi normali.

Va segnalato esplicitamente che diversi omomorfismi possono avere lo stesso nucleo: per esempio $\mathsf{Id}_{\mathbb{Z}}$ e $\lceil\, n \in \mathbb{Z} \mapsto -n \,\rceil$ sono omomorfismi ben diversi ma hanno lo stesso nucleo, $\{0\}$.

Se $H \leq_{GrpN} G$ l'omomorfismo $\lceil\, a \in G \mapsto H\,a \,\rceil \in \lceil\, G \longmapsto\!\triangleright\, G/H \,\rceil$ viene detto **mappa naturale dal gruppo G sul suo sottogruppo H** e viene denotato con $\mathrm{natmap}_{G,H}$.

T22 f.05 Si dice **commutatore di due elementi di un gruppo** a e b del gruppo G l'elemento $a\,b\,a^{-1}\,b^{-1}$.
Per tale elemento useremo anche la notazione $[a, b]$.
Di questa notazione si usa anche l'estensione booleana ai sottogruppi definendo:

$$\forall H, K \leq_{Grp} G \;:\; [H, K] \;:=\; \{h \in H, k \in K :|\, [h, k]\} \;.$$

Le scritture che si servono di queste parentesi quadrate come di parentesi di commutazione possono essere molto più significative di quelle usata nella definizione. Questo si riscontra in particolare per i gruppi costituiti da trasformazioni di spazi vettoriali o di strutture similari.

Evidentemente $[a, b] = e$ sse i due elementi a e b commutano.
Mentre per un gruppo abeliano il commutatore di ogni coppia di elementi è uguale all'unità e quindi i commutatori non presentano interesse, per un gruppo nonabeliano i commutatori possono fornire informazioni interessanti.

Ha particolare interesse il sottogruppo del gruppo generato dai suoi commutatori; questo sottogruppo si denota con G' e viene chiamato **derivato del gruppo** G.

Va segnalato che l'insieme dei commutatori di un gruppo G, $[G, G]$, non è chiuso rispetto al prodotto e quindi per avere un sottogruppo contenente tutti i commutatori occorre aggiungere al suddetto insieme tutti i prodotti che si possono ottenere dai commutatori.

Va segnalato che taluni autori, in particolare molti cultori della teoria dei gruppi, danno del commutatore una diversa definizione: $[a, b]_{_} \;:=\; a^{-1}\,b^{-1}\,a\,b$; si ha quindi $[a, b]_{_} \;=\; [a^{-1}, b^{-1}]$.
Anche servendosi di questa notazione abbiamo che due elementi a e b commutano sse $[a, b]_{_} = e$ e ancora si definisce il derivato di un gruppo G come il gruppo generato dai commutatori di G.

T22 f.06 Per i commutatori di un gruppo $\langle G, \cdot, {}^{-1}, e\rangle$ valgono le formule che seguono.

(1) Prop.: $\forall g, h \in G \;:\; [h, g] = [g, h]^{-1}$ ∎

(2) Prop.: $\forall g, h \in G \;:\; h^g = [g, h]h$ ∎

(3) Prop.: $\forall g, h, k \in G \;:\; [g, h\,k] = [g, h] \cdot [g, k]^h$ ∎

(4) Prop.: $\forall g, h \in G \;:\; [g, h^{-1}] = [h, g]^{h^{-1}} \;,\; [g^{-1}, h] = [h, g]^{g^{-1}}$ ∎

(5) Prop.: $\forall g, h, k \in G \;:\; [[g, h^{-1}], k]^h \cdot [[h, k^{-1}], g]^k \cdot [[k, g^{-1}], h]^g = e \;,$
$[[g, h], k^g] \cdot [[h, k], g^h] \cdot [[k, g], h^k] = e$ ∎

T22 f.07 (1) Prop.: Per ogni gruppo G il sottogruppo normale si può esprimere come

$$G' \;=\; \{n \in \mathbb{P} \;,\; g_1, ..., g_n \in G :|\, g_1\,g_2 ... g_n\,{g_1}^{-1}\,{g_2}^{-1} ... {g_n}^{-1}\} \;.$$

Dim.: Si osserva (con Weichsel) che

$$\forall g, h, j, k \in G \;:\; (ghg^{-1}h^{-1})(jkj^{-1}k^{-1}) = g(hg^{-1})h^{-1}j(kj^{-1})k^{-1}\,g^{-1}(gh^{-1})hj^{-1}(jk^{-1})k \;,$$

cioè che ogni prodotto di due commutatori si può esprimere nella forma enunciata per $n \leq 6$ ∎

(2) Prop.: Di ogni gruppo G il sottogruppo derivato G' è sottogruppo normale.

Dim.: . . . . . ∎

T22 f.08 (1) Prop.: Si abbiano un gruppo G e due suoi diversi sottogruppi propri S e T. Se uno di essi è normale, allora $S\,T = S$ oppure $T\,S = T$.

Dim.: $S,T <_{Grp} G \Longrightarrow S,T \subseteq S\,T \wedge T\,S \subseteq G$.
Siano $T <_{GrpN} G$, $s_1t_1, s_2t_2 \in ST$; allora $(s_1t_1)(s_2t_2)^{-1} = s_1(t_1{t_2}^{-1}){s_2}^{-1} = s_1{s_2}^{-1} \cdot t_3$ per un opportuno $t_3 \in T$; quindi $(s_1t_1)(s_2t_2)^{-1} \in ST$, cioè $S\,T <_{Grp} G$.
Per dualità-LR si trova $T\,S <_{Grp} G$ ∎

(2) Prop.: Si abbiano un gruppo G e due suoi diversi sottogruppi propri S e T.

$$S\,T \leq_{Grp} G \iff S\,T = T\,S\ .$$

Dim.: "$\Longrightarrow$": $TS = T^{-1}\,S^{-1} = (S\,T)^{-1} = S\,T$.

"$\Longleftarrow$": $\forall s_1, s_2 \in S\ ,\ t_1, t_2 \in T\ :\ s_1t_1 \cdot s_2t_2 = s_1s'_2t'_1t_2$ per un opportuno $s'_2 \in S$ e un opportuno $t'_1 \in T$; quindi $S\,T$ è sottogruppo di G ∎

T22 f.09 Eserc. Dimostrare gli enunciati che seguono.

(1) Prop.: (**proprietà modulare dei sottogruppi normali**) Siano L, M ed N sottogruppi normali del gruppo G con $L \subset M$.

$$L \cap N = M \cap N\ ,\ LN = MN \implies L = M\ .$$

(2) Prop.: (**proprietà di Dedekind dei sottogruppi normali**) Siano L, M ed N sottogruppi normali del gruppo G con $L \subset N$;

$$LM \cap N = L(M \cap N)\ .$$

T22 f.10 Consideriamo $L \subset M \subset G$ con $L <_{GrpN} G$ ed $M <_{Grp} G$. Ovviamente $\forall g \in G : gLg^{-1} = L$ implica $\forall m \in M : mLm^{-1} = L$, cioè $L <_{GrpN} M$; e mentre gli elementi di G/L sono i laterali Lg con $g \in G$, gli elementi di M/L sono i laterali Lm con $m \in M$.

Consideriamo insieme a un sottogruppo normale $L <_{GrpN} G$, il generico sottogruppo $S <_{Grp} G$; in tal caso $L \subseteq LS = SL \subseteq G$, per f07(2) $LS <_{Grp} G$, e $L <_{GrpN} LS$ e LS/L è il sottogruppo di G/L costituito dai laterali esprimibili come Lls ovvero come Ls, ovvero è costituito da tutti e soli i laterali di L che hanno un rappresentante in S.

Di conseguenza, in forza di f07(1) e della formula del prodotto relativo a due sottogruppi $S,T <_{Grp} G$ $\searrow$ $|S\,T||S \cap T| = |S||T|$, abbiamo che se S e T sono due sottogruppi di G uno (almeno) dei quali normale, allora si ha $|TS|/|T| = |S|/S \cap T|$.

T22 f.11 Teorema (**secondo teorema di isomorfismo dei sottogruppi normali**)
Se $S <_{Grp} G$ e $N <_{GrpN} G$, allora $S \cap N <_{GrpN} S$ e $S/(S \cap N) \lhd\!\!\rightarrow_{Grp} NS/N$.

Dim.: Consideriamo $\nu := \mathrm{natmap}(G, G/N)$ e la sua restrizione ad S $\nu_{|_S}$. Questa funzione è un omomorfismo il cui nucleo è $S \cap N$. Il teorema f01(1) implica $S \cap N <_{GrpN} S$ e $S/(S \cap N) \lhd\!\!\rightarrow \mathrm{img}(\nu_{|_S})$. Per le considerazioni in f09 $\mathrm{img}(\nu_{|_S})$ è precisamente la collezione dei laterali di N che hanno rappresentativi in S e questi sono precisamente i laterali costituenti NS/N ∎

T22 f.12 Teorema (**terzo teorema di isomorfismo dei sottogruppi normali**)
Si abbiano $M, N <_{GrpN} G$ con $M \subset N$.

Allora $N/M <_{GrpN} G/M$ e $(G/M)/(N/M) \lhd\!\!\rightarrow_{Grp} G/N$.

Dim.: Esaminiamo la mappa $f := \lceil Mg \in G/M \mapsto Ng \rceil \in \lceil G/M \longmapsto G/N \rceil$.
Si verifica che tale funzione è ben definita ed è un omomorfismo il cui nucleo è in N/M e la cui immagine è G/N. All'enunciato si giunge ancora in virtù di f01(1) ∎

T22 f.13 Forniamo ora un risultato che può considerarsi un quarto teorema di isomorfismo.
Esso arricchisce la seguente situazione riguardante la più elemenetare nozione di funzione tra insiemi.
Denotiamo con G e H due insiemi e sia $f \in \lceil\!\lceil\, G \longmapsto\!\!\triangleright\, H \,\rceil\!\rceil$.
L'estensione booleana della f, $\lceil\!\lceil\, S \subseteq G \,\mapsto\, \mathrm{img}_f(S) \,\rceil\!\rceil$, costituisce un'applicazione di $\mathfrak{P}(G)$ sopra una parte di $\mathfrak{P}(H)$; nel senso opposto la funzione $\lceil\!\lceil\, T \subseteq H \,\mapsto\, \mathrm{coim}_f(T) \,\rceil\!\rceil$ è un'applicazione di $\mathfrak{P}(H)$ sopra una parte di $\mathfrak{P}(G)$.

T22 f.14 (1) Teorema (**teorema di corrispondenza dei gruppi**)
Consideriamo $K <_{GrpN} G$, $\nu := \mathrm{natmap}(G, G/K)$ e l'estensione booleana di questa ν^{be}.
Conveniamo di denotare con $\mathbf{S}_G(K)$ l'insieme dei sottogruppi di G che contengono K, con S e T due generici sottogruppi in $S \in \mathbf{S}_G(K)$ e di scrivere $S^* := \nu^{be}(S)$ e $T^* := \nu^{be}(T)$.

(a) ν^{be} determina una biiezione tra $\mathbf{S}_G(K)$ e $\boldsymbol{SbGrp}(G/K)$.
(b) $S^* = S/K$;
(c) $T \subseteq S \iff T^* \subseteq S^*$, $[S : T] = [S^* : T^*]$;
(d) $T \leq_{GrpN} S \iff T^* \leq_{GrpN} S^*$, $S/T \lhd\!\!\longrightarrow\!\!\triangleright_{Grp} S^*/T^*$.

Dim.: (a) Dimostriamo la biunivocità della ν^{be}, cioè che. $\forall S, T \in \mathbf{S}_G(K) \;:\; S/K = T/K \Longrightarrow S = T$.
Per ogni $s \in S$ si ha $Ks = Kt$ per un opportuno $t \in T$; quindi $s = kt$ per qualche $k \in K$ e di conseguenza $S \subseteq T$; per dualità-LR anbbiamo $T \subseteq S$, ovvero $S = T$.

(b) Dimostriamo la suriettività della ν^{be}, ossia per ogni $A \leq_{Grp} G/K$ troviamo un $B \in \mathbf{S}_K$ tale che $B/K = A$. Consideriamo $B := \nu^{-\mathbf{1}}(A)$ e si trova facilmente che B è in $\mathbf{S}_G(K)$; inoltre abbiamo $B/K = \nu^{be}(B) = \nu^{be}({\nu^{be}}^{-\mathbf{1}}(A)) = A$.

(c) È evidente che ν^{be} rispetta l'inclusione. Per dimostrare $[S : T] = [S^* : t^*]$ dobbiamo mostrare che $\{s \in S :|\, Ts\}$ è in biiezione con $\{s^* \in S^* :|\, T^* s^*\}$. Questa biiezione è $\lceil\!\lceil\, s \in S :|\, Ts \,\mapsto\, \nu(s) \,\rceil\!\rceil$.

(d) Se $T \leq_{GrpN} S$ il terzo teorema di isomorfismo [d11] comporta $T/K \leq_{GrpN} s/K$ e $(S/K)/(T/K) \cong S/T$, cioè $T^* \leq_{GrpN} S^*$ e $S^*/T^* \cong S/T$.
Viceversa se $T^* \leq_{GrpN} S^*$, introduciamo: $\eta := \mathrm{natmap}(S^*, S^*/T^*)$ e consideriamo $\nu\restriction_S$.
Si verifica che T è il nucleo della mappa $\nu\restriction_S \circ_{rl} \eta\restriction_S \in \lceil\!\lceil\, S \longmapsto\!\!\triangleright\, S^*/T^* \,\rceil\!\rceil$; questo implica $T \leq_{GrpN} S$ ∎

T22 g. azioni di un gruppo su un insieme

T22 g.01 Diciamo **gruppo di permutazioni** ogni struttura della forma $\langle G, \circ, {}^{-\mathbf{1}}, \mathsf{Id}_U \rangle$ con G sottoinsieme di $\mathbf{Perm}[U]$, della totalità delle permutazioni di un dato insieme U, sottoinsieme chiuso rispetto alla composizione di tali permutazioni e rispetto al passaggio alla permutazione inversa.

I gruppi come il precedente G si ottengono imponendo alle permutazioni richieste di conservazione di oggetti (configurazioni, valutazioni, ...) influenzabili dalle permutazioni e richieste di invarianza di funzioni di un genere $\lceil U \longmapsto \bullet \rceil$.

Precisando con oculatezza le accennate richieste si riescono a individuare gruppi di permutazioni di grande interesse nell'ambito della stessa matematica e nei vari campi applicativi.

Per esempio tra le permutazioni del piano $\mathbb{R} \times \mathbb{R}$ e dello spazio $\mathbb{R}^{\times 3}$ si individuano quelle che mantengono le distanze tra i punti, le trasformazioni chiamate isometrie [B46].
Tra queste si individuano quelle che mantengono fisso un punto C queste sottopongono tutti i rimanenti punti del piano o dello spazi a rotazioni dello stesso angolo, osia le rotazioni di centro C.
Tra queste si possono scegliere quelle che trasformano in se un poligono o un poliedro con centro in C regolari o dotati di qualche caratteristica di quasiregolarità.

Ad esempio richiedendo la trasformazione in se di un esagono regolare si tindividuano le sei rotazioni che costituiscono un gruppo di sei elementi.
Tra queste si possono selezionare le rotazioni che trasformano in se uno dei due triangoli regolari individuati da una terna di vertici mutuamente non adiacenti dell'esagono (in effetti queste rotazioni conservano entrambi i triangoli ottenibili in questo modo); con questa ulteriore restrizione si individua un gruppo costituito solo da tre delle precedenti rotazioni.

Si osserva anche che ogni aggiunta di restrizioni porta a un sottogruppo del precedente gruppo di permutazioni.

T22 g.02 Da queste considerazioni emerge in particolare l'opportunità di prestare attenzione ai sottogruppi di un gruppo di permutazioni G relativi ad ampliamenti dell'insieme dei cosiddetti **invarianti**.
Questi oggetti possono essere elementi, insiemi, proprietà o costruzioni relative all'ambiente che vengono mantenuti dalle trasformazioni che costituiscono gruppo. e Passando da un insieme di invarianti a uno più esteso, evidentemente, si può avere una restrizione dell'insieme delle permutazioni che lo rispettano.

T22 g.03 Tra le permutazioni di un insieme U si possono evidenziare quelle che non modificano una determinata costruzione B riguardante U. Evidentemente la costruzione B viene conservata dalla applicazione successiva di due permutazioni che la conservano, dalla permutazione inversa di ogni permutazione che la conserva e, ovviamente, dalla identità Id_U.

Siamo quindi indotti a prendere in considerazione anche le strutture ottenute riducendo Sym_U a un gruppo di trasformazioni che non modificano un determinato insieme di costruzioni B. Ciascuna di queste strutture costituisce un gruppo di permutazioni di U e viene chiamata **sottogruppo di permutazioni** del gruppo Sym_U.

T22 g.04 Semplici tipi di richieste di conservazione sono i seguenti:

(1) non modificare, ovvero mantenere fissi, determinati elementi di U;
(2) rispettare un sottoinsieme V di U, cioè trasformare ogni elemento di V in un elemento di V;

(3) rispettare una data partizione di U, cioè trasformare gli elementi di ciascun blocco della partizione in altri elementi dello stesso blocco (questo tipo di richiesta costituisce un rafforzamento della richiesta di (2));
(4) mantenere determinate relazioni tra gli elementi di U: un caso ben comprensibile riguarda le permutazioni dei nodi di un grafo che mantengono l'adiacenza [D35] ;
(5) conservare i valori di determinate funzioni definite sugli elementi di U (questa richiesta intuitivamente quando si tratta di configurazioni discrete come digrafi o cammini si può descrivere come mantenimento di colori assegnati.

Queste proprietà di conservazione si possono esprimere anche facendo riferimento agli invarianti. Le proprietà di conservazione nelle richieste (1) riguardano l'invarianza di elementi dell'ambiente; nelle (5) le richieste concernono una funzione invariante; nella (2) si vuole invariante l'appartenenza a un sottoinsieme e nella (3) l'appartenenza a ciascun blocco della partizione; nella (4) l'appartenenza o meno delle coppie di elementi dell'ambiente a una data relazione.

T22 h. teoremi di Sylow

T22 h.01 Nel seguito con p si denota un arbitrario numero primo.

Definiamo **gruppo-p** ogni gruppo finito i cui elementi hanno come periodo una potenza di p.
L'insieme dei p-gruppi lo denotiamo con $\mathsf{Grp}_{p^{\mathbb{P}}}$.

Diciamo sottogruppo-p di un qualsiasi gruppo G ogni suo sottogruppo che è gruppo-p e per il loro insieme scriviamo $\boldsymbol{SbGrp}_{p^{\mathbb{P}}}(G) := \boldsymbol{SbGrp}(G) \cap \mathsf{Grp}_{p^{\mathbb{P}}}$.

Chiaramente sono p-gruppi:
i gruppi ciclici di ordine p;
i prodotti diretti di due (o più) p-gruppi.

Il gruppo di Klein, isomorfo a $\{1,-1\} \times \{1,-1\}$, è un 2-gruppo.

I p-gruppi godono di varie proprietà e questo comporta che la individuazione dei p-sottogruppi di un gruppo finito tendenzialmente complesso risulti molto utile per la conoscenza delle sue proprietà.

T22 h.02 (1) Prop.: Sia A un gruppo finito abeliano il cui ordine è multiplo di p; allora A contiene un elemento di periodo p.

Dim.: Procediamo per induzione sull'ordine dei gruppi da esaminare. Se $|A| = p$ il gruppo è ciclico e ogni elemento diverso da e ha periodo p.
Supponiamo poi l'enunciato vero per ogni gruppo abeliano il cui ordine sia minore di $p\,m$: dobbiamo dimostrare che ogni A di ordine $p\,m$ contiene un elemento di periodo p.
Sia $a \in A \setminus \{e\}$. Se $\mathrm{prd}(a) = p\,m$, allora $(a^m)^p = e$, cioè $\mathrm{prd}(a^m) = p$.
Sia invece $b \in A \setminus \{e\}$ con $t := prd(b)$ coprimo con p. Per la commutatività di A il sottogruppo $\langle {}_G b \rangle$ è normale e $A_1 := A/\langle {}_G b \rangle$ è un gruppo abeliano di ordine $|A|/t$.
Per l'ipotesi induttiva in A_1 si trova un c di periodo p; sia $d \in A$ tale che $\mathrm{natmap}_{A,A_1}(d) = c = \langle {}_G b \rangle\, d$.
Il periodo di d è un multiplo di p e quindi si ricade nel caso visto sopra dell'elemento a con periodo $\mathrm{prd}(a) = p\,m$ ∎

T22 h.03 Diciamo **centralizzatore di un elemento di un gruppo** $g \in G$ il sottoinsieme di G costituito dagli elementi che commutano con g; per tale sottoinsieme usiamo la notazione

$$\mathsf{Znsr}_G(g) := \{z \in G \;\; ST \;\; z\,g = g\,z\} \ .$$

Evidentemente per ogni $g \in G$ si ha $g \in \mathsf{Znsr}_G(g)$.

Consideriamo la funzione chiamata coniugazione

$$\lceil\, \langle x, g\rangle \in G \times G \mapsto g^x := x\,g\,x^{-1} \,\rceil \;\in\; \lceil\, G \times G \longmapsto G \,\rceil \ .$$

Denotiamo con $\mathsf{CnjC}_G(g)$ la collezione delle classi di coniugio di g.

Inoltre introduciamo la notazione $\mathbf{S}_G$ per la collezione degli insiemi di rappresentativi delle classi di coniugio di G con più di un elemento (al di fuori di $\mathrm{Zntm}(G)$).

T22 h.04 Consideriamo la partizione di G in classi di coniugio: per i cardinali abbiamo per ogni $S \in \mathbf{S}_G$

$$|G| \;=\; |\mathrm{Zntm}(G)| + \sum_{g \in S} [G : \mathsf{Znsr}_G(g)] \ . \tag{1}$$

Questa uguaglianza si dice **equazioni delle classi di coniugio** di G.

(2) Teorema (**teorema di Cauchy dei gruppi finiti**) Sia G un gruppo finito il cui ordine è multiplo di un intero p; G contiene un elemento di periodo p.

Dim.: Per ogni $g \in G$ il numero dei coniugati con g è $[G : \mathsf{Znsr}_G(g)]$. Se $g \notin \mathrm{Zntm}(G)$, allora $|\mathsf{Znsr}_G(g)| < |G|$ e se p divide $|\mathsf{Znsr}_G(g)|$ si può procedere per induzione similmente a quanto fatto in h02.
Se invece per ogni $g \notin \mathrm{Zntm}(G)$ p non divide $|\mathsf{Znsr}(g)|$; dato che $|G| = [G : \mathsf{Znsr}(g)] \cdot |\mathsf{Znsr}(g)|$, per ogni $g \notin \mathrm{Zntm}(G)$ il numero primo p divide $[G : \mathsf{Znsr}(g)]$.
Dato che p divide sia $|G|$ che $\sum_{g \in S} [G : \mathsf{Znsr}_G(g)]$, deve dividere anche $|\mathrm{Zntm}(G)|$.
Il centro è un sottogruppo abeliano ed g02 implica che deve contenere un elemento di periodo p ∎

(2) Coroll.: Consideriamo un gruppo finito G. G è un p-gruppo $\iff$ $|G|$ è una potenza di p.

"$\Longrightarrow$" Se vi fosse un primo $q \neq p$ che divide $|G|$, per il teorema di Cauchy (1) si avrebbe in G un elemento di periodo q, contro l'ipotesi che G sia p-gruppo.

"$\Longleftarrow$" Segue subito dal teorema di Lagrange ∎

T22 h.05 (1) Prop.: Se $H \triangleleft G$ con $H, G/H \in \mathsf{Grp}_{p^{\mathbb{P}}}$, allora $G \in \mathsf{Grp}_{p^{\mathbb{P}}}$.

Dim.: Se $|H| = p^h$ e $|G/H| = p^k$, allora $|G| = p^{h+k}$ ∎

(2) Teorema Se G è un p-gruppo finito non banale, allora il suo centro ha come cardinale un multiplo di p.

Dim.: Consideriamo l'equazione delle classi del gruppo h.04(1); per ciascuno degli elementi g $\mathsf{Znsr}_G(g)$ è sottogruppo proprio di G e quindi per h04(2) $[G : \mathsf{Znsr}(g)]$ è una potenza di p. Di conseguenza p divide ciascuno degli addendi $[G : \mathsf{Znsr}_G(g)]$ e quindi anche $|\mathrm{Zntm}(G)|$ ∎

(2) Coroll.: Ogni gruppo G di ordine p^2 è abeliano.

Dim.: Se G fosse nonabeliano, sarebbe $\mathrm{Zntm}(G) \neq G$ e dovrebbe essere $|\mathrm{Zntm}(G)| = p$ e quindi $G/\mathrm{Zntm}(G)$ di ordine p e quindi ciclico. Ma in generale se G è nonabeliano allora $G/\mathrm{Zntm}(G)$ non può essere ciclico ∎

T22 h.06 Eserc. Dimostrare le proprietà che seguono.

(a) Sia $G \in \mathsf{Grp}_{p^m}$ per qualche $m \in \mathbb{P}$. Allora $\forall k = 0, 1, ..., m-1 : G$ contiene un sottogruppo normale di ordine p^k.

(b) Sia $G \in \mathsf{Grp}_{p^{\mathbb{P}}}$ e $H \in \boldsymbol{SbGrp}(G)$. Allora $\{e\} \subset H \cap \mathrm{Zntm}(G)$.

(c) Sia $G \in \mathsf{Grp}_{p^{\mathbb{P}}}$ e $N \in \boldsymbol{SbGrpN}_{p^*}(G)$. Allora $N \leq_{Grp} \mathrm{Zntm}(G)$.

(d) Sia $G \in \mathsf{Grp}_{p^m}$ e $H \in \boldsymbol{SbGrp}_{p^h}(G)$ con $h < m$. Si trova $K \in \boldsymbol{SbGrp}_{p^{h+1}}(G)$ con $H <_{Grp} K$. Di conseguenza i sottogruppi massimali di G hanno indice p, ossia ordine $|G|/p$.

T22 h.07 Nell'equazione delle classi h04(1) tutti gli addendi del secondo membro sono divisori di $n := |G|$ e quindi può assumere la forma

$$1 = \sum_{j=1}^{m} \frac{1}{k_j} \quad \text{con} \quad k_1, ..., k_n \in (n] \ .$$

A questo punto serve un risultato dovuto a Edmund Landau.

(1) Prop.: Per ogni $m \in \mathbb{P}$ e $q \in \mathbb{Q}$ è finito l'insieme delle m-uple $\langle k_1, ..., k_m \rangle$ tali che $q = \sum_{j=1}^{n} \frac{1}{k_j}$.

Dim.: Per l'insieme delle sequenze di interi basta considerare quelle non decrescenti, cioè tali che $k_1 \leq k_2 \leq \cdots \leq k_n$, le restanti potendosi ottenere mediante un insieme finito di permutazioni.
Si procede quindi per induzione constatando che l'enunciato è evidente per $n = 1$ e ipotizzando che l'enunciato valga per le sequenze di lunghezza inferiore ad m. Per la m-upla costituita da $k_1 \leq k_2 \leq \cdots \leq k_n$ si ha

$$q = \frac{1}{k_1} + \frac{1}{k_2} + \cdots + \frac{1}{k_m} \leq \frac{1}{k_1} + \frac{1}{k_1} + \cdots + \frac{1}{k_1} = \frac{m}{k_1} \ ,$$

cioè vale la limitazione $k_1 \leq \dfrac{m}{q}$; dunque si ha un numero finito di possibilità per k_1.
L'ipotesi induttiva dice che si ha solo un numero finito di possibilità per i rimanenti k_j in quanto questi interi positivi devono soddisfare la relazione $\ q - \dfrac{1}{k_1} = \displaystyle\sum_{j=2}^{n} \frac{1}{k_j}$ ∎

T22 h.08 (1) Teorema Per ogni $m \in \mathbb{P}$ è finito l'insieme dei gruppi finiti che possiedono esattamente m classi di coniugio.

Dim.: Consideriamo un gruppo G finito che presenta m classi di coniugio e scriviamo $c := |\mathrm{Zntm}(G)|$. Scriviamo per la equazione delle classi di G

$$|G| = |\mathrm{Zntm}(G)| + \sum_{j=c+1}^{m} [G : \mathsf{Znsr}_G(g_j)] \ .$$

Scriviamo inoltre $k_j = |G|$ per $j = 1, ..., c$ e $k_j := |G|/[G : \mathsf{Znsr}_G(g_j)] = |\mathsf{Znsr}_G(g_j)|$ per $j = c+1, ..., m$.
Si ha quindi $\ 1 = \displaystyle\sum_{j=1}^{n} \frac{1}{k_j}$ e per g06 esiste solo un numero finito di m-uple $\langle k_1, ..., k_m \rangle$ che soddisfano tale equazione; dunque per ogni m esiste un massimo, che denotiamo con M_m, per i valori dei vari k_j. Di conseguenza un gruppo finito con m classi di coniugio ha ordine non superiore ad M_m e l'insieme dei gruppi finiti di tali ordini, a meno di isomorfismi, è finito ∎

T22 h.09 Un sottogruppo del gruppo G si dice **sottogruppo-p di Sylow** sse è un suo p-sottogruppo massimale. Denotiamo con $\boldsymbol{SbGrpSyl}_p(G)$ l'insieme di tali sottogruppi.

Si osserva che ogni p-sottogruppo di un gruppo G è contenuto in un p-sottogruppo di Sylow. Questo è facile da dimostrare per un gruppo finito, mentre la sua dimostrazione per gruppi infiniti richiede di servirsi del lemma di Zorn.

Se in particolare un gruppo G possiede un solo p-sottogruppo di Sylow, questo è un suo sottogruppo normale.

Grazie alla conservazione del periodo per coniugio si ha che nell'ambito di un gruppo G ogni coniugato di un p-sottogruppo di Sylow è anch'esso un p-sottogruppo di Sylow.

T22 h.10 Sia S un p-sottogruppo di Sylow di un gruppo finito G.
(1) Prop.: $\mathsf{Nlzr}_G(S)/S$ non possiede elementi il cui periodo sia una potenza positiva di p.

Dim.: Supponiamo di avere un $t \in \mathsf{Nlzr}_G(S)/S$ con periodo $p^r > 1$ e poniamo $T^* := \langle {}_G t \rangle \in \boldsymbol{SbGrp}(\mathsf{Nlzr}_G(S)/S)$; chiaramente T^* è un p-gruppo.
Per il teorema di corrispondenza d13 esiste un sottogruppo di G contenente S tale che $T/S \cong T^*$. Grazie a h05(1) S è un p-sottogruppo di G contenente S, o meglio grazie alla massimalità di S, è un p-sottogruppo coincidente con S. Di conseguenza $T^* = \{e\}$ e deve essere $t = e$ ∎

(2) Prop.: Se $g \in G$ con $\mathrm{prd}(g) = p^m$ tale che $g\,S\,g^{-1} = S$, allora $g \in S$.

Dim.: Abbiamo $g \in \mathsf{Nlzr}_G(S)$ e poniamo $\nu := \mathrm{natmap}(\mathsf{Nlzr}_G(S), \mathsf{Nlzr}_G(S)/S)$.

Come g anche $\nu(g)$ ha come periodo una potenza di p; grazie a (1) $\nu(g)$ non può essere che l'unità, e quindi $g \in \boldsymbol{ker}\,\nu = S$ ∎

T22 h.11 Teorema (**primo teorema di Sylow**)
Consideriamo $G \in \mathsf{GrpF}$ ed $S \in \boldsymbol{SbGrpSyl}_p(G)$.
Tutti gli eventuali altri sottogruppi di Sylow di G sono coniugati di S e $|\boldsymbol{SbGrpSyl}_p(G)| = 1\ mod\ p$.

Dim.: Si tratta di dimostrare che la coniugazione per ogni $g \in G$ manda un elemento di $\boldsymbol{SbGrpSyl}_p(G)$ in un altro sottogruppo dello stesso genere. ∎

Vale anche il viceversa: se un gruppo finito ha un p-sottogruppo di Sylow normale, questo è l'unico di questi sottogruppi.

T22 h.12 Teorema (**secondo teorema di Sylow**)
Consideriamo un $G \in \mathsf{GrpF}$ di ordine $p^k\,m$ con $p \perp m$. Ogni S p-sottogruppo di Sylow di G ha ordine p^k.

Dim.: Consideriamo $[G : S] = [G : \mathsf{Nlzr}(S)] \cdot [\mathsf{Nlzr}(S), S]$.
Abbiamo visto in h110 che $[G : Nlzr(S)]$ è uguale a $|\boldsymbol{SbGrpSyl}_p(G)| = 1\ mod\ p$ e quindi essere coprimo con p. $[\mathsf{Nlzr}(S), S] = |\mathsf{Nlzr}(S)/S|$ e questo gruppo quoziente, a causa di h09(1), non possiede elementi di periodo p; per il teorema di Cauchy h03(2), di conseguenza, $|\mathsf{Nlzr}(S)/S| \perp p$. In conclusione deve essere $[G : S] \perp p$.
Per il teorema di Lagrange $|S| = p^h$ per qualche $h \leq k$ e quindi $|G|/|S| = m\,p^{k-n}$; dovendo però essere $|G|/|S| = [G : S]$ un intero coprimo di p, deve essere $k = n$ ∎

T22 h.13 (1) Coroll.: Consideriamo $G \in \mathsf{GrpF}$ e $p \in PRIM$. se p^k divide $|G|$, allora G contiene un sottogruppo di ordine p^k.

Dim.: Se $S \in \boldsymbol{SbGrpSyl}_p(G)$, allora $p^k \preceq_: |G|$ a causa di h11. Grazie a h04(1) S, e con esso G, contiene un sottogruppo di ordine p^k ∎

T22 h.14 Le proprietà dimostrate possono servire a individuare situazioni reciproche rispetto a quelle derivanti dal teorema di Lagrange.

Se l'intero m divide $|G|$ ed è una potenza di un numero primo, allora G contiene un sottogruppo di ordine m, Se m presenta due diversi fattori primi si trova un gruppo, si tratta di Alt_4, tale che m divide il suo ordine e che non contiene alcun sottogruppo di ordine m.
Può servire anche il teorema che segue.

(1) Teorema (**teorema di Grattini**) Consideriamo $G \in \mathsf{GrpF}$ e $K \lhd_= G$. Per ogni $S \in \boldsymbol{SbGrpSyl}_p(K)$ per qualche $p \in PRIM$, allora $G = K\,\mathsf{Nlzr}_G(S)$.

Dim.: Per ogni $g \in G$ $g\,S\,g^{-1} \subseteq g\,K\,g^{-1} = K$, a causa della normalità di K; quindi $g\,S\,g^{-1} \in \boldsymbol{SbGrpSyl}_p(K)$ e pertanto $K \ni k$ con $k\,S\,k^{-1} = g\,S\,g^{-1}$.
Di conseguenza $S = (k^{-1}\,g)S(k^{-1}\,g)^{-1}$ e quindi $k^{-1}\,g \in \mathsf{Nlzr}_G(S)$ e $g \in K\,\mathsf{Nlzr}_G(S)$ ∎

T22 i. serie normali di un gruppo

T22 i.01 Consideriamo una catena di sottogruppi di un gruppo G

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{s-1} \supset G_s = \{e\} \ .$$

L'intero s viene detto **lunghezza della catena di sottogruppi**.
Una tale catena si dice **serie di composizione del gruppo** G sse per $i = 1, 2, ..., s$ si ha che G_i è normale massimale in G_{i-1}. I quozienti G_{i-1}/G_i sono detti **quozienti della catena di sottogruppi** ed i loro ordini $|G_{i-1}|/|G_i|$ sono detti **fattori di composizione della catena di sottogruppi**.

Il gruppo Sym_3 possiede solo la serie di composizione $\mathsf{Sym}_3 \supset Cycl_3 \supset \{e\}$; i suoi quozienti sono $Cycl_2$ e $Cycl_3$ e i suoi fattori di composizione sono 2 e 3.

Il gruppo $Cycl_6$ ha invece due serie di composizione: $Cycl_6 \supset Cycl_3 \supset \{e\}$, con fattori $Cycl_2$ e $Cycl_3$, e $Cycl_6 \supset Cycl_2 \supset \{e\}$, con fattori $Cycl_3$ e $Cycl_2$.

Questi due semplici esempi mostrano che lunghezza, quozienti e fattori delle serie di composizioni possono non determinare il gruppo.

T22 i.02 Un gruppo G è semplice sse possiede solo la serie di composizione di lunghezza 1: $G \supset \{e\}$.

Ogni gruppo finito non banale possiede almeno una serie di composizione.

Vi sono gruppi infiniti che non possiedono serie di composizione ed altri che ne posseggono. Il gruppo additivo degli interi non possiede serie di composizione: infatti i suoi sottogruppi sono costituiti dagli insiemi $h\,\mathbb{Z}$ per $h = 2, 3, 4, ...$ e i sottogruppi di $h\,\mathbb{Z}$ sono costituiti dagli insiemi $h\,k\,\mathbb{Z}$ per $k = 2, 3, 4, ...$ Un processo di costruzione di una serie di composizione non può arrestarsi dopo un numero finito di passi.

Più in generale ogni gruppo abeliano infinito non possiede alcuna serie di composizione. Infatti se avesse una serie di lunghezza s G_{s-1} essendo abeliano semplice avrebbe ordine $p \in PRIM$; similmente G_{s-2}/G_s avrebbe ordine $q \in PRIM$ e G_{s-2} avrebbe ordine pq. Procedendo con questo genere di costruzione di catene di composizione si possono incontrare solo gruppi finiti e nessun gruppo infinito.

T22 i.03 Teorema (**teorema di Jordan-Hoelder**)
Due serie di composizione di un gruppo finito G hanno la stessa lunghezza ed i quozienti di una serie sono isomorfi, a meno di un riordinamento, con i fattori dell'altra.

Dim.: Consideriamo le due serie

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{s-1} \supset G_s = \{e\} \quad , \quad G = G_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{t-1} \supset G_t = \{e\}$$

e procediamo per induzione supponendo che il teorema valga per gruppi di ordine inferiore a $|G|$. ∎

T22 j. gruppi liberi e presentazioni dei gruppi

T22 j.01 I gruppi liberi costituiscono uno strumento che consente di inquadrare con robustezza formale alcune importanti nozioni concernenti i gruppi, come questioni di decidibilità e la definizione delle presentazioni dei gruppi.

I gruppi liberi si possono introdurre in due modi: con una costruzione formale che fa riferimento alla nozione, sostanzialmente semplice, di monoide libero e con una richiesta basata sopra una proprietà universale espressa mediante un diagramma funzionale.

Qui si procede nel primo modo che consente di accostare la nozione in modo più graduale e supportabile con esempi; la proprietà universale viene ottenuta successivamente come teorema.
Con il secondo modo di procedere la costruzione formale viene introdotta per dimostrare un teorema di esistenza di un gruppo libero a partire da un insieme arbitrario.

T22 j.02 Sia B un insieme qualsiasi; ad esso in questa sezione attribuiamo il ruolo di **insieme di base di un gruppo libero**. Osserviamo che questo termine si serve del nome, "gruppo libero", che dobbiamo ancora introdurre.

Collocandoci in un piano nel quale più concretamente ci si preoccupa della effettiva trattabilità delle situazioni particolari, consideriamo tre casi più specifici.

B può essere un semplice insieme finito e quindi può essere definito come un insieme di segni, ossia come un alfabeto.

B può essere un insieme numerabile il quale potrebbe essere introdotto come successione di segni ciascuno dei quali contrassegnato da un elemento di un insieme numerabile maneggevole, ad esempio da $\mathbb{P}$.

È interessante anche il caso di B insieme continuo i cui elementi possono essere caratterizzati da uno o più parametri continui come gli elementi di $\mathbb{R}$ (questo può farsi per il gruppo delle traslazioni della retta) o come le terne di angoli di Eulero (queste consentono di esaminare il gruppo delle rotazioni in 3D).

Introduciamo anche un insieme B' disgiunto da B e in biiezione con esso. In altro modo, servendoci di un segno particolare, $^{-1}$, introduciamo una biiezione $\mathfrak{I}$ tra B e l'insieme costituito dai simboli ottenuti giustapponendo a ciascuno degli elementi di B il detto segno. Scriviamo dunque

$$B' := \{b \in B :| b^{-1}\} \qquad \text{e} \qquad \mathfrak{I} := \lceil b \mapsto b^{-1} \rceil \ . \tag{2}$$

Introduciamo un ulteriore segno, μ estraneo sia a B che a B' che, coerentemente con B01 e D50, chiamiamo "parola muta".

Definiamo poi $\mathsf{C} := B \dot\cup B' \dot\cup \{\mu\}$, insieme che chiamiamo **alfabeto di un gruppo libero**; gli elementi di questo alfabeto li diremo **lettere di un gruppo libero**.

Per ogni $b \in B$ identifichiamo b^1 con b, $b^{-1\,1}$ con b^{-1}, $b^{-1\,-1}$ con b; inoltre estendiamo la biiezione $\mathfrak{I}$ alla involuziona

$$\mathfrak{J} := \lceil b \in B \ , \ h \in \{1,-1\} \ : \ b^h \mapsto b^{-h} \rceil \dot\cup \langle \mu, \mu \rangle \in \lceil \mathsf{C} \lhd\!\!\rightarrow\!\!\rhd \mathsf{C} \rceil \ . \tag{3}$$

A ogni elemento di $B \dot\cup B'$ si può dare la forma b^ϵ con $\epsilon \in \{1,-1\}$ e al suo associato $(b^\epsilon)\mathfrak{J}$ la forma $b^{-\epsilon}$.

Scriviamo inoltre C^+ per l'insieme delle sequenze $\langle c_1, c_2, ..., c_s \rangle$ di elementi di C e definiamo $\mathsf{C}^* := \mathsf{C}^+ \dot\cup \{\mu\}$; gli elementi di questo insieme le chiamiamo parole su C e, un po' più genericamente, **parole di un gruppo libero**.

Muniamo C^* dell'operazione di giustapposizione che potremo denotare con il segno "$\shortmid$", ma riservandoci di semplificare le formule che li contengono facendo scomparire le sue occorrenze, ossia esprimendo la giustapposizione con il semplice accostamento delle parole fattori. Chiediamo inoltre che μ sia il relativo elemento neutro; in tal modo $\mathcal{C} := \langle \mathsf{C}, \shortmid, \mu \rangle$ costituisce un monoide libero.

Osserviamo infine che anche il terreno di questo monoide si ripartisce negli insiemi finiti costituiti dalle parole delle diverse lunghezze.

T22 j.03 Diciamo **parola riducibile** di $\mathcal{C}$ ogni parola nella quale compaiono coppie della forma $b^\epsilon b^{-\epsilon}$ con $\epsilon \in \{1, -1\}$.
Diciamo **parole ridotte** gli elementi rimanenti di $\mathcal{C}$; tra queste vi sono μ e gli altri elementi di $\mathsf{C}\ b^\epsilon$.
Diciamo passo di riduzione la eliminazione da una parola riducibile di un infisso della forma $b^\epsilon\, b^{-\epsilon}$, cioè in una parola la cui lunghezza è abbassata di 2.
Diciamo processo di riduzione una sequenza di passi di riduzione che trasforma una parola riducibile in una ridotta.

Per molte parole riducibili si possono attuare diversi processi di riduzione; ad esempio si hanno i due seguenti:

$ab\underline{cc^{-1}}b^{-1}daa^{-1}aa^{-1}ad \ \to\ a\underline{bb^{-1}}daa^{-1}aa^{-1}ad \ \to\ adaa^{-1}a\underline{a^{-1}a}d \ \to\ adaa^{-1}ad \ \to\ adad$

$abcc^{-1}b^{-1}da\underline{a^{-1}a}a^{-1}ad \ \to\ ab\underline{cc^{-1}}b^{-1}daa^{-1}ad \ \to\ a\underline{bb^{-1}}daa^{-1}ad \ \to\ ada\underline{a^{-1}a}d \ \to\ adad$

Si trova tuttavia che tutti questi processi hanno lo stesso effetto.

(1) Prop.: Tutti i processi di riduzione di una parola conducono a una unica parola ridotta.

Dim.: In ogni parola non ridotta si individuano uno o più fattori che possono essere ridotte separatamente a μ. Essi possono essere fattori che chiamiamo telescopici della forma

$$a^{\epsilon_1} b^{\epsilon_2} ... c^{\epsilon_3} c^{-eps_3} ... b^{-\epsilon_2} a^{-eps_1} \ ,$$

fattori riconducibili alla forma $w \shortmid s\mathfrak{I}(w)$.
Abbiamo quindi la endofunzione che denotiamo con rdctn che a ogni parola di $\mathcal{C}$ associa la corrispondente ridotta; abbiamo anche la associata equivalenza che denotiamo con $\sim_{\mathsf{rdctn}}$ in ciascuna delle cui classi si trovano le parole che hanno in comune la stessa parola ridotta.

Questa equivalenza è una congruenza per la giustapposizione delle parole.

(2) Prop.: Consideriamo le parole w, w', x e x'.

$$w \sim_{\mathsf{rdctn}} \overline{w}\ ,\ x \sim_{\mathsf{rdctn}} \overline{x} \implies w \shortmid x \sim_{\mathsf{rdctn}} \overline{w} \shortmid \overline{x}\ \blacksquare$$

Possiamo quindi considerare il monoide quoziente $\mathcal{C}/\sim_{\mathsf{rdctn}}$.

T22 j.04 **(1) Prop.**: Nel monoide $\mathcal{C}/\sim_{rdctn}$ tutti gli elementi sono invertibili.

Dim.: Deriva direttamente dalla invertibilità di $\mathcal{C}$ $\blacksquare$

Dunque il monoide $\mathcal{C}/\sim_{rdctn}$ arricchito con l'operazione di inversione, anche grazie alla associatività della giustapposizione, costituisce un gruppo. Questo viene detto **gruppo libero sull'insieme di lettere** B e in seguito lo denotiamo con $\mathsf{Grpfree}_B$.

Il gruppo libero sopra una sola lettera b è il gruppo di tutte le potenze positive e negative dell'elemento b. Quando si assume come insieme di base un insieme con più elementi, anche in numero finito, si ha un gruppo con una struttura molto più complessa.

T22 j.05 Nonostante la loro segnalata complessità i gruppi liberi costituiscono uno strumento assai utile per la trattazione di tutti i gruppi, cioè dei gruppi i cui generatori oltre a essere soggetti alle

restrizioni della specie di strutture gruppo viste in :a (associatività, esistenza di un elemento neutro, invertibilità), sono soggetti ad altri determinati vincoli.

Ci proponiamo di considerare delle restrizioni ai gruppi $\mathsf{Grpfree}_B$ esprimibili mediante uguaglianze concernenti parole su C. Un sistema di tali relazioni si traduce in una relazione di equivalenza che permette di applicare a $\mathsf{Grpfree}_B$ una ulteriore operazione di quoziente. Per poter ottenere un risultato utile è necessario servirsi di una proprietà di elevata generalità. Questa è espressa dal un enunciato cui viene dato il nome di **proprietà di mappatura del gruppo libero**.

T22 j.06 Prima della presentazione della suddetta proprietà, ricordiamo che per **diagramma funzionale** si intende un digrafo arricchito da etichette sui nodi e da etichette e segni che distinguono vari generi di archi.
Ciascuno dei nodi individua un insieme e ciascuno degli archi una funzione dal nodo iniziale al nodo finale; per ogni arco l'etichetta individua la funzione e la diversa forma della freccia distingue se si tratta o meno di funzione suriettiva, di funzione iniettiva e/o di funzione invertibile.

Si distinguono sul diagramma i cammini transitivi, cammini dai quali si possono ricavare scorrendo i loro archi le corrispondenti funzioni composte ottenute componendo con l'operatore $\circ_{lr}$ le funzioni incontrate sui successivi archi.

Un diagramma funzionale si dice **diagramma funzionale commutativo** sse ogni coppia di cammini transitivi da un dato nodo iniziale a un dato nodo finale fornisce la stessa funzione composta.

T22 j.07 (1) Teorema Sia $F := \mathsf{Grpfree}_B$ e sia G un gruppo qualsiasi. Ogni mappa $\phi \in \lceil\!\lceil B \longmapsto G \rceil\!\rceil$ si estende in un unico modo ad un omomorfismo $\Phi \in \lceil\!\lceil F \longmapsto_{Grp} G \rceil\!\rceil$.

Questo enunciato piuttosto astratto viene utilmente memorizzato osservando il seguente diagramma funzionale e l'affermazione che si tratta di un diagramma commutativo.

input pT22j06

Dim.: L'estensione della ϕ è data da

$$\Phi \;:=\; \dot\cup_{r\in\mathbb{N}} \lceil\!\lceil\, {c_1}^{\epsilon_1}\cdots {c_r}^{\epsilon_r} \in \mathsf{C}^r \;\mapsto\; f\left({c_1}^{\epsilon_1}\right)\cdots f\left({c_r}^{\epsilon_r}\right) \,\rceil\!\rceil \ .$$

Si tratta di dimostrare che tale mappa rispetta l'equivalenza $\sim_{\mathsf{rdctn}\cdot}$
Questo discende dalla semplice osservazione che ogni passo di riduzione di una parola w non cambia la classe d'equivalenza alla quale appartiene un prodotto che abbia w come fattore. Dato che in F il prodotto viene definito a partire dalla giustapposizione, la mappa Φ rispetta tale prodotto, ossia è un omomorfismo di gruppi. Infine si osserva che l'estensione adottata è l'unico modo per estendere la ϕ a un omomorfismo ∎

T22 j.08 Una famiglia S di elementi di un gruppo G si dice **famiglia generatrice del gruppo** sse la mappa Φ dal gruppo libero $\mathsf{Grpfree}_S$ in G è suriettiva. Questo equivale ad affermare che ogni elemento di G si può esprimere come prodotto di elementi di C.
Se invece la mappa Φ non è suriettiva la sua immagine è un sottogruppo di G che, prevedibilmente, viene chiamato sottogruppo generato da S: questo è il sottogruppo costituito da tutti i prodotti degli elementi di S e dei loro inversi.

T22 j.09 Presentazione di un gruppo con generatori e relatori.

Testo fruibile in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php