Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

COMMUTATORI NEL GRUPPO SIMMETRICO

Relatrice:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Eleonora Cicciarella

VI Sessione
Anno Accademico 2018/2019

A mio fratello Francesco
e ai miei genitori Enzo e Lidia.
A loro, per non aver mai smesso di credere in me.

Indice

Introduzione

Il concetto di commutatore nasce oltre 100 anni fa con il tentativo di Dedekind di estendere lo studio dei caratteri di un gruppo anche ai gruppi non abeliani. Il matematico ne parla per la prima volta in una lettera del 1896 indirizzata a Frobenius, dove rivela la sua idea e i suoi risultati. In particolare, a Dedekind si devono i seguenti risultati: il coniugato di un commutatore è ancora un commutatore, e quindi il sottogruppo derivato generato dai commutatori è un sottogruppo normale; in un gruppo G ogni sottogruppo normale N tale che il quoziente G/N è abeliano contiene il sottogruppo derivato; infine, il sottogruppo derivato è banale se e solo se il gruppo è abeliano.

Ad oggi, i commutatori sono uno strumento consolidato e immensamente utile in tutta la teoria dei gruppi e la letteratura scientifica a riguardo è ampiamente sparsa. Nel 1951, il matematico Oystein Ore nell'introduzione del suo articolo *Some remarks on commutators* [6] afferma che in un gruppo il prodotto di due commutatori non è necessariamente un commutatore, di conseguenza il sottogruppo derivato di un dato gruppo non può essere definito come l'insieme dei commutatori, ma solo come il gruppo generato da essi. All'epoca esistevano ancora pochi criteri e strumenti che potessero aiutare a trovare una risposta per la seguente domanda: quand'è che tutti gli elementi del gruppo derivato sono commutatori?

Ore raggiunge due importanti risultati correlati, entrambi i quali hanno generato aree attive di ricerca. Il primo afferma che ogni elemento nel gruppo alterno A_n è un commutatore di elementi del gruppo simmetrico S_n. In particolare, Ore afferma anche che questo risultato può essere utilizzato, con le

opportune modifiche, per dimostrare una cosa ancora più forte, ovvero che ogni permutazione pari può essere scritta come commutatore di permutazioni pari. Il secondo risultato dimostrato, al quale Ore ha dedicato gran parte dell'articolo, è che ogni elemento del gruppo simmetrico $\mathrm{Sym}(X)$, con X insieme numerabile, è un commutatore di elementi di $\mathrm{Sym}(X)$. Quest'ultima dimostrazione è abbastanza complessa, poiché è stata fatta conducendo un'analisi caso per caso delle possibili decomposizioni cicliche di una permutazione.
Ore conclude l'articolo congetturando che in un gruppo semplice finito non abeliano ogni elemento è un commutatore. Dopo la pubblicazione dell'articolo, numerosi matematici provarono la congettura per altri gruppi semplici finiti non abeliani e, infine, nel 2010 la congettura diventò teorema grazie ai matematici M. W. Liebeck, E. A. O'Brien, A. Shalev e P. H. Tiep [4], che ne dimostrarono la validità per i restanti casi, combinando teoria dei caratteri, induzione sulla dimensione e calcoli al computer.
Nel presente elaborato descriviamo i risultati ottenuti da Ore nel suo articolo, suddividendo il lavoro nel seguente modo: nella prima parte diamo una serie di prerequisiti fondamentali riguardanti principalmente le azioni di un gruppo su un insieme. Inoltre dimostriamo, generalizzando anche al caso infinito, due teoremi fondamentali per provare i risultati di Ore: il primo afferma l'esistenza e unicità della decomposizione in cicli disgiunti per una qualunque permutazione, mentre il secondo afferma che due permutazioni sono coniugate se e solo se hanno la stessa struttura ciclica. Successivamente, introduciamo il gruppo alterno, enunciandone le principali proprietà e dimostrandone la semplicità, sia nel caso finito che in quello infinito. Nella seconda parte diamo le prime definizioni e proprietà riguardanti i commutatori e il sottogruppo derivato. Dimostriamo, in particolare, che sotto opportune condizioni, il prodotto di commutatori è ancora un commutatore. Infine, concludiamo l'elaborato dimostrando che ogni permutazione su un insieme numerabile è un commutatore e questo implica, in particolare, che se X è un insieme numerabile il gruppo $\mathrm{Sym}(X)$ coincide col suo sottogruppo derivato.

Capitolo 1

Premesse

Nel seguito e per tutto il resto dell'elaborato, quando si parlerà di *infinito* si starà sempre facendo riferimento ad un'infinità numerabile.

1.1 Azioni e rappresentazioni permutazionali

Definizione 1.1. Siano G un gruppo e X un insieme non vuoto. Un'*azione permutazionale sinistra* di G su X è una mappa $G \times X \to X$, indicata con $(g, x) \mapsto gx$, che verifica le seguenti condizioni:

1. per ogni $x \in X$, si ha $e\,x = x$, dove e denota l'elemento neutro del gruppo G;

2. per ogni $x \in X$ e per ogni $g, h \in G$, si ha $h(gx) = (hg)x$.

Analogamente, si può definire un'*azione permutazionale destra* di G su X come una mappa $X \times G \to X$, che alla coppia (x, g) associa l'elemento xg di X, tale che $x\,e = x$ e $(xg)h = x(gh)$, per ogni $x \in X$ e per ogni $g, h \in G$.

Se un gruppo G agisce su un insieme X, diremo che X è un *G-insieme* o un *G-spazio*.

Osservazione 1.1. Dati un gruppo G e un insieme non vuoto X, esiste una naturale corrispondenza tra azioni sinistre e azioni destre di G su X. Infatti,

per ogni azione sinistra $G \times X \xrightarrow{\cdot} X$, l'applicazione $X \times G \to X$, data da $(x, g) \mapsto g^{-1} \cdot x$, è un'azione destra.
Viceversa, se $X \times G \xrightarrow{*} X$ è un'azione destra, allora l'applicazione $G \times X \to X$, definita da $(g, x) \mapsto x * g^{-1}$, è un'azione sinistra.

Esempio 1.1. Vediamo alcuni esempi di azioni destre e sinistre.

1. Sia G un gruppo e consideriamo l'insieme $X = G$; allora G agisce su se stesso tramite *coniugio* sia a destra: $(h, g) \mapsto g^{-1}hg$, che a sinistra: $(g, h) \mapsto ghg^{-1}$.

2. Siano $\mathbb{K}$ un campo e V un $\mathbb{K}$-spazio vettoriale di dimensione finita n. Il gruppo lineare generale $G = \mathrm{GL}(n, \mathbb{K})$, ossia il gruppo delle matrici invertibili $n \times n$ a coefficienti in $\mathbb{K}$, agisce a sinistra su V e l'azione è data da: $(A, v) \mapsto Av$, dove $(A, v) \in \mathrm{GL}(n, \mathbb{K}) \times V$.

3. Il gruppo additivo $\mathbb{Z}$ agisce (in questo caso a sinistra) su $X = \mathbb{R}$ tramite traslazione: $(n, x) \mapsto x + n$.

Definizione 1.2. Sia ora X un insieme non vuoto. Il *gruppo simmetrico* su X, denotato con $\mathrm{Sym}(X)$, è l'insieme di tutte le permutazioni su X dotato dell'operazione binaria di composizione di funzioni. In particolare, se X è un insieme finito di cardinalità n, possiamo assumere che X coincida con l'insieme $[n] = \{1, 2, \ldots, n\}$. In tal caso, invece di $\mathrm{Sym}(X)$, si suole usare la notazione S_n.

Una permutazione $\sigma \in S_n$ viene solitamente rappresentata nel modo seguente:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \tag{1.1}$$

dove $\sigma(i)$ indica l'immagine di i tramite σ per $i = 1, \ldots, n$.

Definizione 1.3. Un *gruppo di permutazione* su un insieme X è un sottogruppo di $\mathrm{Sym}(X)$.

Definizione 1.4. Siano G un gruppo e X un insieme non vuoto. Una *rappresentazione permutazionale* di G su X è un omomorfismo $\rho : G \to \mathrm{Sym}(X)$. L'immagine di G attraverso ρ è un gruppo di permutazione, denotato con G^X, chiamato il gruppo di permutazione *indotto* da G su X.

Lemma 1.1. *Se un gruppo G agisce a sinistra su un insieme X, ogni elemento di G dà luogo ad una permutazione di X. Più precisamente, la corrispondenza $\varphi_g : X \to X$ data da $\varphi_g(x) = gx$ è, per ogni fissato $g \in G$, una permutazione di X.*

Dimostrazione. Si ha che φ_g è iniettiva, infatti se $gx = gy$, facendo agire g^{-1} su ambo i mebri otteniamo: $g^{-1}(gx) = g^{-1}(gy) \Rightarrow (gg^{-1})x = (gg^{-1})y \Rightarrow 1_G x = 1_G y$, e dunque $x = y$ per ogni scelta di $x, y \in X$, dove la prima implicazione segue dalla seconda condizione nella definizione di azione sinistra.
Inoltre, la φ_g è anche suriettiva: se $x \in X$, sia $y = g^{-1}x$, allora $gy = g(g^{-1}x) = (gg^{-1})x = 1_G x = x$. □

Teorema 1.2. *Siano G un gruppo e X un insieme non vuoto. Allora esiste una biiezione tra l'insieme delle azioni di G su X e l'insieme delle rappresentazioni permutazionali di G su X.*

Dimostrazione. Consideriamo un'azione sinistra $(g, x) \mapsto gx$ di G su X. Come visto nel lemma precedente, per un fissato $g \in G$ si ha che l'applicazione $\varphi_g : x \mapsto gx$ è una permutazione di X. Possiamo allora definire l'applicazione $\varphi : G \to \mathrm{Sym}(X)$ che ad ogni elemento $g \in G$ associa la permutazione φ_g su X. Questa applicazione, definita ponendo $\varphi(g) = \varphi_g$ per ogni $g \in G$, è un morfismo di gruppi. Dobbiamo verificare che per ogni $g, h \in G$ si abbia $\varphi(gh) = \varphi(g) \circ \varphi(h)$. Sia $x \in X$, allora

$$\varphi(gh)(x) = \varphi_{gh}(x) = (gh)x = g(hx) = g(\varphi_h(x)) = \varphi_g(\varphi_h(x)) = \varphi(g) \circ \varphi(h)(x).$$

Dunque, un'azione di gruppo determina un omomorfismo $\varphi : G \to \mathrm{Sym}(X)$, che è una rappresentazione permutazionale di G su X.
Viceversa, sia $\varphi : G \to \mathrm{Sym}(X)$ un morfismo di gruppi. Allora, la mappa

$(g, x) \mapsto \varphi_g(x)$ è un'azione sinistra di G su X. Verifichiamo che sia effettivamente un'azione di gruppo: $1_G x = \varphi_{1_G}(x) = x$ per ogni $x \in X$, perché la permutazione $\varphi(1_G) = \varphi_{1_G}$ altro non è che l'identità su X. Inoltre per ogni $x \in X$ e per ogni $g, h \in G$, $g(hx) = g(\varphi_h(x)) = \varphi_g(\varphi_h(x)) = \varphi_{gh}(x) = (gh)x$, dove il penultimo passaggio segue dal fatto che φ è un omomorfismo di gruppi. Dunque abbiamo costruito una mappa dalle azioni sinistre di G su X alle rappresentazioni permutazionali di G su X e anche una mappa nella direzione opposta. Chiaramente, per costruzione, queste mappe sono una l'inversa dell'altra.
Tutto quanto dimostrato per le azioni sinistre può essere rifatto per le azioni destre: se $(x, g) \mapsto xg$ è un'azione destra di G su X, allora la corrispondente rappresentazione permutazionale è φ dove $\varphi_g(x) = xg^{-1}$. Osserviamo che, in generale, senza inserire l'inverso φ non sarebbe un omomorfismo. □

Dal teorema appena dimostrato segue che possiamo indifferentemente parlare di azioni di gruppo e rappresentazioni permutazionali.
In particolare, nel seguito daremo una serie di definizioni per le rappresentazioni permutazionali che varranno anche per le azioni di gruppo e ometteremo di scrivere tutte le volte "Siano G un gruppo e X un insieme non vuoto".

Definizione 1.5. Sia fissata una rappresentazione permutazionale $\rho : G \to \mathrm{Sym}(X)$. Diamo le seguenti definizioni:

- il *grado* di ρ è la cardinalità di X, cioè $\deg \rho = |X|$;
- per ogni $x \in X$, lo *stabilizzatore* di x (rispetto a ρ) è $\mathrm{St}_\rho(x) = \{g \in G : gx = x\}$. Se $Y \subseteq X$, poniamo $\mathrm{St}_\rho(Y) = \bigcap_{x \in Y} \mathrm{St}_\rho(x) = \{g \in G : \forall x \in Y\ gx = x\}$;
- per ogni $x \in X$, la *ρ-orbita*[1] di x è l'insieme $\mathrm{Orb}_\rho(x) = \{y \in X : y = gx$ per qualche $g \in G\}$. La relazione binaria $\sim_\rho$ in X, definita ponendo, per

[1] Nel caso in cui il contesto chiarisca quale rappresentazione permutazionale di G su X stiamo considerando, possiamo semplicemente dire *orbita* di x in luogo di *ρ-orbita* di x.

ogni $x, y \in X$,

$$x \sim_\rho y \iff \exists g \in G : y = gx$$

è una relazione di equivalenza, che prende il nome di ρ *equivalenza*;

- ρ è *transitiva* se la relazione di equivalenza $\sim \rho$ è quella totale, ovvero se esiste $x \in X$ tale che $\mathrm{Orb}_\rho(x) = X$;
- ρ è *fedele* se è un monomorfismo. In generale, il nucleo di ρ coincide con $\mathrm{St}_\rho(X) = \bigcap_{x \in X} \mathrm{St}_\rho(x)$, quindi ρ è fedele quando questa intersezione è il sottogruppo identico;
- ρ è *regolare* se è fedele e transitiva.

Osservazione 1.2. Per ogni $x \in X$, $\mathrm{Orb}_\rho(x)$ è precisamente la $\sim_\rho$ classe di equivalenza a cui appartiene x. Pertanto, le orbite sono a due a due disgiunte e costituiscono, dunque, una partizione di X.

Proposizione 1.3. *Sia $\rho : G \to \mathrm{Sym}(X)$ una rappresentazione permutazionale. Allora per ogni $x \in X$ e $Y \subseteq X$ si ha che $\mathrm{St}_\rho(x)$ e $\mathrm{St}_\rho(Y)$ sono sottogruppi di G.*

Dimostrazione. Sia $x \in X$. $\mathrm{St}_\rho(x)$ è non vuoto, in quanto 1_G vi appartiene. Se $g, h \in \mathrm{St}_\rho(x)$, allora $gx = x = hx$ e dunque $(gh^{-1})x = (gh^{-1})(hx) = g(hh^{-1})x = g1_G x = gx = x$. Ne segue che anche gh^{-1} appartiene a $\mathrm{St}_\rho(x)$, che quindi è un sottogruppo di G. Per quanto riguarda $\mathrm{St}_\rho(Y)$, per come è stato definito esso è intersezione di sottogruppi di G, dunque è anch'esso sottogruppo di G. □

Proposizione 1.4. *Sia $\rho : G \to \mathrm{Sym}(X)$ una rappresentazione permutazionale e sia Y un sottoinsieme di X. Allora*

(i) per ogni $g \in \mathrm{St}_\rho(X \setminus Y)$, è ben definita la permutazione $g^{\bar\rho} : x \mapsto gx$ di Y e l'applicazione $\mathrm{St}_\rho(X \setminus Y) \to \mathrm{Sym}(Y)$ che manda $g \mapsto g^{\bar\rho}$ è una rappresentazione permutazionale di nucleo $\mathrm{Ker}(\rho)$.

(ii) $\mathrm{Sym}(Y)$ è isomorfo a $\mathrm{St}_{\mathrm{Sym}(X)}(X \setminus Y)$.

Dimostrazione. Poniamo $Y' = X \setminus Y$.

(i) per ogni $g \in \mathrm{St}_\rho(Y')$, si ha $g^\rho Y = g^\rho(X \setminus Y') = g^\rho X \setminus g^\rho Y' = X \setminus Y' = Y$, perché g^ρ è una permutazione. Dunque, Y è fissato da $\mathrm{St}_\rho(Y')$. La rappresentazione indicata nell'enunciato non è altro che quella indotta su Y dalla restrizione di ρ a $\mathrm{St}_\rho(Y')$. Il suo nucleo è $\mathrm{St}_{\mathrm{St}_\rho(Y')}(\mathrm{St}_\rho(Y)) = \mathrm{St}_\rho(Y) \cap \mathrm{St}_\rho(Y') = \mathrm{St}_\rho(Y \cup Y') = \mathrm{St}_\rho(X) = \mathrm{Ker}(\rho)$.

(ii) Sia $H = \mathrm{St}_{\mathrm{Sym}(X)}(Y')$. Applichiamo il punto precedente al gruppo di permutazioni $\mathrm{Sym}(X)$, scegliendo cioè per ρ l'identità in $\mathrm{Sym}(X)$. Allora la rappresentazione $\varphi : H \to \mathrm{Sym}(Y)$, che ad ogni $h \in H$ associa la permutazione $h^\varphi : x \mapsto hx$ di Y, è ben definita ed è un monomorfismo. Inoltre, è anche suriettiva: per ogni $\sigma \in \mathrm{Sym}(Y)$, l'applicazione $\bar{\sigma}$ di X in sé definita da $x^{\bar{\sigma}} = x$ se $x \in Y'$ e $x^{\bar{\sigma}} = x^\sigma$ se $x \in Y$ è una permutazione appartenente ad H e $\sigma = \bar{\sigma}^\varphi$. Dunque, φ è un isomorfismo.

□

Quest'ultima proposizione afferma, in termini più semplici, che se $Y \subseteq X$ allora $\mathrm{Sym}(Y)$ si immerge in $\mathrm{Sym}(X)$. Nelle notazioni della precedente proposizione, un monomorfismo è dato da $\sigma \mapsto \bar{\sigma}$. Tale monomorfismo viene detto *monomorfismo canonico* di $\mathrm{Sym}(Y)$ in $\mathrm{Sym}(X)$.

Definizione 1.6. Sia $\rho : G \to \mathrm{Sym}(X)$ una rappresentazione permutazionale. Per ogni $g \in G$, definiamo $\mathrm{Fix}_\rho(g) = \{x \in X : gx = x\}$ l'insieme dei *punti fissati* da ρ. Inoltre, chiamiamo *supporto* di g l'insieme $\mathrm{supp}_\rho(g) = X \setminus \mathrm{Fix}_\rho(g) = \{x \in X : gx \neq x\}$. Se $K \subseteq G$, si pone anche $\mathrm{Fix}_\rho(K) = \bigcap_{g \in K} \mathrm{Fix}_\rho(g)$ e $\mathrm{supp}_\rho(K) = X \setminus \mathrm{Fix}_\rho(K) = \bigcup_{g \in K} \mathrm{supp}_\rho(g)$.

Osservazione 1.3. In nessun caso il supporto di un permutazione è un singleton. Infatti, sia $g \in G$ e supponiamo che $\mathrm{supp}_\rho(g) = \{\bar{x}\}$, allora si ha $g\bar{x} \neq \bar{x}$ e per ogni $x \in X \setminus \{\bar{x}\}$, $gx = x$. Dunque $\bar{x}$ non sta nell'immagine della permutazione che quindi non è suriettiva, il che è assurdo.

Osservazione 1.4. Per ogni permutazione σ si ha $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$.

Osservazione 1.5. Siano σ e τ due permutazioni. Allora $\text{supp}(\sigma\tau) \subseteq \text{supp}(\sigma) \cup \text{supp}(\tau)$.

Definizione 1.7. Due permutazioni σ e τ si dicono *disgiunte* se $\text{supp}(\sigma) \cap \text{supp}(\tau) = \varnothing$.

Definizione 1.8. Una permutazione σ su un insieme X si dice *finitaria* se $\text{supp}(\sigma)$ è finito. Denotiamo con FSym(X) l'insieme delle permutazioni finitarie su X.

Osservazione 1.6. Di fatto, una singola permutazione finitaria si comporta come una permutazione su un insieme finito. Infatti, se X è un insieme infinito e $\sigma \in \text{FSym}(X)$, allora possiamo supporre $\text{supp}(\sigma) = \{x_1, x_2, \ldots, x_k\}$. Dunque, poiché σ muove soltanto k elementi di X, possiamo vedere σ come permutazione di S_k.

Lemma 1.5. *Sia X un insieme non vuoto. Se $\sigma, \tau \in \text{Sym}(X)$, allora* $\text{supp}(\tau\sigma\tau^{-1}) = \tau(\text{supp}(\sigma))$.

Dimostrazione. $x \in \tau(\text{supp}(\sigma)) \Leftrightarrow \tau^{-1}(x) \in \text{supp}(\sigma) \Leftrightarrow \sigma\tau^{-1}(x) \neq \tau^{-1}(x) \Leftrightarrow \tau\sigma\tau^{-1}(x) \neq x \Leftrightarrow x \in \text{supp}(\tau\sigma\tau^{-1})$. □

Proposizione 1.6. *Sia X un insieme non vuoto. Allora:*

1. $\text{FSym}(X)$ *è sottogruppo normale di* $\text{Sym}(X)$*;*
2. $\text{FSym}(X)$ *è transitivo.*

Dimostrazione. 1. Per ogni $\sigma, \tau \in \text{FSym}(X)$, si ha che $\sigma\tau^{-1} \in \text{FSym}(X)$. Infatti, sfruttando le Osservazioni 1.4 e 1.5, si ha che $\text{supp}(\sigma\tau^{-1}) \subseteq \text{supp}(\sigma) \cup \text{supp}(\tau)$. Poiché $\text{supp}(\sigma)$ e $\text{supp}(\tau)$ sono finiti per ipotesi, segue che anche $\text{supp}(\sigma\tau^{-1})$ è finito, dunque $\text{FSym}(X)$ è sottogruppo di $\text{Sym}(X)$. Per mostrare che $\text{FSym}(X)$ è normale in $\text{Sym}(X)$ bisogna provare che per ogni $\sigma \in \text{FSym}(X)$ e per ogni $\tau \in \text{Sym}(X)$ si ha che $\tau\sigma\tau^{-1} \in \text{FSym}(X)$. La dimostrazione si completa utilizzando il lemma precedente e, in particolare, osservando che $|\text{supp}(\tau\sigma\tau^{-1})| =$

$|\tau(\mathrm{supp}(\sigma))| = |\mathrm{supp}(\sigma)|$. Dunque, se σ è una permutazione finitaria, anche $\tau\sigma\tau^{-1}$ lo è, qualunque sia $\tau \in \mathrm{Sym}(X)$.

2. Mostriamo che $\mathrm{FSym}(X)$ è transitivo: bisogna provare che presi due qualunque elementi $x, y \in X$ esiste $\sigma \in \mathrm{FSym}(X)$ tale che $\sigma(x) = y$. Se $x = y$, allora basta considerare $\sigma = id$ (dove con *id* si intende la permutazione identica) che è banalmente finitaria in quanto il suo supporto è vuoto. Se $x \neq y$, allora consideriamo la permutazione σ che muove x in y, y in x e lascia invariati tutti gli altri elementi di X. Poiché $\mathrm{supp}(\sigma) = \{x, y\}$, si ha che $\sigma \in \mathrm{FSym}(X)$.

□

1.2 Permutazioni in notazione ciclica

Abbiamo già visto un modo comodo per rappresentare le permutazioni finitare (che, in particolare, sono permutazioni finite) in (1.1). Un secondo modo è quello di usare la notazione ciclica.

Definizione 1.9. Siano X un insieme non vuoto e $k \in \mathbb{N}$, $k > 1$. Una permutazione $\sigma \in \mathrm{Sym}(X)$ si dice *ciclo di lunghezza k* (o anche brevemente *k-ciclo*) se esistono $x_1, x_2, \ldots, x_k$ elementi distinti di X tale che:

(i) per ogni $1 \leq i \leq k-1$, $\sigma x_i = x_{i+1}$ e $\sigma x_k = x_1$;

(ii) $\sigma x = x$ per ogni $x \in X \setminus \{x_1, x_2, \ldots, x_k\}$.

In tal caso, scriveremo $\sigma = (x_1\ x_2\ \ldots\ x_k)$.

Definizione 1.10. I 2-cicli sono anche detti *trasposizioni*.

Proposizione 1.7. *Siano X un insieme non vuoto e $\sigma = (x_1\ x_2\ \ldots\ x_k)$ un k-ciclo in* $\mathrm{Sym}(X)$*, con $k > 2$. Allora $\sigma = (x_1\, x_k)(x_1\, x_{k-1}) \cdots (x_1\, x_3)(x_1\, x_2)$, ovvero ogni k-ciclo è prodotto di $k-1$ trasposizioni.*

Dimostrazione. Dimostriamolo per induzione su k.
Se $k = 3$, allora si verifica facendo i conti che $(x_1\, x_2\, x_3) = (x_1\, x_3)(x_1\, x_2)$.
Adesso, supponiamo la proprietà vera per ogni $k > 2$ e dimostriamo che vale anche per $k + 1$. Per induzione, sappiamo che

$$(x_1 \ \dots \ x_k) = (x_1\, x_k)(x_1\, x_{k-1}) \cdots (x_1\, x_2);$$

dobbiamo mostrare che $(x_1 \ \dots \ x_{k+1}) = (x_1\, x_{k+1})(x_1\, x_k) \cdots (x_1\, x_2)$. Usando l'ipotesi induttiva, il secondo membro diventa: $(x_1\, x_{k+1})(x_1 \ \dots \ x_k)$. Efettuando tale prodotto, si prova quanto voluto. □

Osservazione 1.7. La notazione ciclica può essere estesa anche al caso di permutazioni non finitarie e in questo caso si parla di *cicli infiniti*. Innanzitutto osserviamo che, qualunque sia X insieme infinito, anche non numerabile, i cicli infiniti hanno tutti lunghezza numerabile. Infatti, prendiamo $\sigma \in \mathrm{Sym}(X)$ e consideriamo il sottogruppo ciclico di $\mathrm{Sym}(X)$ generato da σ: $\langle\sigma\rangle = \{\sigma^n \,|\, n \in \mathbb{Z}\}$. Se $x \in \mathrm{supp}(\sigma)$ e $\mathrm{Orb}_{\langle\sigma\rangle}(x)$ è infinito, allora $\mathrm{Orb}_{\langle\sigma\rangle}(x) = \{\sigma^n x \,|\, n \in \mathbb{Z}\}$ ha lunghezza numerabile. Una rappresentazione di un ciclo infinito è della forma:

$$\sigma = (\dots\ x_{-n}\ \ x_{-n+1}\ \dots\ x_{-1}\ \ x_0\ \ x_1\ \dots\ x_{n-1}\ \ x_n\ \dots)$$

dove $\sigma x_i = x_{i+1}$ per ogni $i \in \mathbb{Z}$.

Esempio 1.2. Un esempio di ciclo infinito è la permutazione $n \mapsto n + 1$ di $\mathbb{Z}$, che si può scrivere anche come $(\dots\ -n\ \dots\ -2\ \ -1\ 0\ 1\ 2\ \dots\ n\ \dots)$.

Definizione 1.11. Sia $\rho : G \to \mathrm{Sym}(X)$ una rappresentazione permutazionale. Chiamiamo *classe completa di rappresentanti* delle orbite di ρ, e la indichiamo con $\mathcal{R}$, un sottoinsieme di X a cui appartiene esattamente un elemento di ciascuna ρ-orbita.

Definizione 1.12. Sia $\rho : G \to \mathrm{Sym}(X)$ una rappresentazione permutazionale e sia $\mathcal{R} = \{x_i\}_{i\in I}$, I famiglia di indici, una classe completa di rappresentanti delle orbite di ρ. Per ogni $i \in I$ denotiamo con X_i l'orbita cui appartiene x_i e sia $\rho_i : G \to \mathrm{Sym}(X_i)$ la rappresentazione permutazionale indotta da ρ

su X_i. Le rappresentazioni ρ_i sono dette *componenti transitive* di ρ (il fatto che ciascuna ρ_i sia transitiva segue banalmente dalla sua definizione). Si dice anche che ρ è *somma disgiunta* delle sue componenti transitive ρ_i.

Osservazione 1.8. La terminologia *somma disgiunta* è giustificata dal fatto che le ρ_i determinano ρ. Infatti, conoscendo le ρ_i si può ricostruire ρ in questo modo: per ogni $g \in G$ il dominio X di g^ρ (dove g^ρ indica l'immagine di g tramite ρ) è l'unione disgiunta dei domini X_i delle permutazioni g^{ρ_i} e ogni $x \in X$ viene mandato da g^ρ in $g^{\rho_i}x$, dove i è l'unico indice tale che $x \in X_i$.

È utile adesso dare una definizione di prodotto infinito di permutazioni:

Definizione 1.13. Siano X un insieme non vuoto e J un insieme arbitrario di indici. Siano date poi una famiglia $\{Y_j\}_{j\in J} \subseteq X$ di sottoinsiemi di X a due a due disgiunti e una famiglia di permutazioni $\{\sigma_j\}_{j\in J} \subseteq \mathrm{Sym}(X)$, con la proprietà che $\mathrm{supp}(\sigma_j) \subseteq Y_j$, per ogni $j \in J$. Allora, per ogni $x \in X$, definiamo il *prodotto infinito* σ delle permutazioni σ_j nel seguente modo:

$$\begin{cases} \sigma(x) = \sigma_j(x) & \text{se esiste } j \text{ tale che } x \in \mathrm{supp}(\sigma_j) \\ \sigma(x) = x & \text{altrimenti} \end{cases} \tag{1.2}$$

e scriviamo

$$\sigma = \prod_{j\in J} \sigma_j. \tag{1.3}$$

Osservazione 1.9. Facciamo alcune importanti osservazioni riguardanti la definizione appena data.

(i) Dalla definizione segue, ovviamente, che $\mathrm{supp}(\sigma_h) \cap \mathrm{supp}(\sigma_k) = \varnothing$, per ogni $k \neq h$.

(ii) La definizione è ben posta. Infatti, il fatto che i supporti siano a due a due disgiunti garantisce che esiste al più un $j \in J$ tale che $x \in \mathrm{supp}(\tau_j)$.

(iii) La definizione di σ non dipende dall'ordine delle permutazioni σ_j nel prodotto (1.3).

Per scrivere una permutazione in notazione ciclica utilizziamo il seguente fatto:

Teorema 1.8. *Sia X un insieme non vuoto e sia σ una permutazione non identica di* $\mathrm{Sym}(X)$*. Allora σ si decompone in modo unico, a meno dell'ordine, come prodotto di cicli non identici a due a due disgiunti.*

Dimostrazione. Dimostriamo adesso il teorema.
Esistenza. Sia $\mathcal{R} = \{x_i\}_{i\in I}$, I famiglia di indici, una classe completa di rappresentanti delle σ-orbite non banali e indichiamo con X_i la σ orbita cui appartiene l'elemento x_i di $\mathcal{R}$, cioè $X_i = \{\sigma^k x_i \,|\, k \in \mathbb{Z}\}$. Notiamo che per come abbiamo scelto $\mathcal{R}$ si ha $|X_i| > 1$, per ogni $i \in I$. Adesso, per ogni $i \in I$, poniamo $\widetilde{\sigma_i} = \sigma|_{X_i}$. Osserviamo che per definizione di restrizione di una funzione e poiché ogni orbita X_i è σ-invariante, segue che $\widetilde{\sigma_i} \in \mathrm{Sym}(X_i)$, per ogni $i \in I$. Ogni $\widetilde{\sigma_i}$ si può estendere ad una permutazione $\sigma_i \in \mathrm{Sym}(X)$ nel seguente modo:

$$\begin{cases} \sigma_i(x) = \widetilde{\sigma_i}\,(x) & \text{se } x \in X_i \\ \sigma_i(x) = x & \text{se } x \in X \setminus X_i. \end{cases}$$

Dunque, σ_i è la permutazione di X che opera come σ sugli elementi di X_i e stabilizza $X \setminus X_i$. Evidentemente, ogni σ_i è un ciclo avente supporto X_i. Osserviamo che $\mathrm{supp}(\sigma_i) \cap \mathrm{supp}(\sigma_j) = \varnothing$, per ogni $i \neq j$, poiché le orbite sono a due a due disgiunte. Ne segue che il prodotto $\sigma = \prod_{i\in I} \sigma_i$ è ben definito.
Unicità. Se $\sigma = \prod_{k\in K} \tau_k$ è un'altra decomposizione di σ come prodotto di cicli non identici a due a due disgiunti, allora i supporti dei cicli τ_k sono precisamente le σ-orbite contenute in $\mathrm{supp}(\sigma)$, cioè: $\{\mathrm{supp}(\tau_k) \,|\, k \in K\} = \{X_i \,|\, i \in I\} = \{\mathrm{supp}(\sigma_i) \,|\, i \in I\}$. Inoltre, se $k \in K$ e i è l'unico elemento di J tale che $\mathrm{supp}(\tau_k) = \mathrm{supp}(\sigma_i)$, si ha: $\tau_k x = \sigma x = \sigma_i x$ per ogni $x \in X_i$, il che implica che $\tau_k = \sigma_i$. Ciò prova che $\{\tau_k \,|\, k \in K\} = \{\sigma_i \,|\, i \in I\}$ e quindi la decomposizione di σ è unica. □

Nel seguito quando parleremo di *decomposizione ciclica* di una permutazione σ, intenderemo sempre la decomposizione di σ come prodotto di cicli non identici a due a due disgiunti.

Esempio 1.3. Sia σ la permutazione di S_7 data da $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 5 & 4 & 7 \end{pmatrix}$. Scegliamo $\mathcal{R} = \{1, 4\}$ come classe completa di rappresentanti delle orbite non banali, allora le σ orbite non banali saranno $X_1 = \{1, 2, 3\}$ e $X_4 = \{4, 6\}$. Utilizzando le stesse notazioni della dimostrazione precedente, si ha che $\sigma_1 = (1\ 2\ 3)$ e $\sigma_4 = (4\ 6)$ corrispondono alle orbite contenute in $\mathrm{supp}(\sigma)$; otteniamo dunque la fattorizzazione $\sigma = \sigma_1\sigma_4$ in prodotto di cicli disgiunti non identici.

Definizione 1.14. Siano X un insieme non vuoto e sia $\sigma \in \mathrm{Sym}(X)$. Sia, inoltre, $\sigma = \prod_{i\in I} \sigma_i$ la decomposizione ciclica di σ. Il *tipo ciclico* (o anche *struttura ciclica*) di σ è la seguente scrittura simbolica: $1^{a_1}\, 2^{a_2} \cdots k^{a_k} \cdots \aleph_0^{a_0}$, dove $a_0 = |\{\sigma_j\,,\, |\mathrm{supp}(\sigma_j)| \geq \aleph_0\}|$, $a_1 = |\mathrm{Fix}(\sigma)|$ e, per ogni $i > 1$, $a_i = |\{\sigma_j\,,\, |\mathrm{supp}(\sigma_j)| = i\}|$, con $a_i \in \mathbb{N} \cup \{\infty\}$, per ogni $i \geq 0$. Chiaramente, se X è finito si ha $a_0 = 0$.

Esempio 1.4. Se $\sigma = (2\,4)(3\,6\,7) \in S_7$, allora il tipo ciclico di σ è $1^2\, 2^1\, 3^1$.

Osservazione 1.10. Siano $\sigma, \tau \in \mathrm{Sym}(X)$. Se $\sigma = \prod_{i\in I} \sigma_i$ e $\tau = \prod_{j\in J} \tau_j$ sono le decomposizioni di σ e τ come prodotto di cicli non identici a due a due disgiunti, allora σ e τ hanno lo stesso tipo ciclico se esiste una biiezione $\varphi : I \to J$ tale che, per ogni $i \in I$, il ciclo σ_i abbia la stessa lunghezza del ciclo $\tau_{\varphi(i)}$, e se, inoltre, $|\mathrm{Fix}(\sigma)| = |\mathrm{Fix}(\tau)|$.

Prima di proseguire con un importante teorema, ricordiamo una definizione.

Definizione 1.15. Sia G un gruppo. Diciamo che due elementi $a, b \in G$ sono *coniugati* in G se esiste $g \in G$ tale che $a = gbg^{-1}$.

Teorema 1.9. *Due permutazioni σ e τ su uno stesso insieme non vuoto X sono coniugate in* $\mathrm{Sym}(X)$ *se e solo se hanno lo stesso tipo ciclico.*

Dimostrazione. Supponiamo dapprima che σ e τ siano permutazioni coniugate in $\mathrm{Sym}(X)$. Allora esiste $\alpha \in \mathrm{Sym}(X)$ tale che $\tau = \alpha\sigma\alpha^{-1}$. Se $\sigma = \prod_{i\in I} \sigma_i$ è la decomposizione di σ in prodotto di cicli non identici a due a due disgiunti, allora possiamo scrivere $\tau = \prod_{i\in I} \alpha\sigma_i\alpha^{-1}$ ed è facile mostrare che i

cicli $\alpha\sigma_i\alpha^{-1}$ sono a due a due disgiunti. Inoltre, per il Lemma 1.5, si ha che $\mathrm{supp}(\alpha\sigma_i\alpha^{-1}) = \alpha(\mathrm{supp}(\sigma_i))$, per ogni $i \in I$, da cui segue, in particolare, che $|\mathrm{supp}(\alpha\sigma_i\alpha^{-1})| = |\mathrm{supp}(\sigma_i)|$, per ogni $i \in I$. Dunque σ e τ hanno lo stesso tipo ciclico.

Viceversa, supponiamo che σ e τ abbiano lo stesso tipo ciclico. Siano $\sigma = \prod_{i\in I}\sigma_i$ e $\tau = \prod_{j\in J}\tau_j$ le decomposizioni cicliche, rispettivamente, di σ e τ. Allora, per quanto visto nell'Osservazione 1.10, avremo che $|I| = |J|$, per cui, senza perdita di generalità, possiamo supporre $I = J$ e avremo anche $|\mathrm{supp}(\sigma_i)| = |\mathrm{supp}(\tau_i)|$. Inoltre, $\mathrm{Fix}(\sigma)$ e $\mathrm{Fix}(\tau)$ hanno uguale cardinalità, per cui esiste un'applicazione biiettiva $f : \mathrm{Fix}(\sigma) \to \mathrm{Fix}(\tau)$ che manda ogni elemento fissato da σ in un elemento fissato da τ. Sia adesso $k \in I$ e consideriamo i cicli σ_k e τ_k. Indichiamo con a_i gli elementi del supporto di σ_k e con b_i quelli del supporto di τ_k. Definiamo una mappa $g_k : \mathrm{supp}(\sigma_k) \to \mathrm{supp}(\tau_k)$ tale che $a_i \mapsto b_i$, per ogni $1 \leq i \leq |\mathrm{supp}(\sigma_k)|$, mantenendo l'ordine degli elementi nei cicli. Poiché gli elementi a_i e b_i sono a due a due distinti, allora la mappa g_k è iniettiva per ogni $k \in I$, ne segue che è anche suriettiva (perché iniettiva tra insiemi della stessa cardinalità), dunque è una biiezione tra $\mathrm{supp}(\sigma_k)$ e $\mathrm{supp}(\tau_k)$. Proviamo che $g_k\,\sigma_k\,g_k^{-1} = \tau_k$:

$$(g_k\,\sigma_k\,g_k^{-1})b_i = (g_k\,\sigma_k)a_i = g_k\,a_{i+1} = b_{i+1} = \tau_k b_i.$$

Allora, poiché questo vale per ogni $k \in I$, definendo $g : \mathrm{supp}(\sigma) \to \mathrm{supp}(\tau)$ in modo tale che $g|_{\mathrm{supp}(\sigma_k)} \equiv g_k$ per ogni $k \in I$, si ha che g è una biiezione tra i supporti di σ e τ, in quanto sia i cicli di σ che i cicli di τ sono a due a due disgiunti. Infine, l'applicazione $\varphi : X \to X$ definita nel seguente modo:

$$\varphi(x) = \begin{cases} g\,x & \text{se } x \in \mathrm{supp}(\sigma) \\ fx & \text{se } x \in \mathrm{Fix}(\sigma) \end{cases}$$

è una permutazione di X e, per quanto visto precedentemente, si ha che $\varphi\sigma\varphi^{-1} = \tau$. □

1.3 Il gruppo alterno

Il contenuto di questa sezione è riferito esclusivamente alle permutazioni finitarie. Tra queste sono ovviamente comprese tutte le permutazioni su un insieme finito.
Per quanto visto precedentemente, ogni permutazione finitaria è prodotto (finito) di cicli di lunghezza finita, ciascuno dei quali è a sua volta prodotto di trasposizioni (sempre in numero finito). Quanto detto finora implica il seguente fatto fondamentale:

Teorema 1.10. *Sia X un insieme non vuoto. Allora il gruppo* $\mathrm{FSym}(X)$ *è generato dall'insieme delle sue trasposizioni:* $\{(i\,j) \mid i, j \in X, i \neq j\}$.

Una permutazione finitaria σ può essere scritta in modi diversi come prodotto di trasposizioni, sia per i fattori che per il loro numero; ad esempio, in S_4, si ha che $(1\,2\,3) = (1\,2)(1\,3) = (3\,4)(2\,3)(2\,4)(1\,3)$. Quello che tuttavia dipende da σ è la parità del numero di fattori che compare in una sua qualsiasi fattorizzazione. Dimostriamo il seguente risultato:

Proposizione 1.11. *Sia X un insieme non vuoto e sia $\sigma \in \mathrm{FSym}(X)$. Se σ si può scrivere come prodotto di t trasposizioni e anche come prodotto di s trasposizioni, allora vale $t \equiv s \bmod 2$, ovvero t è pari (risp. dispari) se e solo se s è pari (risp. dispari).*

Dimostrazione. Sia $\sigma \in \mathrm{FSym}(X)$ e supponiamo $|\mathrm{supp}(\sigma)| = n < +\infty$. Allora, come già detto precedentemente, possiamo vedere σ come una permutazione di S_n, mettendo $\mathrm{supp}(\sigma)$ in biiezione con l'insieme $\{1, 2, \ldots, n\}$.
Adesso, facciamo agire il gruppo S_n sull'insieme $\mathbb{R}[x_1, \ldots, x_n]$ dei polinimi in n variabili a coefficienti reali, nel seguente modo: data $\sigma \in S_n$ e dato $f(x_1, x_2, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$, σ applicato a $f(x_1, x_2, \ldots, x_n)$ è il polinomio $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Scriveremo:

$$\sigma \cdot f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

In altre parole, l'azione di σ sostituisce nel polinomio f la variabile x_i con la variabile $x_{\sigma(i)}$, per ogni $i = 1, \ldots, n$. Questa è realmente un'azione (in questo caso sinistra), infatti:

i) $id \cdot f(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n)$, per ogni $f(x_1, x_2, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ (dove id indica l'identità di S_n);

ii) per ogni $\sigma, \tau \in S_n$ e per ogni $f(x_1, x_2, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ vale $(\sigma \circ \tau) \cdot f(x_1, x_2, \ldots, x_n) = \sigma \cdot (\tau \cdot f(x_1, x_2, \ldots, x_n))$.

Per proseguire con la dimostrazione, consideriamo, in particolare, il polinomio

$$p(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Sia ora τ la trasposizione $\tau = (a\, b)$, con $1 \leq a < b \leq n$, e studiamo l'azione $\tau \cdot p(x_1, x_2, \ldots, x_n)$. Tale azione non modifica i fattori $(x_i - x_j)$ in cui i e j sono diversi da a e b. Invece, per quanto riguarda i fattori che contengono x_a o x_b, si ha che:

- per ogni m tale che $1 \leq m < a$, l'azione di τ scambia fra loro i due fattori $(x_m - x_a)$ e $(x_m - x_b)$;
- per ogni m tale che $b < m \leq n$, l'azione di τ scambia fra loro i due fattori $(x_a - x_m)$ e $(x_b - x_m)$;
- per ogni k tale che $a < k < b$, l'azione di τ trasforma i fattori del tipo $(x_a - x_k)$ in $(x_b - x_k)$ e i fattori del tipo $(x_k - x_b)$ in $(x_k - x_a)$. Dunque, cambiando il segno ad entrambi i fattori, il prodotto $(x_a - x_k)(x_k - x_b)$ rimane invariato;
- infine, l'azione di τ cambia il segno del fattore $(x_a - x_b)$.

Per quanto appena visto, risulta dunque che per ogni trasposizione $\tau \in S_n$ vale

$$\tau \cdot p(x_1, x_2, \ldots, x_n) = -p(x_1, x_2, \ldots, x_n).$$

A questo punto possiamo concludere la dimostrazione del teorema: data una permutazione $\sigma \in S_n$ che si può scrivere come prodotto di t trasposizioni, per sapere come agisce σ su $p(x_1, x_2, \ldots, x_n)$ basta applicare una dopo l'altra queste t trasposizioni. Dunque, vale

$$\sigma \cdot p(x_1, x_2, \ldots, x_n) = (-1)^t p(x_1, x_2, \ldots, x_n). \tag{1.4}$$

Se σ si può scrivere anche come prodotto di s trasposizioni, allora per lo stesso ragionamento si ha che

$$\sigma \cdot p(x_1, x_2, \ldots, x_n) = (-1)^s p(x_1, x_2, \ldots, x_n). \tag{1.5}$$

Poiché le espressioni 1.4 e 1.5 sono equivalenti, deve valere $(-1)^t = (-1)^s$, cioè deve essere $t \equiv s \bmod 2$. □

In virtù del risultato precedente è ben posta la seguente:

Definizione 1.16. Una permutazione finitaria su un insieme X non vuoto si dice *pari* (rispettivamente *dispari*) se si può scrivere come prodotto di un numero pari (rispettivamente dispari) di trasposizioni.

Definizione 1.17. Il *segno* di una permutazione finitaria σ è 1 se σ è pari, -1 se essa è dispari. Dunque, se σ è il prodotto di d trasposizioni, allora il suo segno è $sgn(\sigma) = (-1)^d$.

Osservazione 1.11. Dalla Proposizione 1.7 segue che un k-ciclo di $\mathrm{Sym}(X)$ è pari se e solo se k è dispari, viceversa è dispari se e solo se k è pari.

Proposizione 1.12. *Sia X un insieme con almeno due elementi. Il segno di una permutazione finitaria definisce un omomorfismo suriettivo dal gruppo* $\mathrm{FSym}(X)$ *al gruppo moltiplicativo* $\{+1, -1\}$.

Dimostrazione. Sia f l'applicazione da $\mathrm{FSym}(X)$ a $\{+1, -1\}$ che ad ogni $\sigma \in \mathrm{FSym}(X)$ associa la parità della permutazione, ponendo dunque $f(\sigma) = sgn(\sigma)$ per ogni $\sigma \in \mathrm{FSym}(X)$. Dobbiamo mostrare che per ogni $\sigma, \tau \in \mathrm{FSym}(X)$ vale $f(\sigma \cdot \tau) = f(\sigma) \cdot f(\tau)$.

Siano $\sigma, \tau \in \mathrm{FSym}(X)$. Poiché sappiamo che ogni permutazione finitaria si può scrivere come prodotto di trasposizioni, possiamo supporre che sia $\sigma = \alpha_1 \cdots \alpha_k$ e $\tau = \beta_1 \cdots \beta_m$, con α_i e β_j trasposizioni per ogni $i = 1, \ldots, k$ e $j = 1, \ldots, m$. Adesso, per quanto visto precedentemente, si ha $f(\sigma) = sgn(\sigma) = (-1)^k$ e $f(\tau) = sgn(\tau) = (-1)^m$. Il prodotto di σ e τ sarà dato da $k + m$ trasposizioni e precisamente sarà $\sigma \cdot \tau = \alpha_1 \cdots \alpha_k \cdot \beta_1 \cdots \beta_m$. Ma allora

$$f(\sigma \cdot \tau) = sgn(\sigma \cdot \tau) = (-1)^{k+m} = (-1)^k (-1)^m = f(\sigma) \cdot f(\tau).$$

Ne segue che f è omomorfismo di gruppi.
Per quanto concerne la suriettività, siano x_1, x_2 due elementi distinti di X; allora $-1 = f((x_1\ x_2))$ e $1 = f(id)$. □

Definizione 1.18. Denotiamo con $\mathrm{Alt}(X)$ il nucleo dell'omomorfismo definito nella proposizione precedente, ovvero $\mathrm{Alt}(X) = \{\sigma \in \mathrm{FSym}(X) \mid \sigma \text{ è pari}\}$. Per le proprietà del nucleo di un omomorfismo, $\mathrm{Alt}(X)$ è un sottogruppo normale di $\mathrm{FSym}(X)$, detto *gruppo alterno*. Se X è finito di ordine n, $\mathrm{Alt}(X)$ si denota con A_n.

Osservazione 1.12. Dal primo teorema di omomorfismo di gruppi segue che $\mathrm{FSym}(X)/\mathrm{Alt}(X)$ è isomorfo a $\{+1, -1\}$ e quindi $|\mathrm{FSym}(X)/\mathrm{Alt}(X)| = 2$.

Osservazione 1.13. Si osserva facilmente che $\mathrm{Alt}(X)$ è un sottogruppo normale anche di $\mathrm{Sym}(X)$. Questo perché per ogni $\pi \in \mathrm{Sym}(X)$ e per ogni $\sigma \in \mathrm{Alt}(X)$, le permutazioni $\pi\sigma\pi^{-1}$ e σ sono coniugate in $\mathrm{Sym}(X)$, dunque, per quanto visto nel Teorema 1.9, hanno lo stesso tipo ciclico e questo, in particolare, implica che hanno anche la stessa segnatura. Ne segue che $\pi\sigma\pi^{-1}$ è una permutazione pari.

1.4 Semplicità del gruppo alterno

Definizione 1.19. Un gruppo G non banale si dice *semplice* se non ha sottogruppi normali propri.

Esempio 1.5. Ogni gruppo finito di ordine primo è semplice. Infatti, dal teorema di Lagrange segue che un tale gruppo non può avere sottogruppi propri.

Riportiamo adesso due risultati che saranno utilizzati per dimostrare la semplicità del gruppo alterno A_n nel caso finito.

Lemma 1.13. *Sia X un insieme. Allora* $\mathrm{Alt}(X)$ *è il gruppo generato dai* 3*-cicli.*

Dimostrazione. Per definizione di gruppo alterno, gli elementi di $\mathrm{Alt}(X)$ sono i prodotti di un numero (finito) pari di trasposizioni, dunque $\mathrm{Alt}(X)$ è generato dagli elementi di $\mathrm{Sym}(X)$ che si esprimono come prodotto di due trasposizioni. Quindi, tenenedo presente che i 3-cicli appartengono ad $\mathrm{Alt}(X)$, basterà verificare che il prodotto di una qualunque coppia di trasposizioni τ_1, τ_2 è anche prodotto di 3-cicli. Esaminiamo separatamente 3 diversi casi:

- se $\tau_1 = \tau_2$ allora $\tau_1\tau_2 = id$, dunque la tesi è verificata;
- se $\tau_1 \neq \tau_2$ e $\mathrm{supp}(\tau_1) \cap \mathrm{supp}(\tau_2) \neq \varnothing$, possiamo supporre esistano elementi $a, b, c \in X$, a due a due distinti, tali che $\tau_1 = (a\ b)$ e $\tau_2 = (a\ c)$ ed è semplice verificare che $\tau_1\tau_2 = (a\ c\ b)$;
- se $\tau_1 \neq \tau_2$ e $\mathrm{supp}(\tau_1) \cap \mathrm{supp}(\tau_2) = \varnothing$, possiamo supporre che esistano elementi $a, b, c, d \in X$ a due a due distinti, tali che $\tau_1 = (a\ b)$ e $\tau_2 = (c\ d)$ e anche in questo caso è semplice verificare che $\tau_1\tau_2 = (c\ b\ a)(d\ a\ c)$.

□

Lemma 1.14. *Sia $n \geq 5$. Comunque presi due* 3*-cicli di A_n, essi sono coniugati in A_n.*

Dimostrazione. Siano σ e τ due cicli di lunghezza 3 in A_n. Poiché A_n è sottogruppo normale di S_n, si ha $\sigma = \pi\tau\pi^{-1}$ per qualche $\pi \in S_n$. Se $\pi \in A_n$ abbiamo finito. Altrimenti, poiché $n \geq 5$, esiste una trasposizione $\gamma \in S_n$ disgiunta da σ. Poiché γ e π sono entrambe dispari, ne segue che $\gamma\pi \in A_n$ e $\sigma = \gamma\sigma\gamma^{-1} = \gamma\pi\tau\pi^{-1}\gamma^{-1}$, cioè σ e τ sono coniugate in A_n. □

Siamo adesso pronti per dimostrare il seguente famoso teorema, dovuto nel caso finito a Galois.

Teorema 1.15. *Sia X un insieme. Se $|X| \geq 5$ oppure $|X| = 3$ allora* $\mathrm{Alt}(X)$ *è semplice.*

Dimostrazione. Riportiamo dapprima la dimostrazione del caso in cui X sia finito di cardinalità n. Allora $\mathrm{Alt}(X) \simeq A_n$.
Il caso $n = 3$ è banale, poiché A_3 è ciclico di ordine 3, dunque è semplice.
Ora, sia $n \geq 5$ e sia $N \trianglelefteq A_n$, $N \neq \{id\}$. Bisogna dimostrare che $N = A_n$, ovvero che N contiene tutti i cicli di lunghezza 3 (che, come abbiamo già visto nel Lemma 1.13, costituiscono un insieme di generatori di A_n). Un modo standard di provarlo è il seguente: bisogna mostrare che N contiene almeno un ciclo di lunghezza 3; dopodiché, dal Lemma 1.14 e dalla normalità di N, seguirà che N contiene tutti i 3-cicli di A_n e, dunque, $N = A_n$.
Per mostrare che N contiene un 3-ciclo, consideriamo una permutazione non identica $\sigma \in N$; se σ non è un 3-ciclo, possiamo costruire un'altra permutazione $\sigma' \in N$, $\sigma' \neq id$, che fissa un numero maggiore di elementi rispetto a σ. Se σ' non è un 3-ciclo, possiamo applicare ad essa la stessa costruzione. Dopo un numero finito di passi, arriviamo ad ottenere un 3-ciclo.
Supponiamo dunque che $\sigma \in N$, $\sigma \neq id$, non sia un 3-ciclo. Bisogna considerare due casi:

(i) supponiamo che σ sia prodotto di trasposizioni disgiunte (almeno due, poiché σ è non banale e pari), $\sigma = (i\ j)(r\ s)\cdots$. Poiché $n \geq 5$, esiste un elemento k distinto da i, j, r, s. Sia $\tau = (i\ j)(r\ k)$ e poniamo $\sigma' = \sigma^{-1}\tau\sigma\tau^{-1}$. Poiché N è sottogruppo normale di A_n e τ è pari, ne segue che $\sigma' \in N$. Scriviamo $\sigma = (i\ j)(r\ s)\gamma$, con γ disgiunta da $(i\ j)$ e $(r\ s)$. Allora γ commuta con $(i\ j)$ e $(r\ s)$, che a loro volta commutano tra loro, dunque abbiamo:

$$\sigma' = ((i\ j)(r\ s)\,\gamma\,(i\ j)(r\ k))^2 = ((r\ s)\,\gamma\,(r\ k))^2.$$

Poiché $\sigma'(k) = r$, σ' è non banale. Inoltre, notiamo che σ' fissa i, j e ogni elemento fissato da σ, con l'unica possibile eccezione di k. In particolare, da questo segue che σ' fissa almeno un elemento in più rispetto a σ.

(ii) Adesso consideriamo la decomposizione in cicli disgiunti di σ e supponiamo che in essa compaia un ciclo di lunghezza almeno 3. Scriviamo $\sigma = (i\ j\ k \cdots)\gamma$, con γ disgiunta da $(i\ j\ k \cdots)$. Poiché σ non è un 3-ciclo ed è pari, σ muove almeno 5 elementi. Dunque, esistono elementi r ed s distinti da i, j, k che non sono fissati da σ. Sia $\tau = (k\ r\ s)$. Come nel caso precedente, sia $\sigma' = \sigma^{-1}\tau\sigma\tau^{-1} \in N$. Poiché τ fissa i e j così come ogni elemento fissato da σ, σ' fissa i ed ogni elemento fissato da σ. Dunque, σ' fissa un elemento in più rispetto a σ. Infine, poiché $\sigma'(j) = \sigma^{-1}(r) \neq j$, segue che σ' non è l'identità.

Abbiamo dimostrato così quanto precedentemente affermato e concluso la dimostrazione della semplicità di A_n nel caso finito.
Supponiamo ora che X sia infinito. Sia N sottogruppo normale non banale di $\mathrm{Alt}(X)$; anche in questo caso dobbiamo provare che $N = \mathrm{Alt}(X)$. Indichiamo con $\mathcal{F}$ l'insieme delle parti finite di X di cardinalità maggiore di 4. Per ogni $Y \in \mathcal{F}(X)$ poniamo $A_Y = \mathrm{St}_{\mathrm{Alt}(X)}(X \setminus Y)$. L'isomorfismo da $\mathrm{St}_{\mathrm{Sym}(X)}(X \setminus Y)$ a $\mathrm{Sym}(Y)$, introdotto nella Proposizione 1.4, induce un isomorfismo da A_Y a $\mathrm{Alt}(Y)$, dunque, poiché ogni $Y \in \mathcal{F}$ ha cardinalità finita, A_Y è semplice per ogni $Y \in \mathcal{F}$. Inoltre, si ha $\mathrm{Alt}(X) = \bigcup_{Y\in\mathcal{F}} A_Y$. Essendo $N \neq id$, esiste $Y_0 \in \mathcal{F}$ tale che $N \cap A_{Y_0} \neq id$. Per ogni $Y \in \mathcal{F}$ si ha, ovviamente, $A_{Y\cup Y_0} \geq A_{Y_0}$, quindi $N \cap A_{Y\cup Y_0} \neq id$. Poiché $N \cap A_{Y\cup Y_0} \lhd A_{Y\cup Y_0}$ e $A_{Y\cup Y_0}$ è semplice, allora $N \cap A_{Y\cup Y_0} = A_{Y\cup Y_0}$, cioè $N \supseteq A_{Y\cup Y_0}$; inoltre $A_{Y\cup Y_0} \geq A_Y$ e quindi $N \supseteq A_Y$. Ma allora $N \supseteq \bigcup_{Y\in\mathcal{F}} A_Y = \mathrm{Alt}(X)$, cioè $N = \mathrm{Alt}(X)$, come volevamo dimostrare. □

Il risultato ottenuto nel teorema precedente si completa osservando che, nei casi indicati nell'enunciato, il gruppo alterno è il minimo sottogruppo normale non identico di $\mathrm{Sym}(X)$.

Concludiamo questo capitolo riportando un caso particolare di un teorema del 1934 dovuto al matematico tedesco R. Baer:

Teorema 1.16. *Sia X un insieme. Se $|X| = 3$ oppure $|X| \geq 5$, allora* $\mathrm{Alt}(X)$ *è sottogruppo normale minimale sia di* $\mathrm{Sym}(X)$ *che di* $\mathrm{FSym}(X)$ *ed, in particolare, è l'unico sottogruppo normale non banale di* $\mathrm{FSym}(X)$*,*

Dimostrazione. Poiché $\mathrm{Alt}(X)$ è semplice, allora è sottogruppo normale minimale sia in $\mathrm{Sym}(X)$ che in $\mathrm{FSym}(X)$. Inoltre, $|\mathrm{FSym}(X) : \mathrm{Alt}(X)| = 2$ e quindi $\mathrm{Alt}(X)$ è un sottogruppo massimale di $\mathrm{FSym}(X)$. Allora, se $\{id\} \neq N \triangleleft \mathrm{FSym}(X)$, da $\mathrm{Alt}(X) \leq N$ segue $N = \mathrm{Alt}(X)$ oppure $N = \mathrm{FSym}(X)$. □

Osservazione 1.14. Osserviamo che, in particolare, $\mathrm{Alt}(X)$ è l'unico sottogruppo normale minimale in $\mathrm{Sym}(X)$. Ciò si traduce dicendo che $\mathrm{Alt}(X)$ è il *monolite* di $\mathrm{Sym}(X)$.

Osservazione 1.15. Ovviamente, il teorema 1.16 afferma, nel caso in cui X sia finito, che A_n è l'unico sottogruppo normale non banale di S_n, con le sole eccezioni dei casi $n \leq 2$, per i quali $A_n = \{id\}$, ed $n = 4$ perché, com'è noto, i sottogruppi normali di S_4 sono due: A_4 e il gruppo di Klein.

Capitolo 2

Commutatori e gruppo derivato

2.1 Prime definizioni e proprietà

In questo capitolo introduciamo un sottogruppo che si può considerare una misura di quanto un gruppo si discosti dall'essere abeliano.

Definizione 2.1. Sia G un gruppo e siano $a, b \in G$. L'elemento $aba^{-1}b^{-1}$ si chiama *commutatore* di a e b (in questo ordine) e si denota con $[a, b]$.

Definizione 2.2. Sia G un gruppo. Definiamo il gruppo *derivato* (o gruppo commutatore) di G come il sottogruppo generato dall'insieme di tutti i commutatori di G, ovvero $[G, G] = \langle [a, b] \mid a, b \in G \rangle$. Indicheremo con G' il derivato di G.

Osserviamo che il prodotto di due commutatori non è necessariamente un commutatore, motivo per cui il sottogruppo derivato di un dato gruppo non può essere definito come l'insieme di tutti i commutatori, ma solo come il gruppo generato da essi.

Osservazione 2.1. È chiaro che due elementi permutano se e solo se il loro commutatore è l'unità, e quindi un gruppo G è abeliano se e solo se $G' = \{e\}$.

Definizione 2.3. Sia G un gruppo e sia H un sottogruppo di G. H si dice *caratteristico* se $\phi(H) = H$ per ogni automorfismo ϕ di G.

Osservazione 2.2. Ogni sottogruppo caratteristico di un gruppo G è anche normale. Questo perché un sottogruppo è normale in G se e solo se è fissato da ogni automorfismo interno di G, ovvero da ogni automorfismo indotto da un elemento $g \in G$ tramite coniugio.

Proposizione 2.1. *Sia G un gruppo e sia G' il suo derivato. Allora valgono le seguenti affermazioni:*

1. *G' è caratteristico in G, e quindi è anche normale in G;*

2. *il quoziente G/G' è abeliano;*

3. *se $N \triangleleft G$ e G/N è abeliano, allora $G' \subseteq N$.*

Dimostrazione. 1. Sia ϕ un automorfismo di G e siano $a, b \in G$. Allora $\phi([a,b]) = \phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = [\phi(a), \phi(b)]$; un automorfismo di G porta dunque commutatori in commutatori e perciò $\phi(G') \subseteq G'$. D'altra parte, $[a,b] = \phi([\phi^{-1}(a), \phi^{-1}(b)])$, e quindi $G' \subseteq \phi(G')$, il che prova l'uguaglianza.

2. Per il punto (1) G' è, in particolare, normale in G, per cui ne possiamo considerare il quoziente. Se $a\,G', b\,G' \in G/G'$, con $a, b \in G$, si ha:

$$a\,G'\,b\,G' = ab\,G' = ba[a^{-1}, b^{-1}]\,G' = ba\,G' = b\,G'\,a\,G',$$

dove la terza uguaglianza segue dal fatto che $[a^{-1}, b^{-1}] \in G'$.

3. Sia $N \triangleleft G$ e supponiamo che G/N sia abeliano. Se $aN\,bN = bN\,aN$, per ogni $a, b \in N$, allora $ab\,N = ba\,N$ e $a^{-1}b^{-1}ab\,N = N$, da cui $[a^{-1}, b^{-1}] \in N$, ovvero $G' \subseteq N$.

□

Il punto (3) del teorema precedente si esprime anche dicendo che G' è il più piccolo sottogruppo di G rispetto al quale il quoziente è abeliano.

2.2 Commutatori e sottogruppo derivato del gruppo simmetrico

Nel suo articolo [6] Oystein Ore mostra due importanti risultati strettamente correlati. Il primo riguarda il gruppo alterno A_n su un insieme finito e afferma che ogni suo elemento è un commutatore di elementi di S_n. Il secondo risultato, al quale Ore ha dedicato più di metà dell'articolo, è più complesso e afferma che ogni elemento del gruppo simmetrico su un insieme X numerabile è un commutatore.

Teorema 2.2. *Per ogni n, A_n è il derivato di S_n.*

Dimostrazione. Per $n \leq 2$ non c'è nulla da provare. Supponiamo dunque $n \geq 3$. Poiché S_n/A_n è un gruppo con due elementi, è abeliano. Allora, essendo A_n normale in S_n, dal punto (3) del teorema precedente segue che $[S_n, S_n] \subseteq A_n$.
Adesso, siano i, j, k tre elementi diversi nell'insieme $\{1, 2, \ldots, n\}$. Allora abbiamo che:

$$[(i\ j), (i\ k)] = (i\ j)(i\ k)(i\ j)(i\ k) = (i\ j\ k).$$

Ma A_n è generato dai 3-cicli, per cui $[S_n, S_n] \supseteq A_n$. □

Osservazione 2.3. Un commutatore è un elemento ottenuto moltiplicando un certo elemento di un gruppo per il coniugato del suo inverso: $a \cdot ba^{-1}b^{-1}$. Dunque, poiché sappiamo già che in un gruppo simmetrico ogni elemento è coniugato al suo inverso, ne segue che in un gruppo simmetrico un commutatore può essere descritto come il prodotto di due elementi appartenenti alla stessa classe di coniugio[1].

Dimostriamo quanto appena osservato nel seguente:

Lemma 2.3. *Sia X un insieme qualunque. Una permutazione $\sigma \in \mathrm{Sym}(X)$ è un commutatore se e solo se si può scrivere come prodotto $\sigma = \tau\varrho$ di due permutazioni coniugate τ e ϱ in* $\mathrm{Sym}(X)$.

[1] La *classe di coniugio* di un elemento altro non è che l'orbita di quello stesso elemento rispetto all'azione data dal coniugio.

Dimostrazione. Supponiamo dapprima che τ e ϱ siano coniugate in $\mathrm{Sym}(X)$. Allora esiste $\alpha \in \mathrm{Sym}(X)$ tale che $\varrho = \alpha\tau\alpha^{-1}$, dunque $\tau\varrho = \tau\alpha\tau\alpha^{-1}$. Dopodiché, dato che l'inversa di una permutazione si ottiene invertendo l'ordine degli elementi in ogni ciclo della decomposizione, anche τ e τ^{-1} sono coniugate, dunque esiste $\beta \in \mathrm{Sym}(X)$ tale che $\tau = \beta\tau^{-1}\beta^{-1}$. Ma allora

$$\sigma = \tau\varrho = \tau\alpha\tau\alpha^{-1} = \tau\alpha\beta\tau^{-1}\beta^{-1}\alpha^{-1} = [\tau, \delta],$$

dove abbiamo posto $\delta = \alpha\beta$.
Adesso, supponiamo che σ sia un commutatore. Esistono allora $\alpha, \beta \in \mathrm{Sym}(X)$ tale che $\sigma = [\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$. Notiamo subito che $\beta\alpha^{-1}\beta^{-1}$ è la coniugata di α^{-1} tramite β e inoltre, poiché α e α^{-1} sono coniugate in $\mathrm{Sym}(X)$, esiste $\tau \in \mathrm{Sym}(X)$ tale che $\alpha^{-1} = \tau\alpha\tau^{-1}$. Dunque $\beta\alpha^{-1}\beta^{-1} = \beta\tau\alpha\tau^{-1}\beta^{-1} = \delta\alpha\delta^{-1}$, dove abbiamo posto $\delta = \beta\tau$. Abbiamo mostrato, quindi, che $\sigma = \alpha \cdot \delta\alpha\delta^{-1}$ è il prodotto di due permutazioni coniugate in $\mathrm{Sym}(X)$. □

Adesso dimostriamo un fatto che sarà fondamentale per il resto dell'elaborato e cioè che, sotto opportune ipotesi, il prodotto di commutatori è uguale al commutatore dei prodotti.

Osservazione 2.4. Siano X un insieme non vuoto, I un insieme arbitrario di indici e $\{Y_i\}_{i\in I} \subseteq X$ una famiglia di sottoinsiemi di X con la proprietà che $Y_j \cap Y_k = \varnothing$, per ogni $j \neq h$. Siano date poi delle permutazioni $\alpha_i, \beta_i \in \mathrm{Sym}(X)$, per ogni $i \in I$, tali che $\mathrm{supp}(\alpha_i), \mathrm{supp}(\beta_i) \subseteq Y_i$, per ogni $i \in I$. Allora, sono ben definite le seguenti permutazioni di X:

$$\alpha = \prod_{i\in I} \alpha_i \qquad \text{e} \qquad \beta = \prod_{i\in I} \beta_i.$$

Proposizione 2.4. *Nelle notazioni dell'osservazione precedente, si ha*

$$[\alpha, \beta] = \prod_{i\in I} [\alpha_i, \beta_i].$$

Dimostrazione. Innanzitutto, per ogni $i \in I$ si ha che $[\alpha_i, \beta_i] \in \mathrm{Sym}(X)$. Dopodiché, osserviamo che per ogni $i \in I$ vale: $\mathrm{supp}([\alpha_i, \beta_i]) = \mathrm{supp}(\alpha_i\beta_i\alpha_i^{-1}\beta_i^{-1}) \subseteq$

$\text{supp}(\alpha_i) \cup \text{supp}(\beta_i) \subseteq Y_i$, per come sono state scelte le permutazioni α_i e β_i. Questa osservazione, in particolare, dice che $\text{supp}([\alpha_i, \beta_i]) \cap \text{supp}([\alpha_j, \beta_j]) = \varnothing$, per ogni $i \neq j$. Allora, da queste premesse segue che, per ogni $x \in X$, possiamo definire il commutatore $[\alpha, \beta]$ nel seguente modo:

$$\begin{cases} [\alpha, \beta](x) = [\alpha, \beta]|_{Y_i}(x) & \text{se } x \in Y_i \\ [\alpha, \beta](x) = x & \text{altrimenti,} \end{cases}$$

dove, per definizione di restrizione di una funzione, $[\alpha, \beta]|_{Y_i} = [\alpha_i, \beta_i]$, per ogni $i \in I$. In conclusione, si ha:

$$[\prod_{i \in I} \alpha_i, \prod_{i \in I} \beta_i] = [\alpha, \beta] = \prod_{i \in I} [\alpha_i, \beta_i]$$

e la definizione risulta ben posta. □

Nel Teorema 2.2 abbiamo mostrato che il gruppo alterno è il gruppo commutatore del gruppo simmetrico su un insieme finito. Adesso mostriamo qualcosa di più forte:

Teorema 2.5. *Ogni elemento del gruppo alterno A_n è un commutatore di elementi di S_n.*

Dimostrazione. Sia $\sigma \in A_n$. La decomposizione in cicli disgiunti di σ può contenere cicli di lunghezza dispari, che hanno segnatura $+1$, e un numero sempre pari di cicli di lunghezza pari, che invece hanno segnatura -1. Per mostrare il teorema, dunque, basta mostrare che ogni ciclo di lunghezza dispari e ogni prodotto di due cicli di lunghezza pari sono commutatori.
Sia dunque $\sigma \in A_n$ un ciclo di lunghezza dispari, per semplificare la notazione usiamo gli interi positivi per denotare gli elementi dell'insieme su cui agisce A_n. Possiamo scrivere $\sigma = (1\ 2 \cdots 2i+1)$, dove $i \in \mathbb{Z}$, $i \geq 1$. È facile notare che:

$$\sigma = (1\ 2 \cdots i+1) \cdot (i+1\ i+2 \cdots 2i+1). \tag{2.1}$$

Poiché abbiamo scritto σ come prodotto di due cicli aventi stessa lunghezza pari a $i+1$, per il Lemma 2.3 concludiamo che σ è un commutatore.

Consideriamo adesso una coppia di cicli di lunghezza pari, $\alpha = (1\ 2 \cdots 2i)$ e $\beta = (2i+1\ \ 2i+2 \cdots 2i+2j)$, dove $i, j \in \mathbb{Z}$, $i, j \geq 1$. Supponiamo inoltre che sia $j \geq i$. Allora possiamo scrivere il loro prodotto, e si verifica facilmente facendo i conti, nel seguente modo:

$$\alpha\beta = (1\ 2 \cdots 2i\ \ 2i+1 \cdots i+j+1) \cdot (2i\ \ i+j+1\ \ i+j+2 \cdots 2i+2j). \quad (2.2)$$

Dunque abbiamo scritto $\alpha\beta$ come il prodotto di due cicli aventi stessa lunghezza pari a $i+j+1$. Anche in questo caso, per il Lemma 2.3 concludiamo che il prodotto di due cicli di lunghezza pari è un commutatore. □

2.3 Commutatori nel gruppo simmetrico infinito

In questa sezione dimostriamo che ogni permutazione del gruppo simmetrico su un insieme infinito è un commutatore. Nella dimostrazione verrà condotta un'analisi caso per caso, dove i diversi casi sono date da tutte le possibili decomposizioni cicliche di una permutazione. Riportiamo prima tutti i risultati preliminari utili per tale dimostrazione.

Lemma 2.6. *Sia X un insieme infinito. Allora ogni ciclo infinito $\sigma \in \mathrm{Sym}(X)$ è un commutatore di cicli di $\mathrm{Sym}(X)$ aventi supporto incluso nel supporto di σ.*

Dimostrazione. Per mostrare il teorema è sufficiente provare l'esistenza di un singolo ciclo infinito che soddisfa quanto richiesto nell'enunciato. Rappresentiamo gli elementi dell'insieme X con un doppio indice: $X = \{a_{i,j} \mid i \in \mathbb{Z}, j \in \mathbb{N}\}$. Notiamo che X è un insieme numerabile e che gli elementi $a_{i,j}$ sono tutti distinti tra loro. Con questa notazione, costruiamo i seguenti cicli aventi supporto numerabile:

$$\sigma_j = (\cdots\ a_{-1,j}\ \ a_{0,j}\ \ a_{1,j}\ \cdots), \qquad \text{per ogni } j \in \mathbb{N}. \quad (2.3)$$

In seguito, poniamo

$$\sigma = \prod_{j\geq 0} \sigma_j, \tag{2.4}$$

dove i cicli σ_j sono a due a due disgiunti, il che ci garantisce che il prodotto sia ben definito. Geometricamente, se interpretiamo gli elementi $a_{i,j}$ come punti di un reticolo nel semipiano $y \geq 0$ del piano cartesiano, ogni ciclo σ_j può essere visualizzato come $\mathbb{Z} \times \{j\}$. Allora, se identifichiamo l'elemento $a_{i,j} \in X$ col punto del reticolo di coordinate (i, j), la permutazione σ agisce su X mandando un punto di coordinate (i, j) nel punto di coordinate $(i+1, j)$. In altre parole, le rette orizzontali del reticolo sono σ-invarianti.
Adesso costruiamo altri cicli, che denotiamo con τ_i, definiti come segue:

$$\begin{aligned}
\tau_1 &= (\cdots\ a_{-1,2}\ \ a_{-1,1}\ \ a_{-1,0}\ \ a_{1,0}\ \ a_{1,1}\ \ a_{1,2}\ \cdots), \\
\tau_2 &= (\cdots\ a_{-2,2}\ \ a_{-2,1}\ \ a_{-2,0}\ \ a_{0,0}\ \ a_{2,0}\ \ a_{2,1}\ \ a_{2,2}\ \cdots), \\
&\ \ \vdots \\
\tau_i &= (\cdots\ a_{-i,2}\ \ a_{-i,1}\ \ a_{-i,0}\ \ a_{0,i-2}\ \ a_{i,0}\ \ a_{i,1}\ \ a_{i,2}\ \cdots).
\end{aligned} \tag{2.5}$$

Notiamo che i cicli τ_i sono a due a due disgiunti, per cui ha senso la seguente scrittura:

$$\tau = \prod_{i\geq 1} \tau_i. \tag{2.6}$$

Anche in questo caso possiamo descrivere geometricamente i cicli τ_i: ogni ciclo τ_i muove ogni punto del reticolo appartenente alla retta verticale $x = -i$ di un passo verso il basso; quando un punto raggiunge l'asse x viene mandato nel punto di coordinate $(0, i-2)$, corrispondente all'elemento $a_{0,i-2}$, e da lì viene mandato nel punto di coordinate $(i, 0)$ per poi risalire verso l'alto nella i-esima colonna. Osserviamo che il ciclo τ_1 è l'unico lievemente irregolare, poiché non contiene punti del reticolo sull'asse y. Dunque, il punto di coordinate $(-1, 0)$ viene mandato direttamente nel punto di coordinate $(1, 0)$.
Da questa costruzione segue che il supporto di entrambe le permutazioni σ e τ coincide con l'insieme X. Dunque, poiché nella decomposizione in cicli disgiunti di σ e τ ogni ciclo ha supporto di cardinalità numerabile ed entrambe

le permutazioni non fissano alcun elemento di X, ne segue che σ e τ hanno lo stesso tipo ciclico e, dunque, sono coniugate. Allora, per quanto affermato nel Lemma 2.3, la permutazione $\pi = \tau\sigma^{-1}$ è un commutatore. La dimostrazione del teorema si conclude osservando che π è effettivamente un ciclo infinito il cui supporto coincide con l'insieme X. In particolare si verifica che π è il seguente ciclo:

$$\begin{aligned}\pi = (&\cdots\cdots\cdots\cdots\cdots\cdots\\ &a_{0,4}\ \ a_{-1,3}\ \ a_{-2,2}\ \ a_{-3,1}\ \ a_{-4,0}\\ &\qquad a_{0,3}\ \ a_{-1,2}\ \ a_{-2,1}\ \ a_{-3,0}\\ &\qquad\qquad a_{0,2}\ \ a_{-1,1}\ \ a_{-2,0}\\ &\qquad\qquad\qquad a_{0,1}\ \ a_{-1,0}\\ &\qquad\qquad\qquad\qquad a_{0,0}\\ &\qquad\qquad\qquad\qquad a_{1,0}\\ &\qquad\qquad\qquad\quad a_{2,0}\ \ a_{1,1}\\ &\qquad\qquad\qquad a_{3,0}\ \ a_{2,1}\ \ a_{1,2}\\ &\cdots\cdots\cdots\cdots\cdots\cdots).\end{aligned} \tag{2.7}$$

Come si può vedere, π rappresenta una progressione diagonale attraverso i punti del reticolo del semipiano superiore. □

Lemma 2.7. *Sia X un insieme infinito e siano $\alpha, \beta \in \mathrm{Sym}(X)$ due cicli disgiunti. Supponiamo che α abbia supporto infinito, mentre β abbia supporto finito. Allora il prodotto $\alpha\beta$ è il commutatore di due permutazioni di X i cui supporti sono contenuti in* $\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)$.

Dimostrazione. Per comodità, identifichiamo X con l'insieme dei numeri interi $\mathbb{Z}$. Senza perdita di generalità, possiamo supporre che:

$$\alpha = (\cdots -1\ \ 0\ \ a+1\ \ a+2\cdots) \text{ e } \beta = (1\ \ 2\cdots a),$$

dove $a \in \mathbb{Z}$, $a \geq 2$. È facile verificare che:

$$\alpha\beta = (\cdots -2\ \ -1\ \ 0\ \ 1\ \ 2\cdots)\cdot(0\ \ a).$$

Adesso consideriamo il ciclo π descritto in (2.7), costruito nella dimostrazione del Teorema 2.6, e osserviamo che esistono $a_{i,j}, a_{k,l} \in \mathrm{supp}(\pi)$ tali che $j \neq l$ e $a_{i,j} = \pi^a(a_{k,l})$. Notiamo che possiamo sempre trovare due elementi che soddisfino questa condizione. Poniamo $\chi = (a_{i,j} \;\; a_{k,l})$ e moltiplichiamo π a destra per χ. Poiché avevamo scritto $\pi = \tau\sigma^{-1}$, otteniamo:

$$\pi\chi = \tau\sigma^{-1}\chi = \tau(\chi\sigma)^{-1},$$

dove abbiamo usato che $\chi = \chi^{-1}$. Studiamo il prodotto $\chi\sigma$, ricordando che avevamo scritto $\sigma = \prod_{n\geq 0}\sigma_n$, con i σ_n cicli infiniti a due a due disgiunti, notando che $a_{i,j} \in \mathrm{supp}(\sigma_j)$ e $a_{k,l} \in \mathrm{supp}(\sigma_l)$. Allora, poiché i cicli σ_n commutano e utilizzando la proprietà associativa del prodotto, segue che:

$$\chi\sigma = \chi\prod_{n\geq 0}\sigma_n = (\chi\sigma_j\sigma_l)\prod_{n\neq j,l}\sigma_n.$$

Si verifica successivamente che:

$$\chi\sigma_j\sigma_l = (\cdots\; a_{i-2,j} \;\; a_{i-1,j} \;\; a_{k,l} \;\; a_{k+1,l}\;\cdots)(\cdots\; a_{k-2,l} \;\; a_{k-1,l} \;\; a_{i,j} \;\; a_{i+1,j}\;\cdots),$$

ovvero $\chi\sigma_j\sigma_l$ è il prodotto di due cicli infiniti disgiunti. Dunque $\chi\sigma$ è ancora un prodotto infinito di cicli infiniti a due a due disgiunti, per cui $\chi\sigma$ e $\tau = \prod_{i\in I}\tau_i$ sono permutazioni coniugate. Da questo segue che $\pi\chi$ è un commutatore. Adesso, poiché gli elementi $a_{i,j}$ e $a_{k,l}$ sono stati scelti appositamente per far sì che il prodotto $\pi\chi$ avesse la stessa struttura ciclica del prodotto $\alpha\beta$, ne segue che anche $\alpha\beta$ è un commutatore. □

Lemma 2.8. *Sia X un insieme infinito e sia $\sigma \in \mathrm{Sym}(X)$. Se la decomposizione ciclica di σ è data da infiniti cicli non banali di ordine finito allora σ è il commutatore di due permutazioni di X i cui supporti sono contenuti in* $\mathrm{supp}(\sigma)$.

Dimostrazione. Scriviamo σ nel seguente modo:

$$\sigma = \prod_{j=1}^{\infty}\sigma_j = \cdots\;(a_1\;\cdots\;a_{i_1})(b_1\;\cdots\;b_{i_2})(c_1\;\cdots\;c_{i_3})\;\cdots, \tag{2.8}$$

con $i_k \geq 2$ per ogni $k \in \mathbb{Z}$ e dove i $\sigma_j \in \mathrm{FSym}(X)$ sono a due a due disgiunti. Distinguiamo due casi:

- **Caso 1**. Supponiamo che nella decomposizione ciclica (2.8) compaia un numero arbitrario di cicli pari e un numero infinito di cicli dispari. Allora, per quanto visto nel Teorema 2.5, questi ultimi possono essere accoppiati in modo tale che il prodotto di due di loro sia un commutatore. Inoltre, nello stesso teorema abbiamo anche dimostrato che i cicli pari sono commutatori. Ne segue che σ è prodotto infinito di commutatori σ_i del tipo $\sigma_i = [\alpha_i, \beta_i]$ con $\mathrm{supp}(\alpha_i), \mathrm{supp}(\beta_i) \subseteq \mathrm{supp}(\sigma_i)$. La dimostrazione si conclude osservando che poiché i cicli σ_i sono a due a due disgiunti, dalla Proposizione 2.4 segue che σ è un commutatore.

- **Caso 2**. Supponiamo adesso che il numero di cicli dispari che compare nella decomposizione ciclica di σ sia finito. Sia adesso η la permutazione definita nel modo seguente:

$$\eta = (\cdots a_1\ a_{i_1}\ b_1\ b_{i_2}\ c_1\ c_{i_3} \cdots) \cdots (a_2) \cdots (a_{i_1-1})(b_2) \cdots (b_{i_2-1})(c_2) \cdots .$$

  Dunque, η è formata da un unico ciclo infinito e da un insieme numerabile di elementi fissati. Sia $\vartheta = \sigma\eta$, allora si verifica che:

$$\vartheta = (\cdots a_2\ \ a_3 \cdots a_{i_1}\ \ b_2 \cdots b_{i_2}\ \ c_2 \cdots c_{i_3} \cdots) \cdots (a_1)(b_1)(c_1) \cdots .$$

  Osserviamo che anche ϑ è composta da un unico ciclo infinito e da un insieme numerabile di punti fissati. Ne segue che ϑ e η hanno la stessa struttura ciclica, dunque $\sigma = \vartheta\eta^{-1}$ è un commutatore.

□

Lemma 2.9. *Sia X un insieme infinito. Allora ogni permutazione finitaria $\sigma \in \mathrm{FSym}(X)$ è un commutatore.*

Dimostrazione. È chiaro che l'asserto non è vero nel caso in cui si consideri un insieme finito dato dal supporto della permutazione. Per poter scrivere una qualunque permutazione finitaria come un commutatore, bisogna che l'insieme sia numerabile. La dimostrazione è suddivisa in due passi: nel primo mostreremo che un qualunque ciclo di lunghezza finita è un commutatore. Dopodiché,

nel secondo passo, la dimostrazione verrà estesa ad una qualunque permutazione finitaria, utilizzando il fatto che quest'ultima può essere sempre scritta come prodotto finito di cicli finiti a due a due disgiunti.
Supponiamo, dunque, che sia $\sigma = (a_1,\ a_2, \cdots, a_i)$, con $i \geq 2$ e $a_j \in X$ per ogni $1 \leq j \leq i$. Adesso, consideriamo due sottoinsiemi infiniti Y_1, Y_2 di X, tale che $Y_1 \cap Y_2 = \varnothing$. Più precisamente, siano:

$$Y_1 = \{\cdots, a_{-2}, a_{-1}, a_0, a_1, \cdots, a_i, a_{i+1}, \cdots\} \text{ e } Y_2 = \{b_1, b_2, b_3, \cdots\}.$$

Consideriamo due permutazioni α e β sull'insieme $Y_1 \cup Y_2$, date da:

$$\alpha = (\cdots\ a_{-2}\ \ a_{-1}\ \ a_0\ \ a_1 \cdots a_i\ \ a_{i+1} \cdots)(b_1)(b_2)\cdots,$$

$$\beta = (\cdots\ a_{i+2}\ \ a_{i+1}\ \ a_1\ \ a_0\ \ a_{-1} \cdots)(a_2)(a_3)\cdots(a_i)(b_1)(b_2)\cdots.$$

In altre parole, entrambe le permutazioni sono costituite da un singolo ciclo infinito e da una quantità numerabile di elementi fissati. Inoltre, si verifica che $\sigma = \beta\alpha$. Dunque, poiché α e β sono chiaramente coniugate, ne segue che σ è un commutatore.
Adesso, supponiamo che la permutazione σ sia prodotto finito di cicli finiti: $\sigma = \sigma_1\sigma_2\cdots\sigma_m$. Per ogni ciclo σ_i, con $1 \leq i \leq m$, procediamo come nel punto precedente. Dunque consideriamo $2m$ sottoinsiemi infiniti di X a due a due disgiunti, che indichiamo con $Y_1^{(i)}$ e $Y_2^{(i)}$, costruiamo le permutazioni α_i e β_i e scriviamo $\sigma_i = \beta_i\alpha_i$. Sappiamo che, per ogni $1 \leq i \leq m$, i cicli α_i e β_i sono coniugati. Inoltre, ogni ciclo β_i è chiaramente coniugato al suo inverso β_i^{-1}. Dunque, poiché il coniugio è una relazione di equivalenza, segue che, per ogni $1 \leq i \leq m$, il ciclo α_i è coniugato al ciclo β_i^{-1}. Ovvero, per ogni $1 \leq i \leq m$, esiste $\eta_i \in \mathrm{Sym}(Y_1^{(i)} \cup Y_2^{(i)})$ tale che $\alpha_i = \eta_i\beta_i^{-1}\eta_i^{-1}$. Dunque, ogni ciclo σ_i si può scrivere come commutatore: $\sigma_i = \beta_i\alpha_i = \beta_i\eta_i\beta_i^{-1}\eta_i^{-1} = [\beta_i, \eta_i]$, dove $\mathrm{supp}(\beta_i), \mathrm{supp}(\eta_i) \subseteq Y_3^{(i)} = Y_1^{(i)} \cup Y_2^{(i)}$. A questo punto, abbiamo scritto σ come prodotto finito di commutatori. Il fatto che σ stesso sia un commutatore è assicurato dal fatto che i sottoinsiemi $Y_3^{(i)}$ sono a due a due disgiunti e in un insieme infinito è possibile trovare un numero finito arbitrario di sottoinsiemi numerabili a due a due disgiunti. □

Siamo adesso pronti per dimostrare quanto segue:

Teorema 2.10. *Sia X un insieme numerabile. Allora ogni $\sigma \in \mathrm{Sym}(X)$ è un commutatore.*

Dimostrazione. Sia $\sigma = \prod_{i\in I} \sigma_i$ la decomposizione di σ in prodotto di cicli disgiunti. Il teorema si dimostra analizzando tutte le possibili decomposizioni di σ che non sono state considerate nei quattro lemmi precedenti. L'idea di base è quella di raggruppare i cicli σ_i in modo da poter scrivere $\sigma = \prod_{j\in J} \widetilde{\sigma_j}$ come prodotto di permutazioni disgiunte, dove ciascuna $\widetilde{\sigma_j}$ è del tipo $\widetilde{\sigma_j}= [\alpha_j, \beta_j]$, con $\mathrm{supp}(\alpha_j), \mathrm{supp}(\beta_j) \subseteq \mathrm{supp}(\widetilde{\sigma_j})$, e concludere utilizzando la Proposizione 2.4. Per comodità, siano: a il numero di cicli pari nella decomposizione, b il numero di cicli dispari e c il numero di cicli infiniti.
Esaminiamo i diversi casi possibili:

1. se $b = \infty$ oppure b è pari, allora rispettivamente dal Lemma 2.8 e dal Teorema 2.5, segue che σ è un commutatore. Osserviamo che in questo caso non ha importanza chi siano a e c, perché sappiamo già che cicli pari e cicli infiniti sono commutatori, rispettivamente per il Teorema 2.5 e per il Lemma 2.6.

2. Se $b < \infty$ e b è dispari, bisogna analizzare due sottocasi:

   2.1. se $c > 0$, ovvero nella decomposizione compare almeno un ciclo infinito, allora siamo a posto, perché, per il Lemma 2.7, basta accoppiare un ciclo dispari col ciclo infinito per avere un commutatore, dopodiché resta un numero pari di cicli dispari e ci riconduciamo al caso 1;

   2.2. sia ora $c = 0$, ovvero non ci sono cicli infiniti. Se $a < \infty$ siamo nel caso di una permutazione finitaria, che sappiamo essere un commutatore, grazie al Lemma 2.9. Invece, se $a = \infty$, si conclude utilizzando nuovamente il Lemma 2.8.

Ciò prova il teorema. □

Il seguente importante risultato è una conseguenza immediata del teorema precedente:

Corollario 2.11. *Se X è un insieme numerabile, allora* $\mathrm{Sym}(X)$ *coincide con il suo sottogruppo derivato.*

Concludiamo enunciando, senza dimostrarlo, un risultato di Ore che è possibile ottenere utilizzando le stesse tecniche descritte sopra. Tale risultato ha dato origine a quella che in letteratura scientifica è nota come la *Congettura di Ore*, che afferma che ogni elemento di un gruppo semplice finito non abeliano è un commutatore.

Teorema 2.12. *Quando $n \geq 5$ ogni elemento del gruppo alterno A_n è un commutatore di elementi di A_n.*

Bibliografia

[1] K. Conrad, *Generating sets* (2009), https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf

[2] G. Cutolo, *Azioni permutazionali di gruppi (Appunti per il corso di Algebra Superiore)* (1997)

[3] J. D. Dixon, B. Mortimer, *Permutation Groups*, Springer New York, 1996 doi:10.1007/978-1-4612-0731-3

[4] M. W. Liebeck, E. A. O'Brien, S. Alev, P. H. Tiep, *The Ore conjecture*, Journal of the European Mathematical Society **12** (2010), 939-1008 doi:10.4171/JEMS/22G iv

[5] A. Machì, *Gruppi. Una introduzione a idee e metodi della Teoria dei Gruppi*, Springer Milano, 2007 doi:10.1007/978-88-470-0623-2

[6] O. Ore, *Some remarks on commutarors*, Proc. Amer. Math. Soc. **2** (1951), 307-314 doi:https://doi.org/10.1090/S0002-9939-1951-0040298-4 iii, 25

[7] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer New York, 2012 doi:10.1007/978-1-4419-8594-1