Università del Salento
Dipartimento di Matematica
"Ennio De Giorgi"

Wenchang Chu

Teoria dei Gruppi Finiti ed Applicazioni Combinatorie

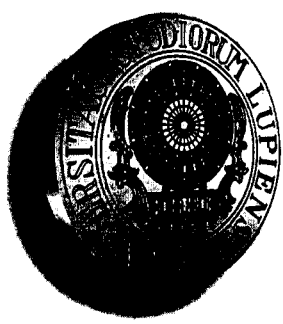
Quaderno 1/2007: ISBN 978-88-8305-048-0

Università del Salento – Coordinamento SIBA

Università del Salento
Dipartimento di Matematica
"Ennio De Giorgi"

Wenchang Chu

Teoria dei Gruppi Finiti ed Applicazioni Combinatorie



Quaderno 1/2007: ISBN 978-88-8305-048-0

Università del Salento – Coordinamento SIBA

QUADERNI DI MATEMATICA

Una pubblicazione a cura del

DIPARTIMENTO DI MATEMATICA

"ENNIO DE GIORGI"

UNIVERSITÀ DEL SALENTO

I QUADERNI del Dipartimento di Matematica dell'Università del Salento documentano gli aspetti di rilievo dell'attività di ricerca e didattica del Dipartimento. Nei Quaderni sono pubblicati articoli di carattere matematico che siano:

(a) lavori di rassegna e monografie su argomenti di ricerca;
(b) testi di seminari di interesse generale, tenuti da docenti o ricercatori del Dipartimento o esterni;
(c) lavori di specifico interesse didattico.

La pubblicazione dei lavori è soggetta all'approvazione del Comitato di Redazione, che decide tenendo conto del parere di un *referee*, nominato di volta in volta sulla base delle competenze specifiche.

Quaderno 1/2007: ISBN 978-88-8305-048-0

Università del Salento – Coordinamento SIBA

Teoria dei Gruppi Finiti ed Applicazioni Combinatorie

CHU Wenchang

DIPARTIMENTO DI MATEMATICA
UNIVERSITÀ DEL SALENTO
LECCE-ARNESANO P. O. BOX 193
73100 LECCE, ITALIA
EMAIL *chu.wenchang@unile.it*

2000 *Mathematics Subject Classification.*

03E04, 03E05, 05A15, 05E25
06A06, 06A07, 11A25, 11P83
20D10, 20D20, 20D30, 20D40,
20F14, 20F16, 20F18, 20F19

SOMMARIO. Questo testo presenta, in modo autosufficiente con esposizione dettagliata, un'introduzione alla teoria dei gruppi finiti ed alle applicazioni combinatorie, sottolineando l'importanza dell'utilizzo di azioni di gruppi su insiemi con particolare riferimento agli aspetti quantitativi dell'algebra moderna.

Prefazione

Questo quaderno è maturato dall'esperienza didattica sulle lezioni tenute dall'autore nel corso di *Algebra Superiore* per gli studenti del corso di laurea triennale in matematica dell'Università di Lecce, negli ultimi dieci anni.

L'obiettivo è di fornire, in modo autosufficiente con esposizione dettagliata, un'introduzione alla teoria dei gruppi finiti ed alle applicazioni combinatorie, sottolineando l'importanza dell'utilizzo di azioni di gruppi su insiemi con particolare riferimento agli aspetti quantitativi dell'algebra moderna.

Il testo è diviso in sette capitoli. Il capitolo **A** costituisce una breve introduzione ai concetti fondamentali dei gruppi e ai teoremi di omomorfismo ed isomorfismo, necessari per lo sviluppo successivo. Il capitolo **B** studia le strutture dei gruppi abeliani finitamente generati. In particolare, si evidenzia la funzione generatrice delle partizioni dei numeri naturali nel conteggio dei gruppi abeliani finiti e nella trattazione del teorema di Hall riguardante gli automorfisimi dei p-gruppi finiti. Partendo dall'azione di gruppo su un insieme, il capitolo **C** approfondisce ampiamente le orbite e gli stabilizzatori, l'equazione delle classi, transitività e normalità. I teoremi di Sylow e loro applicazioni per la determinazione delle strutture dei gruppi finiti si trovano nel capitolo **D**. Il capitolo **E** tratta concisamente i gruppi risolubili e nilpotenti in relazione alle serie normali, centrali e al sottogruppo di Frattini.

Gli ultimi due capitoli sono dedicati alle applicazioni combinatorie. Esaminando l'azione di gruppo sulle applicazioni fra due insiemi, il capitolo **F** presenta la teoria enumerativa di Pólya-Redfield e l'applicazione nel conteggio combinatorio, che viene facilitato inoltre dalle formule dimostrate per gli indici di gruppi finiti. Infine, il capitolo **G** espone la teoria dell'inversione di Möbius-Rota sugli insiemi parzialmente ordinati, che viene applicata sistematicamente alle funzioni aritmetiche, al principio di inclusione ed esclusione, agli spazi vettoriali di dimensione finita sui campi finiti e ai coefficienti binomiali gaussiani, alla funzione di Möbius del reticolo delle partizioni e infine alla formula di Ryser per calcolare il permanente della matrice rettangolare.

Lecce, 7 luglio 2007 CHU Wenchang

CAPITOLO A

Teoria Introduttiva dei Gruppi

Un gruppo è un insieme di elementi munito di una operazione binaria che verifica la proprietà associativa, nel quale esiste un elemento particolare, detto elemento neutro, e in cui ogni elemento ammette il suo inverso.

Quando l'operazione del gruppo verifica anche la proprietà commutativa il gruppo viene chiamato *abeliano*; se inoltre il gruppo è generato da un numero finito di suoi elementi si dice *gruppo abeliano finitamente generato.*

In questo capitolo introdurremo nozioni della teoria dei gruppi, che saranno la base per i capitoli successivi. Indispensabili saranno il teorema di Lagrange, i teoremi di isomorfismo ed il prodotto diretto con la sua caratterizzazione. Infine, alcuni teoremi della teoria dei numeri sono dimostrati come applicazioni esemplari.

A1. Gruppi e sottogruppi

Definizione A1.1. *Sia G un insieme non vuoto munito di un'operazione binaria "$\cdot$". La struttura algebrica $(G, \cdot)$ viene chiamata* gruppo *se gode delle seguenti proprietà:*

(a) Proprietà associativa*: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ per x, y, $z \in G$.*
(b) Elemento neutro*: Esiste $e \in G$ tale che $x \cdot e = e \cdot x = x$ per ogni $x \in G$.*
(c) Inverso*: $\forall x \in G$, esiste un $y \in G$ tale che $x \cdot y = y \cdot x = e$.*

Definizione A1.2. *Sia $(G, \cdot)$ un gruppo. Si dice* $(G, \cdot)$ gruppo finito *se l'insieme G è finito; altrimenti $(G, \cdot)$ viene detto* gruppo infinito.

Definizione A1.3. *Sia $(G, \cdot)$ un gruppo. Si dice* $(G, \cdot)$ gruppo abeliano *se $\forall x, y \in G$ vale la proprietà agguntiva $x \cdot y = y \cdot x$, detta* proprietà commutativa.

Definizione A1.4. *Siano G un gruppo e g un elemento di G. Il più piccolo intero positivo n tale che $g^n = e$ è detto* ordine *di g o anche periodo di g,*

che viene indicato con $o(g) = n$. *Se tale ordine non esiste, si dice* g *di periodo infinito.*

Definizione A1.5. *Un gruppo* $(G, \cdot)$ *è detto* gruppo ciclico *se esiste* $g \in G$ *tale che* $G = \langle g \rangle := \{g^k \mid k \in \mathbb{Z}\}$, *cioè se* G *è generato da un suo elemento. In tal caso, la cardinalità di* G *coincide con l'ordine* $o(g)$ *del generatore* g.

Indichiamo con $\mathbb{N}$ e $\mathbb{N}_0$ rispettivamente l'insieme dei numeri naturali e quello dei numeri interi non negativi. Allora si verifica facilmente che nessuna delle quattro strutture $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{N}_0, +)$ e $(\mathbb{N}_0, \times)$ forma un gruppo. Invece, abbiamo i seguenti gruppi sulla base dei sistemi dei numeri:

- $\mathbb{Z}$ - numeri interi: $(\mathbb{Z}, +)$ è un gruppo ciclico infinito.
- $\mathbb{Q}$ - numeri razionali: $(\mathbb{Q}, +)$ e $(\mathbb{Q}\backslash\{0\}, \times)$ sono gruppi abeliani infiniti.
- $\mathbb{R}$ - numeri reali: $(\mathbb{R}, +)$ e $(\mathbb{R}\backslash\{0\}, \times)$ sono gruppi abeliani infiniti.
- $\mathbb{C}$ - numeri complessi: $(\mathbb{C}, +)$ e $(\mathbb{C}\backslash\{0\}, \times)$ sono gruppi abeliani infiniti.
- $\mathbb{Z}_m$ - l'insieme completo delle classi residue modulo m: $(\mathbb{Z}_m, +)$ è un gruppo ciclico finito.
- $\mathbb{Z}_m^\times$ - l'insieme ridotto delle classi residue modulo m (le classi rappresentate dai primi relativi a m): $(\mathbb{Z}_m^\times, \times)$ è un gruppo abeliano finito.

Definizione A1.6. *Sia* $(G, \cdot)$ *un gruppo. Un sottoinsieme stabile* H *di* G *si dice un* sottogruppo *di* G *se la sottostruttura* $(H, \cdot)$ *è un gruppo.*

NOTAZIONE: Con $H \leq G$ e $H < G$ indichiamo H sottogruppo e sottogruppo proprio di G, rispettivamente.

Per verificare che $(H, \cdot)$ è un gruppo dovremmo prima di tutto controllare che $\forall x, y \in H$, vale $x \cdot y \in H$ dopo di che dimostrare le tre proprietà che caratterizzano la struttura algebrica di gruppo; alternativamente potremmo usare la seguente equivalenza: Se H è un sottoinsieme non vuoto del gruppo G, allora H è un sottogruppo se e solo se per ogni coppia (x, y) di elementi di H anche il prodotto $x \cdot y^{-1}$ appartiene ad H.

Siano G un gruppo, H un sottogruppo di G e x un elemento di G. Definiamo *laterale sinistro* e *laterale destro* di H in G determinati da x rispettivamente come segue:

$$\begin{aligned} xH &= \{xh \mid \forall h \in H\}, \\ Hx &= \{hx \mid \forall h \in H\}. \end{aligned}$$

Ovviamente, laterali destri (sinistri) distinti di H in G sono anche disgiunti e H coincide con il laterale sinistro hH e destro Hh per qualunque $h \in H$.

L'insieme dei laterali sinistri (destri) è una partizione di G. Inoltre, tutti i laterali (sinistri e destri) di H in G sono equipotenti ad H.

Teorema A1.7 (Teorema di Lagrange). *Siano G un gruppo finito e H un suo sottogruppo, allora l'ordine di H divide quello di G.*

DIMOSTRAZIONE. Denotiamo con n il numero dei laterali destri di H in G. Allora $\forall g \in G$, $|Hg| = |H|$, cioè ogni laterale destro è formato da $|H|$ elementi. I laterali destri non sono altro che le classi di equivalenza di G rispetto alla relazione "$\sim$" tale che $\forall x, y \in G$, si ha che

$$x \sim y \iff x \cdot y^{-1} \in H$$

quindi per le proprietà delle relazioni d'equivalenza sappiamo che i laterali sono a due a due disgiunti ed esauriscono G. Allora $|G| = n \cdot |H|$, perciò $|H|$ divide $|G|$. □

Proposizione A1.8 (Gruppo di ordine p). *Sia G un gruppo finito di ordine p, con p primo. Allora G è ciclico.*

DIMOSTRAZIONE. Dato che $|G| = p > 1$, esiste un elemento $g \in G$ tale che $o(g) > 1$. Allora consideriamo il sottogruppo ciclico $H = \langle g \rangle$ generato da g. Secondo il teorema di Lagrange, si ha $1 < |H| = o(g)|p = |G|$, che implica $|H| = o(g) = p$ e $H = G$. Quindi G è un gruppo ciclico. □

A2. Sottogruppi normali e gruppi quozienti

Definizione A2.1. *Siano G un gruppo e H un suo sottogruppo. Se $\forall x \in G$, risulta $Hx = xH$, allora si dice H* sottogruppo normale *di G e si usa la notazione $H \triangleleft G$.*

OSSERVAZIONE: Per $x \in G$, definiamo il coniugato di H sotto x con $H^x := x^{-1}Hx$. Allora per ogni $x \in G$, $xH = Hx$ equivale a $H^x = H$. Perciò H è sottogruppo normale di G se solo se $H^x = H$ per ogni $x \in G$.

Analogamente, per due elementi x e y in un gruppo G, si dice che y è coniugato a x se esiste un $g \in G$ tale che $y = x^g := g^{-1}xg$. Per un fissato $x \in G$, si definisce *classe di coniugio* di x in G come l'insieme di tutti gli elementi coniugati a x in G e si denota con $\mathrm{Cl}(x)$. Allora, H è un sottogruppo normale di un gruppo G se e solo se H contiene tutti i coniugati di tutti suoi elementi.

Per un gruppo G e un suo sottogruppo normale H, possiamo definire l'operazione indotta "$\circ$" per due laterali Hx e Hy come segue:

$$Hx \circ Hy = H \circ xHx^{-1}(xy) = H(xy).$$

Allora per l'insieme dei laterali destri di H in G:

$$G/H \quad = \quad \{Hg \mid g \in G\}$$

abbiamo l'operazione binaria indotta da quella su G:

$$\begin{aligned} \text{“}\circ\text{”}: \quad & G/H \times G/H \longrightarrow G/H; \\ & Hx \circ Hy \quad = \quad H(xy). \end{aligned}$$

Non è difficile vedere che $(G/H, \circ)$ è un gruppo.

Definizione A2.2. *Se G è gruppo e H un sottogruppo normale di G, allora G/H si dice* gruppo quoziente.

A3. Omomorfismo ed isomorfismo

Definizione A3.1. *Siano $(G, \cdot)$ e $(H, \diamond)$ due gruppi. Un'applicazione f da G in H si dice un* omomorfismo *se $f(x \cdot y) = f(x) \diamond f(y)$ per ogni coppia $x, y \in G$. Quando l'applicazione f è iniettiva, suriettiva e biiettiva, l'omomorfismo f viene denominato rispettivamente monomorfismo, epimorfismo e isomorfismo. Nell'ultimo caso, i due gruppi G e H si dicono* isomorfi *e si denotano con $G \cong H$.*

Sia $f : G \longrightarrow H$ un omomorfismo. Si dice nucleo di f e si indica con il simbolo $\ker f$, l'insieme degli elementi di G la cui immagine risulta l'elemento neutro di H. Non è difficile verificare che il nucleo $\ker f$ è un sottogruppo normale di G.

Teorema A3.2 (Primo teorema di omomorfismo). *Siano G e H due gruppi e f un epimorfismo da G ad H. Allora $G/\ker f$ è isomorfo ad H.*

DIMOSTRAZIONE. Per semplicità, denotiamo con $K = \ker f$. Dato che K è un sottogruppo normale di G, allora il gruppo quoziente G/K è ben definito. Consideriamo l'applicazione canonica ϕ indotta da f:

$$\begin{aligned} G/K \xrightarrow{\phi} H \quad & : \quad \phi(Kx) = f(x) \quad \text{per} \quad Kx \in G/K; \\ \phi(Kx \cdot Ky) \quad & = \quad \phi(Kx) \circ \phi(Ky) \quad = \quad f(x) \circ f(y) \\ & = \quad \phi\big(K(x \cdot y)\big) = f(x \cdot y) = f(x) \circ f(y). \end{aligned}$$

Ricordando che f è epimorfismo da G ad H, si ha che ϕ è suriettivo da G/K ad H. Per ogni due laterali Kx e Ky in G/K, se $\phi(Kx) = \phi(Ky)$,

allora $f(x) = f(y)$. Quest'ultima equivale a $f(xy^{-1}) = f(x)f^{-1}(y) = e_H$, dove e_H è l'elemento neutro di H. Dunque abbiamo $xy^{-1} \in K = \ker f$, che implica $Kx = Ky$. Allora ϕ è anche iniettivo, perciò biiettivo. Quindi ϕ è un isomorfismo da G/K ad H. □

Teorema A3.3 (Secondo teorema di isomorfismo). *Sia G un gruppo e siano H e N due sottogruppi normali di G tali che $H \triangleleft N$. Allora il gruppo $\frac{G/H}{N/H}$ è isomorfo a G/N.*

DIMOSTRAZIONE. Consideriamo due epimorfismi canonici:

$$G \xrightarrow{\phi} G/H \quad : \quad \phi(x) = xH \quad \text{per} \quad x \in G;$$
$$G/H \xrightarrow{\psi} \frac{G/H}{N/H} \quad : \quad \psi(xH) = xH(N/H) \quad \text{per} \quad xH \in G/H.$$

Allora l'applicazione composta

$$G \xrightarrow{\psi\diamond\phi} \frac{G/H}{N/H} \; : \; \psi\big(\phi(x)\big) = xH(N/H) \quad \text{per} \quad x \in G$$

è ancora un epimorfismo. Secondo il teorema d'omomorfismo, abbiamo subito che $G/\ker(\psi \diamond \phi)$ è isomorfo a $\frac{G/H}{N/H}$. Rimane da confermare il fatto che $N = \ker(\psi \diamond \phi)$. Infatti, $x \in G$ appartiene a $\ker(\psi \diamond \phi)$ se e solo se $xH(N/H) = N/H$, cioè se e solo se $xH \in N/H$. Quest'ultima è equivalente a $x \in N$. Dunque $N = \ker(\psi \diamond \phi)$ e G/N è isomorfo a $\frac{G/H}{N/H}$. □

Teorema A3.4 (Terzo teorema di isomorfismo). *Sia G un gruppo e siano H ed N rispettivamente un sottogruppo ed un sottogruppo normale di G. Valgono:*

(a) *HN è un sottogruppo di G.*
(b) *N è sottogruppo normale di HN.*
(c) *$HN/N \cong H/(H \cap N)$.*

DIMOSTRAZIONE. Verifichiamo separatamente ognuna di queste tesi.

[a] Osserviamo che HN è sottoinsieme di G perché lo sono sia N che H, inoltre si tratta di un insieme chiuso rispetto a "$\cdot$". Infatti, per due elementi h_1a_1 e h_2a_2 di HN, si nota

$$(h_1a_1) \cdot (h_2a_2) = (h_1h_2) \cdot \big\{(h_2^{-1}a_1h_2) \cdot a_2\big\}$$

appartiene ad HN, perché N è sottogruppo normale di G, quindi si ha $a_1 \cdot h_2 \cdot a_1^{-1} \in N$. Restano da provare le proprietà del gruppo. È ovvio che vale la proprietà associativa perché $HN \subseteq G$. Esiste l'elemento neutro $e \in HN$, lo stesso $e \in G$. Per ogni $ha \in HN$, esiste il suo inverso $a^{-1}h^{-1}$ perché $(ha)^{-1} = a^{-1}h^{-1} = h^{-1}(ha^{-1}h^{-1}) \in HN$.

[b] Osserviamo che N è sottoinsieme di HN perché $N = eN$, inoltre N è sottogruppo normale di G quindi N è sottogruppo normale di HN.

[c] Non è difficile vedere che $H \cap N$ è un sottogruppo normale di H. Consideriamo ϕ la funzione da HN/N in $H/(H \cap N)$ che trasforma, per ogni $ha \in HN$, il generico laterale $haN = hN$ di HN/N in $h(H \cap N) \in H/H \cap N$. Per ogni $h \in H$ e $a \in N$, scriviamo esplicitamente:

$$\phi : HN/N \longrightarrow H/(H \cap N);$$
$$\phi(hN) = \phi(haN) = h(H \cap N).$$

Dimostriamo che ϕ è un isomorfismo.

- ϕ è un omomorfismo. Siano h_1a_1N e h_2a_2N due laterali di HN/N vale che

$$\begin{aligned} &\phi\big((h_1a_1N)\cdot(h_2a_2N)\big) = \phi\big((h_1a_1)\cdot(h_2a_2)N\big) \\ &= \phi\big((h_1h_2)(a_1^{h_2}a_2)N\big) = \phi\big((h_1h_2)N\big) = (h_1h_2)(H \cap N) \\ &= h_1(H \cap N)\cdot h_2(H \cap N) = \phi(h_1a_1N)\cdot\phi(h_2a_2N). \end{aligned}$$

- ϕ è iniettiva. Siano h_1a_1N e h_2a_2N due laterali di HN/N dobbiamo verificare

$$\phi(h_1a_1N) = \phi(h_2a_2N) \implies h_1a_1N = h_2a_2N.$$

Infatti

$$\phi(h_1a_1N) = \phi(h_2a_2N) \implies h_1(H \cap N) = h_2(H \cap N)$$

che implica $h_1h_2^{-1} \in N$, perciò $h_1N = h_2N$ e $h_1a_1N = h_2a_2N$.

- La suriettività è ovvia.

Dunque HN/N è isomorfo a $H/(H \cap N)$. □

A4. Prodotto diretto

Definizione A4.1. *Sia $(G,\cdot)$ un gruppo e siano $H_1, H_2, \cdots, H_n$ sottogruppi di G. Si dice che G è* prodotto diretto *degli $\{H_k\}_{k=1}^n$ se risulta*

(a) *per ogni elemento $g \in G$, si esprime in modo unico come prodotto $g = h_1h_2\cdots h_n$, dove $h_k \in H_k$ per $k = 1, 2, \cdots, n$.*
(b) *ogni elemento di H_i è permutabile con tutti gli elementi di H_j per $i, j = 1, 2, \cdots, n$ con $i \neq j$.*

I gruppi H_k con $k = 1, 2, \cdots, n$ si chiamano fattori diretti *di G. Useremo il seguente simbolo per indicare che G è prodotto diretto degli $\{H_k\}_{k=1}^n$:*

$$G = \bigotimes_{k=1}^{n} H_k = H_1 \otimes H_2 \otimes \cdots \otimes H_n.$$

OSSERVAZIONE: È utile chiarire la precedente definizione:

- La prima proprietà del prodotto diretto dice che ogni elemento g di G si scrive in modo unico come $g = h_1 h_2 \cdots h_n$, il che significa $H_1 H_2 \cdots H_n$ è sottoinsieme di G. Precisa inoltre che $G = H_1 H_2 \cdots H_n$.
- Se G è prodotto diretto dei sottogruppi $H_1, H_2, \cdots, H_n$, non conta l'ordine in cui vengono scritti gli H_i nel prodotto, l'importante è che ognuno di questi compaia una sola volta.
- Se tutti gli H_i sono gruppi abeliani anche G è abeliano.

Teorema A4.2 (Teorema di caratterizzazione). *Siano G un gruppo e $\{H_k\}_{k=1}^n$ sottogruppi di G, allora G è prodotto diretto degli H_k con $k = 1, 2, \cdots, n$ se e solo se*

(a) *tutti gli $\{H_k\}_{k=1}^n$ sono normali.*
(b) $G = \langle H_1, H_2, \cdots, H_n \rangle$.
(c) $\{e\} = H_k \bigcap \langle H_i \mid i \neq k \text{ con } 1 \leq i \leq n \rangle$.

Il sottogruppo $\langle H_1, H_2, \cdots, H_n \rangle$ è generato da $H_1, H_2, \cdots, H_n$, cioè il più piccolo sottogruppo che contiene $H_1, H_2, \cdots, H_n$. Con $\langle H_i \mid i \neq k \rangle$ si indica il sottogruppo generato da tutti gli H_i con $i = 1, 2, \cdots, n$ tranne H_k.

DIMOSTRAZIONE. Supponendo che G sia prodotto diretto degli $\{H_k\}_{k=1}^n$, vogliamo verificare le condizioni necessarie **[a]**, **[b]** e **[c]**.

[a] Dobbiamo dimostrare che, dato $k = 1, 2, \cdots, n$, H_k è sottogruppo normale cioè che

$$\forall g \in G \quad \Longrightarrow \quad H_k^g = g^{-1} H_k g = H_k.$$

Se $g \in G$, sappiamo che esistono $h_i \in H_i$ con $i = 1, 2, \cdots, n$ tali che $g = h_1 \cdot h_2 \cdots h_n$, dove $\{h_i\}_{i=1}^n$ sono due a due permutabili. Osservando che H_k è permutabile con ogni h_i si ha che $H_k^{h_i} = H_k$ con $i \neq k$. Dunque

$$H_k^g = H_k^{h_1 \cdot h_2 \cdots h_n} = H_k^{h_k} = H_k.$$

[b] Dalla definizione di prodotto diretto deriva che $G = \langle H_1, H_2, \cdots, H_n \rangle$.

[c] Dimostriamo che $\forall\ x \in H_k \bigcap \langle H_i \mid i \neq k \rangle\rangle$ risulta $x = e$. Dato che $x \in H_k \bigcap \langle H_i \mid i \neq k \rangle$, esistono $h_j \in H_j$ con $j = 1, 2, \cdots, n$ tali che

$$\begin{aligned} x = \quad h_k \quad &= e \ \cdots e \quad h_k \ e \quad \cdots e \\ &= \prod_{j \neq k} h_j = h_1 \cdots h_{k-1} \ e \ h_{k+1} \cdots h_n. \end{aligned}$$

Per la prima proprietà del prodotto diretto, x ha un'unica fattorizzazione, perciò

$$h_1 = h_2 = \cdots = h_n = e \quad \text{e} \quad x = e.$$

Ora dimostriamo le condizioni sufficienti.

Per ogni $x \in H_i$ e $y \in H_j$ con $i \neq j$, vale $x \cdot y = y \cdot x$.

Siano $x \in H_i$ e $y \in H_j$ generici con $i \neq j$. Osserviamo che:

$$\begin{aligned} x^{-1} \cdot y^{-1} \cdot x \cdot y &= \left(x^{-1} \cdot y^{-1} \cdot x\right) \cdot y \\ &= \left(y^{-1}\right)^x \cdot y \in H_j \end{aligned}$$

dato che $y \in H_j$ e $(y^{-1})^x \in H_j$ perché H_j è un sottogruppo normale.

Analogamente, si ha che

$$\begin{aligned} x^{-1} \cdot y^{-1} \cdot x \cdot y &= x^{-1} \cdot \left(y^{-1} \cdot x \cdot y\right) \\ &= x^{-1} \cdot x^y \in H_i \end{aligned}$$

dato che $x^y \in H_i$ e $x^{-1} \in H_i$ perché H_i è normale.

Quindi

$$x^{-1} \cdot y^{-1} \cdot x \cdot y \in H_i \cap H_j \subseteq H_i \cap \langle H_k \mid k \neq i \rangle = \{e\}$$

perciò $x \cdot y = y \cdot x$, che conferma la proprietà **[b]**.

Dimostriamo che $\forall g \in G$, esistono unici $h_i \in H_i$ con $i = 1, 2, \cdots, n$ tali che $g = h_1 h_2 \cdots h_n$.

Dall'ipotesi **[b]**, si ha che $G = \langle H_1, H_2, \cdots, H_n \rangle$. Conseguentemente abbiamo $G = H_1 \cdot H_2 \cdots H_n$ perché $\{H_k\}_{k=1}^n$ sono a due a due permutabili elemento per elemento.

Resta da provare l'unicità. Sia g un generico elemento di G. Supponiamo che

$$g = h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$$

per $h_k, h'_k \in H_k$ con $k = 1, 2, \cdots, n$. Allora si ottiene che

$$h_1 h_2 \cdots h_n = h'_1 h'_2 \cdots h'_n \quad \Longrightarrow \quad h_k {h'_k}^{-1} = \prod_{\substack{i=1 \\ i \neq k}}^{n} h_i^{-1} h'_i$$

che è giustificato dalla permutabilità dimostrata nella prima parte.

Allora per $k = 1, 2, \cdots, n$ vale

$$h_k {h'_k}^{-1} \in H_k \bigcap \langle \{H_j \mid j \neq k \text{ con } 1 \leq j \leq n\} \rangle = \{e\}.$$

Quindi $h_k {h'_k}^{-1} = e$ che equivale a $h_k = h'_k$ per ogni k con $1 \leq k \leq n$. □

Corollario A4.3. *Siano $\{H_k\}_{k=1}^n$ sottogruppi finiti di un gruppo G a due a due permutabili elemento per elemento. Il loro prodotto è un sottogruppo di G, ed è un prodotto diretto se e solo se ha per ordine il prodotto degli ordini degli H_k con $k = 1, 2, \cdots, n$.*

Notiamo che se per ogni $i = 1, 2, \cdots, n$ si ha H_i finito, allora anche il prodotto $H_1 H_2 \cdots H_n$ è un insieme finito. Se invece gli H_i sono solamente sottogruppi di G, non si può dire che $H_1 H_2 \cdots H_n$ è sottogruppo di G. Però, se $\{H_i\}$ sono sottogruppi finiti del gruppo G a due a due permutabili elemento per elemento, si verifica che $H_1 H_2 \cdots H_n$ è un sottogruppo di G. Infatti:

- $H_1 H_2 \cdots H_n$ è diverso dal vuoto perché $e \in H_i$ per ogni $i = 1, 2, \cdots, n$ quindi $e \in H_1 H_2 \cdots H_n$.
- $H_1 H_2 \cdots H_n$ è sottoinsieme di G (banale).
- Siano $a, b \in H_1 H_2 \cdots H_n$ dimostriamo che ab^{-1} appartiene a $H_1 H_2 \cdots H_n$. Per ogni $i = 1, 2, \cdots, n$ esistono due elementi x_i e y_i appartenenti ad H_i tali che $a = x_1 x_2 \cdots x_n$ e $b = y_1 y_2 \cdots y_n$. Allora:

  $$ab^{-1} = (x_1 x_2 \cdots x_n)(y_1^{-1} y_2^{-1} \cdots y_n^{-1}) = (x_1 y_1^{-1})(x_2 y_2^{-1}) \cdots (x_n y_n^{-1}).$$

DIMOSTRAZIONE. Verifichiamo la condizione necessaria della tesi del corollario. Per ipotesi H è prodotto diretto degli $\{H_k\}_{k=1}^n$, quindi per ogni $h \in H$ esistono $h_i \in H_i$ con $i = 1, 2, \cdots, n$ tali che $h = h_1 h_2 \cdots h_n$. Mostriamo che si deve necessariamente verificare

$$|H| < |H_1| \cdot |H_2| \cdots |H_n| \qquad \text{oppure} \qquad |H| = |H_1| \cdot |H_2| \cdots |H_n|.$$

Infatti, variando nel suddetto prodotto $h_1 h_2 \cdots h_n$ un generico h_k con un altro elemento di H_k, si ottiene un altro elemento di H. Ovviamente h_k può variare in $|H_k|$ modi diversi, quindi, variando tutti gli h_k in tutti i modi possibili, otteniamo $|H_1| \cdot |H_2| \cdots |H_n|$ elementi di H, quindi il numero di

elementi che formano H non può essere inferiore al prodotto delle cardinalità dei vari H_k con $k = 1, 2, \cdots, n$.

Passiamo ora a dimostrare la condizione sufficiente. Per ipotesi

$$H = H_1 H_2 \cdots H_n \quad \text{e} \quad |H| = |H_1| \cdot |H_2| \cdots |H_n|$$

dimostriamo che per ogni $h \in H$ esistono $h_k \in H_k$ con $k = 1, 2, \cdots, n$ tali che $h = h_1 h_2 \cdots h_n$ dove questi h_k sono unici. L'esistenza degli h_k è ovvia in quanto $H = H_1 H_2 \cdots H_n$; resta da provare la loro unicità. Supponiamo per assurdo che esista un elemento $g \in H$ tale che $g = h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$ con almeno un indice k tra questi n tale che $h_k \neq h_k'$. Allora g scritto in due modi diversi contribuisce una volta in $|H_1 H_2 \cdots H_n|$ e due volte in $|H_1| \cdot |H_2| \cdots |H_n|$ per cui $|H_1 H_2 \cdots H_n| < |H_1| \cdot |H_2| \cdots |H_n|$ il che è assurdo! □

A5. Applicazione alla teoria dei numeri

A5.1. Il piccolo teorema di Fermat. Sia p un primo. Denotiamo con $\mathbb{Z}_p^\times$ l'insieme dei residui modulo p diversi da zero. Dimostrare:

(a) $\mathbb{Z}_p^\times$ è un gruppo con la moltiplicazione modulare.
(b) per ogni numero intero n, vale $n^p \equiv n \pmod{p}$.

DIMOSTRAZIONE. Prima di tutto, è facile vedere che $1 \in \mathbb{Z}_p^\times$ è l'elemento neutro di $\mathbb{Z}_p^\times$. Per due elementi $m,\ n \in \mathbb{Z}_p^\times$, il loro prodotto modulo p è diverso da zero, quindi appartiene ancora a $\mathbb{Z}_p^\times$. Perciò $\mathbb{Z}_p^\times$ è chiuso rispetto alla moltiplicazione modulare. Per ogni intero $m \in \mathbb{Z}_p^\times$, consideriamo $M = \{m, m^2, \cdots, m^p\}$, p-interi generati dalle potenze di m. Dato che la cardinalità di $\mathbb{Z}_p^\times$ è uguale a $p-1$, allora esistono due numeri m^i e m^j in M con $1 \leq i < j \leq p$ tali che $m^i \equiv m^j \pmod{p}$. Notando che $\mathrm{mcd}(m, p) = 1$ e $\mathrm{mcd}(m^i, p) = 1$, possiamo subito dedurre che

$$m^{j-i} = m \times m^{j-i-1} \equiv 1 \pmod{p}.$$

Questa congruenza significa che m^{j-i-1} è inverso di m in $\mathbb{Z}_p^\times$. È ovvio che $\mathbb{Z}_p^\times$ è commutativo e anche associativo. Dunque $\mathbb{Z}_p^\times$ è un gruppo abeliano di ordine $p-1$.

Per qualunque numero intero n, se $p|n$, abbiamo

$$n^p \equiv n \equiv 0 \pmod{p}.$$

Altrimenti, consideriamo il sottogruppo $\langle n \rangle$ di $\mathbb{Z}_p^\times$ generato da n. Secondo il teorema di Lagrange, l'ordine d di $\langle n \rangle$ è un divisore dell'ordine di $\mathbb{Z}_p^\times$, che implica

$$n^{p-1} = \left(n^d\right)^{(p-1)/d} \equiv 1 \pmod{p}.$$

Moltiplicado con n, otteniamo in questo caso la stessa congruenza

$$n^p \equiv n \pmod{p}.$$

Così abbiamo dimostrato il piccolo teorema di Fermat tramite la teoria dei gruppi finiti. □

A5.2. Funzione Eulero. Per un numero naturale m, sia $\Phi(m)$ l'insieme degli interi da 1 a m, primi relativi a m.

(a) Dimostrare che $\Phi(m)$ è un gruppo con la moltiplicazione modulare rispetto a m.
(b) *Teorema Eulero*: Per ogni intero k con $\mathrm{mcd}(k, m) = 1$, dimostrare la congruenza $k^{\varphi(m)} \equiv 1 \pmod{m}$ dove $\varphi(m)$ è la funzione di Eulero.
(c) Per $n > 1$ un altro numero naturale, dimostrare che m divide $\varphi(n^m - 1)$.

DIMOSTRAZIONE. Seguendo la stessa procedura della dimostrazione del piccolo teorema di Fermat, possiamo confermare che $\Phi(m)$ è veramente un gruppo con la moltiplicazione modulare rispetto a m ed il teorema Eulero

$$k^{\varphi(m)} \equiv 1 \pmod{m} \quad \text{se} \quad \mathrm{mcd}(k, m) = 1.$$

Per l'affermazione (c), consideriamo il sottogruppo $\langle n \rangle$ di $\Phi(n^m - 1)$ generato da n. Non è difficile verificare $\langle n \rangle = \{1, n, n^2, n^{m-1}\}$, che implica $|\langle n \rangle| = m$. Allora $m | \varphi(n^m - 1)$, in virtù del teorema di Lagrange. □

A5.3. Funzione Eulero ancora. Sia G un gruppo ciclico. Dimostrare le seguenti affermazioni:

(a) Ogni sottogruppo H di G è ciclico. Determinare il numero dei generatori di H.
(b) Se G è finito con $|G| = m < \infty$, allora per ogni $n | m$, esiste un solo sottogruppo di ordine n in G.
(c) La formula della somma finita $m = \sum_{n|m} \varphi(n)$, dove φ è la funzione di Eulero.

DIMOSTRAZIONE. Se $G = \langle g \rangle$ è infinito, allora G è isomorfo a $(\mathbb{Z}, +)$ e quindi ha solo due generatori g e g^{-1}. Se $G = \langle g \rangle$ invece è finito con l'ordine $|G| = m$, allora il numero dei generatori è uguale a $\varphi(m)$. Infatti,

se g^k è un qualunque generatore di G, allora $\mathrm{mcd}(k,m) = 1$. Altrimenti, $\mathrm{mcd}(k,m) > 1$ ci porterebbe alla seguente espressione:

$$m = o(g^k) = \left|\{g^k, g^{2k}, \cdots, g^{k\times\frac{m}{\mathrm{mcd}(k,m)}}\}\right| \leq \frac{m}{\mathrm{mcd}(k,m)} < m.$$

Quindi ogni generatore g^k di G corrisponde a un numero naturale k con $1 \leq k \leq m$ tale che $\mathrm{mcd}(k,m) = 1$. Perciò il numero dei generatori del gruppo G è proprio uguale alla funzione Eulero $\varphi(m)$.

[a] Sia $G = \langle g\rangle$ un gruppo ciclico generato da g. Per un sottogruppo $H < G$, consideriamo l'elemento g^n di H come minima potenza positiva di g. Allora $H = \langle g^n\rangle$. Altrimenti, esiste un numero intero positivo k con $n\nmid k$, tale che $g^k \in H$. Secondo l'algoritmo di Euclide, esistono due interi q e r con $0 < r < n$ tali che $k = nq + r$. Allora troviamo un elemento

$$g^r = g^k \cdot \left(g^n\right)^{-q} \in H$$

che contraddice il fatto che g^n sia l'elemento di H con minima potenza positiva di g. Quindi H è ciclico.

Quando G è infinito, generato da g, è facile vedere che ogni sottogruppo $H = \langle g^n\rangle$ è infinito ed ha solo due generatori g^n e g^{-n}. Invece, se G è finito con $|G| = m$, allora H pure è finito. Supponendo che $|H| = n$, si ha che il numero dei generatori di H è uguale a $\varphi(n)$.

[b] Per ogni divisore $n|m$, è evidente che il sottogruppo ciclico

$$H := \langle g^{\frac{m}{n}}\rangle = \left\{g^{\frac{m}{n}}, g^{\frac{2m}{n}}, \cdots g^{\frac{(n-1)m}{n}}, g^m = e\right\}$$

ha ordine n. Vogliamo verificare che, fissando l'ordine n, questo è l'unico sottogruppo di G.

Ricordando che per $G = \langle g\rangle$, ogni sottogruppo ciclico di ordine n è generato da qualche g^k con $o(g^k) = n$, se proviamo che $g^k \in H$, allora H è l'unico sottogruppo di ordine n in G.

Dato che $o(g^k) = n$, si ha che $g^{kn} = e$. Allora esiste un numero naturale d tale che $kn = md$ perché $o(g) = m$. Da questo possiamo dedurre:

$$g^k = g^{md/n} = \left(g^{\frac{m}{n}}\right)^d \in H.$$

Dunque, per ogni $n|m = |G|$, esiste un solo sottogruppo ciclico di ordine n.

[c] Ora, ogni elemento di G è generatore di qualche sottogruppo di G e vice versa, ogni sottogruppo H ha i generatori in numero $\varphi(|H|)$. Classificando

i generatori (tutti gli elementi di G) secondo l'ordine dei sottogruppi di G, otteniamo la seguente formula:

$$m = |G| = \sum_{H \leq G} \varphi(|H|) = \sum_{n|m} \varphi(n).$$

Così abbiamo completato la soluzione del problema. □

A5.4. Teorema di Wilson. Se G è un gruppo abeliano finito con $G = \{g_k\}_{k=1}^n$, dimostrare che $\prod_{k=1}^n g_k$ è un elemento di G il cui quadrato è l'elemento neutro.

(a) Se il gruppo G non ha elementi di ordine 2, dimostrare che $\prod_{k=1}^n g_k = e$ (l'elemento neutro).
(b) Se il gruppo G ha un solo elemento x di ordine 2, dimostrare che $\prod_{k=1}^n g_k = x$.
(c) (Teorema di Wilson) Per un numero primo p, dimostrare la congruenza

$$(p-1)! \equiv -1 \pmod{p}.$$

DIMOSTRAZIONE. Consideriamo un automorfismo su G definito da

$$\psi : G \longrightarrow G \quad \text{con} \quad \psi(x) = x^{-1} \quad \text{per} \quad x \in G.$$

Allora si ha che

$$g = \prod_{k=1}^{n} g_k = \prod_{k=1}^{n} g_k^{-1} = g^{-1}$$

che implica $g^2 = e$, l'elemento neutro di G.

Se $G = \{g_k\}_{k=1}^n$ ha un solo elemento di ordine 2, allora $\{g_1, g_2, \cdots, g_n\}$ possono essere raggruppati in coppie di elementi reciproci più l'elemento neutro e ed un elemento x di ordine 2. Allora si ha che

$$g = \prod_{k=1}^{n} g_k = e \cdot x = x.$$

Ricordiamo che $\mathbb{Z}_p^\times$, l'insieme ridotto dei residui modulo p, è un gruppo abeliano di ordine $p-1$ (in più, $\mathbb{Z}_p^\times$ è ciclico) co la moltiplicazione modulare rispetto a p. Evidentemente $p-1$ è un elemento di ordine 2 in $\mathbb{Z}_p^\times$. Non ci sono altri elementi di ordine 2 in $\mathbb{Z}_p^\times$. Infatti, supponiamo che esista un $k \in \mathbb{Z}_p^\times$ tale che $k^2 \equiv 1 \pmod{p}$. Allora $k \equiv \pm 1 \pmod{p}$, in cui il segno "+" corrisponde all'elemento neutro mentre quello "−" a $p-1$. Dunque

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

che è il teorema di Wilson. □

A5.5. Numeri armonici: Teorema di Wolstenholme. Per un primo dispari p, si definisce la somma parziale

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} \;=\; \frac{m}{n}$$

dove m e n sono numeri naturali. Dimostrare che $p|m$. Inoltre se $p>3$, si ha che $p^2|m$.

DIMOSTRAZIONE. Consideriamo di nuovo il gruppo $\mathbb{Z}_p^\times$, l'insieme ridotto dei residui modulo p co la moltiplicazione modulare rispetto a p. Definiamo un automorfismo su $\mathbb{Z}_p^\times$ come segue:

$$\psi:\ \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times \quad \text{con} \quad \psi(k)=k^{-1} \quad \text{per} \quad k\in\mathbb{Z}_p^\times.$$

Scriviamo la somma armonica come segue:

$$\frac{m}{n} \;=\; \sum_{k=1}^{p-1}\frac{1}{k} \;=\; \frac{S(p)}{(p-1)!} \quad \text{dove} \quad S(p):=\sum_{k=1}^{p-1}\frac{(p-1)!}{k}.$$

Per dimostrare $p|m$, è sufficiente verificare che p divide $S(p)$.

Secondo il teorema di Wilson, si ha che

$$\begin{aligned} S(p) \;&=\; \sum_{k=1}^{p-1}\frac{(p-1)!}{k} \;\equiv_p\; -\sum_{k\in\mathbb{Z}_p^\times} k^{-1} \\ &\equiv_p\; -\sum_{k\in\mathbb{Z}_p^\times} k \;\equiv_p\; -\binom{p}{2} \;\equiv_p\; 0 \end{aligned}$$

che significa $p|S(p)$, da cui si deduce $p|m$.

Per $p>3$, possiamo riformulare la somma $S(p)$ come segue:

$$\begin{aligned} S(p) \;=\; \sum_{k=1}^{p-1}\frac{(p-1)!}{k} \;&=\; \sum_{k=1}^{(p-1)/2}\left\{\frac{(p-1)!}{k}+\frac{(p-1)!}{p-k}\right\} \\ &=\; p\sum_{k=1}^{(p-1)/2}\frac{(p-1)!}{k(p-k)}. \end{aligned}$$

Per dimostrare $p^2|m$, dobbiamo verificare che p divide la somma destra.

Per il sottogruppo $\mathbb{Z}_p^{\times 2}$ composto dai quadrati degli elementi di $\mathbb{Z}_p^{\times}$, ψ induce pure un automorfismo. Allora possiamo procedere come segue:

$$\sum_{k=1}^{(p-1)/2} \frac{(p-1)!}{k(p-k)} \equiv_p \sum_{k\in\mathbb{Z}_p^{\times 2}} k^{-1} \equiv_p \sum_{k\in\mathbb{Z}_p^{\times 2}} k$$

$$\equiv_p \sum_{k=1}^{(p-1)/2} k^2 \equiv_p \frac{p(p^2-1)}{24}.$$

Notando che $p \equiv \pm 1 \pmod 6$, si ha che $24|(p^2-1)$. Conseguentemente, la frazione destra è un intero che è multiplo di p. Dunque $p^2|m$ per $p > 3$. $\square$

CAPITOLO B

Gruppi Abeliani Finitamente Generati

Data la notevole importanza dei gruppi abeliani finitamente generati nello studio delle matematica astratta e della fisica teorica, questo capitolo tratterà la struttura dei:

- gruppi abeliani finiti;
- gruppi abeliani liberi finitamente generati;
- gruppi abeliani misti finitamente generati.

Questa suddivisione ci permette di analizzare i gruppi abeliani finitamente generati in base all'ordine (finito o infinito) dei propri elementi.

Per quanto riguarda i gruppi abeliani finiti, si presentano tre metodi per decomporre un gruppo abeliano finito. Si stabiliscono per tale obbiettivo il teorema fondamentale dei gruppi abeliani finiti, il teorema di decomposizione primaria ciclica ed il suo corollario, la decomposizione in p-gruppi finiti. Con questi teoremi, inoltre, saremo in grado di ottenere il numero di gruppi abeliani tra loro non isomorfi di ordine n, numero naturale fissato, ma ci sarà utile un breve studio sulle partizioni e sulla funzione generatrice che ci permetterà di semplificare notevolmente i vari calcoli.

Proseguiremo lo studio dei gruppi abeliani liberi finitamente generati e dimostreremo che sono il prodotto diretto di un certo numero di gruppi ciclici isomorfi a $(\mathbb{Z}, +)$; mentre per i gruppi abeliani misti finitamente generati dimostreremo che sono isomorfi al prodotto diretto di gruppi ciclici che possono essere p-gruppi (come nel caso dei gruppi abeliani finiti) o sottogruppi isomorfi a $(\mathbb{Z}, +)$ (come nel caso dei gruppi abeliani liberi finitamente generati). Infine, vengono approfonditi le partizioni e teorema di Hall sugli automorfismi dei p-gruppi abeliani finiti.

B1. Teorema fondamentale dei gruppi abeliani finiti

Siano G un gruppo e g un elemento di G. Ricordiamo che *ordine* di g è stato definito come il più piccolo intero positivo n tale che $g^n = e$ ed indicato con

$o(g) = n$. Allora per ogni numero naturale m, vale che $g^{mn} = e$. Viceversa, abbiamo il seguente:

Lemma B1.1. *Siano G un gruppo e $g \in G$ un elemento di ordine finito $o(g) = n < \infty$. Allora per un intero m, valgono:*

(a) *g^m è l'elemento neutro di G se e solo se $n|m$.*
(b) *$o(g^m) = n/\mathrm{mcd}(m, n)$ per qualunque numero intero m diverso da zero.*

DIMOSTRAZIONE. Se $n|m$, esiste un intero ℓ tale che $m = n\ell$. Allora abbiamo che $g^m = (g^n)^\ell = e^\ell = e$. Ora, supponiamo per assurdo che $n \nmid m$, allora esistono q, r interi tali che $m = nq + r$ con $0 < r < n$, quindi $g^m = g^{nq+r} = g^r \cdot (g^n)^q = g^r$. Da qui si evince che se $g^m = e$ vale anche $g^r = e$ con $0 < r < n = o(g)$, che contraddice il fatto che l'ordine di g è uguale ad n.

Sia $d := \mathrm{mcd}(m, n)$, allora esistono m' e n' interi coprimi tali che $m = m'd$ e $n = n'd$. Osserviamo che

$$(g^m)^{n'} = (g^{m' \cdot d})^{n'} = (g^n)^{m'} = e$$

inoltre per ogni k tale che $(g^m)^k = e$ vale che $n'|k$.

Infatti, se $(g^m)^k = e$ si ha $g^{mk} = e$, quindi per l'osservazione precedente $o(g) = n$ e $n|(mk)$ per cui $(n'd)|(m'dk)$ cioè $n'|(m'k)$; essendo n' e m' coprimi, allora $n'|k$. Abbiamo così ottenuto $o(g^m) = n' = n/\mathrm{mcd}(n, m)$. □

Lemma B1.2. *Siano G un gruppo abeliano e $x, y \in G$ due elementi di ordine m e n rispettivamente. Allora*

(a) *l'ordine di xy divide* $\mathrm{mcm}(m, n)$.
(b) *in particolare, si ha che $o(xy) = mn$ se* $\mathrm{mcd}(m, n) = 1$.
(c) *esiste un elemento in G il cui ordine è* $\mathrm{mcm}(m, n)$.

DIMOSTRAZIONE. Ricordando che esistono due interi $m_1, n_1 \in \mathbb{N}$ tali che $\mathrm{mcm}(m, n) = m_1 m = n_1 n$, quindi

$$(xy)^{\mathrm{mcm}(m,n)} = x^{\mathrm{mcm}(m,n)} y^{\mathrm{mcm}(m,n)} = x^{mm_1} y^{nn_1} = e.$$

Per Lemma **B1.1**, $\mathrm{mcm}(m, n)$ è multiplo di $o(xy)$, cioè $o(xy)|\mathrm{mcm}(m, n)$.

Vogliamo ora dimostrare che se $\mathrm{mcd}(m, n) = 1$ vale $o(xy) = mn$. È evidente che $(xy)^{mn} = e$, inoltre mn è il minimo numero verificante la proprietà $(xy)^{mn} = e$. Infatti, se k un generico intero tale che $(xy)^k = e$, dato che G è abeliano vale che $x^k = y^{-k}$. Non sarà difficile verificare che k è un multiplo di mn.

Elevando ambo i membri a m si ottiene $x^{mk} = y^{-mk} = e$ dato che $o(x) = m$, cioè $o(y) = n|(mk)$ per Lemma **B1.1**. Secondo il teorema di Euclide, si ha che $n|k$ dato che $\mathrm{mcd}(m, n) = 1$.

Analogamente, elevando ambo i membri della stessa a n si ha che $x^{nk} = y^{-nk} = e$, quindi $o(x) = m|(nk)$. A questo punto otteniamo che $m|k$.

Richiamando $\mathrm{mcd}(m, n) = 1$, possiamo concludere che $(nm)|k$, cioè ogni intero k tale che $(xy)^k = e$ è multiplo di mn.

Secondo il teorema fondamentale dell'aritmetica, possiamo scrivere

$$m = \prod_k p_k^{\lambda_k} \quad \text{e} \quad n = \prod_k p_k^{\mu_k}$$

dove $\{p_k\}$ sono un numero finito di primi distinti e $\{\lambda_k, \mu_k\}$ numeri interi non negativi.

Allora valgono le seguenti relazioni:

$$\begin{aligned} \mathrm{mcd}(m, n) &= \prod_k p_k^{\min(\lambda_k, \mu_k)}, \\ \mathrm{mcm}(m, n) &= \prod_k p_k^{\max(\lambda_k, \mu_k)}. \end{aligned}$$

Per un sottoinsieme dei numeri naturali definito da

$$\sigma = \{k \mid \lambda_k \geq \mu_k\}$$

introduciamo due divisori di m e n rispettivamente con

$$m' = \prod_{k \in \sigma} p_k^{\lambda_k} \qquad \text{e} \qquad n' = \prod_{k \notin \sigma} p_k^{\mu_k}.$$

Si vede subito che $m'n' = \mathrm{mcm}(m, n)$ con $\mathrm{mcd}(m', n') = 1$.

Per due elementi $x' = x^{m/m'}$ e $y' = y^{n/n'}$, possiamo stabilire i loro ordini come segue:

$$\begin{aligned} o(x') = o\big(x^{m/m'}\big) &= \frac{m}{\mathrm{mcd}(m, m/m')} = m', \\ o(y') = o\big(y^{n/n'}\big) &= \frac{n}{\mathrm{mcd}(n, n/n')} = n'. \end{aligned}$$

Quindi il punto **[b]** appena dimostrato conferma che $x'y'$ ha ordine $m'n' = \mathrm{mcm}(m, n)$. □

Il precedente lemma vale anche indebolendo le sue ipotesi. Infatti la sua tesi è vera anche se G non è abeliano quando x e y sono permutabili.

Lemma B1.3. *Siano G un gruppo abeliano finito e x un elemento di G di ordine massimo. Se y è un qualunque elemento di G, allora l'ordine di y divide l'ordine di x.*

La finitezza di G garantisce l'esistenza di un elemento di ordine massimo; ovviamente possono esistere anche più elementi che hanno lo stesso ordine, anche se l'ordine è massimo.

DIMOSTRAZIONE. Denotiamo con n e m rispettivamente l'ordine di x e y. Supponiamo per assurdo che $m \nmid n$. Sotto queste ipotesi esisterà p primo, tale che

$$\begin{aligned} m = m' \cdot p^{\alpha} : &\qquad \mathrm{mcd}(m', p) = 1, \\ n = n' \cdot p^{\gamma} : &\qquad \mathrm{mcd}(n', p) = 1; \end{aligned}$$

con $\alpha > \gamma$. Introduciamo ora un terzo elemento: $z := x^{p^{\gamma}} y^{m'}$ ed osserviamo che $o(x^{p^{\gamma}}) = n'$ e $o(y^{m'}) = p^{\alpha}$ con $\mathrm{mcd}(n', p^{\alpha}) = 1$. Allora da $\alpha > \gamma$, deduciamo

$$o(z) \;=\; o(x^{p^{\gamma}})\, o(y^{m'}) \;=\; n' p^{\alpha} > n' p^{\gamma} = n = o(x).$$

Questo è assurdo perché x è elemento di ordine massimo. □

Lemma B1.4. *Siano G un gruppo abeliano finito e $H = \langle x \rangle$, con x elemento di G di ordine massimo. Sia Hy un laterale di G/H di ordine m. Allora nel laterale Hy esiste un elemento di ordine m.*

DIMOSTRAZIONE. H è il sottogruppo generato da x che è l'elemento di ordine massimo, $H = \langle x \rangle = \{x^k \mid k = 1, 2, \cdots, o(x)\}$, quindi $|H| = o(x)$.

Prima di tutto, H è un sottogruppo normale di G perché G è abeliano, quindi $(Hy)^m = Hy^m$. Per ipotesi m è l'ordine di Hy, allora $(Hy)^m = Hy^m = H$ cioè $y^m \in H$, per cui esiste $k \in \mathbb{N}$ tale che $y^m = x^k$.

Posto $z := x^{-k/m} y$, dimostriamo che $z \in Hy$ e che $o(z) = m$.

Infatti denotando con n e ℓ rispettivamente l'ordine di x e di y, vale

$$\frac{\ell}{\mathrm{mcd}(\ell, m)} = o(y^m) = o(x^k) = \frac{n}{\mathrm{mcd}(n, k)}.$$

Osserviamo che $(Hy)^{\ell} = Hy^{\ell} = H$ perché $o(y) = \ell$, quindi $m | \ell$ e $\mathrm{mcd}(\ell, m) = m$. Allora abbiamo la seguente implicazione:

$$\frac{k}{m} = \frac{k}{\mathrm{mcd}(n, k)} \cdot \frac{\mathrm{mcd}(n, k)}{m} = \frac{k}{\mathrm{mcd}(n, k)} \frac{\mathrm{mcd}(n, k)}{\mathrm{mcd}(\ell, m)} = \frac{k}{\mathrm{mcd}(n, k)} \cdot \frac{n}{\ell}.$$

Notiamo che $\frac{k}{\text{mcd}(n,k)}$ e $\frac{n}{\ell}$ sono due interi dove l'ultimo lo è per il Lemma **B1.3** perché n è l'ordine massimo degli elementi di G ed ℓ è l'ordine di $y \in G$. Concludendo $-\frac{k}{m}$ è un intero e, per come è definito H, $x^{-\frac{k}{m}}$ è un suo elemento, quindi $z \in Hy$.

Rimane da provare che l'ordine di z è m. Osserviamo che $z^m = (x^{-\frac{k}{m}}y)^m = x^{-k}y^m$, ricordando che $y^m = x^k$, allora $z^m = x^{-k}x^k = e$ da cui $o(z)|m$. Sappiamo che $x^{-\frac{k}{m}}$ appartiene ad H, per cui $Hz = Hx^{-\frac{k}{m}}y = Hy$; conseguentemente $o(Hz) = o(Hy) = m$. Notando che

$$(Hz)^{o(z)} = Hz^{o(z)} = H$$

allora $m|o(z)$, per cui $o(z) = m$. □

Teorema B1.5 (Teorema fondamentale dei gruppi abeliani finiti). *Sia G un gruppo abeliano finito di ordine n. Allora G è isomorfo al prodotto diretto*

$$G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell \qquad (\star\star)$$

di gruppi ciclici G_k di ordini e_k con $k = 1, 2, \cdots, \ell$. Gli interi $\{e_k\}$ godono delle seguenti proprietà:

(a) *e_k divide e_{k-1} per $k = 2, 3, \cdots, \ell$.*
(b) *il prodotto degli $\{e_k\}$ uguaglia l'ordine di G: $n = e_1 e_2 \cdots e_\ell$.*
(c) *gli $\{e_k\}$ sono univocamente determinati dalle proprietà* **[a]** *e* **[b]**, *essi sono denominati* fattori invarianti *del gruppo G.*

DIMOSTRAZIONE. Dimostriamo **[a]** e **[b]** per induzione su n.

Se $n = 1$, cioè $|G| = 1$ è banale. Supponiamo vera la tesi per i gruppi di ordine minore di $n > 1$ e dimostriamo la sua veridicità anche per i gruppi di ordine n.

Sia G un gruppo abeliano finito con $|G| = n$, sappiamo che esiste g_1 elemento di massimo ordine in G con $o(g_1) = e_1 > 1$. Definiamo $G_1 = \langle g_1 \rangle$ dato che G è abeliano allora G_1 è sottogruppo normale di G. Possiamo allora formare il gruppo quoziente G/G_1, per il Teorema **A1.7** di Lagrange si ha che $|G/G_1| = n/e_1 < n$. Applicando ora l'ipotesi induttiva al gruppo G/G_1:

$$G/G_1 \cong H_2 \otimes H_3 \otimes \cdots \otimes H_\ell$$

dove H_k è un gruppo ciclico per ogni $k = 2, 3, \cdots, \ell$, cioè esiste un $h_k \in G$ tale che $H_k = \langle h_k G_1 \rangle$ con $|H_k| = e_k$. Inoltre, si ha ovviamente $|G/G_1| = e_2 \cdots e_\ell = n/e_1$ e $e_k|e_{k-1}$ per $k = 3, 4, \cdots, \ell$.

Per il Lemma **B1.4** in ogni laterale $h_k G_1$ esiste un elemento g_k avente ordine e_k. Denotiamo con G_k il gruppo ciclico generato da g_k, allora per ogni $k = 2, 3, \cdots, \ell$ si ha che $G_k \cong H_k$ con $|G_k| = e_k$ e $e_{k+1}|e_k$. Ponendo

$H = G_2 \cdot G_3 \cdots G_\ell$, vogliamo dimostrare $H = G_2 \otimes G_3 \otimes \cdots \otimes G_\ell$ verificando che $|H| = e_2 \cdot e_3 \cdots e_\ell$ per la caratterizzazione del prodotto diretto.

Consideriamo la restrizione ad H dell'epimorfismo canonico

$$\phi : G \longrightarrow G/G_1 \quad \text{tale che} \quad \phi(g) = gG_1.$$

Osserviamo che ogni elemento di H può essere scritto come $h = g_2^{\gamma_2} g_3^{\gamma_3} \cdots g_\ell^{\gamma_\ell}$ perché $H = G_2 \cdot G_3 \cdots G_\ell = \langle g_2 \rangle \cdot \langle g_3 \rangle \cdots \langle g_\ell \rangle$, per cui la sua immagine è $\phi_{|H}(h) = (g_2^{\gamma_2} G_1)(g_3^{\gamma_3} G_1) \cdots (g_\ell^{\gamma_\ell} G_1)$. Per ogni $k = 2, 3, \cdots, \ell$, l'elemento g_k è nel laterale $h_k G_1$ con $o(g_k) = e_k$, allora $g_k G_1 = h_k G_1$ e $g_k^{\gamma_k} G_1 \subseteq \langle h_k G_1 \rangle$, quindi

$$\phi_{|H}(h) \in \langle h_2 G_1 \rangle \cdot \langle h_3 G_1 \rangle \cdots \langle h_\ell G_1 \rangle = H_2 \otimes H_3 \otimes \cdots \otimes H_\ell \cong G/G_1.$$

Si osserva che $|\phi(H)| = |G/G_1|$ perché

$$\begin{aligned} \phi(H) &= \phi(\langle g_2 \rangle) \cdot \phi(\langle g_3 \rangle) \cdots \phi(\langle g_\ell \rangle) \\ &= \langle g_2 G_1 \rangle \cdot \langle g_3 G_1 \rangle \cdots \langle g_\ell G_1 \rangle \\ &= \langle h_2 G_1 \rangle \cdot \langle h_3 G_1 \rangle \cdots \langle h_\ell G_1 \rangle \\ &= H_2 \otimes H_3 \otimes \cdots \otimes H_\ell \cong G/G_1. \end{aligned}$$

Quindi la funzione è suriettiva, da cui si ottiene $|H| \geq |\phi(H)| = e_2 e_3 \cdots e_\ell$, dato che è assurdo che un insieme abbia meno elementi della sua immagine. Ricordando come è definita H, si ha che $|H| \leq e_2 e_3 \cdots e_\ell$ per cui si conferma l'uguaglianza $|H| = e_2 e_3 \cdots e_\ell$. Secondo il Corollario **A4.3** H è il prodotto diretto degli $\{G_i\}$:

$$H = G_2 \otimes G_3 \otimes \cdots \otimes G_\ell.$$

Ora verifichiamo che $G = HG_1$. Infatti $HG_1 \subseteq G$ perché $H \leq G$ e $G_1 \leq G$. Inoltre si ha che $HG_1 \supseteq G$ visto che se $g \in G$ esiste $h \in H$ tale che $hG_1 = \phi(g) = gG_1$ allora esiste $g' \in G_1$ tale che $g = hg'$ per cui $g \in HG_1$.

Secondo l'isomorfismo $H \cong G/G_1$, sappiamo ora che $|H| = |G/G_1| = |HG_1/G_1|$, inoltre G_1 è sottogruppo normale di G e $H \leq G$; allora per il Teorema **A3.4** di isomorfismo $HG_1/G_1 \cong H/(H \cap G_1)$, quindi $|H \cap G_1| = 1$ cioè $H \cap G_1 = \{e\}$.

Per la caratterizzazione del prodotto diretto, abbiamo $G \cong H \otimes G_1$. Dato che $H \cong G_2 \otimes \cdots \otimes G_\ell$ allora $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$ con $|G_k| = e_k$ per ogni $k = 1, 2, \cdots, \ell$. Si verificano anche $e_k | e_{k-1}$ per $k = 2, 3, \cdots, \ell$ utilizzando il fatto che e_1 è ordine massimo quindi $e_2 | e_1$ e l'ipotesi induttiva applicata a $G/G_1 \cong H_2 \otimes H_3 \otimes \cdots \otimes H_\ell$.

Abbiamo così dimostrato le prime due tesi. Rimane solo da verificare l'ultima; ovvero l'unicità.

Supponiamo che $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$ ed anche $G \cong G'_1 \otimes G'_2 \otimes \cdots \otimes G'_{\ell'}$ con $|G_\ell| > 1$ e $|G'_{\ell'}| > 1$ tali che valgano **[a]** e **[b]** per entrambe. Senza perdere di generalità, si assume che $\ell \leq \ell'$. Allora

$$G_1 = \langle g_1 \rangle \quad \text{con } g_1 \text{ elemento di ordine massimo in } G \Rightarrow e'_1 | e_1,$$
$$G'_1 = \langle g'_1 \rangle \quad \text{con } g'_1 \text{ elemento di ordine massimo in } G \Rightarrow e_1 | e'_1;$$

quindi $e_1 = e'_1$, allora $G_1 \cong G'_1$ e $G/G_1 \cong G/G'_1$ ovvero

$$G_2 \otimes G_3 \otimes \cdots \otimes G_\ell \cong G'_2 \otimes \cdots \otimes G'_{\ell'}.$$

Ripetiamo il procedimento

$$G_2 = \langle g_2 \rangle \text{ con } g_2 \text{ elemento di ordine massimo in } G_2 \otimes G_3 \otimes \cdots \otimes G_\ell,$$
$$G'_2 = \langle g'_2 \rangle \text{ con } g'_2 \text{ elemento di ordine massimo in } G'_2 \otimes G'_3 \otimes \cdots \otimes G'_{\ell'};$$

quindi $e_2 = e'_2$, ed analogamente

$$G_1 \otimes G_2 \cong G'_1 \otimes G'_2$$

il che implica

$$G_3 \otimes G_4 \otimes \cdots \otimes G_\ell \cong G'_3 \otimes \cdots \otimes G'_{\ell'}.$$

Continuando a ripetere il procedimento per $G_3, G_4, G_5, \cdots$ fino a G_ℓ, otteniamo $G_\ell \cong G'_\ell \otimes \cdots \otimes G'_{\ell'}$. Analogamente $e_\ell = e'_\ell$ e $G_\ell \cong G'_\ell$ per cui risulta

$$G_\ell/G_\ell = \{e\} = G'_\ell \otimes \cdots \otimes G'_{\ell'}/G'_\ell$$

ciò significa $\ell = \ell'$. Ricapitolando possiamo concludere che $|G_k| = |G'_k|$ per ogni $k = 1, 2, \cdots, \ell = \ell'$. □

B2. p-gruppi e decomposizione primaria ciclica

Denotiamo con $\mathbb{P}$ l'insieme dei numeri primi. Fissato un numero primo $p \in \mathbb{P}$, un *p-elemento* di un gruppo G è un elemento il cui ordine è una potenza di p. Se tutti gli elementi di G tranne l'elemento neutro sono p-elementi allora G si dice *p-gruppo*.

L'esempio più semplice è il gruppo di Klein che è un p-gruppo con $p = 2$. Infatti, fissate nel piano due rette perpendicolari a e b, e detto c il loro punto d'intersezione, le riflessioni $\sigma_a, \sigma_b, \sigma_c$ rispetto ad a, b, c formano un gruppo abeliano di ordine 4 assieme alla funzione identica I. Si osserva che ogni riflessione è l'inversa di se stessa, perché $\sigma_a \sigma_a = \sigma_a \sigma_a^{-1} = I$ quindi $o(\sigma_a) = 2$ ed analogamente per $o(\sigma_c) = 2$ con $\sigma_c = \sigma_a \cdot \sigma_b$. Conseguentemente questo gruppo è formato esclusivamente da p-elementi con $p = 2$.

Denotiamo con $(U_n, \cdot)$ il gruppo delle n-sime radici dell'unità. Quando $n = 9$, si ha che $(U_9, \cdot)$ è un p-gruppo con $p = 3$, che è isomorfo al gruppo

$(\mathbb{Z}_9, +)$. In generale, per ogni $n = p^k$, con p primo i gruppi $(U_n, \cdot)$ e $(\mathbb{Z}_n, +)$ sono dei p-gruppi.

Teorema B2.1 (Cauchy). *Se p è un primo che divide l'ordine di un gruppo finito G, allora esiste in G un sottogruppo di ordine p.*

DIMOSTRAZIONE. Sia G un gruppo, $|G| = n < \infty$ e sia $p \in \mathbb{P}$ tale che $p|n$. Dimostrando che G contiene un elemento x di ordine p, si ottiene l'esistenza in G di un sottogruppo di ordine p, il sottogruppo generato dall'elemento x. Costruiamo un insieme di p-uple di elementi di G:

$$\Omega := \{(x_1, x_2, \cdots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = e\}.$$

Essendo G finito possiamo contare le p-uple che formano Ω. Variando un solo elemento nella p-upla, ad esempio x_1, otteniamo n p-uple distinte, perché x_1 può variare in G in n modi. Variando due elementi si hanno n^2 p-uple distinte. Procedendo in questo modo arriveremo a variare i primi $p-1$ elementi ottenendo n^{p-1} p-uple distinte. L'ultimo elemento della p-upla invece non può variare perché deve essere $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$ in modo che la p-upla stia in Ω. Dunque $\Omega = n^{p-1}$. Definiamo ora una permutazione π su Ω tale che:

$$\pi(x_1, x_2, \cdots, x_p) := (x_2, x_3, \cdots x_p, x_1).$$

Osserviamo che il gruppo ciclico generato da π ha ordine p. Infatti, per $k = 1, 2, \cdots, p$ si vede facilmente che

$$\pi^k(x_1, x_2, \cdots, x_p) = (x_{k+1}, x_{k+2}, \cdots, x_p, x_1, x_2, \cdots, x_k)$$

e π^p è evidentemente la permutazione identica.

Fissata la p-upla $(x_1, x_2, \cdots, x_p)$ chiamiamo $\mathcal{C}$ l'insieme delle sue permutazioni tramite π^k con $k = 1, 2, \cdots, p$. Per ogni $k = 1, 2, \cdots, p$ si ha che

$$x_1 = x_2 = \cdots = x_p \quad \Longrightarrow \quad \pi^k(x_1, x_2, \cdots, x_p) = (x_1, x_2, \cdots, x_p)$$

cioè tutte le le permutazioni sono uguali: $|\mathcal{C}| = 1$.

Se invece in $(x_1, x_2, \cdots, x_p)$ esistono due componenti distinte, dette x_i e x_j con $i < j$ si ha che $|\mathcal{C}| = p$. Infatti, se per assurdo fosse $|\mathcal{C}| < p$ allora esisterebbero $\imath$ e $\jmath$ con $\imath < \jmath$ tali che

$$\pi^\imath(x_1, x_2, \cdots, x_p) = \pi^\jmath(x_1, x_2, \cdots, x_p)$$

che equivale alla seguente

$$(x_1, x_2, \cdots, x_p) = \pi^{\jmath-\imath}(x_1, x_2, \cdots, x_p).$$

Allora π^{j-i} genera un sottogruppo invariante di $\langle\pi\rangle$ di ordine p. Ricordiamo che $\langle\pi^{j-i}\rangle \neq \{id = \pi^p\}$ in quanto $i \neq j$. Dunque $\langle\pi^{j-i}\rangle = \{\pi\}$ che implica

$$\pi^{i-1}(x_1, x_2, \cdots, x_p) = \pi^{j-1}(x_1, x_2, \cdots, x_p).$$

Secondo la definizione di π

$$\begin{aligned} \pi^{i-1}(x_1, x_2, \cdots, x_p) &= (x_i, x_{i+1} \cdots, x_p, x_1, x_2, \cdots, x_{i-1}), \\ \pi^{j-1}(x_1, x_2, \cdots, x_p) &= (x_j, x_{j+1} \cdots, x_p, x_1, x_2, \cdots, x_{j-1}); \end{aligned}$$

si stabilisce $x_i = x_j$, che è assurdo.

Concludendo possiamo dividere Ω in due classi distinte: Ω_1 formata dalle p-uple tali che $|\mathcal{C}| = 1$ e Ω_2 formata dalle p-uple tali che $|\mathcal{C}| = p$. Siano r ed s rispettivamente le cardinalità di tali classi, allora $|\Omega| = r + s$, cioè $n^{p-1} = r + s$. Per ipotesi $p|n$ per cui $p|n^{p-1} = r + s$, s è multiplo di p perché ogni membro di Ω_2 genera una classe di p membri, quindi $p|r$ dove $r \neq 0$ perché $(e, e, \cdots, e) \in \Omega_1$. Allora esistono altri membri con componenti identici, ma diversi dall'elemento neutro in Ω_1.

Sia $(x, x, \cdots, x)$ un membro di Ω_1 con $x \neq e$, sappiamo che $x^p = e$ per cui $o(x)|p$ ed essendo $p \in \mathbb{P}$ e $o(x) \neq 1$ si ha $o(x) = p$. Dunque $\langle x\rangle$ è un sottogruppo di ordine p in G. □

Corollario B2.2. *Sia G un p-gruppo finito, allora l'ordine di G è una potenza di p.*

DIMOSTRAZIONE. Supponiamo $|G| = n$. Sia $q \in \mathbb{P}$ tale che $q|n$. Per il teorema di Cauchy esiste in G un sottogruppo di ordine q, e, come abbiamo visto, esso è il sottogruppo ciclico $\langle x\rangle$ dove x è un q-elemento. Osserviamo che x deve essere un p-elemento perché G è un p-gruppo, ovvero $p = q$. Riassumendo, per ogni $q \in \mathbb{P}$ tale che $q|n$, si ha che $p = q$. Ne segue che n contiene nella sua fattorizzazione in numeri primi solo p ripetuto un certo numero di volte, ovvero n è una potenza di p. □

OSSERVAZIONE: Siano $\ell_1, \ell_2, \cdots, \ell_n$ coprimi, cioè $\mathrm{mcd}(\ell_1, \ell_2, \cdots, \ell_n) = 1$, allora esistono n interi $\lambda_1, \lambda_2, \cdots, \lambda_n$ non tutti nulli tali che $\sum_{k=1}^{n} \ell_k \lambda_k = 1$.

DIMOSTRAZIONE. Dimostriamo la tesi per induzione su m.

Per $n = 2$, la tesi è un fatto già conosciuto. Ora supponiamo vera la tesi per n numeri interi e dimostriamo che vale per $n+1$. Siano $\ell_0, \ell_1, \ell_2, \cdots, \ell_n$ interi coprimi e sia $d := \mathrm{mcd}(\ell_1, \ell_2, \cdots, \ell_n)$, si ha che $\mathrm{mcd}(\ell_0, d) = 1$ per cui esistono λ_0, β interi tali che $\ell_0\lambda_0 + d\beta = 1$. Applichiamo l'ipotesi induttiva

a $\{\ell_1/d, \ell_2/d, \cdots, \ell_n/d\}$, che sono banalmente coprimi ed otteniamo che esistono $\mu_1, \mu_2, \cdots, \mu_n$ interi non tutti nulli tali che

$$\sum_{k=1}^{n} \frac{\ell_k}{d}\mu_k = 1 \quad \Longrightarrow \quad \sum_{k=1}^{n} \ell_k \mu_k = d \quad \Longrightarrow \quad \ell_0\lambda_0 + \beta \sum_{k=1}^{n} \ell_k \mu_k = 1$$

definendo $\lambda_k := \beta\mu_k$ per ogni $k = 1, 2, \cdots, n$ si ha $\sum_{k=0}^{n} \ell_k \lambda_k = 1$. □

Lemma B2.3. *Siano G un gruppo e g un elemento di ordine finito. Allora*

(a) *se $o(g) = mn$, con m e n primi tra loro, allora g si scrive in modo unico come prodotto di due elementi x e y di potenze di g, i quali sono permutabili e di ordine m e n rispettivamente.*

(b) *se $o(g) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ è la scomposizione di $o(g)$ in fattori primi con $p_1, p_2, \cdots, p_n$ distinti, g si scrive in modo unico come prodotto di n elementi $x_1, x_2, \cdots, x_n$ di potenze di g, i quali sono a due a due permutabili e di ordini $p_1^{m_1}$, $p_2^{m_2}, \cdots, p_n^{m_n}$ rispettivamente.*

DIMOSTRAZIONE. Verifichiamo separatamente le due tesi.

[a] Da $(m, n) = 1$ segue l'esistenza di α, γ interi tali che $m\alpha + n\gamma = 1$. Definendo $x := g^{n\gamma}$ e $y := g^{m\alpha}$, possiamo allora verificare che $xy = yx = g^{m\alpha+n\gamma} = g$, perciò g si scrivere come prodotto di xy o di yx, dove x e y sono potenze di g.

Resta da dimostrare che $o(x) = m$ e $o(y) = n$ e che x ed y sono gli unici elementi di questo tipo. Vale che

$$x^m = (g^{n\gamma})^m = (g^{mn})^\gamma = e \quad \Longrightarrow \quad o(x)|m;$$
$$y^n = (g^{m\alpha})^n = (g^{mn})^\alpha = e \quad \Longrightarrow \quad o(y)|n.$$

Per il Lemma **B1.2**, segue

$$mn = o(g) = o(xy) \mid \mathrm{mcm}\{o(x), o(y)\} \mid mn.$$

Allora $o(xy) = o(x)o(y) = mn$ quindi $o(x) = m$ e $o(y) = n$.

Infine, dobbiamo provare l'unicità; supponiamo che $g = xy$ ed anche $g = x_1y_1$ tali che $o(x) = o(x_1) = m$ e $o(y) = o(y_1) = n$. Allora da $xy = g = x_1y_1$ otteniamo $x_1^{-1}x = y_1y^{-1}$ moltiplicando a sinistra per x_1^{-1} e a destra per y^{-1}. Posto $z = x_1^{-1}x = y_1y^{-1}$ vale che $o(z)|m$ e $o(z)|n$, in quanto $z^m = (x_1^{-1}x)^m = x_1^{-m}x^m = e$, ed inoltre $z^n = (y_1y^{-1})^n = y_1^n y^{-n} = e$, quindi $o(z)$ è comune divisore di m ed n, ma $\mathrm{mcd}(m, n) = 1$ quindi $o(z) = 1$ che equivale a dire $x = x_1$ e $y = y_1$.

[b] Definendo

$$\ell_k := \frac{o(g)}{p_k^{m_k}} \quad \text{per} \quad k = 1, 2, \cdots, n$$

osserviamo che

$$\ell_k = \frac{o(g)}{p_k^{m_k}} = \prod_{\substack{i=1 \\ i\neq k}}^{n} p_i^{m_i} \qquad \Longrightarrow \qquad p_k \nmid \ell_k$$

per cui non esiste nessun p_k divisore comune per $\{\ell_k\}_{k=1}^n$ e dunque si ha che $\text{mcd}(\ell_1, \ell_2, \cdots, \ell_n) = 1$. Per l'osservazione precedente esistono $\lambda_1, \lambda_2, \cdots, \lambda_n$ interi tali che $\sum_{k=1}^n \ell_k \lambda_k = 1$. Ponendo $x_k = g^{\ell_k \lambda_k}$ per ogni $k = 1, 2, \cdots, n$, si ha che

$$g = x_1 x_2 \cdots x_\ell = g^{\ell_1 \lambda_1} g^{\ell_2 \lambda_2} \cdots g^{\ell_n \lambda_n}.$$

Verifichiamo ora che $o(x_k) = p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$.

$$x_k^{p_k^{m_k}} = (g^{\ell_k \lambda_k})^{p_k^{m_k}} = (g^{o(g)})^{\lambda_k} = e$$

quindi $o(x_k) | p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$. Per il Lemma **B1.2**

$$o(g) = o(x_1 x_2 \cdots x_n) \mid \text{mcm}\{o(x_1), o(x_2), \cdots, o(x_n)\}$$

$$= o(x_1) o(x_2) \cdots o(x_m) \mid o(g) = \prod_{k=1}^{n} p_k^{m_k}$$

ne segue

$$o(x_1) o(x_2) \cdots o(x_n) = o(g) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}.$$

Quindi $o(x_k) = p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$.

Resta ora da provare l'unicità. Sia $g = x_1 x_2 \cdots x_n$ ed anche che $g = y_1 y_2 \cdots y_n$ con $o(x_k) = o(y_k) = p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$. Da

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_n$$

si ha che

$$x_k y_k^{-1} = \prod_{\substack{i=1 \\ i\neq k}}^{n} x_i^{-1} y_i \quad \text{per ogni} \quad k = 1, 2, \cdots, n.$$

Posto

$$z_k = x_k y_k^{-1} = \prod_{\substack{i=1 \\ i\neq k}}^{n} x_i^{-1} y_i \quad \text{si osserva che} \quad o(z_k) | p_k^{m_k} \quad \text{e} \quad o(z_k) | \ell_k.$$

Notando $o(x_k) = o(y_k) = p_k^{m_k}$, si ha che

$$z_k^{p_k^{m_k}} = (x_k y_k^{-1})^{p_k^{m_k}} = x_k^{p_k^{m_k}} y_k^{-p_k^{m_k}} = e \quad \text{e} \quad z_k^{\ell_k} = \prod_{\substack{i=1 \\ i\neq k}}^{n} (x_i^{-1} y_i)^{\ell_k} = e$$

dove l'ultimo passaggio si giustifica col fatto che ℓ_k è un multiplo di $p_i^{m_i}$ per $i \neq k$. Ricordando che $\text{mcd}(\ell_k, p_k^{m_k}) = 1$ si ha $o(z_k) = 1$ che equivale a $x_k = y_k$ per $k = 1, 2, \cdots, n$. □

Teorema B2.4 (Decomposizione primaria ciclica). *Un gruppo abeliano finito G è isomorfo al prodotto diretto di p-gruppi ciclici, gli ordini dei quali sono univocamente determinati. Tali ordini dei p-gruppi ciclici si chiamano* divisori elementari *di G.*

DIMOSTRAZIONE. Sia $|G| = \prod_{k=1}^{n} p_k^{m_k}$, dove $\{p_k\}_{k=1}^{n}$ sono i numeri primi distinti e $\{m_k\}_{k=1}^{n}$ sono i numeri naturali. Per il Teorema fondamentale **B1.5** dei gruppi abeliani finiti, vale che $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$ dove G_k è un gruppo ciclico con $|G_k| = e_k$ per $k = 1, 2, \cdots, \ell$ che soddisfano $|G| = e_1 e_2 \cdots e_\ell$ e $e_k | e_{k-1}$ per $k = 2, 3, \cdots, \ell$.

Dato che $|G| = e_1 e_2 \cdots e_\ell$, è evidente che e_i è prodotto di alcuni primi nella decomposizione di $|G|$, così $e_i = \prod_{k=1}^{n} p_k^{m_{ki}}$ per $i = 1, 2, \cdots, \ell$ (banalmente $m_{ki} \leq m_k$ per $k = 1, 2, \cdots, n$ e $i = 1, 2, \cdots, \ell$).

Consideriamo ciascuno di tali gruppi ciclici $G_i = \langle g_i \rangle$ con $g_i \in G$ ed $o(g_i) = e_i$, per il Lemma **B2.3** esistono n elementi $g_{i1}, g_{i2}, \cdots, g_{in} \in G$ tali che $o(g_{ik}) = p_k^{m_{ki}}$ e $g_i = g_{i1} g_{i2} \cdots g_{in}$. Per il Corollario **A4.3**, $G_i = \langle g_i \rangle$ è isomorfo al prodotto dei p_k-gruppi ciclici $\langle g_{ik} \rangle$ con $k = 1, 2, \cdots, n$. Applicando il teorema fondamentale dei gruppi abeliani finiti, otteniamo la decomposizione primaria ciclica come segue:

$$G \cong \bigotimes_{i=1}^{\ell} G_i \cong \bigotimes_{i=1}^{\ell} \bigotimes_{k=1}^{n} \langle g_{ik} \rangle.$$

L'unicità dei divisori elementari discende banalmente dall'unicità dei fattori invarianti e_i e dall'unicità della loro decomposizione in fattori primi. □

Corollario B2.5 (Decomposizione in p-gruppi). *Un gruppo abeliano finito è isomorfo al prodotto diretto di p-sottogruppi, gli ordini dei quali sono univocamente determinati.*

DIMOSTRAZIONE. Raggruppando i componenti del doppio prodotto diretto nel teorema della primaria ciclica, si ha che

$$G \cong \bigotimes_{i=1}^{\ell} \bigotimes_{k=1}^{n} \langle g_{ik} \rangle \cong \bigotimes_{k=1}^{n} \left\{ \bigotimes_{i=1}^{\ell} \langle g_{ik} \rangle \right\}$$

dove il prodotto interno nelle parentesi graffe è un p_k-gruppo finito. □

B3. Fattori invarianti e divisori elementari

Per decomporre un generico gruppo abeliano finito di ordine n e per trovare quindi, quanti sono i gruppi abeliani di ordine n a meno di isomorfismi, si hanno a disposizione tre metodi dati dai seguenti teoremi:

- Il teorema fondamentale dei gruppi abeliani finiti: **B1.5**.
- Il teorema di decomposizione primaria ciclica: **B2.4**.
- Il corollario di decomposizione in p-gruppi: **B2.5**.

Esempio B3.1 (p-gruppo abeliano finito). *Sia $m = p^n$ con p primo. Secondo il Teorema* **B1.5**, *i fattori invarianti di un gruppo abeliano di ordine p^n hanno le forme:*

$$e_k = p^{\lambda_k} \quad con \quad \begin{cases} \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0, \\ \lambda_1 + \lambda_2 + \cdots + \lambda_\ell = n; \end{cases}$$

essi sono anche i divisori elementari. Dunque, esiste una corrispondenza fra i gruppi abeliani non isomorfi di ordine p^n e l'insieme delle successioni $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n > 0$ con $\lambda_1 + \lambda_2 + \cdots + \lambda_n = n$.

Esempio B3.2. *Sia $m = 36 = 2^2 \cdot 3^2$. La seguente tabella illustra la struttura dei gruppi abeliani di ordine 36, dove si denota con C_n un gruppo ciclico di ordine n:*

No	Fattori Invarianti	Divisori Elementari
C_6	2×3	2, 3
C_6	2×3	2, 3
C_{18}	2×3^2	2, 3^2
C_2	2	2
C_{12}	$2^2 \times 3$	2^2, 3
C_3	3	3
C_{36}	$2^2 \times 3^2$	2^2, 3^2

Dunque esistono 4 gruppi abeliani non isomorfi di ordine 36:

$$\begin{aligned} G_1 &\cong C_6 \otimes C_6, \\ G_2 &\cong C_{18} \otimes C_2, \\ G_3 &\cong C_{12} \otimes C_3, \\ G_4 &\cong C_{36}. \end{aligned}$$

Analogamente i gruppi abeliani non isomorfi di ordine 36 hanno decomposizione primaria ciclica come segue:

$$\begin{aligned} G_1 &\cong C_2 \otimes C_2 \otimes C_3 \otimes C_3, \\ G_2 &\cong C_2 \otimes C_2 \otimes C_9, \\ G_3 &\cong C_3 \otimes C_3 \otimes C_4, \\ G_4 &\cong C_4 \otimes C_9. \end{aligned}$$

Esempio B3.3. *Sia $m = p^2q^3$ con p e q primi distinti. Esistono 6 gruppi abeliani non isomorfi di ordine p^2q^3. Vengono tabulati i fattori invarianti e i divisori elementari rispettivemente come segue:*

No	Fattori Invarianti	Divisori Elementari
C_{pq}	pq	$p,\ q$
C_{pq}	pq	$p,\ q$
C_q	q	q
C_{pq^2}	pq^2	$p,\ q^2$
C_{pq}	pq	$p,\ q$
C_{pq^3}	pq^3	$p,\ q^3$
C_p	p	p
C_{p^2q}	p^2q	$p^2,\ q$
C_q	q	q
C_q	q	q
$C_{p^2q^2}$	p^2q^2	$p^2,\ q^2$
C_q	q	q
$C_{p^2q^3}$	p^2q^3	$p^2,\ q^3$

Secondo il teorema dei gruppi abeliani, abbiamo le seguenti decomposizioni:

$$\begin{aligned} H_1 &\cong C_{pq} \otimes C_{pq} \otimes C_q, \\ H_2 &\cong C_{pq^2} \otimes C_{pq}, \\ H_3 &\cong C_{pq^3} \otimes C_p, \\ H_4 &\cong C_{p^2q} \otimes C_q \otimes C_q, \\ H_5 &\cong C_{p^2q^2} \otimes C_q, \\ H_6 &\cong C_{p^2q^3}. \end{aligned}$$

Resta da provare

$$H_k \cap \langle H_i \mid i \neq k \text{ con } 1 \leq i \leq n \rangle \;=\; \{e\}$$

con "e" elemento neutro di G. Supponiamo per assurdo che esista un elemento $y \neq e$ appartenente all'intersezione, allora esistono gli interi $\{m_k\}_{k=1}^{n}$ non tutti nulli tali che

$$y \;=\; x_k^{-m_k} \;=\; x_1^{m_1} x_2^{m_2} \cdots x_{k-1}^{m_{k-1}} x_{k+1}^{m_{k+1}} \cdots x_n^{m_n}$$

per cui valgono le ipotesi del teorema precedente:

$$x_1^{m_1} x_2^{m_2} \cdots x_{k-1}^{m_{k-1}} \cdot x_k^{m_k} \cdot x_{k+1}^{m_{k+1}} \cdots x_n^{m_n} \;=\; e$$

il quale garantisce l'esistenza di un elemento di periodo finito, diverso dall'elemento neutro in G. Questo è assurdo perché G è privo di torsione. □

Corollario B4.4. *Sia G un gruppo abeliano libero* (privo di torsione) *e finitamente generato. Se valgono*

$$\begin{aligned} G &\cong H_1 \otimes H_2 \otimes \cdots \otimes H_m, \\ G &\cong K_1 \otimes K_2 \otimes \cdots \otimes K_n; \end{aligned}$$

dove H_i e K_j sono gruppi ciclici infiniti, allora $m = n$.

DIMOSTRAZIONE. Supponiamo per assurdo che $m \neq n$ e ipotizziamo $m > n$ senza perdere di generalità. Sia x_i il generatore di H_i e y_j quello di K_j, allora $\{x_i\}_{i=1}^{m}$ e $\{y_j\}_{j=1}^{n}$ sono due sistemi di generatori per G; conseguentemente ogni generatore dei due sistemi si può esprimere in funzione degli elementi dell'altro sistema, in particolare per ogni x_i esistono s_{ij} interi tali che $x_i = \prod_{j=1}^{n} y_j^{s_{ij}}$. Consideriamo la matrice di elementi s_{ij}, questa è una matrice di ordine $m \times n$. Il numero delle righe è maggiore di quello delle colonne, per cui le m righe sono linearmente dipendenti, cioè esistono m numeri interi $\{r_i\}_{i=1}^{m}$ non tutti nulli tali che

$$\sum_{i=1}^{m} r_i \cdot s_{ij} \;=\; 0 \quad \text{per} \quad j = 1, 2, \cdots, n.$$

Si osserva che

$$\begin{aligned} x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m} \;&=\; \prod_{i=1}^{m} \Big\{ \prod_{j=1}^{n} y_j^{s_{ij}} \Big\}^{r_i} \;=\; \prod_{i=1}^{m} \prod_{j=1}^{n} y_j^{r_i s_{ij}} \\ &=\; \prod_{j=1}^{n} \prod_{i=1}^{m} y_j^{r_i s_{ij}} \;=\; \prod_{j=1}^{n} y_j^{\sum_{i=1}^{m} r_i s_{ij}} \end{aligned}$$

per cui si ottiene

$$x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m} \;=\; \prod_{j=1}^{n} y_j^{0} \;=\; e.$$

Ora, supponendo $r_1 \neq 0$, possiamo riformulare

$$x_1^{r_1} = \prod_{i=2}^{m} x_i^{-r_i} \quad \Longrightarrow \quad H_1 \bigcap \langle H_i \mid i = 2, 3, \cdots, m \rangle = \langle x_1^{r_1} \rangle \neq \{e\}.$$

Quest'ultimo è in contraddizione con il fatto che G è prodotto diretto di H_i con $i = 1, 2, \cdots, m$. In conclusione, abbiamo dimostrato $m = n$. □

Teorema B4.5. *Sia G un gruppo abeliano finitamente generato. Allora G è isomorfo al prodotto diretto di gruppi ciclici, nel quale ciascun fattore è o un p-gruppo ciclico oppure è isomorfo al gruppo $\mathbb{Z}$.*

DIMOSTRAZIONE. Sia T l'insieme di tutti gli elementi di G di periodo finito. Si dimostra banalmente che T è gruppo abeliano:

- $T \neq \emptyset$ perché $e \in T$;
- Per ogni $x \in T$, vale anche $x^{-1} \in T$;
- $\forall x, y \in T$, il loro prodotto è permutabile: $x \cdot y = y \cdot x$;
- $\forall x, y \in T$, si ha che $x \cdot y \in T$ (infatti il prodotto di due elementi di periodo finito ha periodo finito).

T viene detto *sottogruppo di torsione di G*. Si osserva che $T \subseteq G$ e G finitamente generato, allora anche T sarà finitamente generato, inoltre ogni generatore di T è di periodo finito, quindi genera un numero finito di elementi, in conclusione T è finito.

Dato che T è sottogruppo normale (in quanto è abeliano) possiamo considerare il gruppo quoziente G/T. Si dimostra che G/T è un gruppo finitamente generato ed è privo di torsione. L'unico elemento di periodo finito di G/T è il suo elemento neutro, T. Infatti, sia Tx un generico elemento di G/T, se questo è di ordine finito, esiste un numero naturale ℓ tale che $(Tx)^\ell = T$, ma ciò significa che $Tx^\ell = T$, il che avviene se $x^\ell \in T$. Per definizione di T si ha che x^ℓ è di periodo finito quindi anche x è di periodo finito. Allora $x \in T$ e $Tx = T$, cioè l'elemento neutro del gruppo quoziente. G/T è gruppo abeliano libero finitamente generato per cui valgono le ipotesi del Teorema **B4.3** e del Corollario **B4.4** pertanto esiste un unico numero naturale n minimo tale che G/T è isomorfo al prodotto diretto di n gruppi ciclici, quindi

$$G/T = \langle Tx_1 \rangle \otimes \langle Tx_2 \rangle \otimes \cdots \otimes \langle Tx_n \rangle.$$

Ora definiamo un sottogruppo di G con

$$H = \langle x_1 \rangle \cdot \langle x_2 \rangle \cdots \langle x_n \rangle.$$

È facile verificare che questo è un prodotto diretto

$$H = \langle x_1 \rangle \otimes \langle x_2 \rangle \otimes \cdots \otimes \langle x_n \rangle.$$

Infatti, tutti i gruppi ciclici $\{\langle x_i\rangle\}_{i=1}^{n}$ sono normali, inoltre, l'intersezione tra $\langle x_j\rangle$ ed il sottogruppo generato dagli $\langle x_i\rangle$ con $i \neq j$ è composta dal solo elemento neutro. Altrimenti avremo un elemento in comune della forma

$$x_j^{-m_j} = \prod_{i\neq j} x_i^{m_i}$$

dove $m_1, m_2, \cdots, m_n$ sono numeri interi non tutti nulli; il che equivale alla relazione

$$x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} = e \quad \Longrightarrow \quad Tx_1^{m_1} \cdot Tx_2^{m_2} \cdots Tx_n^{m_n} = T.$$

Questo è assurdo perché G/T è prodotto diretto dei gruppi ciclici $\langle Tx_i\rangle$ con $i = 1, 2, \cdots, n$.

Analogamente si verifica che H è privo di torsione, perciò $T \cap H = \{e\}$. Per confermare che G è prodotto diretto di T e H, dobbiamo provare prima di tutto che $G = TH$.

Per ogni $g \in G$, abbiamo che $g \in Tg \in G/T$. Allora esistono n numeri interi $\{\ell_i\}_{i=1}^{n}$ tali che

$$Tg = Tx_1^{\ell_1} \cdot Tx_2^{\ell_2} \cdots Tx_n^{\ell_n} = Th \quad \text{con} \quad h = x_1^{\ell_1} x_2^{\ell_2} \cdots x_n^{\ell_n} \in H.$$

Questa relazione significa che esiste $t \in T$ tale che $g = th$. Così abbiamo dimostrato che $G = TH$.

Dato che T è un gruppo abeliano finito, allora T è prodotto diretto di p-gruppi ciclici secondo la decomposizione primaria ciclica. Inoltre, H è un gruppo abeliano finitamente generato privo di torsione, quindi H è prodotto diretto di gruppi ciclici isomorfi a $(\mathbb{Z}, +)$.

In conclusione, G è isomorfo al prodotto diretto di gruppi ciclici, nel quale ciascun fattore è o un p-gruppo ciclico oppure è isomorfo al gruppo $\mathbb{Z}$. □

B5. Partizioni e numero dei gruppi abeliani finiti

Definizione B5.1. *Un p-gruppo abeliano finito di divisori elementari* (fattori invarianti) $\{p^{\lambda_k}\}_{k=1}^{\ell}$ *con* $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0$ *si dice p-gruppo di* tipo $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$.

Sia G un p-gruppo abeliano finito, allora esiste $n \in \mathbb{N}$ tale che $|G| = p^n$. Per il Teorema **B1.5** si ha che $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$, dove G_k è un gruppo ciclico di ordine e_k con $k = 1, 2, \cdots, \ell$ che soddisfano $p^n = |G| = e_1 e_2 \cdots e_\ell$ e $e_k | e_{k-1}$ per $k = 2, 3, \cdots, \ell$. Allora ogni e_k è una potenza di p con $e_k = p^{\lambda_k}$, per cui $p^n = p^{\lambda_1} p^{\lambda_2} \cdots p^{\lambda_\ell}$ e $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0$. Perciò i fattori

invarianti sono $\left\{p^{\lambda_k}\right\}_{k=1}^{\ell}$ si ha che i gruppi ciclici G_k sono p-gruppi. Per il Teorema **B2.4** di decomposizione primaria ciclica, questi fattori invarianti coincidono con i divisori elementari di G ordinati in modo decrescente.

OSSERVAZIONE: Siano G e G' due p-gruppi abeliani finiti, rispettivamente di tipo $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ e $(\lambda'_1, \lambda'_2, \cdots, \lambda'_{\ell'})$ aventi medesimo ordine $|G| = |G'| = p^n$, allora

$$G \cong G' \iff (\lambda_1, \lambda_2, \cdots, \lambda_\ell) = (\lambda'_1, \lambda'_2, \cdots, \lambda'_{\ell'}).$$

Infatti, se $G \cong G'$ consideriamo le decomposizioni in p-gruppi ciclici

$$G_1 \otimes G_2 \otimes \cdots \otimes G_\ell \cong G'_1 \otimes G'_2 \otimes \cdots \otimes G'_{\ell'}$$

dove G_i e G'_j sono ciclici con

$$|G_i| = p^{\lambda_i} \quad \text{per} \quad 1 \le i \le \ell: \quad n = \sum \lambda_i, \quad \lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_\ell > 0;$$
$$|G'_j| = p^{\lambda'_j} \quad \text{per} \quad 1 \le j \le \ell': \quad n = \sum \lambda'_j, \quad \lambda'_1 \ge \lambda'_2 \ge \cdots \ge \lambda'_{\ell'} > 0.$$

Questo significa che tali p-gruppi G_k e G'_k sono corrispondentemente isomorfi, per cui hanno stesso ordine e allora i fattori invarianti di G e G' sono gli stessi.

Viceversa, siano G_k e G'_k i p_k-gruppi ciclici avente ordine p^{λ_k} con $\lambda_k = \lambda'_k$ per $k = 1, 2, \cdots, \ell = \ell'$. Allora G e G' sono isomorfi.

Definizione B5.2. *Sia n un numero intero positivo. Si dice che λ è una* partizione *di n, indicata con $\lambda \vdash n$, se λ è una sequenza $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ tale che $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_\ell > 0$ e $n = |\lambda| := \sum_{k=1}^{\ell} \lambda_k$. Ogni λ_k viene detto* parte *della partizione ed $\ell := \ell(\lambda)$ è la* lunghezza *della partizione.*

Lemma B5.3. *Il numero dei p-gruppi abeliani* (non isomorfi) *di ordine p^n è dato da $p(n)$, il numero delle partizioni di n.*

DIMOSTRAZIONE. Per l'osservazione precedente due p-gruppi abeliani finiti dello stesso ordine p^n sono non isomorfi se e solo se sono di tipo diverso. Allora l'insieme dei p-gruppi abeliani (non isomorfi) di ordine p^n è formato da tutti i tipi differenti di p-gruppo abeliano di ordine p^n. Quindi la cardinalità di questo insieme è data dal numero di sequenze distinte $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ che si possono formare con $n = \sum_{k=1}^{\ell} \lambda_k$ ed $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_\ell = 0$. Queste infatti definiscono i differenti tipi $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ di p-gruppo. Per definizione di partizione si ha poi la tesi. □

Lemma B5.4. *Il numero dei gruppi abeliani* (non isomorfi) *di ordine n, dove $n = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$ con $\{p_i\}_{i=1}^{\ell}$ primi distinti è dato dal prodotto dei*

DIMOSTRAZIONE. Sia G un gruppo abeliano finito. Per il Corollario **B2.5**, esistono p_k-gruppi H_k tali che $|H_k| = p_k^{n_k}$ con $k = 1, 2, \cdots, \ell$ ed il loro prodotto diretto:

$$G \cong H_1 \otimes H_2 \otimes \cdots \otimes H_\ell.$$

Dato che per ogni H_k con $k = 1, 2, \cdots, \ell$, il numero dei p_k-gruppi di ordine $p_k^{n_k}$ tra loro non isomorfi è uguale a $p(n_k)$. Ogni componente nel prodotto diretto ha una struttura algebrica indipendente dagli altri. Allora i gruppi abeliani di ordine n (non isomorfi) sono in numero $\prod_{k=1}^{\ell} p(n_k)$. □

Ricordando l'Esempio **B3.3**. Avevamo trovato 6 gruppi abeliani di ordine $m = p^2q^3$: infatti per il Lemma **B5.4**, $p(2)\,p(3) = 2 \cdot 3 = 6$ come si può facilmente vedere:

$$2:\ 2 = 2,\ 2 = 1+1 \quad \text{e} \quad 3:\ 3 = 3,\ 3 = 2+1,\ 3 = 1+1+1.$$

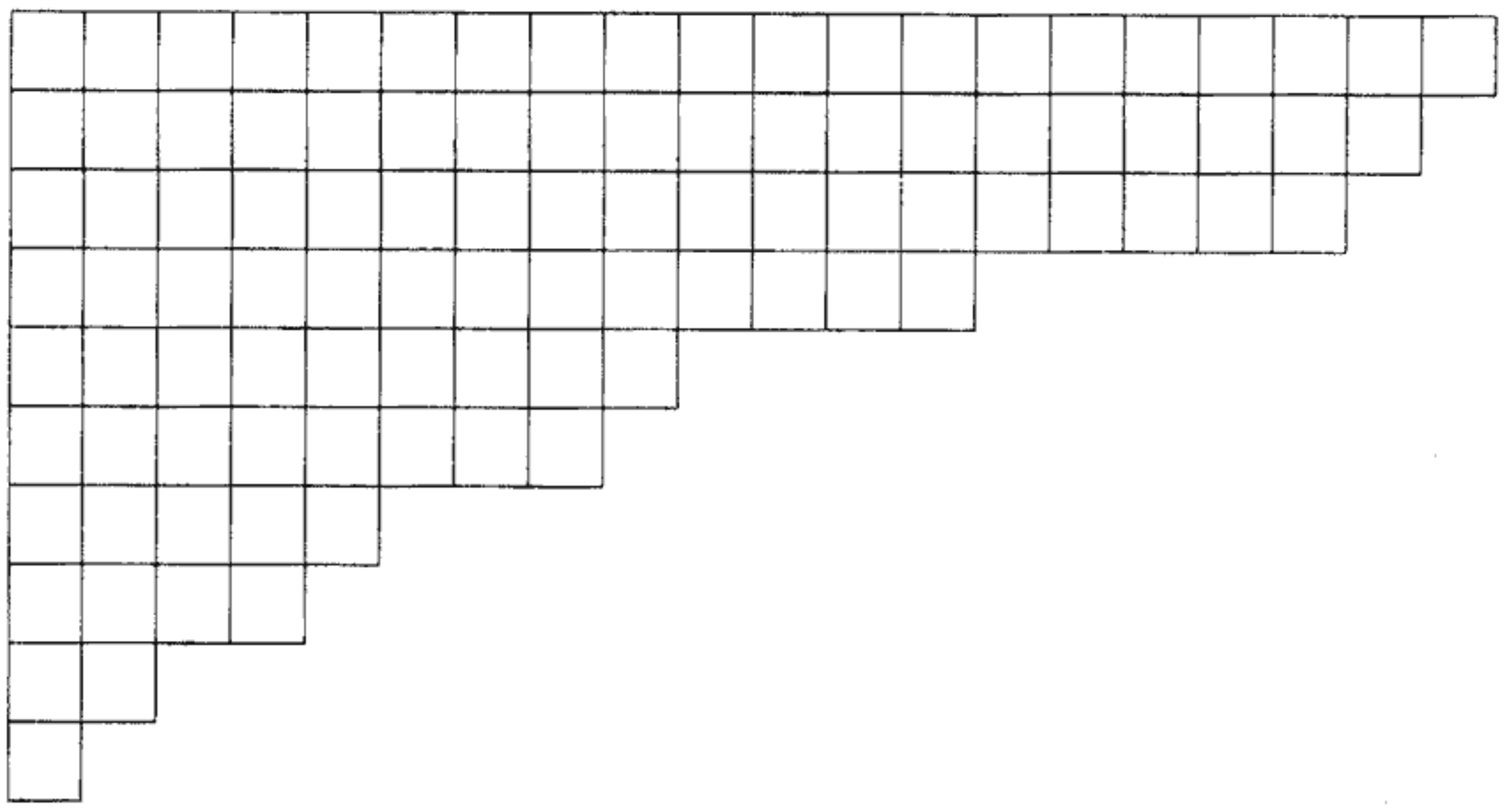
Per $m = 36$ ne avevamo trovati 4 precedentemente, infatti $36 = 2^2 \cdot 3^2$ e $4 = p(2)\,p(2) = 2 \cdot 2$. È evidente che trovare il numero delle partizioni di $n_1, n_2, \cdots, n_m$ non è sempre facile e immediato come negli esempi appena visti, per questo è indispensabile uno studio a parte delle partizioni. Se, ad esempio, $n = 5$ si hanno 7 partizioni distinte:

5=5	5	(5)
5=4+1	4≥ 1	(4,1)
5=3+2	3≥ 2	(3,2)
5=3+1+1	3 ≥ 1 ≥ 1	(3,1,1)
5=2+2+1	2 ≥ 2 ≥ 1	(2,2,1)
5=2+1+1+1	2 ≥ 1 ≥ 1 ≥ 1	(2,1,1,1)
5=1+1+1+1+1	1 ≥ 1 ≥ 1 ≥ 1 ≥ 1	(1,1,1,1,1)

È possibile rappresentare le partizioni di un numero naturale tramite il così detto *diagramma di Ferrers* cioè tramite caselle o scatole. Per esempio, una partizione λ di 99 con

$$\lambda = (20, 19, 18, 13, 9, 8, 5, 4, 2, 1)$$

viene illustrata come segue:



Quando il diagramma di Ferrers viene letto secondo le colonne (invece delle righe), la partizione corrispondente si chiama la *partizione coniugata*. Per esempio, la partizione coniugata alla λ di 99 risulta come segue:

$$\lambda' = (10, 9, 8, 8, 7, 6, 6, 6, 5, 4, 4, 4, 4, 3, 3, 3, 3, 3, 2, 1).$$

Inoltre ogni partizione di n può essere scritta come $(1^{m_1}, 2^{m_2}, \cdots, n^{m_n})$ con $n = \sum_{k=1}^{n} km_k$. Dunque possiamo anche scrivere le due partizioni λ e λ':

$$\begin{aligned} \lambda &= (1^1, 2^1, 4^1, 5^1, 8^1, 9^1, 13^1, 18^1, 19^1, 20^1), \\ \lambda' &= (1^1, 2^1, 3^5, 4^4, 5^1, 6^3, 7^1, 8^2, 9^1, 10^1). \end{aligned}$$

Analogamente, le sette partizioni di 5 vengono tabulate come segue:

$(1^0, 2^0, 3^0, 4^0, 5^1)$	5=5	(5)
$(1^1, 2^0, 3^0, 4^1, 5^0)$	$5 = 1 \times 1 + 1 \times 4$	(4,1)
$(1^0, 2^1, 3^1, 4^0, 5^0)$	$5 = 1 \times 2 + 1 \times 3$	(3,2)
$(1^2, 2^0, 3^1, 4^0, 5^0)$	$5 = 2 \times 1 + 1 \times 3$	(3,1,1)
$(1^1, 2^2, 3^0, 4^0, 5^0)$	$5 = 1 \times 1 + 2 \times 2$	(2,2,1)
$(1^3, 2^1, 3^0, 4^0, 5^0)$	$5 = 3 \times 1 + 1 \times 2$	(2,1,1,1)
$(1^5, 2^0, 3^0, 4^0, 5^0)$	$5 = 5 \times 1$	(1,1,1,1,1)

Quindi possiamo dire che $(1^{m_1}, 2^{m_2}, \cdots, n^{m_n})$ è una rappresentazione della partizione del numero naturale $n = \sum_{k=1}^{n} km_k$, dove per $1 \leq k \leq n$ si indica con $m_k \in \mathbb{N}_0$ il numero delle copie di parte k. Da ciò otteniamo che il numero delle partizioni di n è dato dal numero delle successioni $\{m_k\}_{k=0}^{n}$ tali che $n = \sum_{k=1}^{n} km_k$.

Sfruttando delle nozioni analitiche si riesce a trovare un metodo pratico per il calcolo di $p(n)$. Definiamo *funzione generatrice* della successione esplicita $\{c_k\}_{k=0}^{\infty}$ tramite la serie formale di potenze $f(x) = \sum_{k=0}^{\infty} c_k x^k$. Il coefficiente c_k di x^k in $f(x)$ viene indicato con $[x^k]f(x)$. Siano $\mathbb{N}$ l'insieme dei numeri naturali e $\mathbb{S}$ un sottoinsieme di $\mathbb{N}$. Denotiamo con $p(n|\mathbb{S})$ il numero delle partizioni di n con le parti in $\mathbb{S}$. Ovviamente si ha che $p(n) = p(n|\mathbb{N})$. Prima di tutto, vogliamo dimostrare che la funzione generatrice per $p(n|\mathbb{S})$ risulta il seguente prodotto:

$$G(q|\mathbb{S}) := \sum_{n=0}^{\infty} p(n|\mathbb{S})q^n \;=\; \prod_{k\in\mathbb{S}}^{\infty} \frac{1}{1-q^k}.$$

Volendo trovare il coefficiente di q^n, è inutile considerare nella somma e/o nel prodotto gli indici superiori ad n, quindi

$$p(n|\mathbb{S}) \;=\; [q^n]G(q|\mathbb{S}) \;=\; [q^n] \prod_{\substack{k\in\mathbb{S}\\ k\le n}} \frac{1}{1-q^k}.$$

Sostituendo y con q^k nella serie

$$1/(1-y) \;=\; \sum_{m=0}^{\infty} y^m$$

otteniamo

$$1/(1-q^k) \;=\; \sum_{m=0}^{\infty} q^{km}$$

da cui risulta

$$p(n|\mathbb{S}) = [q^n] \prod_{\substack{k\in\mathbb{S}\\ k\le n}} \frac{1}{1-q^k} = [q^n] \prod_{\substack{k\in\mathbb{S}\\ k\le n}} \sum_{m_k=0}^{n} q^{km_k}.$$

Allora il coefficiente di q^n è proprio il numero delle successioni $\{m_k\}$ con $k \in \mathbb{S}$ e $k \le n$ tale che $\sum_{k=0}^{n} km_k = n$, cioè il numero $p(n|\mathbb{S})$ delle partizioni di n con le parti in $\mathbb{S}$. □

Esempio B5.5. *Calcoliamo il numero dei gruppi abeliani non isomorfi di ordine* $n = 10.668.672$.

♢ Scomponiamo in fattori primi il numero n:

$$10.668.672 = 2^7 \cdot 3^5 \cdot 7^3.$$

♢ Calcoliamo il numero delle partizioni di $7, 5, 3$:

$$p(7) \;=\; 15, \qquad p(5) \;=\; 7, \qquad p(3) \;=\; 3.$$

$\diamondsuit$ Moltiplichiamoli per ottenere il numero dei gruppi abeliani non isomorfi di ordine 10.668.672:

$$p(7)p(5)p(3) = 315.$$

Ci limitiamo a prendere $p(5)$ come un esempio per mostrare come si calcola $p(n)$ per un fissato n:

$$p(5) = [q^5] \prod_{k=1}^{5} \frac{1}{1-q^k} = [q^5] \left\{ \frac{1}{1-q} \cdot \frac{1}{1-q^2} \cdot \frac{1}{1-q^3} \cdot \frac{1}{1-q^4} \cdot \frac{1}{1-q^5} \right\}$$

dalle nozioni di analisi appena viste abbiamo:

$$\begin{aligned}
\frac{1}{1-q} &= \sum_{m_1=0}^{\infty} q^{m_1} &&= 1 + q + q^2 + q^3 + q^4 + q^5 + (q^6 + \cdots), \\
\frac{1}{1-q^2} &= \sum_{m_2=0}^{\infty} q^{2m_2} &&= 1 + q^2 + q^4 + (q^6 + \cdots), \\
\frac{1}{1-q^3} &= \sum_{m_3=0}^{\infty} q^{3m_3} &&= 1 + q^3 + (q^6 + \cdots), \\
\frac{1}{1-q^4} &= \sum_{m_4=0}^{\infty} q^{4m_4} &&= 1 + q^4 + (q^8 + \cdots), \\
\frac{1}{1-q^5} &= \sum_{m_5=0}^{\infty} q^{5m_5} &&= 1 + q^5 + (q^{10} + \cdots).
\end{aligned}$$

ovviamente ciò che è in parentesi non viene preso in considerazione, in quanto gli esponenti sono maggiori di 5; successivamente dovremo fare i prodotti ed anche in quel caso ci dovremo ricordare di eliminare i termini con esponente maggiore di 5, ottenendo così

$$p(5) = [q^5]\{1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5\} = 7.$$

Denotiamo inoltre con $p_m(n|\mathbb{S})$ il numero delle partizioni di n con m parti in $\mathbb{S}$. Possiamo analogamente dimostrare che la funzione generatrice bivariata è uguale al prodotto:

$$\sum_{m,n=0}^{\infty} p_m(n|\mathbb{S}) q^n x^m = \prod_{k\in\mathbb{S}}^{\infty} \frac{1}{1-q^k x}.$$

In particolare, la funzione generatrice delle partizioni con i diagrammi di Ferrers contenuti nel rettangolo $m \times n$ risulta il seguente coefficiente binomiale gaussiano:

$$\sum_{\lambda \subseteq [m\times n]} q^{|\lambda|} = \begin{bmatrix} m+n \\ m \end{bmatrix} = \frac{(q;q)_{m+n}}{(q;q)_m (q;q)_n}.$$

DIMOSTRAZIONE. Secondo la funzione generatrice bivariata, si vede facilmente che la funzione generatrice delle partizioni con i diagrammi di Ferrers contenuti nel rettangolo $m \times n$ è uguale al coefficiente $[x^m]\frac{1}{(x;q)_{n+1}}$.

Consideriamo le serie di Maclaurin

$$\frac{1}{(x;q)_{n+1}} = \sum_{m=0}^{\infty} \mathcal{A}_m x^m \quad \text{e} \quad \frac{1}{(qx;q)_{n+1}} = \sum_{m=0}^{\infty} \mathcal{A}_m (qx)^m.$$

Moltiplicando le due equazioni con $1-x$ e $1-q^{n+1}x$ rispettivamente, otteniamo la relazione:

$$\frac{1}{(qx;q)_n} = (1-x)\sum_{m=0}^{\infty} \mathcal{A}_m x^m = (1-q^{n+1}x)\sum_{m=0}^{\infty} \mathcal{A}_m (qx)^m.$$

Estraendo il coefficiente di x^m, abbiamo la relazione ricorrente:

$$\mathcal{A}_m - \mathcal{A}_{m-1} = q^m \mathcal{A}_m - q^{m+n}\mathcal{A}_{m-1} \quad \Longleftrightarrow \quad \mathcal{A}_m = \mathcal{A}_{m-1}\frac{1-q^{m+n}}{1-q^m}.$$

Iterando quest'ultima relazione per m-volte, si deduce che

$$\mathcal{A}_m = \mathcal{A}_0 \begin{bmatrix} m+n \\ m \end{bmatrix} \qquad \text{con} \qquad \mathcal{A}_0 = 1$$

dove $\mathcal{A}_0 = 1$ viene confermato ponendo $x = 0$ nelle serie di Maclaurin. □

B6. Automorfismi dei p-gruppi e teorema di Hall

Siano p un primo e n un numero naturale. Allora il numero dei gruppi abeliani (non isomorfi) di ordine p^n è uguale a $p(n)$, il numero delle partizioni di n. Indichiamo con q il reciproco di p, cioè $pq = 1$. Allora il fattoriale crescente di ordine n in base q viene definito come segue:

$$(q;q)_0 = 1 \quad \text{e} \quad (q;q)_n = (1-q)(1-q^2)\cdots(1-q^n) \quad \text{per} \quad n \in \mathbb{N}.$$

Lemma B6.1 (Hall, 1938). *Sia G un p-gruppo abeliano di ordine p^n con il tipo $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$ dove $n = \sum_{k=1}^{n} k m_k$. Allora l'ordine del gruppo degli automorfismi di G è dato dal seguente prodotto:*

$$|\operatorname{Aut} G| \;=\; \prod_{k=1}^{\ell} p^{\lambda_k^2}(q;q)_{m_k}$$

dove $\lambda := (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ è la partizione coniugata alla $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$.

DIMOSTRAZIONE. Determiniamo l'ordine degli automofismi del gruppo abeliano G di ordine p^n secondo il tipo di G, cioè, le partizioni di n.

[A] Sia G ciclico di tipo (n). Allora ogni automorfismo di G è identificabile con un generatore di G. Dunque l'ordine di $\operatorname{Aut} G$ risulta come segue:

$$|\operatorname{Aut} G| = \varphi(p^n) = p^n(1-q) = p^n(q;q)_1.$$

[B] Sia G un *gruppo elementare* di tipo (1^n). Allora G è prodotto diretto

$$G \cong \bigotimes_{k=1}^{n} H_k \quad \text{dove} \quad H_k = \langle x_k \rangle \quad \text{con} \quad o(x_k) = p.$$

È facile vedere che tutti gli elementi diversi dal'elemento neutro hanno l'ordine p. Ogni automorfismo ψ di G è determinato dalle immagini dei generatori $\{x_k\}_{k=1}^n$ come segue:

$$\begin{aligned}
&\psi(x_1) \in G\backslash\{e\} && \Longrightarrow \quad |\psi(x_1)| = p^n - 1;\\
&\psi(x_2) \in G\backslash\langle\psi(x_1)\rangle && \Longrightarrow \quad |\psi(x_2)| = p^n - p;\\
&\psi(x_3) \in G\backslash\langle\psi(x_1,x_2)\rangle && \Longrightarrow \quad |\psi(x_3)| = p^n - p^2;\\
&\qquad\vdots && \quad\vdots \qquad\qquad \vdots\\
&\psi(x_n) \in G\backslash\big\langle\psi(\{x_k|1\le k<n\})\big\rangle && \Longrightarrow \quad |\psi(x_n)| = p^n - p^{n-1}.
\end{aligned}$$

Allora l'ordine di $\operatorname{Aut} G$ uguaglia il prodotto:

$$|\operatorname{Aut} G| = \prod_{k=1}^{n}(p^n - p^{n-k}) = p^{n^2}(q;q)_n.$$

[C] Sia G di tipo (ℓ^m) con $n = m\ell$. Allora G è prodotto diretto

$$G \cong \bigotimes_{k=1}^{m} H_k \quad \text{dove} \quad H_k = \langle x_k \rangle \quad \text{con} \quad o(x_k) = p^\ell.$$

Definiamo il sottoinsieme di G con $\Omega_k := \{x \in G \mid o(x) < p^k\}$. Allora ogni automorfismo ψ di G è determinato dalle immagini dei generatori $\{x_k\}_{k=1}^m$ con $o(\psi(x_k)) = p^\ell$:

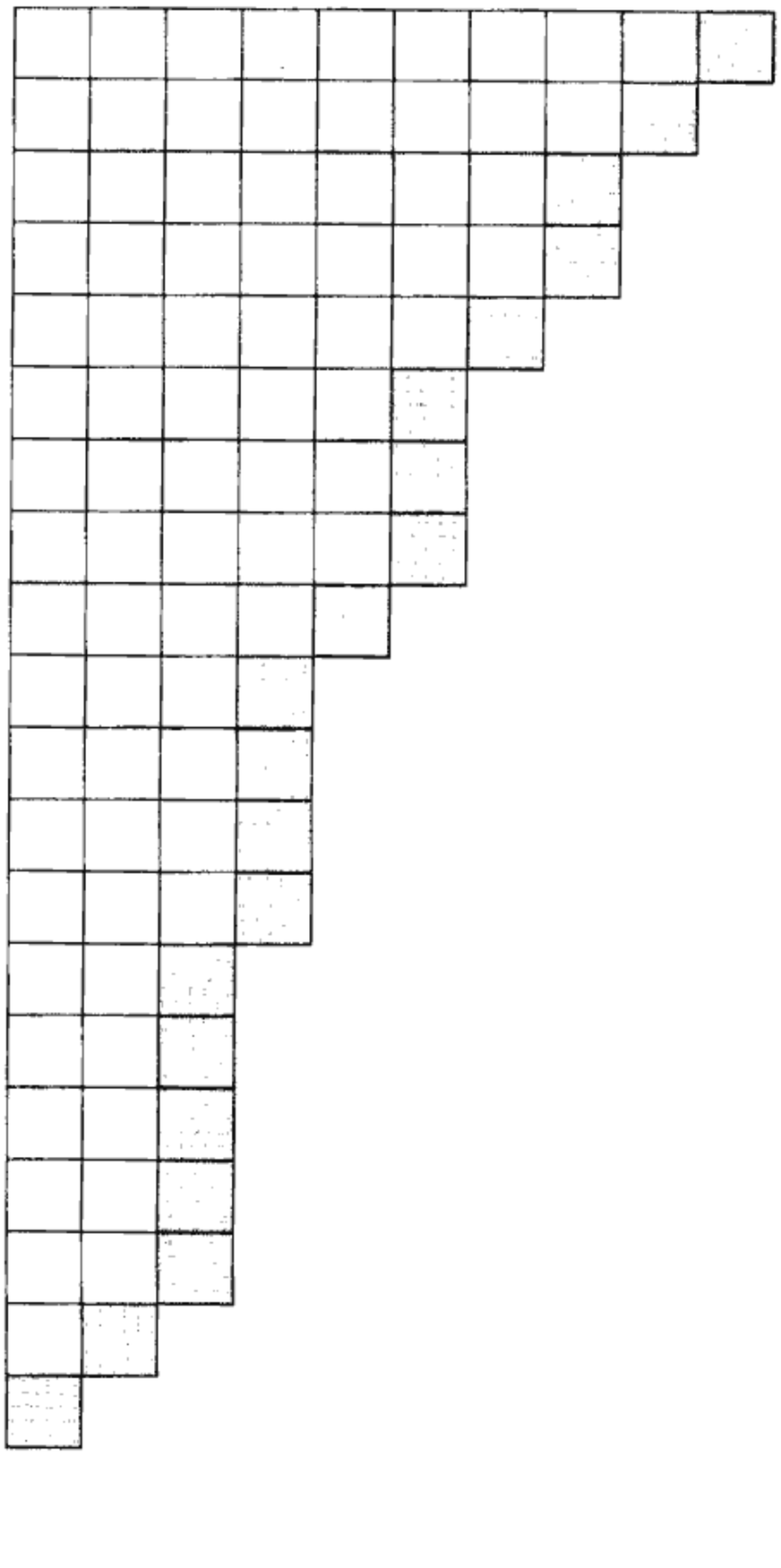
$$\begin{aligned}
&\psi(x_1) \in G\backslash\Omega_\ell && \Longrightarrow \quad |\psi(x_1)| = p^n - p^{n-m};\\
&\psi(x_2) \in G\backslash\langle\Omega_\ell,\psi(x_1)\rangle && \Longrightarrow \quad |\psi(x_2)| = p^n - p^{n-m+1};\\
&\psi(x_3) \in G\backslash\langle\Omega_\ell,\psi(x_1,x_2)\rangle && \Longrightarrow \quad |\psi(x_3)| = p^n - p^{n-m+2};\\
&\qquad\vdots && \quad\vdots \qquad\qquad \vdots\\
&\psi(x_m) \in G\backslash\big\langle\Omega_\ell,\psi(\{x_k|1\le k<m\})\big\rangle && \Longrightarrow \quad |\psi(x_m)| = p^n - p^{n-1}.
\end{aligned}$$

Allora l'ordine di $\operatorname{Aut} G$ uguaglia il prodotto:

$$|\operatorname{Aut} G| = \prod_{k=1}^{m} (p^n - p^{n-k}) = p^{mn}(q;q)_m.$$

In generale, sia G di tipo $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$ con $n = \sum_{k=1}^{\ell} km_k$. Allora G è prodotto diretto

$$G \cong \bigotimes_{k=1}^{\ell} \bigotimes_{i=1}^{m_k} H_{ki} \quad \text{dove} \quad H_{ki} = \langle x_{ki} \rangle \quad \text{con} \quad o(x_{ki}) = p^k.$$



Indichiamo con

$$\lambda := (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell)$$

la partizione coniugata alla

$$(1^{m_1}2^{m_2}\cdots\ell^{m_\ell}).$$

Allora non è difficile stabilire le relazioni:

$\lambda_k = \sum_{j=k}^{\ell} m_j$ per $1 \leq k \leq \ell$.

Indichiamo inoltre per semplicità con X_k e X_k^ν dei sottoinsiemi dei generatori nel modo seguente:

$$X_k = \{x_{ki} | 1 \leq i \leq m_k\};$$

$$X_k^\nu = \{x_{ki} | 1 \leq i \leq \nu\}.$$

Allora ogni automorfismo ψ di G è determinato dalle immagini dei generatori $\{x_{ki}\}$ con $o(\psi(x_{ki})) = p^k$ per ogni k e i soggetti alle condizioni $1 \leq i \leq m_k$ e $1 \leq k \leq \ell$.

Prima vediamo le immagini dei generatori dell'ordine massimo p^ℓ:

$$\begin{aligned}
&\psi(x_{\ell 1}) \in G\backslash\Omega_\ell && \Longrightarrow && |\psi(x_{\ell 1})| = p^n - p^{n-m_\ell};\\
&\psi(x_{\ell 2}) \in G\backslash\langle\Omega_\ell, \psi(X_\ell^1)\rangle && \Longrightarrow && |\psi(x_{\ell 2})| = p^n - p^{n-m_\ell+1};\\
&\psi(x_{\ell 3}) \in G\backslash\langle\Omega_\ell, \psi(X_\ell^2)\rangle && \Longrightarrow && |\psi(x_{\ell 3})| = p^n - p^{n-m_\ell+2};\\
&\quad\vdots && && \quad\vdots\\
&\psi(x_{\ell m_\ell}) \in G\backslash\langle\Omega_\ell, \psi(X_\ell^{m_\ell-1})\rangle && \Longrightarrow && |\psi(x_{\ell m_\ell})| = p^n - p^{n-1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine p^ℓ risulta il seguente prodotto:

$$\big|\psi(X_\ell)\big| = \prod_{i=1}^{m_\ell}(p^n - p^{n-i}) = p^{nm_\ell}(q;q)_{m_\ell}.$$

Per i generatori di ordine $p^{\ell-1}$, si ha che

$$\begin{aligned}
&\psi(x_{\ell-1,1}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell)\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,1})| = p^{n-\lambda_\ell} - p^{n-\lambda_{\ell-1}};\\
&\psi(x_{\ell-1,2}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell, X_{\ell-1}^1)\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,2})| = p^{n-\lambda_\ell} - p^{n-\lambda_{\ell-1}+1};\\
&\psi(x_{\ell-1,3}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell, X_{\ell-1}^2)\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,3})| = p^{n-\lambda_\ell} - p^{n-\lambda_{\ell-1}+2};\\
&\quad\vdots \qquad\qquad \vdots \qquad\qquad \vdots\\
&\psi(x_{\ell-1,m_{\ell-1}}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell, X_{\ell-1}^{m_{\ell-1}-1})\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,m_{\ell-1}})| = p^{n-\lambda_\ell} - p^{n-\lambda_\ell-1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine $p^{\ell-1}$ risulta il seguente prodotto:

$$\big|\psi(X_{\ell-1})\big| = \prod_{i=1}^{m_{\ell-1}}(p^{n-\lambda_\ell} - p^{n-i-\lambda_\ell}) = p^{(n-\lambda_\ell)m_{\ell-1}}(q;q)_{m_{\ell-1}}.$$

Per i generatori di ordine $p^{\ell-2}$, si ha che

$$\begin{aligned}
&\psi(x_{\ell-2,1}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X_{\ell-1})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-2,1})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-m_{\ell-2}}; \\
&\psi(x_{\ell-2,2}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X_{\ell-1}, X^1_{\ell-2})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-2,2})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-m_{\ell-2}+1}; \\
&\psi(x_{\ell-2,3}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X^2_{\ell-1}, X^2_{\ell-2})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-1,3})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-m_{\ell-2}+2}; \\
&\quad\vdots \qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \\
&\psi(x_{\ell-2,m_{\ell-2}}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X_{\ell-1}, X^{m_{\ell-2}-1}_{\ell-2})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-2,m_{\ell-2}})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine $p^{\ell-2}$ risulta il seguente prodotto:

$$\big|\psi(X_{\ell-2})\big| = \prod_{i=1}^{m_{\ell-2}} (p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-i-\lambda_\ell-\lambda_{\ell-1}}) = p^{(n-\lambda_\ell-\lambda_{\ell-1})m_{\ell-2}}(q;q)_{m_{\ell-2}}.$$

Dopo aver calcolato le cardinalità degli automorfismi determinati dai generatori $\{X_\ell, X_{\ell-1}, \cdots, X_{k+1}\}$, possiamo proseguire a valutare quella degli automorfismi determinati dai generatori di ordine p^k:

$$\begin{aligned}
&\psi(x_{k,1}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,1})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - m_k}; \\
&\psi(x_{k,2}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X^1_k, X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,2})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - m_k+1}; \\
&\psi(x_{k,3}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X^2_k, X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,3})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - m_k+2}; \\
&\quad\vdots \qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \\
&\psi(x_{k,m_k}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X^{m_k-1}_k, X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,m_k})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - 1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine p^k risulta il seguente prodotto:

$$\big|\psi(X_k)\big| = \prod_{i=1}^{m_k} (p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - i}) = p^{m_k\sum_{j\le k}\lambda_j}(q;q)_{m_k}.$$

Infine, la cardinalità degli automorfismi determinati dai generatori di ordine p risulta il seguente prodotto:

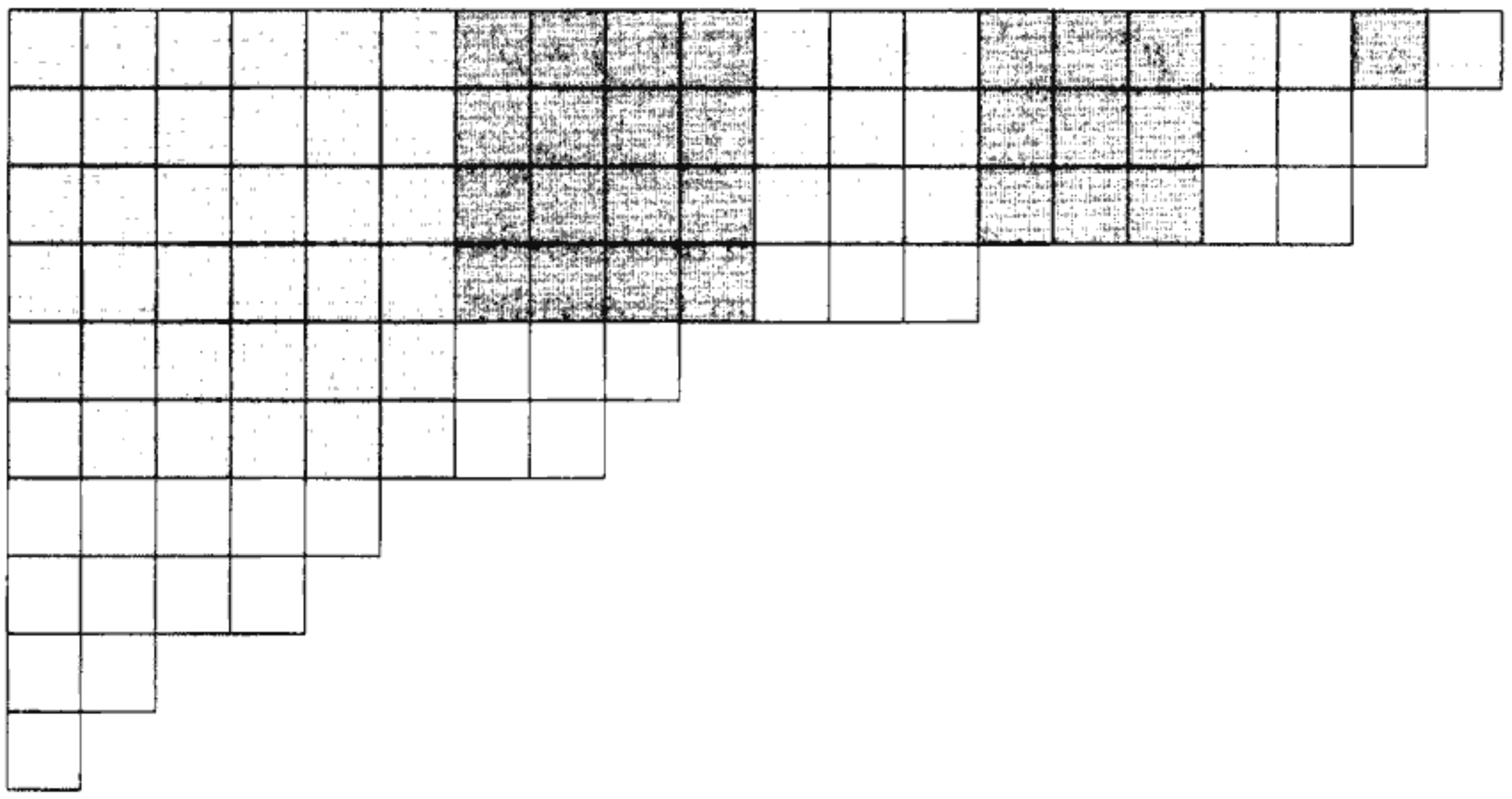
$$\left|\psi(X_1)\right| = \prod_{i=1}^{m_1}(p^{\lambda_1} - p^{\lambda_1 - i}) = p^{\lambda_1 m_1}(q;q)_{m_1}.$$

Ricapitolando quanto fatto, per un gruppo abeliano G di ordine p^n con il tipo $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$, l'ordine del gruppo degli automorfismi di G è dato dal seguente prodotto:

$$|\mathrm{Aut}\, G| = \prod_{k=1}^{\ell} p^{m_k \sum_{j\le k}\lambda_j}(q;q)_{m_k} = \prod_{k=1}^{\ell} p^{\lambda_k^2}(q;q)_{m_k}$$

dove abbiamo applicato la seguente identità:

$$\sum_{k=1}^{\ell} m_k \sum_{j=1}^{k}\lambda_j = \sum_{j=1}^{\ell}\lambda_j \sum_{k=j}^{\ell}(\lambda_k - \lambda_{k+1}) = \sum_{j=1}^{\ell}\lambda_j^2. \qquad \square$$



Si osserva che la frazione $\frac{q^n}{(q;q)_n}$ è la funzione generatrice delle partizioni con la parte massimale uguale a n. Classifichiamo le partizioni secondo i quadrati di Durfee, i cui lati formano una partizione λ di n. Nella figura viene illustrata $n = 20$ e $\lambda = (6,4,3,3,2,1,1)$. La funzione generatrice per il primo quadrato di Durfee λ_1^2 e le partizioni sotto esso risulta $\frac{q^{\lambda_1^2}}{(q;q)_{\lambda_1}}$. La funzione generatrice per il secondo quadrato di Durfee λ_2^2 e le partizioni sotto esso risulta $\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix} q^{\lambda_2^2}$. In generale, la funzione generatrice per il k-esimo quadrato di Durfee λ_k^2 e le partizioni sotto esso risulta $\begin{bmatrix}\lambda_{k-1}\\ \lambda_k\end{bmatrix} q^{\lambda_k^2}$. Quindi

la funzione generatrice delle partizioni con i quadrati di Durfee determinati dalla partizione $\lambda \vdash n$ è data dal seguente prodotto:

$$\frac{q^{\lambda_1^2}}{(q;q)_{\lambda_1}} \prod_{k=2}^{\ell(\lambda)} \begin{bmatrix} \lambda_{k-1} \\ \lambda_k \end{bmatrix} q^{\lambda_k^2} = \prod_{k=1}^{\ell(\lambda)} \frac{q^{\lambda_k^2}}{(q;q)_{\lambda_k - \lambda_{k+1}}}.$$

Sommando su tutte le partizioni $\lambda \vdash n$, otteniamo l'identità:

$$\frac{q^n}{(q;q)_n} = \sum_{\lambda \vdash n} \prod_{k=1}^{\ell(\lambda)} \frac{q^{\lambda_k^2}}{(q;q)_{\lambda_k - \lambda_{k+1}}}.$$

Combinando quest'identità con il Lemma **B6.1**, abbiamo subito il seguente importante risultato.

Teorema B6.2 (Hall, 1938). *Sia Λ_n l'insieme dei gruppi abeliani* (non isomorfi) *di ordine p^n. Allora vale la seguente identità:*

$$\frac{q^n}{(q;q)_n} = \sum_{G \in \Lambda_n} \frac{1}{|\mathrm{Aut}\, G|}.$$

Classificando le partizioni secondo la parte massimale, si deduce conseguentemente un ulteriore risultato tramite la formula di Eulero.

Corollario B6.3 (Funzione generatrice).

$$\frac{1}{(qx;q)_\infty} = \sum_{n=0}^{\infty} \frac{(qx)^n}{(q;q)_n} = \sum_{n=1}^{\infty} \sum_{G \in \Lambda_n} \frac{x^n}{|\mathrm{Aut}\, G|}.$$

□

CAPITOLO C

Azione di Gruppo su un Insieme

La nozione di gruppo che agisce su un insieme generalizza quella di permutazioni di un insieme. La fondamentale rilevanza di questo argomento risiede nel fatto che trova notevoli applicazioni nel calcolo algebrico combinatorio e nello studio delle strutture dei gruppi finiti.

Questo capitolo è interamente dedicato allo studio di questo argomento, dopo aver introdotto le definizioni di orbita e stabilizzatore ed illustrato le relative proprietà, vengono approfondite l'equazione delle classi, transitività e normalità.

C1. Azione di gruppo su un insieme

Definizione C1.1. *Dati un insieme* $\Omega = \{\alpha, \beta, \gamma, \cdots\}$ *ed un gruppo* G, *si dice che* G *agisce su* Ω *quando è assegnata una funzione*

$$\Omega \times G \longrightarrow \Omega$$

che denoteremo così

$$(\alpha, g) \longmapsto \alpha^g \quad \textit{per ogni} \quad \alpha \in \Omega \quad e \quad g \in G$$

tale che valgono le proprietà:

(a) $(\alpha^g)^h = \alpha^{gh}$ *per ogni* $\alpha \in \Omega$ *e* $g, h \in G$.
(b) $\alpha^e = \alpha$ *per ogni* $\alpha \in \Omega$, *dove* e *è l'elemento neutro di* G.

La funzione assegnata si chiama azione *di* G *su* Ω. *Denoteremo con* (G, Ω) *un gruppo* G *che agisce su un insieme* Ω.

Se H è un sottogruppo di G e G agisce su Ω allora anche H agisce su Ω. Se Ω è un gruppo e $G = \mathrm{Aut}(\Omega)$ allora G agisce su Ω.

Se Ω è un insieme qualsiasi, il gruppo simmetrico S_Ω agisce su Ω e così ogni suo sottogruppo.

La nozione di gruppo che agisce su un insieme generalizza quella di gruppo di permutazioni di un insieme.

Lemma C1.2. *Se un gruppo G agisce su un insieme Ω, ogni elemento di G dà luogo ad una permutazione di Ω. Più precisamente, la corrispondenza*

$$\phi : \alpha \longmapsto \alpha^g$$

è, per ogni fissato $g \in G$, una permutazione di Ω.

DIMOSTRAZIONE. Ricordiamo che una permutazione su un generico insieme Ω è una biiezione da Ω su Ω, cioè un'applicazione iniettiva e suriettiva, quindi dobbiamo provare che per ogni $g \in G$:

$$\phi_g : \Omega \longrightarrow \Omega \quad \text{con} \quad \phi_g(\alpha) = \alpha^g$$

è una funzione iniettiva e suriettiva. Se dimostriamo questo per un arbitrario $g \in G$, essa sarà valida per ogni elemento di G.

Siano $g \in G$ e $\alpha, \beta \in \Omega$ tali che $\alpha^g = \beta^g$. Poiché G è un gruppo, ogni suo elemento è invertibile, quindi se $g \in G$ anche $g^{-1} \in G$, pertanto, applicando la definizione di gruppo che agisce su un insieme, possiamo scrivere:

$$\alpha = \alpha^e = \alpha^{(gg^{-1})} = (\alpha^g)^{g^{-1}} = (\beta^g)^{g^{-1}} = \beta^{(gg^{-1})} = \beta^e = \beta.$$

Dunque se due membri hanno la stessa immagine questi risultano coincidenti, cioè ϕ_g è iniettiva.

Sia $\beta \in \Omega$ e poniamo $\gamma = \beta^{g^{-1}}$. Poiché G agisce su Ω si ha $\gamma \in \Omega$ e

$$\gamma^g = (\beta^{g^{-1}})^g = \beta^{(g^{-1}g)} = \beta^e = \beta.$$

Quindi, preso un arbitrario membro del codominio, questo risulta sempre essere l'immagine di un membro del dominio, ne segue che ϕ_g è suriettiva. Dunque ϕ_g è biiettiva da Ω a Ω. □

Nota C1.3. *Sia S_Ω il gruppo simmetrico su Ω, cioè il gruppo che ha come elementi l'insieme delle permutazioni su Ω e, come operazione, l'usuale composizione di funzioni.*

Se un gruppo G agisce su Ω, la corrispondenza

$$\theta : G \longrightarrow S_{|\Omega|} \quad \text{con} \quad g \longmapsto \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots \\ \alpha^g, & \beta^g, & \gamma^g, & \cdots \end{pmatrix}$$

associa ad ogni elemento $g \in G$, una permutazione di Ω. Tale corrispondenza, che prende il nome di rappresentazione di G come gruppo di permutazioni di Ω, è un omomorfismo. Infatti, premesso che

$$\forall\ g \in G: \quad \Omega = \{\alpha, \beta, \gamma, \cdots\} = \{\alpha^g, \beta^g, \gamma^g, \cdots\}$$

allora se $g, f \in G$, vale

$$\theta(g) \circ \theta(f) = \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots \\ \alpha^g, & \beta^g, & \gamma^g, & \cdots \end{pmatrix} \circ \begin{pmatrix} \alpha^g, & \beta^g, & \gamma^g, & \cdots \\ (\alpha^g)^f, & (\beta^g)^f, & (\gamma^g)^f, & \cdots \end{pmatrix}$$

$$= \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots \\ \alpha^{gf}, & \beta^{gf}, & \gamma^{gf}, & \cdots \end{pmatrix} = \theta(g \cdot f).$$

Il suo *nucleo* (si chiama nucleo dell'azione) è dato da

$$K = \{g \in G \mid \alpha^g = \alpha, \quad \forall\ \alpha \in \Omega\}$$

il quale, per il teorema d'omomorfismo per i gruppi, risulta essere un sottogruppo normale di G. Se $K = \{e\}$, si dice che l'azione è *fedele*, ovvero che G agisce fedelmente su Ω. In tal caso, G è isomorfo ad un sottogruppo del gruppo simmetrico S_Ω sempre per il teorema citato precedentemente; si dirà allora che G è un gruppo di permutazioni di Ω.

Esempio C1.4. *Fissiamo Ω uguale all'insieme degli elementi del gruppo G e definiamo un'azione di G su Ω in questo modo*

$$\forall\ \alpha, g \in G: \quad \alpha^g = \alpha g.$$

Vediamo se l'azione di G su Ω così definita, verifica le proprietà della definizione, sfruttando la proprietà associativa dei gruppi come segue:

- Per ogni $\alpha \in \Omega$ e $g, h \in G$, vale $(\alpha^g)^h = (\alpha g)^h = (\alpha g)h = \alpha(gh) = \alpha^{gh}$.
- Per ogni $\alpha \in \Omega$ e l'elemento neutro e di G, si ha che $\alpha^e = \alpha \cdot e = \alpha$.

Il nucleo dell'azione è l'identità di G (l'elemento neutro di G), quindi essa è un'azione fedele di G su Ω e l'omomorfismo $G \longrightarrow S_\Omega$ è un isomorfismo tra G e un sottogruppo del suo gruppo simmetrico $S_{|G|}$. Tale omomorfismo prende il nome di rappresentazione regolare destra di G, dal momento che esso si ottiene moltiplicando a destra gli elementi di G per un elemento fissato.

La moltiplicazione a sinistra non definisce un'azione (a meno che G non sia abeliano) perché viene meno la condizione [**a**] della definizione dell'azione di un gruppo su un insieme. Sostituendo la suddetta definizione con $\alpha^g = g^{-1}\alpha$, si ha una teoria perfettamente analoga a quella esposta.

Teorema C1.5 (Cayley). *Ogni gruppo G è isomorfo ad un sottogruppo di $S_{|G|}$, il gruppo simmetrico sugli elementi di G. In particolare, un gruppo finito di ordine n è isomorfo ad un sottogruppo di S_n, il gruppo simmetrico di n lettere.* □

C2. Orbita e stabilizzatore

Definizione C2.1. *Se G agisce su Ω e $\alpha \in \Omega$, si chiama* orbita *di α sotto l'azione di G, e si indica con α^G, il sottoinsieme di Ω così definito:*

$$\alpha^G = \{\alpha^g \mid g \in G\}$$

cioè l'insieme dei membri di Ω in cui α è portato dai vari elementi di G. Allora si deduce che

$$\Omega = \bigcup_{\alpha \in \Omega} \alpha^G.$$

Nota C2.2. *Sia G un gruppo che agisce su un insieme Ω e definiamo su Ω la seguente relazione "$\sim$":*

$$\forall \alpha, \beta \in \Omega: \quad \alpha \sim \beta \Longleftrightarrow \exists g \in G \quad \textit{tale che} \quad \alpha^g = \beta.$$

Tale relazione è una equivalenza su Ω e le classi da essa indotte altro non sono che le orbite degli elementi di Ω. Pertanto due orbite o coincidono o sono disgiunte.

L'azione di un gruppo G su un insieme Ω induce, quindi, una partizione su Ω e allora

$$\Omega \quad = \quad \biguplus_{\alpha \in C} \alpha^G$$

dove C è un sistema di rappresentanti delle orbite di Ω. In particolare se Ω è finito, si ottiene l'identità

$$|\Omega| \quad = \quad \sum_{\alpha \in C} |\alpha^G|.$$

Definizione C2.3. *Se G agisce su Ω e $\alpha \in \Omega$, si chiama* stabilizzatore *di α, e si indica con G_α, il sottoinsieme di G così definito:*

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$$

cioè l'insieme degli elementi di G che fissano α.

Esso rappresenta l'insieme degli elementi di G che fissano α. Osserviamo che se un elemento di G appartiene ad ogni stabilizzatore, allora appartiene

al nucleo dell'azione; viceversa, il nucleo K dell'azione di G su Ω si può ottenere come intersezione degli stabilizzatori degli elementi di Ω

$$K \quad = \quad \bigcap_{\alpha \in \Omega} G_\alpha.$$

Le relazioni tra orbite e stabilizzatori sono messe in evidenza dal teorema seguente.

Teorema C2.4. *Sia G un gruppo che agisce su un insieme Ω. Allora*

(a) *due orbite o coincidono o sono disgiunte.*
(b) *lo stabilizzatore G_α di un membro $\alpha \in \Omega$, è un sottogruppo di G.*
(c) *se β appartiene all'orbita di α, allora G_β è coniugato di G_α; più precisamente, se $\beta = \alpha^g$, si ha che $G_\beta = G_{\alpha^g} = G_\alpha^g$.*
(d) *l'indice in G dello stabilizzatore di un membro è uguale alla cardinalità dell'orbita del membro*

$$[G : G_\alpha] = |\alpha^G|.$$

DIMOSTRAZIONE. Procediamo per ordine, partendo dal primo punto.

[a] Siano $\alpha, \beta \in \Omega$ e supponiamo che le rispettive orbite abbiano intersezione non vuota, cioè $\alpha^G \cap \beta^G \neq \emptyset$.

Dimostriamo che $\alpha^G = \beta^G$ tramite la doppia inclusione, osservando che è sufficiente far vedere che

$$\beta \in \alpha^G \qquad \text{e} \qquad \alpha \in \beta^G.$$

Supponendo $\alpha^G \cap \beta^G \neq \emptyset$, ne segue che esiste $\gamma \in \Omega$ tale che

$$\gamma \in \alpha^G \cap \beta^G \quad \Longrightarrow \quad \exists\, g, h \in G : \quad \gamma = \alpha^g = \beta^h$$

da cui segue

$$(\alpha^g)^{g^{-1}} = (\beta^h)^{g^{-1}} \quad \text{e} \quad (\alpha^g)^{h^{-1}} = (\beta^h)^{h^{-1}}$$

quindi

$$\alpha = \beta^{(hg^{-1})} \quad \Longrightarrow \quad \alpha \in \beta^G \quad \Longrightarrow \quad \alpha^G \subseteq \beta^G$$

mentre

$$\beta = \alpha^{(gh^{-1})} \quad \Longrightarrow \quad \beta \in \alpha^G \quad \Longrightarrow \quad \beta^G \subseteq \alpha^G.$$

Pertanto dalla doppia inclusione, si ha $\alpha^G = \beta^G$.

[b] Per la caratterizzazione dei sottogruppi basta dimostrare che

- G_α è chiuso rispetto alla moltiplicazione.
- Per ogni $g \in G_\alpha$ esiste $g^{-1} \in G_\alpha$ tale che $gg^{-1} = g^{-1}g = e$.

Siano $g, h \in G_\alpha$, allora $\alpha^g = \alpha \quad \text{e} \quad \alpha^h = \alpha$. Poiché G agisce su Ω, possiamo scrivere

$$\alpha^{gh} = (\alpha^g)^h = \alpha^h = \alpha \quad \Longrightarrow \quad gh \in G_\alpha$$

pertanto G_α è chiuso. Se $g \in G_\alpha$ allora $\alpha^g = \alpha$, quindi

$$\alpha^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha^e = \alpha$$

ne segue che $g^{-1} \in G_\alpha$.

Ora, poiché abbiamo anche dimostrato che ogni elemento di G_α è invertibile, possiamo concludere che G_α è un sottogruppo di G.

[c] Sia $\beta \in \alpha^G$, allora esiste $g \in G$ tale che $\beta = \alpha^g$. Dobbiamo provare che $G_\beta = G_\alpha^g$, dove con G_α^g indichiamo il coniugato di G_α sotto coniugio di g. Proviamola con la doppia inclusione.

"$\subseteq$" Sia $y \in G_\beta \implies \beta^y = \beta$. Ma $\beta = \alpha^g$ pertanto

$$(\alpha^g)^y = \alpha^g \quad \Longrightarrow \quad \alpha^{gy} = \alpha^g \quad \Longrightarrow \quad \alpha^{gyg^{-1}} = \alpha$$

quindi gyg^{-1} appartiene allo stabilizzatore di α per cui vale anche

$$y = g^{-1}(gyg^{-1})g \quad \Longrightarrow \quad y \in G_\alpha^g.$$

Poiché y è un elemento arbitrario di G_β, otteniamo $G_\beta \subseteq G_\alpha^g$.

"$\supseteq$" Sia $x \in G_\alpha^g \implies \exists\, y \in G_\alpha : \; x = g^{-1}yg \implies y = gxg^{-1}$ ora, poiché y appartiene allo stabilizzatore di α, si ha

$$\alpha^{gxg^{-1}} = \alpha \quad \Longrightarrow \quad \alpha^{gx} = \alpha^g \quad \Longrightarrow \quad (\alpha^g)^x = \alpha^g$$

ma $\alpha^g = \beta$, quindi $\beta^x = \beta$, cioè $x \in G_\beta$. In questo caso abbiamo dimostrato che $G_\alpha^g \subseteq G_\beta$ e quindi possiamo concludere che $G_\beta = G_\alpha^g$.

[d] Poiché $G_\alpha \leqslant G$, possiamo considerare l'insieme dei laterali destri di G_α in G, che indichiamo con $\mathcal{L}$:

$$\mathcal{L} = \{G_\alpha g \mid g \in G\}.$$

Definendo l'applicazione

$$\psi : \quad \mathcal{L} \longrightarrow \alpha^G \quad \text{con} \quad \psi(G_\alpha g) = \alpha^g$$

e ricordando che $|\mathcal{L}| = [G : G_\alpha]$, per ottenere la tesi è sufficiente provare che ψ è biiettiva.

Prima di tutto, dobbiamo verificare che ψ è ben posta. Infatti, per un laterale destro di G_α con due rapprasentanti diversi $g, h \in G$, si ha che $G_\alpha g = G_\alpha h$. Allora esiste un $x \in G_\alpha$ tale che $h = xg$. Ne segue

$$\psi(G_\alpha h) = \alpha^h = \alpha^{xg} = (\alpha^x)^g = \alpha^g.$$

Siano $g, h \in G$ tali che $\alpha^g = \alpha^h$. Poiché valgono le seguenti implicazioni

$$\alpha^{gh^{-1}} = \alpha \quad \Longrightarrow \quad gh^{-1} \in G_\alpha \quad \Longrightarrow \quad G_\alpha g = G_\alpha h$$

ψ è una applicazione iniettiva. La funzione ψ è ovviamente suriettiva. □

Corollario C2.5. *Se G agisce su Ω, si ha:*

(a) *Ω è unione disgiunta delle orbite $\{\alpha^G\}$ dei suoi membri*

$$\Omega = \biguplus_{\alpha \in C} \alpha^G$$

e quindi, se Ω è finito, vale

$$|\Omega| = \sum_{\alpha \in C} |\alpha^G|$$

dove C è un sistema di rappresentanti per le orbite di Ω.

(b) *Se G è finito, allora*

$$|G| = |\alpha^G| \cdot |G_\alpha| \quad \textit{per ogni} \quad \alpha \in \Omega.$$

DIMOSTRAZIONE. Procediamo per ordine iniziando dal primo punto.

[a] Segue banalmente dal punto **[a]** del Teorema **C2.4**.

[b] Per il teorema di Lagrange

$$|G| = [G : G_\alpha] \cdot |G_\alpha|$$

e per il punto **[d]** del Teorema **C2.4**

$$[G : G_\alpha] = |\alpha^G| \quad \Longrightarrow \quad |G| = |G_\alpha| \cdot |\alpha^G|. \qquad \square$$

Proposizione C2.6. *Siano G un p-gruppo finito* (cioè ogni elemento di G ha come ordine una potenza di p) *che agisce su un insieme Ω finito e*

$$\Omega_0 = \{\alpha \in \Omega \mid \alpha^g = \alpha \quad \forall\ g \in G\}.$$

Allora

$$|\Omega| \equiv |\Omega_0| \pmod{p}.$$

DIMOSTRAZIONE. Se C è un sistema di rappresentanti per le orbite dei membri di Ω, per il punto **[a]** del Corollario **C2.5** si ha

$$|\Omega| = \sum_{\alpha \in C} |\alpha^G|$$

inoltre possiamo scrivere che

$$\Omega_0 = \left\{\alpha \in C \mid \alpha^G = \{\alpha\}\right\}$$

quindi posto

$$D = C \backslash \Omega_0 = \left\{\alpha \in C \mid |\alpha^G| > 1\right\}$$

risulta che D è un sistema di rappresentanti per le orbite di Ω che hanno cardinalità maggiore di 1, dunque

$$|\Omega| = |\Omega_0| + \sum_{\alpha \in D} |\alpha^G|.$$

Per ipotesi G è un p-gruppo finito, quindi la sua cardinalità è una potenza di p in base al Corollario **B2.2**, cioè

$$\exists\, n \in \mathbb{N} \quad \text{tale che} \quad |G| = p^n.$$

Osserviamo che per ogni $\alpha \in \Omega_0$, si ha che

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\} = G$$

mentre, se consideriamo $\alpha \in D$, si ha $G_\alpha \neq G$. Infatti

$$\alpha \in D \quad \Longrightarrow \quad [G : G_\alpha] = |\alpha^G| > 1 \quad \Longrightarrow \quad G_\alpha \neq G$$

quindi $|G_\alpha| < p^n$. Anche G_α è un p-gruppo finito, allora $|G_\alpha|$ risulta una potenza di p. Ora, essendo $|\alpha^G| = |G|/|G_\alpha|$, anche l'ordine di α^G è una potenza di p e pertanto

$$\sum_{\alpha \in D} |\alpha^G|$$

è un multiplo di p. Dalla relazione

$$|\Omega| = |\Omega_0| + \sum_{\alpha \in D} |\alpha^G|$$

si ha che $|\Omega| - |\Omega_0|$ è un multiplo di p, cioè $|\Omega| \equiv |\Omega_0| \pmod{p}$. □

Applicando il Teorema **C2.4** ed il Corollario **C2.5**, possiamo dimostrare alcune proprietà dei gruppi finiti, introducendo opportune azioni su particolari insiemi. Vediamo un esempio.

Esempio C2.7. *Siano G un gruppo finito e A, B due sottogruppi di G. Allora*

$$|A \cdot B| = \frac{|A| \cdot |B|}{|A \cap B|} \quad \textit{dove} \quad A \cdot B = \Big\{ab \mid a \in A, b \in B\Big\}.$$

DIMOSTRAZIONE. Sia Ω l'insieme dei sottoinsiemi non vuoti di G:

$$\Omega := \{S \subseteq G \mid S \neq \emptyset\}.$$

Facciamo agire G su Ω definendo $S^g := Sg$ per ogni $g \in G$, dove con Sg indichiamo il prodotto del sottoinsieme S con g. Questa è effettivamente un'azione e la verifica è immediata.

Ora, il sottogruppo A è un membro di Ω e B agisce su Ω. Sotto l'azione di B lo stabilizzatore di A è:

$$B_A = \{g \in B \mid A\,g = A\}$$

da cui $B_A = A \cap B$, mentre l'orbita di A è data da:

$$A^B = \{A\,g \mid g \in B\}.$$

Per il Corollario **C2.5**, si ha subito che

$$|A^B| = [B : B_A] = \frac{|B|}{|A \cap B|}.$$

Ma $|Ag| = |A|$ e quindi $|A^B| = \frac{|A \cdot B|}{|A|}$, il numero dei laterali è uguale alla cardinalità di $A \cdot B$ diviso il numero degli elementi di ogni laterale. Ne segue

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

da cui la tesi. □

C3. Equazione delle classi

Per due elementi $a, b \in G$, si dice che b è coniugato ad a in G se esiste un elemento $g \in G$ tale che $b = g^{-1}ag$. Chiameremo coniugio questa relazione, la quale, essendo una relazione di equivalenza, induce una partizione di G in classi di equivalenza disgiunte (le classi di coniugio). Per ogni $\alpha \in G$, indichiamo con $\mathrm{Cl}(\alpha)$ la *classe di coniugio* a cui α appartiene.

Definizione C3.1. *Se $a \in G$, si definisce centralizzante di a in G, e si indica con $C_G(a)$, l'insieme:*

$$C_G(a) = \{x \in G \mid xa = ax\}.$$

$C_G(a)$ è l'insieme degli elementi di G che permutano con a. Inoltre, si definisce centro di un gruppo G, l'insieme

$$Z(G) = \{x \in G \mid xg = gx \quad \forall\, g \in G\}.$$

Evidentemente si ha che

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

Esempio C3.2. *Sia G un gruppo finito, $\Omega = G$ e consideriamo (G, Ω) tramite coniugio nel seguente modo:*

$$\alpha^g = g^{-1}\alpha g \quad \textit{per ogni} \quad \alpha \in \Omega \quad e \quad g \in G.$$

Verifichiamo che si tratta effettivamente di un'azione di G su Ω. Per ogni $\alpha \in \Omega$ e per ogni $g, h \in G$ si vede facilmente che

$$\alpha^e = e^{-1}\alpha e = \alpha \quad e \quad (\alpha^g)^h = h^{-1}(g^{-1}\alpha g)h = (gh)^{-1}\alpha(gh) = \alpha^{gh}.$$

Determiniamo ora, orbite e stabilizzatore sotto l'azione di G.

$$\begin{aligned} \forall\ \alpha \in \Omega: \quad \alpha^G &= \{\alpha^g \mid g \in G\} = \{g^{-1}\alpha g \mid g \in G\} = \mathrm{Cl}(\alpha); \\ G_\alpha &= \{g \in G \mid \alpha^g = \alpha\} = \{g \in G \mid g^{-1}\alpha g = \alpha\} \\ &= \{g \in G \mid \alpha g = g\alpha\} = C_G(\alpha). \end{aligned}$$

Quindi per il punto **[d]** *del* Teorema **C2.4** *segue che*

$$|\mathrm{Cl}(\alpha)| = [G : C_G(\alpha)].$$

Dall'ultimo esempio, si evince che il nucleo dell'azione è il centro $Z(G)$ in G. Ne consegue l'equazione delle classi.

Proposizione C3.3 (Equazione delle classi). *Sia G un gruppo finito. Vale la seguente*

$$|G| = |Z(G)| + \sum_{k=1}^{m} |\mathrm{Cl}(x_k)| = |Z(G)| + \sum_{k=1}^{m} [G : C_G(x_k)]$$

dove $\{x_k\}_{k=1}^m$ è un sistema di rappresentanti delle classi di coniugio di G ciascuna delle quali ha più di un elemento, mentre con $\{C_G(x_k)\}_{k=1}^m$ abbiamo indicato i rispettivi centralizzanti.

DIMOSTRAZIONE. Poiché $\Omega = G$, ne segue che il centro di G coincide con l'insieme

$$\Omega_0 = \{\alpha \in \Omega \mid \alpha^g = \alpha \quad \forall\ g \in G\} = Z(G).$$

Quindi dalla relazione

$$|\Omega| = |\Omega_0| + \sum_{\alpha \in D} |\alpha^G|$$

si ha che

$$|G| = |Z(G)| + \sum_{k=1}^{m} |\mathrm{Cl}(x_k)|$$

dove $D = \{x_1, x_2, \cdots, x_m\}$ costituisce un sistema di rappresentanti delle classi di coniugio ciascuna delle quali contiene più di un elemento. □

Teorema C3.4. *Un p-gruppo finito ha il centro non banale.*

DIMOSTRAZIONE. Osserviamo che per un qualsiasi gruppo G, $|Z(G)| \neq 0$, in quanto $Z(G)$ contiene almeno l'elemento neutro. Sia G un p-gruppo finito, dimostriamo che $|Z(G)| > 1$. Per la Proposizione **C2.6**, considerando l'azione di G tramite coniugio su $\Omega = G$ con $\Omega_0 = Z(G)$, si ha che $|G| \equiv |Z(G)| \pmod{p}$. Inoltre, essendo G un p-gruppo abbiamo

$$p \mid |G| \implies p \mid |Z(G)|.$$

Poiché $|Z(G)| \neq 0$, ne segue $|Z(G)| \geq p$. □

Corollario C3.5. *Sia G un gruppo finito di ordine p^2 con p primo. Allora G è abeliano.*

DIMOSTRAZIONE. Se G ha ordine p^2, allora G è un p-gruppo, quindi per il Teorema **C3.4**, il centro $Z(G)$ è non banale, pertanto

$$Z(G) \leq G \implies |Z(G)| \mid |G| = p^2 \implies |Z(G)| \in \{p, p^2\}.$$

Se $|Z(G)| = p^2$, allora $G = Z(G)$ è abeliano. Altrimenti per $|Z(G)| = p$, dato che il centro $Z(G)$ è un sottogruppo normale di G, possiamo considerare il gruppo quoziente $G/Z(G)$ il cui ordine è dato da:

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

quindi $Z(G)$ e $G/Z(G)$ sono dei gruppi ciclici, in quanto il loro ordine è un numero primo. Allora

$$\exists\, a \in G : \; Z(G) = \langle a \rangle,$$
$$\exists\, b \in G \backslash Z(G) : \; G/Z(G) = \langle bZ(G) \rangle;$$

da cui segue che $G = \langle a, b \rangle$; inoltre

$$a \in Z(G) \implies ab = ba$$

perciò G è abeliano. □

C4. Transitività

In questa sezione sarà illustrata una particolare tipologia di azione di un gruppo su un insieme, l'azione transitiva.

Definizione C4.1. *Se G agisce su un insieme Ω, si dice che G è* transitivo *su Ω se esiste una sola orbita*

$$\alpha^G = \Omega \quad \textit{per ogni} \quad \alpha \in \Omega.$$

In altre parole, se dati comunque due elementi $\alpha, \beta \in \Omega$ esiste $g \in G$ tale che $\alpha^g = \beta$, allora l'azione è transitiva.

Poiché Ω è costituito dall'unione disgiunta di orbite, G è transitivo su Ω se $\alpha^G = \Omega$ per almeno un $\alpha \in \Omega$. Inoltre è ovvio che se H è un sottogruppo di G e H è transitivo su Ω, allora G è transitivo su Ω.

Lemma C4.2. *Un gruppo finito G non può essere unione insiemistica di sottogruppi* (propri) *coniugati.*

DIMOSTRAZIONE. Sia G un gruppo finito. Indicato con H un suo sottogruppo proprio, proviamo che

$$G \neq \bigcup_{g \in G} H^g.$$

La tesi è ovviamente vera se H è normale in G. Dunque dobbiamo sostanzialmente provarla quando H è un sottogruppo proprio, ma non normale.

Richiamiamo la nozione di normalizzante di un sottogruppo: Se H è un sottogruppo di G, si definisce normalizzante di H in G l'insieme

$$N_G(H) = \{g \in G \mid H^g = H\}.$$

$N_G(H)$ è un sottogruppo di G; inoltre $H \triangleleft N_G(H)$, in quanto se $g \in H$ ne segue che $H^g = H$, quindi possiamo scrivere

$$H \triangleleft N_G(H) \leq G.$$

Introduciamo ora l'insieme $\mathcal{L}$ dei laterali destri di $N_G(H)$ in G:

$$\mathcal{L} = \{N_G(H)g \mid g \in G\}$$

e poniamo

$$|G| = m, \quad |H| = h \quad e \quad |N_G(H)| = n.$$

Ne segue che

$$|\mathcal{L}| = [G : N_G(H)] = \frac{|G|}{|N_G(H)|} = \frac{m}{n}.$$

Consideriamo inoltre l'insieme $\mathcal{T}$ dei sottogruppi di G coniugati ad H:

$$\mathcal{T} = \{ H^g \mid g \in G \}$$

e proviamo che l'applicazione

$$\phi: \quad \mathcal{L} \longrightarrow \mathcal{T} \quad \text{con} \quad N_G(H)g \longmapsto H^g$$

è biiettiva. Ovviamente ϕ è ben posta e suriettiva.

Siano $N_G(H)g_1, N_G(H)g_2 \in \mathcal{L}$ due laterali tali che $H^{g_1} = H^{g_2}$. Allora

$$g_1^{-1}Hg_1 = g_2^{-1}Hg_2 \iff (g_1g_2^{-1})^{-1}Hg_1g_2^{-1} = H$$

quindi il coniugato di H rispetto $g_1g_2^{-1}$ coincide con H, pertanto

$$g_1g_2^{-1} \in N_G(H) \implies N_G(H)g_1 = N_G(H)g_2.$$

Dunque ϕ è anche iniettiva. Ne segue

$$|\mathcal{T}| = |\mathcal{L}| = \frac{m}{n}.$$

Osservando che ogni membro di $\mathcal{T}$ contiene l'elemento neutro ed ha cardinalità uguale ad $h \leq n$, risulta

$$\left| \bigcup_{g \in G} H^g \right| \leq (h-1)\frac{m}{n} + 1 \leq (n-1)\frac{m}{n} + 1 = m - \frac{m}{n} + 1 < m$$

perché $m > n$ in quanto H non è normale in G. Pertanto in ogni caso G non può essere unione insiemistica di sottogruppi propri coniugati. □

Teorema C4.3. *Sia G un gruppo finito transitivo su un insieme Ω. Allora*

(a) *Ω è finito e $|\Omega|$ divide $|G|$.*

(b) *esiste $g \in G$ tale che $\alpha^g \neq \alpha$ per ogni $\alpha \in \Omega$, cioè esiste un elemento di G che muove tutti gli elementi di Ω.*

DIMOSTRAZIONE. Procediamo per ordine partendo dal primo punto.

[a] Poiché G è transitivo su Ω si ha

$$\forall\, \alpha \in \Omega: \quad \alpha^G = \Omega$$

quindi

$$|\Omega| = |\alpha^G| = [G : G_\alpha] < \infty$$

in quanto G è un gruppo finito; inoltre per ogni $\alpha \in \Omega$, si ha che

$$|\Omega| = \frac{|G|}{|G_\alpha|} \implies |\Omega| \mid |G|.$$

[b] Per il Teorema **C2.4** si ha che

$$\forall\, \alpha \in \Omega: \quad G_\alpha \leq G.$$

Inoltre, essendo G transitivo, esiste una sola orbita, quindi per ogni $\beta \in \Omega$, G_β è un sottogruppo coniugato di G_α, cioè tutti gli stabilizzatori di G risultano tra loro coniugati. Per ogni $\alpha \in \Omega$, lo stabilizzatore G_α è un sottogruppo proprio di G, altrimenti esisterebbe un $\alpha \in \Omega$ tale che

$$G = G_\alpha = \{g \in G \mid \alpha^g = \alpha\} \implies \alpha^G = \{\alpha\} \neq \Omega.$$

Poiché G è finito, per il Lemma **C4.2**

$$\exists\, g \in G:\ g \notin \bigcup_{\beta\in\Omega} G_\beta$$

ne segue che $\beta^g \neq \beta$ per ogni $\beta \in \Omega$. □

C5. Normalità

Esaminiamo ora un esempio particolare di azione transitiva.

Esempio C5.1. *Siano G un gruppo e H un sottogruppo di G. Poniamo*

$$\Omega = \{Hx \mid x \in G\}$$

l'insieme dei laterali destri di H in G.

Possiamo ora definire un'azione di G su Ω nel seguente modo:

$$\begin{aligned} \psi: \quad \Omega \times G &\longrightarrow \Omega; \\ (Hx, g) &\longmapsto (Hx)^g = Hxg. \end{aligned}$$

Verifichiamo che si tratta effettivamente di un'azione di G su Ω.

(a) $\forall\ Hx \in \Omega:\quad (Hx)^e = Hxe = Hx.$

(b) $\forall\ g, h \in G:\quad \big((Hx)^g\big)^h = (Hxg)^h = Hxgh = (Hx)(gh) = (Hx)^{gh}.$

Ora, presi due membri qualunque Hx e Hy di Ω, è sempre possibile trovare un $g \in G$ tale che $Hx = (Hy)^g$ (basta porre $g = y^{-1}x$). *Pertanto G risulta essere transitivo su Ω, cioè*

$$(Hx)^G = \Omega.$$

Lo stabilizzatore di Hx è $G_{Hx} = \{g \in G \mid (Hx)^g = Hx\}$, quindi, se g è un elemento dello stabilizzatore di Hx, deve valere

$$(Hx)^g = Hx \iff Hxg = Hx \iff Hxgx^{-1} = H.$$

Dunque $xgx^{-1} \in H$ e $g \in H^x$. Ne segue che

$$G_{Hx} = H^x.$$

Per il risultato ottenuto, il nucleo di tale azione è

$$K = \bigcap_{Hx\in\Omega} G_{Hx} = \bigcap_{x\in G} H^x$$

che risulta anche un sottogruppo normale di G.

Banalmente K è un sottogruppo normale di G contenuto in H. Sia ora T un arbitrario sottogruppo normale di G tale che $T \triangleleft H < G$. Proviamo che T è un sottogruppo di K. Notiamo che vale

$$T \triangleleft G \quad \Longrightarrow \quad \forall\, x \in G: \quad T^x = T.$$

Essendo $T \subset H$, si ha che $T^x \subset H^x$ per ogni $x \in G$ e dunque

$$T = \bigcap_{x \in G} T^x \subset \bigcap_{x \in G} H^x = K.$$

Ne segue che K è il più grande sottogruppo normale di G contenuto in H.

Teorema C5.2 (Poincarè). *Se un gruppo ha un sottogruppo di indice finito, allora necessariamente ha un sottogruppo normale di indice finito.*

DIMOSTRAZIONE. Siano G un gruppo, $H \leq G$ tale che $[G : H] = n$. Preso $\Omega = \{Hx | x \in G\}$, consideriamo l'azione di G su Ω definita nell'Esempio **C5.1**:

$$(Hx, g) \longmapsto (Hx)^g = Hxg$$

avente nucleo

$$K = \bigcap_{x \in G} H^x$$

che come abbiamo visto, è il più grande sottogruppo normale di G contenuto in H; quindi per avere la tesi, basta provare che $[G : K] < \infty$.

Se G è finito, evidentemente la tesi è banale in quanto

$$K \triangleleft H < G \quad \Longrightarrow \quad [G : K] = \frac{|G|}{|K|} < \infty.$$

Supponendo G infinito, proviamo che $|W|$ è finito, dove $W = \{Kg \mid g \in G\}$.

Nella dimostrazione del Lemma **C4.2**, abbiamo visto che esiste una biiezione tra l'insieme dei laterali destri di $N_G(H)$ in G e l'insieme dei sottogruppi di G coniugati ad H, quindi

$$|\{H^x \mid x \in G\}| = [G : N_G(H)] = m \leq n$$

in quanto $H \triangleleft N_G(H) < G$ e $[G : N_G(H)] \leq [G : H] = n$. Dunque esistono m elementi $x_1, x_2, \cdots, x_m \in G$ tali che

$$K = \bigcap_{\lambda=1}^{m} H^{x_\lambda}.$$

Ora, ogni laterale di K in G è $Kg = \left(\bigcap_{\lambda=1}^{m} H^{x_\lambda}\right)g$, quindi

$$W = \left\{Kg \mid g \in G\right\} = \left\{\left(\bigcap_{\lambda=1}^{m} H^{x_\lambda}\right)g \,\middle|\, g \in G\right\}$$

ma

$$\left(\bigcap_{\lambda=1}^{m} H^{x_\lambda}\right)g = \bigcap_{\lambda=1}^{m} \left(H^{x_\lambda}g\right)$$

pertanto ogni laterale di K in G è una intersezione dei laterali

$$H^{x_1}g, H^{x_2}g, \cdots, H^{x_m}g.$$

Posto

$$\mathfrak{W} = \left\{ \bigcap_{\lambda=1}^{m} H^{x_\lambda}g_\lambda \mid g_\lambda \in G \right\}$$

si ha che $W \subset \mathfrak{W}$, inoltre poiché due sottogruppi coniugati hanno lo stesso indice, risulta

$$[G : H^{x_\lambda}] = [G : H] = n.$$

Siccome per ogni H^{x_λ} vi sono n laterali, si ha che la cardinalità di $\mathfrak{W}$ è minore o uguale a n^m. Pertanto $|W| \leq n^m \implies [G : K] \leq n^m$. □

Proposizione C5.3. *Siano G un gruppo finito e p il più piccolo divisore primo dell'ordine di G. Sia H un sottogruppo di G di indice p. Allora H è un sottogruppo normale di G. In particolare*

(a) *un sottogruppo di indice 2 in un gruppo finito è normale.*
(b) *un sottogruppo di indice p in un p-gruppo finito è normale.*

DIMOSTRAZIONE. È facile vedere che l'enunciato principale implica immediatamente i due punti [**a**] e
textbf[b].

Siano G un gruppo finito, H un sottogruppo di G tale che $[G : H] = p$, dove p è il più piccolo divisore primo dell'ordine di G.

Poniamo $\Omega := \{Hx \mid x \in G\}$ e consideriamo l'azione di G su Ω così definita

$$(Hx, g) \longmapsto (Hx)^g = Hxg.$$

Tale azione corrisponde ad un omomorfismo ϑ tra G ed S_Ω, il gruppo simmetrico di ordine $p!$ (perché S_Ω è il gruppo delle permutazioni di Ω). Il nucleo dell'omomorfismo ϑ (anche il nucleo dell'azione di G su Ω) dato da

$$K = \bigcap_{x \in G} H^x$$

risulta un sottogruppo normale di G, per cui G/K è isomorfo ad un sottogruppo di S_Ω. Per il teorema di Lagrange, si ha che

$$|G/K| \;\Big|\; |S_\Omega| = p!.$$

Inoltre G/K è certamente non banale, in quanto

$$K < H: \quad |G/K| \geq [G:H] = p.$$

Sia ora q un arbitrario numero primo che divide $|G/K|$, allora risulta che

$$q \mid p! \quad \Longrightarrow \quad q \mid 1 \cdot 2 \cdots (p-1) \cdot p \quad \Longrightarrow \quad q \leq p.$$

Inoltre vale

$$q \,\big|\, |G/K| \quad \Longrightarrow \quad q \big|\, |G| \quad \Longrightarrow \quad q \geq p$$

perché p è il più piccolo divisore primo di $|G|$. Allora $p = q$. Ne segue che G/K è un p-gruppo finito, in quanto p è l'unico divisore primo di $|G/K|$ e il suo ordine è una potenza di p.

Supponendo che $|G/K| = p^n$ risulta

$$p^n \mid p! \quad \Longrightarrow \quad n = 1$$

perché G/K è non banale. Allora $|G/K| = p = [G:H]$.

Ricordando $K \leq H \leq G$ si ha che

$$p = [G:K] = [G:H] \cdot [H:K] = p[H:K] \implies [H:K] = 1$$

pertanto

$$[H:K] = 1 \quad \text{e} \quad K \leq H \quad \Longrightarrow \quad H = K.$$

Dunque H è un sottogruppo normale di G. □

CAPITOLO D

Teoremi di Sylow ed Applicazione

Il teorema di Lagrange asserisce che l'ordine di un sottogruppo di un gruppo finito è un divisore dell'ordine del gruppo. Il viceversa è però falso. Non vi sono molti teoremi che garantiscono l'esistenza di un sottogruppo di ordine assegnato in un gruppo finito arbitrario. Il più significativo è un lavoro dovuto al matematico norvegese Sylow.

In questo capitolo tratteremo i teoremi di Sylow che descrivono i sottogruppi di un gruppo finito arbitrario, aventi come ordine una potenza di un numero primo. Il primo teorema garantisce l'esistenza di tali sottogruppi, il secondo mette in evidenza la relazione di coniugio tra i p-sottogruppi di Sylow dello stesso ordine, mentre il terzo mostra le proprietà di divisibilità e congruenza del numero dei p-sottogruppi di Sylow, che in alcuni casi ci consentono di determinare con precisione il loro numero, come del resto avremo occasione di vedere in qualche applicazione. Infine concludiamo con un approfondimento della conoscenza di questi sottogruppi, studiando il loro comportamento in strutture quoziente e prodotti diretti.

D1. Teoremi di Sylow

Definizione D1.1. *Se G è un gruppo finito, p un numero primo e*

$$p^n \big| |G| \quad e \quad p^{n+1} \nmid |G| \quad con \quad n \in \mathbb{N}$$

un sottogruppo di G di ordine p^n si chiama p-sottogruppo di Sylow. Si tratta quindi di un sottogruppo il cui ordine è la massima potenza di p che divide l'ordine di G.

Lemma D1.2. *Siano p un numero primo e m un numero intero positivo. Allora vale la seguente congruenza*

$$\binom{mp^n}{p^n} \equiv m \pmod{p}.$$

DIMOSTRAZIONE. Per definizione di coefficiente binomiale si ha

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k} \equiv_p \begin{cases} 1, & k = 0,\ p; \\ 0, & 0 < k < p; \end{cases}$$

dove con $\equiv_p$ si indica la congruenza modulo p. Ora introdotte due variabili x, y consideriamo lo sviluppo binomiale

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

che ci conduce alle congruenze

$$(x+y)^p \equiv_p \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \equiv_p x^p + y^p,$$
$$(x+y)^{p^2} \equiv_p (x^p + y^p)^p \equiv_p x^{p^2} + y^{p^2}.$$

Continuando così abbiamo

$$(x+y)^{p^n} \equiv_p x^{p^n} + y^{p^n},$$
$$(x+y)^{mp^n} \equiv_p (x^{p^n} + y^{p^n})^m.$$

Sulla base di quest'ultima congruenza, considerando il coefficiente del termine $x^{p^n} y^{(m-1)p^n}$ si ha

$$\binom{mp^n}{p^n} \equiv_p \binom{m}{1} \equiv_p m. \qquad \square$$

Teorema D1.3 (Primo Teorema di Sylow). *Siano G un gruppo finito e p un primo che divide l'ordine di G. Allora G ha un p-sottogruppo di Sylow.*

DIMOSTRAZIONE. Per ipotesi $p \big| |G|$, allora possiamo scrivere

$$|G| = mp^n \quad \text{dove} \quad p \nmid m \quad \text{e} \quad n \geq 1.$$

Dimostriamo che esiste un sottogruppo di ordine p^n. Definiamo l'insieme Ω nel seguente modo

$$\Omega = \left\{ T \subseteq G \;\middle|\; |T| = p^n \right\}$$

e determiniamone la cardinalità.

Poiché il numero di modi di scegliere un sottoinsieme di p^n elementi da un insieme di mp^n è dato dal coefficiente binomiale, si ha

$$|\Omega| = \binom{mp^n}{p^n}.$$

Considerando ora l'azione di G su Ω così definita

$$(g, T) \longmapsto T^g = Tg \quad \text{per ogni} \quad T \in \Omega \quad \text{e} \quad g \in G$$

si ha che

$$\Omega = \bigcup_{T \in C} T^G$$

dove C è un sistema di rappresentanti per le orbite dei membri di Ω, quindi

$$|\Omega| = \sum_{T \in C} |T^G|.$$

Per il Lemma **D1.2**, vale la seguente congruenza

$$\binom{mp^n}{p^n} \equiv m \pmod{p} \quad \Longrightarrow \quad |\Omega| \equiv m \pmod{p}.$$

Dato che $p \nmid |\Omega|$, esiste un'orbita T^G tale che $p \nmid |T^G|$. Ora, considerando lo stabilizzatore di T, per il Teorema **C2.4** si ha $|T^G| = [G : G_T]$. G_T è un sottogruppo di G, se proviamo che $|G_T| = p^n$ abbiamo la tesi.

Dalla relazione $|G| = [G : G_T] \cdot |G_T|$ si ha che

$$|G_T| = \frac{|G|}{[G : G_T]}$$

pertanto

$$p^n \big| |G| \quad \text{e} \quad p \nmid [G : G_T] \quad \Longrightarrow \quad p^n \big| \, |G_T| \quad \Longrightarrow \quad |G_T| \geq p^n.$$

Inoltre dalla definizione di stabilizzatore si ha

$$\forall\, g \in G_T : \quad T^g = Tg = T \quad \Longrightarrow \quad \forall t \in T : \quad tG_T \subseteq T$$

quindi

$$|G_T| = |tG_T| \leq |T| = p^n \quad \Longrightarrow \quad |G_T| \leq p^n.$$

Dalla doppia disuguaglianza si ha $|G_T| = p^n$, pertanto G_T è proprio un p-sottogruppo di Sylow. □

Proposizione D1.4. *Sia G un gruppo finito tale che $|G| = mp^n$, dove p è un primo con* $\mathrm{mcd}(p, m) = 1$. *Allora nel gruppo G esistono p-sottogruppi di ordine $p, p^2, \cdots, p^n$.*

DIMOSTRAZIONE. Procediamo per induzione su $|G|$.

Quando $|G| = p$, la tesi è ovviamente vera. Supponiamo la tesi vera per tutti i gruppi di ordine minore di mp^n e dimostriamo che vale per $|G| = mp^n$.

Ricordiamo l'equazione delle classi

$$|G| = |Z(G)| + \sum_{k=1}^{\ell} |\mathrm{Cl}(x_k)|$$

dove $\{x_k\}_{k=1}^{\ell}$ è un sistema di rappresentanti delle classi di coniugio che contengono più di un elemento. Supponiamo che $p \big| |Z(G)|$, allora per il teorema

di Cauchy, esiste un sottogruppo in $Z(G)$ di ordine p. Ora, indicando con P_1 tale sottogruppo, non è difficile vedere che P_1 risulta un sottogruppo normale di G. Consideriamo il gruppo quoziente G/P_1 il cui ordine è dato da:

$$|G/P_1| = \frac{|G|}{|P_1|} = mp^{n-1} < mp^n$$

quindi, per l'ipotesi induttiva in G/P_1 esistono i sottogruppi

$$P_2/P_1,\ P_3/P_1,\ \cdots,\ P_n/P_1$$

di ordine rispettivamente $p, p^2, \cdots, p^{n-1}$. Ne segue che $P_1, P_2, \cdots, P_n$ sono p-sottogruppi di G di ordine rispettivamente $p, p^2, \cdots, p^n$.

Se $p \nmid |Z(G)|$ per l'equazione delle classi esiste una classe di coniugio $\mathrm{Cl}(x_k)$ tale che $p \nmid |\mathrm{Cl}(x_k)|$; ma

$$|\mathrm{Cl}(x_k)| = [G : C_G(x_k)] = \frac{|G|}{|C_G(x_k)|} \quad \Longrightarrow \quad |C_G(x_k)| = \frac{|G|}{|\mathrm{Cl}(x_k)|}$$

pertanto

$$p^n \big| |G| \quad \text{e} \quad p \nmid |\mathrm{Cl}(x_k)| \quad \Longrightarrow \quad p^n \big| |C_G(x_k)|.$$

Inoltre possiamo dire che

$$|C_G(x_k)| < |G| = mp^n \quad \text{perché} \quad x_k \notin Z(G).$$

Quindi applicando l'ipotesi induttiva si ha che in $C_G(x_k)$ esistono i sottogruppi $P_1, P_2, \cdots, P_n$ di ordine rispettivamente $p, p^2, \cdots, p^n$. Questi sono anche sottogruppi di G perché $C_G(x_k) \leq G$. □

Teorema D1.5 (Secondo Teorema di Sylow). *Siano G un gruppo finito e p un primo che divide l'ordine di G. Se P è un p-sottogruppo di G ed S un p-sottogruppo di Sylow di G, esiste $g \in G$ tale che $P \subseteq S^g$. In particolare:*

- *due p-sottogruppi di Sylow sono coniugati.*
- *ogni p-sottogruppo è un sottogruppo di qualche p-sottogruppo di Sylow.*
- *ogni p-elemento appartiene a qualche p-sottogruppo di Sylow.*

Dimostrazione. Poniamo $\Omega = \{Sg |\ g \in G\}$. Se $|G| = mp^n$ con $\mathrm{mcd}(m, p) = 1$, poiché S è un p-Sylow si ha $|S| = p^n$ e inoltre

$$|\Omega| = [G : S] = \frac{|G|}{|S|} = m \quad \Longrightarrow \quad p \nmid |\Omega|.$$

Definiamo ora un'azione di P su Ω come segue

$$(P, \Omega): \quad (x, Sg) \longmapsto (Sg)^x = Sgx$$

per la Proposizione **C2.6** abbiamo che

$$|\Omega| \equiv |\Omega_0| \pmod{p}$$

dove

$$\begin{aligned}\Omega_0 &= \Big\{Sg \in \Omega \mid Sgx = Sg \quad \forall\, x \in P\Big\} \\ &= \Big\{ \quad Sg \in \Omega \mid (Sg)^P \;=\; \{Sg\} \quad \Big\}.\end{aligned}$$

Poiché $p \nmid |\Omega|$ si ha che $p \nmid |\Omega_0|$; quindi Ω_0 è non vuoto cioè

$$\exists\, Sg \in \Omega_0 : \;\; Sgx = Sg \quad \forall\, x \in P$$

pertanto

$$gxg^{-1} \in S \quad \Longrightarrow \quad x \in S^g \quad \Longrightarrow \quad P \subseteq S^g.$$

Nel caso in cui P è un p-sottogruppo di Sylow

$$|P| = p^n \quad \text{e} \quad P \subseteq S^g \quad \Longrightarrow \quad P = S^g$$

perché $|S^g| = |S| = p^n$ e quindi P ed S risultano coniugati. Come conseguenza immediata, seguono le altre due affermazioni. □

Teorema D1.6 (Terzo Teorema di Sylow). *Siano G un gruppo finito e p un primo che divide l'ordine di G. Se n_p è il numero dei p-sottogruppi di Sylow di G ed S è un tale sottogruppo, allora*

$$n_p \;\Big|\; [G : S] \qquad e \qquad n_p \equiv 1 \pmod{p}.$$

DIMOSTRAZIONE. Ponendo Ω come l'insieme dei p-sottogruppi di Sylow di G, consideriamo la seguente azione di G su Ω

$$(G, \Omega): \quad (g, T) \quad \longmapsto \quad T^g = g^{-1}Tg$$

quindi l'orbita di un membro T, è la classe dei sottogruppi coniugati a cui T appartiene. Ma per il Teorema **D1.5** tutti i p-sottogruppi di Sylow sono coniugati, ne segue che l'azione considerata è transitiva. Pertanto

$$|\Omega| = |S^G| \quad \Longrightarrow \quad n_p = [G : G_S] = [G : N_G(S)].$$

Poiché $n_p = [G : N_G(S)]$ ed $S \leq N_G(S) \leq G$, si ha

$$n_p \;=\; \frac{[G : S]}{[N_G(S) : S]} \quad \Longrightarrow \quad n_p \mid [G : S].$$

Consideriamo un'altra azione

$$(S, \Omega): \quad (s, T) \;\longmapsto\; T^s = s^{-1}Ts.$$

Ricordando la congruenza nella Proposizione **C2.6**

$$|\Omega| \equiv |\Omega_0| \pmod{p}$$

dove

$$\Omega_0 = \big\{T \in \Omega \mid T^S = \{T\}\big\}$$

se proviamo che $|\Omega_0| = 1$ abbiamo subito la tesi dato che $|\Omega| = n_p$.

Osserviamo che

$$\forall\, x \in S : \;\; S^x = S \quad \Longrightarrow \quad S \in \Omega_0 \quad \Longrightarrow \quad \Omega_0 \neq \emptyset.$$

Verifichiamo che S è l'unico membro di Ω_0. Infatti supponendo che esista $T \in \Omega$ tale che $T^S = T$, si ha che

$$\forall\, x \in S: \quad T^x = T \quad \Longrightarrow \quad S \leq N_G(T)$$

quindi S e T sono entrambi p-sottogruppi di Sylow contenuti in $N_G(T)$. Notiamo che T è l'unico p-sottogruppo di Sylow del suo normalizzante $N_G(T)$. Inoltre S e T sono coniugati in $N_G(T)$ per il secondo teorema di Sylow. Allora $S = T$ e $|\Omega_0| = 1$. □

Corollario D1.7. *Sia G un gruppo abeliano finito. Allora*

(a) *G ha uno ed un solo p-sottogruppo di Sylow per ogni primo p che divide l'ordine di G.*
(b) *G è ciclico se e solo se i suoi sottogruppi di Sylow sono ciclici.*

DIMOSTRAZIONE. Procediamo per ordine, partendo dal primo punto.

[a] L'esistenza è garantita dal primo teorema di Sylow. L'unicità deriva dal fatto che due qualsiasi p-sottogruppi di Sylow sono coniugati.

Infatti, se S è un p-sottogruppo di Sylow, poiché G è abeliano, ogni suo sottogruppo è normale. Ne segue che l'insieme dei sottogruppi coniugati ad S in G coincide con S, quindi per ogni primo p che divide l'ordine di G esiste un unico p-sottogruppo di Sylow.

[b] La condizione necessaria segue dal fatto che ogni sottogruppo di un gruppo ciclico è ciclico. Ora dimostriamo la condizione sufficiente. Sia G un gruppo abeliano finito, allora possiamo scomporre l'ordine di G come segue:

$$|G| = \prod_{k=1}^{n} p_k^{m_k}$$

dove $\{p_k\}$ sono primi distinti e $\{m_k\}$ numeri naturali. Poiché G è abeliano, per ogni k esiste un unico p_k-sottogruppo di Sylow che indichiamo con S_k. Ora poiché ogni S_k è ciclico, se denotiamo con g_k il suo generatore si ha:

$$|S_k| = |\langle g_k \rangle| = p_k^{m_k} \quad \text{per} \quad k = 1, 2, \cdots, n.$$

Possiamo dunque definire un elemento $g = g_1 \cdot g_2 \cdots g_n$ che ovviamente appartiene a G, inoltre gli ordini dei generatori $g_1, g_2, \cdots, g_n$ sono coprimi, pertanto

$$o(g) = o(g_1) \cdot o(g_2) \cdots o(g_n) = \prod_{k=1}^{n} p_k^{m_k}.$$

Ne segue che G è un gruppo ciclico generato da g. □

D2. Applicazione e gruppi ciclici

Proposizione D2.1. *Dimostrare che per un primo p il numero dei p-sottogruppi di Sylow di S_p, gruppo simmetrico, è uguale a $(p-2)!$, da cui si deduce il teorema di Wilson*

$$(p-1)! \equiv -1 \pmod{p}.$$

DIMOSTRAZIONE. Indichiamo con n_p il numero dei p-sottogruppi di Sylow del gruppo simmetrico S_p. Se $n_p = (p-2)!$, allora per il terzo teorema di Sylow, si ha che

$$n_p \equiv 1 \pmod{p} \quad \Longrightarrow \quad (p-2)! \equiv 1 \pmod{p}.$$

Sfruttando la proprietà moltiplicativa delle congruenze, possiamo scrivere

$$(p-1)! \;=\; (p-1)(p-2)! \;\equiv_p\; p-1 \;\equiv_p\; -1.$$

A questo punto dimostriamo che il numero dei p-sottogruppi di Sylow di S_p è effettivamente $(p-2)!$. Poiché

$$|S_p| = p! : \qquad p \mid p! \qquad e \qquad p^2 \nmid p!$$

l'ordine di un p-sottogruppo di Sylow non può che essere p. Adesso, essendo p primo, ogni p-sottogruppo di Sylow è ciclico con $p-1$ generatori aventi tutti lo stesso ordine p. Quindi il numero totale dei generatori dei gruppi ciclici di ordine p è uguale a $(p-1)n_p$. Ogni elemento di ordine p in S_p risulta un p-ciclo. Dunque, se calcoliamo il numero dei p-cicli, questo deve coincidere con il numero totale dei generatori dei p-sottogruppi di Sylow. Considerando l'applicazione $\phi: \; S_p \longrightarrow S_p$ con

$$\begin{pmatrix} 1 & 2 & \cdots & p \\ x_1 & x_2 & \cdots & x_p \end{pmatrix} \longmapsto \begin{pmatrix} x_1 & x_2 & \cdots & x_p \\ x_2 & x_3 & \cdots & x_1 \end{pmatrix}$$

per $k = 1, 2, \cdots, p$, le permutazioni

$$\begin{pmatrix} 1 & 2 & \cdots & p-k & p-k+1 & \cdots & p \\ x_{k+1} & x_{k+2} & \cdots & x_p, & x_1 & \cdots & x_k \end{pmatrix}$$

hanno la stessa immagine. Dunque ϕ induce una corrispondenza p a 1, pertanto il numero dei p-cicli è:

$$\frac{p!}{p} = (p-1)! = n_p(p-1) \quad \Longrightarrow \quad n_p = \frac{(p-1)!}{p-1} = (p-2)!$$

che è la formula che volevamo dimostrare. □

Esempio D2.2. *Un gruppo di ordine* $15 = 3 \times 5$ *è ciclico.*

DIMOSTRAZIONE. Sia G un gruppo di ordine 15, indichiamo con n_3 il numero dei sottogruppi di Sylow di ordine 3 e con n_5 il numero dei sottogruppi di Sylow di ordine 5. Per il terzo teorema di Sylow si deve avere:

$$n_3 \equiv 1 \pmod 3 \quad \text{e} \quad n_3 \mid [15:3] = 5 \quad \Longrightarrow \quad n_3 = 1,$$

$$n_5 \equiv 1 \pmod 5 \quad \text{e} \quad n_5 \mid [15:5] = 3 \quad \Longrightarrow \quad n_5 = 1.$$

Quindi questi sottogruppi risultano essere normali in quanto essendo unici sottogruppi di Sylow di ordini 3 e 5 rispettivamente. Inoltre, poiché ogni gruppo finito il cui ordine è un numero primo è ciclico, possiamo scrivere

$$\begin{aligned} X &= \langle x \rangle : \quad \text{sottogruppo normale di ordine 3;} \\ Y &= \langle y \rangle : \quad \text{sottogruppo normale di ordine 5.} \end{aligned}$$

Ora poiché X e Y hanno in comune solo l'elemento neutro, risultano permutabili, infatti

$$x^{-1}y^{-1}xy = \begin{cases} x^{-1}x^y \in X, \\ (y^{-1})^x y \in Y; \end{cases}$$

pertanto

$$x^{-1}y^{-1}xy \in X \cap Y \implies x^{-1}y^{-1}xy = e \implies xy = yx.$$

Allora si ha che

$$o(xy) = \operatorname{mcm}\big(o(x), o(y)\big) = 15 = |G|.$$

Possiamo così concludere che G è ciclico. □

Questo esempio si generalizza con il seguente risultato.

Proposizione D2.3. *Siano p e q due primi con $p < q$ e $p \nmid (q-1)$. Allora ogni gruppo G di ordine pq è ciclico.*

DIMOSTRAZIONE. Indichiamo con n_p ed n_q i numeri dei p e q sottogruppi di Sylow. Per il terzo teorema di Sylow

$$n_p \mid q \quad \text{e} \quad n_p \equiv 1 \pmod p \implies n_p = 1,$$

$$n_q \mid p \quad \text{e} \quad n_q \equiv 1 \pmod q \implies n_q = 1;$$

dove si escludono i casi :

- $n_p = q$ perché per ipotesi $p \nmid (q-1) \implies q \not\equiv 1 \pmod p$;
- $n_q = p$ perché per ipotesi $p < q \implies p \not\equiv 1 \pmod q$.

Ovviamente questi sottogruppi sono ciclici, quindi possiamo scrivere

$$\begin{aligned} A &= \langle a \rangle : \quad \text{sottogruppo normale di ordine } p; \\ B &= \langle b \rangle : \quad \text{sottogruppo normale di ordine } q. \end{aligned}$$

Inoltre si ha che $A \cap B = \{e\}$ perché per qualunque $x \in A \cap B$, risulta che

$$\left.\begin{array}{l} x \in A \implies o(x) | p = |A| \\ x \in B \implies o(x) | q = |B| \end{array}\right\} \quad o(x) = 1 \quad \text{e} \quad x = e.$$

Dato che A è normale in G, consideriamo il gruppo quoziente G/A. Allora $G = \langle A, B \rangle$ se possiamo dimostrare che

$$G/A = \left\{ Ab^k \mid k = 1, 2, \cdots, q \right\}.$$

Infatti, basta verificare che questi q-laterali sono distinti. Supponiamo che esistono i e j con $1 \leq i < j \leq q$, tali che $Ab^i = Ab^j$, allora $A = Ab^{j-i}$ che è equivalente alla relazione $b^{j-i} \in A$. Dunque $o(b^{j-i}) = q | p = |A|$, che è impossibile.

Secondo il Teorema **A4.2**, si ha che G è prodotto diretto di A e B, cioè $G = A \otimes B$. Quindi a e b sono permutabili e $o(a \cdot b) = o(a) \cdot o(b) = pq$, che significa $|G| = pq = o(a \cdot b)$ e $G = \langle ab \rangle$ è ciclico. □

Esempio D2.4. *Un gruppo di ordine* 455 *è ciclico.*

DIMOSTRAZIONE. Se G è un gruppo di ordine 455, si ha che

$$|G| = 455 = 5 \cdot 7 \cdot 13.$$

usando la notazione dell'esempio precedente, denotiamo con

$$\left\{ \begin{array}{l} n_5 \\ n_7 \\ n_{13} \end{array} \right\} \quad \text{numero dei sottogruppi di Sylow di ordini} \quad \left\{ \begin{array}{l} 5 \\ 7 \\ 13 \end{array} \right\}.$$

Per il terzo teorema di Sylow si deve avere:

$$\begin{array}{lllllll} n_{13} \equiv 1 & (\text{mod } 13) & \text{e} & n_{13} \mid [455 : 13] = 35 & \implies & n_{13} = 1; \\ n_7 \equiv 1 & (\text{mod } 7) & \text{e} & n_7 \mid [455 : 7] = 65 & \implies & n_7 = 1; \\ n_5 \equiv 1 & (\text{mod } 5) & \text{e} & n_5 \mid [455 : 5] = 91 & \implies & n_5 = 1, 91. \end{array}$$

I sottogruppi di Sylow di ordine 5, 7, 13 ovviamente sono ciclici ed hanno in comune solo l'elemento neutro. Se proviamo che $n_5 \neq 91$ allora risultano anche tutti normali. Ne segue che G è uguale al prodotto diretto di tali sottogruppi per il Corollario **A4.3**. Dunque G è ciclico in quanto gli ordini dei suddetti sottogruppi sono numeri primi.

Supponiamo per assurdo $n_5 = 91$. Ogni sottogruppo di Sylow di ordine 5 ha 4 generatori di ordine 5, pertanto il numero totale degli elementi di ordine 5 è $91 \cdot 4 = 364$. Siano S_7 l'unico sottogruppo di Sylow di ordine 7 e S_{13} l'unico sottogruppo di Sylow di ordine 13. Allora

$$S_7, S_{13} \trianglelefteq G \quad \text{e} \quad S_7 \cap S_{13} = \{e\} \quad \implies \quad S_7 S_{13} = S_7 \otimes S_{13}.$$

Tutti gli elementi di $S_7 \otimes S_{13}$ hanno ordine coprimo con 5, inoltre

$$|S_7 \otimes S_{13}| = 7 \cdot 13 = 91.$$

Ora, sommando questi elementi con quelli di ordine 5 si ha $91 + 364 = 455$. Se troviamo un altro elemento il cui ordine non appartiene all'insieme

$$\{5, 7, 13, 91\} \quad \text{si ha} \quad |G| > 455$$

e necessariamente $n_5 = 1$ e G è ciclico.

Sia P_5 un qualunque sottogruppo di G di ordine 5. Posto $P = P_5P_7$, dimostriamo che P è un gruppo ciclico.

Siano $xy,\ x_1y_1 \in P$ con $x, x_1 \in P_5$ e $y, y_1 \in P_7$

$$xy = x_1y_1 \implies x_1^{-1}x = y_1y^{-1} \in P_5 \cap P_7 = \{e\}$$

$$\implies \begin{cases} x_1^{-1}x = e \\ y_1y^{-1} = e \end{cases} \implies \begin{cases} x = x_1 \\ y = y_1 \end{cases}$$

ne segue che la rappresentazione di P è unica e $|P| = 35$.

Per ogni $x \in P_5$ e $y \in P_7$, verifichiamo che $xy \in P \implies yx \in P$. Poiché

$$yx = (xx^{-1})yx = x(x^{-1}yx) = xy^x$$

si ha $yx \in P$ in quanto $P_7 \trianglelefteq G$ e $y^x \in P_7$. Quindi

$$(xy)^{-1} = y^{-1}x^{-1} \in P$$

conferma che ogni elemento ha il suo inverso in P.

Analogamente per ogni $x, x_1 \in P_5$ e $y, y_1 \in P_7$ possiamo affermare che

$$xy, x_1y_1 \in P \implies (xy)(x_1y_1) \in P.$$

Infatti, si vede facilmente che

$$(xy)(x_1y_1) = x(x_1x_1^{-1})y(x_1y_1) = xx_1(x_1^{-1}yx_1)y_1 = (xx_1)(y^{x_1}y_1) \in P$$

grazie di nuovo alla normalità di P_7. Pertanto P è chiuso.

Allora P è un gruppo di ordine 35. Inoltre dalla Proposizione **D2.3** segue che P è ciclico, quindi sicuramente contiene un elemento di ordine 35. □

Proposizione D2.5. *Siano p, q due primi distinti. Allora un gruppo di ordine pq^2 non è semplice* (cioè contiene un sottogruppo normale non banale).

DIMOSTRAZIONE. Sia G un gruppo finito con $|G| = pq^2$. Denotiamo con n_p il numero dei p-sottogruppi di Sylow di ordine p e n_q il numero dei q-sottogruppi di Sylow di ordine q^2.

Per confermare la tesi occorre dimostrare che $n_p = 1$ o $n_q = 1$.

Per il terzo teorema di Sylow valgono le seguenti relazioni:

$$n_p \mid \frac{pq^2}{p} = q^2 \quad \text{e} \quad n_p \equiv 1 \pmod{p};$$

$$n_q \mid \frac{pq^2}{q^2} = p \quad \text{e} \quad n_q \equiv 1 \pmod{q}.$$

Supponendo $n_p > 1$ ed $n_q > 1$ si ha

$$n_q = p \implies p \equiv 1 \pmod{q} \implies q \mid (p-1) \implies p > q.$$

Poiché $n_p = q$ implica $p|(q-1)$ e $p < q$, che è incompatibile con $p > q$, ne segue $n_q = p$ e $n_p = q^2$.

Ora per ogni p-sottogruppo di Sylow, abbiamo $p-1$ elementi di ordine p e due qualsiasi p-sottogruppi di Sylow distinti hanno in comune solo l'elemento neutro, quindi il numero totale dei p-elementi è uguale a

$$n_p(p-1) = q^2(p-1).$$

Mentre, se Q_1 e Q_2 sono due q-sottogruppi di Sylow con $Q_1 \neq Q_2$, si ha:

$$|Q_1 \cap Q_2| \mid q^2 \implies |Q_1 \cap Q_2| \leq q.$$

Pertanto il numero dei q-elementi è certamente maggiore o uguale a

$$n_q(q^2-q) + q = p(q^2-q) + q.$$

Poiché G deve contenere tutti i p-elementi e tutti i q-elementi possiamo scrivere

$$|G| \geq q^2(p-1) + p(q^2-q) + q = pq^2 + (p-1)q(q-1) > pq^2.$$

Ma questo è impossibile, quindi necessariamente $n_p = 1$ o $n_q = 1$, cioè G deve contenere un sottogruppo normale non banale. □

D3. Sottogruppo e gruppo quoziente

Lemma D3.1. *Siano G un gruppo finito e H un sottogruppo proprio di G. Se P_1 e P_2 sono due p-sottogruppi di Sylow di H, allora i p-sottogruppi di Sylow di G che li contengono sono distinti. Ne segue che il numero dei p-sottogruppi di Sylow di H non supera il numero dei p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Sia H un sottogruppo di G con $|G| < \infty$. Supponiamo che P_1 e P_2 siano due p-sottogruppi di Sylow distinti di H. Per il secondo

teorema di Sylow, esistono in G due p-sottogruppi di Sylow S_1 e S_2 che contengono rispettivamente P_1 e P_2 come sottogruppi. Dobbiamo dimostrare che $S_1 \neq S_2$.

Supponendo per assurdo che $S_1 = S_2$ si ha che:

$$P_1 \subset H \quad \text{e} \quad P_1 \subset S_1 \quad \Longrightarrow \quad P_1 = H \cap S_1;$$

$$P_2 \subset H \quad \text{e} \quad P_2 \subset S_2 \quad \Longrightarrow \quad P_2 = H \cap S_2;$$

perché P_1 e P_2 sono p-sottogruppi massimali in H. Allora

$$P_1 = H \cap S_1 = H \cap S_2 = P_2.$$

Questo è assurdo perché P_1 e P_2 per ipotesi sono due p-sottogruppi di Sylow distinti di H, pertanto si ha la tesi. □

Proposizione D3.2. *Sia H un sottogruppo normale di un gruppo finito G. Allora valgono le seguenti affermazioni:*

(a) *Se S è un qualsiasi sottogruppo di Sylow di G, allora $H \cap S$ è un p-sottogruppo di Sylow di H.*
(b) *Se $p \nmid [G : H]$, allora H contiene tutti i p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Sia G un gruppo finito con $H \trianglelefteq G$.

[a] Se T è un p-sottogruppo di Sylow di H, allora per il secondo teorema di Sylow esiste $g \in G$ tale che $T \subseteq S^g$ dove S è un p-sottogruppo di Sylow di G. Inoltre $T = H \cap S^g$ ed essendo H normale in G si ha

$$H \cap S^g = H^g \cap S^g = (H \cap S)^g.$$

Quindi $T = (H \cap S)^g$ e, ricordando che due sottogruppi coniugati hanno lo stesso ordine, ne segue

$$|T| = |(H \cap S)^g| = |H \cap S|.$$

Dunque $H \cap S$ risulta un p-sottogruppo di Sylow di H.

[b] Sia p^n la massima potenza di p tale che $p^n \big| |G|$. Poiché per ipotesi $p \nmid [G : H]$ si ha che $p^n \big| |H|$, allora, per il primo teorema di Sylow, esiste un p-sottogruppo di Sylow S contenuto in H con $|S| = p^n$. Ovviamente qualunque p-sottogruppo di Sylow T di G ha ordine p^n e, per il secondo teorema di Sylow, esiste $g \in G$ tale che $T = S^g$. Ora, essendo $H \triangleleft G$, esso contiene tutti i suoi coniugati quindi

$$T = S^g \subseteq H^g = H \quad \Longrightarrow \quad T \subseteq H.$$

Pertanto H contiene tutti i p-sottogruppi di Sylow di G. □

Teorema D3.3. *Siano G un gruppo finito e H un sottogruppo normale di G. Allora tutti e soli i p-sottogruppi di Sylow di G/H si ottengono come immagini dell'omomorfismo canonico dei p-sottogruppi di Sylow di G. Ne segue che il numero dei p-sottogruppi di Sylow di G/H non supera il numero dei p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Poiché H è normale in G, possiamo considerare il gruppo quoziente G/H e l'omomorfismo canonico

$$\begin{aligned} \varphi: \quad G &\longrightarrow G/H; \\ g &\longmapsto Hg. \end{aligned}$$

Se S è un p-sottogruppo di Sylow di G, allora $\varphi(S) = HS/H$. Dobbiamo dimostrare che:

(a) HS/H è un p-sottogruppo di Sylow di G/H.
(b) tutti i p-sottogruppi di Sylow di G/H sono immagini di questo tipo, cioè se T/H è un p-sottogruppo di Sylow di G/H, allora esiste un p-sottogruppo di Sylow S di G tale che $\varphi(S) = HS/H = T/H$.

Queste due affermazioni vengono provate come segue.

[a] Per il teorema d'omomorfismo vale

$$\varphi(S) = \{Hx \mid x \in S\} = HS/H \leq G/H.$$

Non è difficile verificare che HS/H è un p-gruppo con l'ordine uguale a una potenza di p. Calcolando l'indice

$$[G/H : HS/H] = \frac{|G|}{|H|} \cdot \frac{|H|}{|HS|} = [G : HS]$$

risulta che

$$p \nmid [G/H : HS/H] = [G : HS] = \frac{[G : S]}{[HS : S]}$$

perché $S \leq HS \leq G$ e $p \nmid [G : S]$. Pertanto HS/H è un p-sottogruppo di G/H con l'ordine di massima potenza di p, cioè un p-sottogruppo di Sylow nel gruppo quoziente G/H.

[b] Se T/H è un p-sottogruppo di Sylow di G/H allora $p \nmid [G/H : T/H]$ e

$$[G/H : T/H] = \frac{|G|}{|H|} \cdot \frac{|H|}{|T|} = [G : T] \quad \Longrightarrow \quad p \nmid [G : T].$$

Allora, per il primo teorema di Sylow, esiste un p-sottogruppo di Sylow di T, denotato con S, che ovviamente è anche un p-sottogruppo di Sylow di G. Pertanto

$$S \leq T \quad \Longrightarrow \quad \varphi(S) \leq \varphi(T) \quad \Longrightarrow \quad HS/H \leq T/H.$$

Ma HS/H e T/H sono entrambi p-sottogruppi di Sylow di G/H quindi hanno lo stesso ordine, pertanto $T/H = HS/H$, cioè T/H risulta l'immagine di un p-sottogruppo di Sylow S di G mediante l'omomorfismo canonico. □

D4. Normalizzanti e sottogruppi di Sylow

Lemma D4.1. *Siano G un gruppo finito e S un p-sottogruppo di Sylow. Allora per un sottogruppo H con $S \leq N_G(S) \leq H \leq G$ si ha che $H = N_G(H)$. In particolare*

$$H = N_G(S) \quad \Longrightarrow \quad N_G(S) = N_G\big(N_G(S)\big).$$

DIMOSTRAZIONE. Secondo la definizione, vogliamo dimostrare che

$$N_G(H) = \{g \in G \mid H^g = H\} \;=\; H$$

cioè, che per ogni $g \in G$ vale l'implicazione: $H^g = H \implies g \in H$.

Sia $g \in G$ tale che $H^g = H$. Per ipotesi $S \leq H$, quindi S è un p-Sylow di H e $S^g \leq H^g = H$. Per il secondo teorema di Sylow S^g è ancora un p-Sylow di H, allora

$$\exists\, h \in H :\; S^g = S^h \quad \Longrightarrow \quad S^{gh^{-1}} = S.$$

Ne segue che

$$gh^{-1} \in N_G(S) \leq H \quad \Longrightarrow \quad g \in Hh = H. \qquad \square$$

Proposizione D4.2. *Siano G un gruppo finito e P un p-sottogruppo ma non di Sylow. Allora P è un sottogruppo proprio del suo normalizzante in G, cioè $P < N_G(P)$.*

DIMOSTRAZIONE. Per ipotesi P è un p-sottogruppo non di Sylow, quindi $p \,\big|\, [G : P]$. Distinguiamo ora due casi: $p \nmid [G : N_G(P)]$ e $p \mid [G : N_G(P)]$. Nel primo caso, abbiamo subito che $p|[N_G(P) : P]$ e $P < N_G(P)$ perché $[N_G(P) : P] = [G : P]/[G : N_G(P)]$.

Per il secondo caso, definiamo $\Omega := \{P^g | g \in G\}$. Allora seguendo la dimostrazione del Lemma **C4.2**, si ha che $p\big||\Omega| = [G : N_G(P)]$. Consideriamo ora la seguente azione

$$\begin{aligned}(P, \Omega) :\quad & P \times \Omega \;\longrightarrow\; \Omega;\\ & (g, Q) \;\longrightarrow\; Q^g = g^{-1}Qg.\end{aligned}$$

Secondo la Proposizione **C2.6**, vale la congruenza $|\Omega| \equiv |\Omega_0| \pmod p$ dove Ω_0 è l'insieme delle orbite aventi un solo membro. Osservando che $\Omega_0 \neq \emptyset$,

perché $P \in \Omega_0$ e $p \,\big|\, |\Omega_0| \equiv |\Omega| \pmod{p}$, abbiamo $|\Omega_0| > 1$. Pertanto

$$\exists\, Q \in \Omega_0 \text{ con } Q = P^g \neq P \text{ tale che } Q^P = Q \implies P \leq N_G(Q).$$

Dimostriamo che $Q \neq N_G(Q)$. Infatti, supponendo il contrario

$$Q = N_G(Q) \quad \text{e} \quad P \leq N_G(Q) \quad \Longrightarrow \quad P = Q$$

si giunge all'assurdo, pertanto $Q < N_G(Q)$. Allora possiamo concludere che

$$P = Q^{g^{-1}} < N_G^{g^{-1}}(Q) = N_G(Q^{g^{-1}}) = N_G(P)$$

grazie alle seguenti implicazioni bidirezionali:

$$\begin{aligned} x \in N_G^{g^{-1}}(Q) \quad &\Longleftrightarrow \quad g^{-1}xg \in N_G(Q); \\ Q^{(g^{-1}xg)} = Q \quad &\Longleftrightarrow \quad (Q^{g^{-1}})^{xg} = Q; \\ (Q^{g^{-1}})^x = Q^{g^{-1}} \quad &\Longleftrightarrow \quad x \in N_G(Q^{g^{-1}}). \end{aligned}$$

□

Corollario D4.3. *Sia P un p-gruppo finito. Allora ogni sottogruppo proprio non è uguale al suo normalizzante in P, cioè*

$$H < P \quad \Longrightarrow \quad H \neq N_P(H).$$

DIMOSTRAZIONE. Poiché P è un p-gruppo finito, ogni suo sottogruppo proprio non è di Sylow, quindi per la Proposizione **D4.2** segue la tesi.

Questo corollario può essere dimostrato direttamente per induzione su $|P|$.

Per $|P| = p$, non c'è nulla da dimostrare. Supponiamo la tesi vera per $|P| \leq p^n$, cioè ogni sottogruppo proprio di P è strettamente contenuto nel suo normalizzante. Sia $|P| = p^{n+1}$ e indichiamo con Z il centro di P. Dal Teorema **C3.4**, sappiamo che un p-gruppo finito ha il centro non banale, pertanto $|Z| > 1$ e $p \,||Z|$.

Sia H un qualunque sottogruppo proprio di P. Se $Z \nsubseteq H$, allora abbiamo subito che $H \neq N_P(H)$ perché $Z \subseteq N_P(H)$.

Invece nel caso $Z \subset H$, considerando i due gruppi quozienti H/Z e P/Z, si ha che

$$H < P \quad \Longrightarrow \quad H/Z < P/Z.$$

Poiché Z è non banale si ha $|P/Z| \leq p^n$. Per l'ipotesi induttiva $H/Z \neq N_{P/Z}(H/Z)$ dove

$$N_{P/Z}(H/Z) = N_P(H)/Z \qquad (\star)$$

pertanto

$$H/Z \neq N_P(H)/Z \quad \Longrightarrow \quad H \neq N_P(H).$$

La dimostrazione viene completata dalla conferma dell'equazione ($\star$):

$$\begin{aligned} N_{P/Z}(H/Z) &= \{xZ \in P/Z \mid (H/Z)^{xZ} = H/Z\} \\ &= \{xZ \in P/Z \mid H^x/Z = H/Z\} \\ &= \{xZ \in P/Z \mid x \in N_G(H)\} = N_G(H)/Z. \end{aligned}$$ □

D5. Prodotto diretto

Teorema D5.1. *Un gruppo finito G è prodotto diretto dei suoi sottogruppi di Sylow se e solo se ogni sottogruppo di Sylow è normale.*

DIMOSTRAZIONE. Secondo il teorema fondamentale dell'aritmetica vale la seguente scomposizione

$$|G| = \prod_{k=1}^{\ell} p_k^{m_k}$$

dove $p_1, p_2, \cdots, p_\ell$ sono primi distinti e $m_1, m_2, \cdots, m_\ell$ numeri naturali. Allora per ogni k con $1 \leq k \leq \ell$, esiste un p_k-sottogruppo S_k di Sylow in G.

"$\Longrightarrow$" Se $G = S_1 \otimes S_2 \otimes \cdots \otimes S_n$ dove $n \geq \ell$ e gli $\{S_k\}_{k=1}^n$ sono tutti i suoi sottogruppi di Sylow, allora per definizione di prodotto diretto, risultano $n = \ell$ ed ogni S_k compare una sola volta nel prodotto diretto. Quindi per ogni k con $k = 1, 2, \cdots, \ell$, esiste un unico p_k-sottogruppo S_k di Sylow in G, che è anche un sottogruppo normale.

"$\Longleftarrow$" Se $S_i \trianglelefteq G$ con $i = 1, 2, \cdots, \ell$ allora per ogni i esiste un unico p_i-sottogruppo di Sylow. Possiamo quindi considerare il prodotto degli S_i per $i = 1, 2, \cdots, \ell$ e dimostrare che $G = S_1 \otimes S_2 \otimes \cdots \otimes S_\ell$.

Banalmente $|G| = \prod_{i=1}^{\ell} |S_i|$. Ora, consideriamo S_i e S_j con $1 \leq i < j \leq \ell$:

$$\forall\, x \in S_i,\ \forall\, y \in S_j : \quad xy = yx \quad \Longleftrightarrow \quad x^{-1}y^{-1}xy = e.$$

Osserviamo che

$$\begin{cases} x^{-1}y^{-1}xy = x^{-1}x^y \in S_i; \\ x^{-1}y^{-1}xy = (y^{-1})^x y \in S_j. \end{cases}$$

Inoltre, il teorema di Lagrange asserisce che

$$\left.\begin{array}{l} |S_i \cap S_j| \,\big|\, |S_i| \\ |S_i \cap S_j| \,\big|\, |S_j| \end{array}\right\} \quad \Longrightarrow \quad |S_i \cap S_j| = 1.$$

Abbiamo quindi

$$x^{-1}y^{-1}xy \in S_i \cap S_j = \{e\} \quad \Longrightarrow \quad xy = yx.$$

Secondo il Corollario **A4.3**, la tesi segue dal fatto che i sottogruppi $\{S_i\}_{i=1}^{\ell}$ permutano elemento per elemento. □

Corollario D5.2. *Un gruppo finito G è prodotto diretto dei suoi sottogruppi di Sylow se solo se non esiste un sottogruppo proprio in G che è uguale al suo normalizzante.*

DIMOSTRAZIONE. Supponiamo come prima che G sia un gruppo finito con $|G| = \prod_{i=1}^{\ell} p_i^{m_i}$ dove p_i sono primi distinti e m_i numeri naturali.

"$\Longleftarrow$" Sia S_i un p_i-sottogruppo di Sylow, allora per il Lemma **D4.1**

$$N_G(S_i) = N_G\big(N_G(S_i)\big).$$

Ma per ipotesi, non esiste un sottogruppo proprio in G che è uguale al suo normalizzante, per cui $N_G(S_i) = G$. Allora S_i è normale, quindi per ogni indice i esiste un unico p_i-sottogruppo di Sylow S_i e per il Teorema **D5.1** risulta che G è uguale al prodotto diretto dei suoi p-sottogruppi di Sylow.

"$\Longrightarrow$" Siano $\{S_i\}_{i=1}^{\ell}$ sottogruppi di Sylow con $|S_i| = p_i^{m_i}$ tali che

$$G = S_1 \otimes S_2 \otimes \cdots \otimes S_\ell.$$

Per ogni sottogruppo proprio H di G, dobbiamo provare che $H \neq N_G(H)$. Affermiamo prima che vale il seguente prodotto diretto:

$$H = \bigotimes_{k=1}^{\ell} (H \cap S_k). \qquad (\star)$$

Per ogni $h \in H$, si ha che $o(h) \mid |G|$. Allora esistono ℓ-numeri naturali $\{n_i\}$ tali che $o(h) = \prod_{i=1}^{\ell} p_i^{n_i}$ con $0 \leq n_i \leq m_i$. Secondo il Lemma **B2.3**, h si scrive in modo unico come prodotto $h = h_1 h_2 \cdots h_\ell$, dove h_i risulta una potenza di h con $o(h_k) = p_k^{n_k}$. Ricordando che S_k è l'unico p_k-sottogruppo di Sylow di G, allora $h_k \in S_k$. Inoltre, $h_k \in H$ perché h_k è una potenza di h. Dunque $h_k \in H \cap S_k$ e $h \in \bigotimes_{k=1}^{\ell}(H \cap S_k)$. Notando il fatto ovvio $\bigotimes_{k=1}^{\ell}(H \cap S_k) \subseteq H$, otteniamo che $H = \bigotimes_{k=1}^{\ell}(H \cap S_k)$.

Ma H è un sottogruppo proprio di G, perciò esiste k con $1 \leq k \leq m$ tale che $H \cap S_k < S_k$. Grazie al Corollario **D4.3** si ha che

$$H \cap S_k < N_{S_k}(H \cap S_k).$$

Dal prodotto diretto risulta che

$$H = (H \cap S_k) \bigotimes_{i=1,\, i\neq k}^{\ell} (H \cap S_i)$$

$$< N_{S_k}(H \cap S_k) \bigotimes_{i=1,\, i\neq k}^{\ell} (H \cap S_i)$$

$$\leq N_{S_k}(H \cap S_k) \bigotimes_{\substack{i=1\\ i\neq k}}^{\ell} N_{S_i}(H \cap S_i).$$

Il risultato finale $H \neq N_G(H)$ viene conseguito se proviamo la seguente equazione:

$$N_G(H) = \bigotimes_{k=1}^{\ell} N_{S_k}(H \cap S_k). \qquad (\star\star)$$

Ricordando $(\star)$, si ha

$$N_G(H) = \bigotimes_{k=1}^{\ell} \Big\{ S_k \cap N_G(H) \Big\}$$

che implica $(\star\star)$ se possiamo provare che per ogni $1 \leq k \leq \ell$, vale

$$N_{S_k}(H \cap S_k) = S_k \cap N_G(H).$$

Questa equazione si verifica tramite doppia inclusione. Infatti, per ogni $x \in S_k \cap N_G(H)$, abbiamo

$$(H \cap S_k)^x = H^x \cap S_k^x = H \cap S_k$$

che equivale a $x \in N_{S_k}(H \cap S_k)$. Viceversa per ogni $y \in N_{S_k}(H \cap S_k)$, si ha ovviamente $y \in S_k$. Richiamando il prodotto diretto, deduciamo che

$$H^y = \bigotimes_{i=1}^{\ell} (H \cap S_i)^y = (H \cap S_k)^y \bigotimes_{i\neq k} (H \cap S_i)^y = (H \cap S_k) \bigotimes_{i\neq k} (H \cap S_i) = H$$

perché y commuta con tutti gli elementi di $H \cap S_i$ con $i \neq k$. Dunque $y \in N_G(H)$ e conseguentemente $y \in S_k \cap N_G(H)$.

Possiamo anche dimostrare $(\star\star)$ direttamente tramite doppia inclusione.

Per ogni $x \in N_G(H)$, esistono $x_k \in S_k$ e $x_k \in \langle x \rangle$ con $1 \leq k \leq \ell$ tali che

$$x = x_1 x_2 \cdots x_\ell \in \bigotimes_{k=1}^{\ell} N_{S_k}(H \cap S_k)$$

grazie al Lemma **B2.3** ed al prodotto diretto $G = \bigotimes_{k=1}^{\ell} S_k$.

Invece per ogni $y \in \bigotimes_{k=1}^{\ell} N_{S_k}(H \cap S_k)$ esistono $y_k \in N_{S_k}(H \cap S_k)$ tali che $y = y_1 y_2 \cdots y_\ell$. Allora per ogni k con $1 \leq k \leq \ell$, si verifica che

$$\begin{aligned} H^{y_k} &= \left\{ \bigotimes_{i=1}^{\ell} (H \cap S_i) \right\}^{y_k} = \bigotimes_{i=1}^{\ell} (H \cap S_i)^{y_k} \\ &= (H \cap S_k)^{y_k} \bigotimes_{i \neq k} (H \cap S_i)^{y_k} \\ &= (H \cap S_k) \bigotimes_{i \neq k} (H \cap S_i) = H. \end{aligned}$$

Quindi $H^y = H^{y_1 y_2 \cdots y_\ell} = H$, che implica $y \in N_G(H)$. □

Teorema D5.3. *Siano G un gruppo finito e N un sottogruppo normale. Se P è un p-sottogruppo di Sylow di N, allora*

$$G = N_G(P)N.$$

DIMOSTRAZIONE. L'inclusione " $\supseteq$" è ovvia. Per ogni $g \in G$, si vede facilmente che $P \leq N$ implica $P^g \leq N^g = N$; pertanto P e P^g risultano p-sottogruppi di Sylow di N. Per il secondo teorema di Sylow, esiste $x \in N$ tale che $P^g = P^x$. Quest'ultimo equivale a $P^{gx^{-1}} = P$, cioè $gx^{-1} \in N_G(P)$ e quindi $g \in N_G(P)x$, che implica $g \in N_G(P)N$. □

CAPITOLO E

Gruppi Risolubili e Nilpotenti

Il presente capitolo intende fornire una trattazione, non certo esaustiva, di due importanti argomenti riguardanti i gruppi: la risolubilità e la nilpotenza.

Gli argomenti sono divisi in sei sezioni: le prime tre, sui gruppi risolubili, presentano dapprima un'introduzione riguardante i concetti di *commutatori, serie di composizione e derivato* di un gruppo, essenziali per giungere alla definizione di risolubilità, poi analizzano le conseguenze di tali proprietà e, infine, ampliano la prospettiva intrecciando la questione con un altro argomento fondamentale della teoria dei gruppi, i sottogruppi di Sylow.

Le ultime tre sezioni, introducendo i concetti di *serie centrale* inferiore e superiore, preparano allo studio della nilpotenza dei gruppi finiti. Inoltre, sottolineano l'importanza dei sottogruppi di Frattini nel determinare la nilpotenza del gruppo che li contiene.

E1. Serie normale e di composizione

Definizione E1.1 (Serie subnormale e normale). *Consideriamo una successione di sottogruppi di un gruppo G, in cui ogni sottogruppo è un sottogruppo normale del gruppo che lo precede:*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_\ell.$$

Tale successione è detta serie subnormale *e la indicheremo con Σ. Se ogni G_i è anche un sottogruppo normale di G, chiameremo la successione* serie normale.

I gruppi quozienti $\{G_{k-1}/G_k\}_{k=1}^{\ell}$ vengono chiamati fattori della serie Σ ed il numero dei fattori ℓ viene denominato la *lunghezza* di Σ.

Esempio E1.2. *Siano G un gruppo e H un sottogruppo normale di G. Allora $G \trianglerighteq H \trianglerighteq \{e\}$ risulta sempre una serie normale.*

Esempio E1.3 (gruppo simmetrico). *Sia S_4 un gruppo simmetrico di ordine 24. Definiamo due sottogruppi come segue:*

$$\begin{aligned} H_1 : &= \{e, (12)(34), (13)(24), (14)(23)\}; \\ H_2 : &= \{e, (12)(34)\}. \end{aligned}$$

Allora $S_4 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \{e\}$ è una serie subnormale di S_4 ma non normale.

Per indagare meglio la struttura di un gruppo G, si aspetta normalmente che i fattori delle serie subnormali siano i più semplici possibili. Dal punto di vista dei sottogruppi normali, preferiamo che questi fattori siano semplici. Il seguente risultato dice quando G/H è semplice se $H \trianglelefteq G$.

Proposizione E1.4. *Siano G un gruppo e H un sottogruppo normale di G. Allora il gruppo quoziente G/H è semplice se e solo se H è un sottogruppo normale massimale di G*

DIMOSTRAZIONE. Suppponiamo che G/H sia semplice. Se H non è un sottogruppo normale massimale di G, allora esiste un sottogruppo normale N di G tale che $G \trianglerighteq N \trianglerighteq H$. Quindi N/H è un sottogruppo normale non banale di G/H, contrario alla semplicità di G/H.

Viceversa, se G/H non è semplice, esiste un sottogruppo normale non banale N/H di G/H e risulta $G \trianglerighteq N \trianglerighteq H$. Quest'ultima implica che H non è un sottogruppo normale massimale di G. □

Definizione E1.5 (Serie di composizione). *Sia Σ una serie subnormale di un gruppo G senza ripetizione:*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_\ell$$

in cui ciascun G_k risulta un sottogruppo normale massimale del suo predecessore G_{k-1}. Allora Σ si dice serie di composizione. *I fattori di Σ si chiamano* fattori di composizione.

Esempio E1.6 (gruppo quadrinomio di Klein). *Sia $V_4 = \{e, a, b, ab\}$ il gruppo quadrinomio di Klein* (gruppo abeliano non ciclico di ordine 4). *Allora ci sono, in tutto, tre serie di composizione:*

$$\begin{aligned} V_4 &\trianglerighteq \langle a \rangle \trianglerighteq \{e\}, \\ V_4 &\trianglerighteq \langle b \rangle \trianglerighteq \{e\}, \\ V_4 &\trianglerighteq \langle ab \rangle \trianglerighteq \{e\}. \end{aligned}$$

Esempio E1.7 (gruppo dei quaternioni). *Sia* $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ *il gruppo dei quaternioni. Allora ci sono, in tutto, tre serie di composizione:*

$$\begin{aligned} Q_8 &\trianglerighteq \langle i \rangle \trianglerighteq \{\pm 1\} \trianglerighteq \{1\}, \\ Q_8 &\trianglerighteq \langle j \rangle \trianglerighteq \{\pm 1\} \trianglerighteq \{1\}, \\ Q_8 &\trianglerighteq \langle k \rangle \trianglerighteq \{\pm 1\} \trianglerighteq \{1\}. \end{aligned}$$

Definizione E1.8 (Serie di raffinamento). *Siano* Σ *e* Ξ *due serie subnormali di un gruppo* G *rispettivamente date da*

$$\begin{aligned} G &= G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_\ell; \\ G &= H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_\kappa. \end{aligned}$$

Si dice che Ξ *è un* raffinamento *di* Σ *se ogni termine di* Σ *compare nella serie* Ξ. *Se poi* Ξ *contiene strettamente* Σ, *allora si parla di* raffinamento proprio.

Si evince che una serie subnormale Σ di G risulta *serie di composizione* se non ammette alcun raffinamento proprio.

Definizione E1.9 (Isomorfismo fra due serie subnormali). *Siano* Σ *e* Ξ *due serie subnormali di un gruppo* G. *Si dice che* Σ *e* Ξ *sono isomorfe se hanno la stessa lunghezza e i rispettivi fattori isomorfi a meno dell'ordine.*

Per la serie di composizione, vale il seguente importante teorema.

Teorema E1.10 (Jordan-Hölder). *Sia* G *un gruppo finito. Allora due qualunque serie di composizione di* G *sono isomorfe.*

DIMOSTRAZIONE. Sia G un gruppo finito. Proviamo la tesi per induzione su l'ordine di G.

• Per $|G| = 1$, la tesi è ovvia.

• Come ipotesi induttiva assumiamo che la tesi sia vera per tutti i gruppi H con $|H| < |G|$.

• Per il gruppo finito G consideriamo ora due serie di composizioni:

$$\begin{aligned} \mathrm{S}: &\quad G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{e\}, \\ \mathrm{T}: &\quad G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{e\}. \end{aligned}$$

Se $G_1 = H_1$, allora abbiamo due serie di composizioni

$$\begin{aligned} \mathrm{S}': &\quad G_1 \triangleright G_2 \triangleright \cdots \triangleright G_m = \{e\}, \\ \mathrm{T}': &\quad H_1 \triangleright H_2 \triangleright \cdots \triangleright H_n = \{e\}. \end{aligned}$$

che sono isomorfe per l'ipotesi del passo induttivo perché $|G_1| = |H_1| < |G|$.

Se $G_1 \neq H_1$, G_1 e H_1 sono due sottogruppi normali massimali di G, quindi $G = G_1H_1$. Consideriamo allora una qualunque serie di composizione

$$G_1 \cap H_1 = F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}$$

e costruiamo due serie subnormali di G:

$$\begin{aligned} \mathrm{S}'' : &\quad G \rhd G_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}, \\ \mathrm{T}'' : &\quad G \rhd H_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}. \end{aligned}$$

Per il terzo teorema di isomorfismo abbiamo

$$\begin{aligned} G/G_1 = (G_1H_1)/G_1 &\cong H_1/(G_1 \cap H_1) = H_1/F_1, \\ G/H_1 = (G_1H_1)/H_1 &\cong G_1/(G_1 \cap H_1) = G_1/F_1, \end{aligned}$$

dove H_1/F_1 e G_1/F_1 sono gruppi semplici, perché G_1 e H_1 sono sottogruppi normali massimali di G. Allora la $[\mathrm{S}'']$ e la $[\mathrm{T}'']$ sono due serie di composizioni di G isomorfe. Ora, ricordando che $|G_1| < |G|$ e $|H_1| < |G|$, abbiamo che, per l'ipotesi del passo induttivo, la serie di composizione $[\mathrm{S}']$ è isomorfa alla $G_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}$ e la serie di composizione $[\mathrm{T}']$ è isomorfa alla $H_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}$. Dunque la $[\mathrm{S}]$ è isomorfa alla $[\mathrm{S}'']$ e la $[\mathrm{T}]$ è isomorfa alla $[\mathrm{T}'']$. Per la transitività dell'isomorfismo, la $[\mathrm{S}]$ e la $[\mathrm{T}]$ sono isomorfe. □

Da questo teorema, possiamo ricavare subito il seguente risultato.

Corollario E1.11 (Schreier). *Due serie subnormali di un gruppo G ammettono sempre raffinamenti isomorfi.* □

E2. Commutatori e derivati

Sia G un gruppo e siano x, y elementi di G. Si dice *commutatore* della coppia (x, y) e si denota col simbolo $[x, y]$, l'elemento $x^{-1}y^{-1}xy$.

Ovviamente possiamo definire commutatori di ordine superiore, tramite la formula ricorsiva $[x_1, x_2, \cdots, x_{n-1}, x_n] = \big[[x_1, x_2, \cdots, x_{n-1}], x_n\big]$. Questi sono detti *commutatori semplici.*

Più in generale, tutti gli elementi che si possono ottenere tramite commutazioni successive sono detti *commutatori complessi.* (Per esempio, con $a, b, \alpha, \beta, \gamma$ elementi di un gruppo G, $\big[[a, b], [\alpha, \beta, \gamma]\big]$ è un commutatore complesso).

Notiamo ora che,

$$yx[x,y] \;=\; yxx^{-1}y^{-1}xy = xy.$$

Da questa uguaglianza segue che due elementi x e y del gruppo G sono permutabili se e solo se $[x,y] = e$.

In particolare, poi, $\forall x \in G : \; [x,x] = e$, quindi l'unità di G è un commutatore. Inoltre, l'inverso di un commutatore è ancora un commutatore, infatti, se $x, y \in G$, vale

$$[x,y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x].$$

Tuttavia non è assolutamente detto che il prodotto di due commutatori sia un commutatore, sicché l'insieme dei commutatori di un gruppo G, in generale, non è un sottogruppo di G.

Sia G un gruppo e siano H e K sottogruppi di G. Si dice *interderivato* di H e K e si denota con $[H,K]$, il sottogruppo di G generato dall'insieme $\{[h,k] \mid h \in H, k \in K\}$. Poiché, come abbiamo già osservato, $\forall h \in H$ e $\forall k \in K : \; [h,k]^{-1} = [k,h]$, si ha che $[H,K] = [K,H]$.

Consideriamo ora il caso in cui H e K siano normali in G e proviamo che $[H,K]$ è un sottogruppo normale di G. Ricordiamo intanto che se G è un gruppo e $g \in G$, l'applicazione

$$\begin{aligned} \phi_g : \qquad & G \longrightarrow G, \\ & x \longmapsto x^g = g^{-1}xg; \end{aligned}$$

è un isomorfismo. In generale, supponiamo che ϕ sia un omomorfismo fra due gruppi G_1 e G_2. Allora per due generici elementi $x, y \in G_1$, vale l'identità: $\phi\big([x,y]\big) = \big[\phi(x), \phi(y)\big]$. Infatti, l'affermazione segue immediatamente dalla seguente relazione:

$$\phi\big([x,y]\big) = \phi(x^{-1}y^{-1}xy) = \phi^{-1}(x)\phi^{-1}(y)\phi(x)\phi(y) = \big[\phi(x), \phi(y)\big].$$

Pertanto, se H e K sono due sottogruppi normali in G, allora per ogni $g \in G$ vale $[H,K]^g = [H^g, K^g] = [H,K]$, cioè $[H,K]$ è normale in G.

Sia G un gruppo. Si dice *derivato* (o *sottogruppo commutatore*) di G e si indica col simbolo G' l'interderivato $[G,G]$, cioè il sottogruppo generato da tutti i commutatori di elementi di G.

Per quanto detto circa l'interderivato, segue immediatamente che il derivato G' è un sottogruppo caratteristico di G, cioè invariante sotto qualunque automorfismo di G; esso à evidentemente un sottogruppo normale di G. Inoltre, poiché due elementi $x, y \in G$ sono permutabili se e solo se $[x,y] = e$, si ha che G è abeliano se e solo se $G' = \{e\}$.

Diamo ora una caratterizzazione del derivato di un gruppo. Il derivato G' di un gruppo G è il minimo sottogruppo normale N di G (*rispetto alla relazione di inclusione*) tale che il quoziente G/N sia abeliano. Questa è una conseguenza del seguente teorema.

Teorema E2.1. *Siano G un gruppo e G' il derivato di G. Allora*

(a) *il quoziente G/G' è un gruppo abeliano.*
(b) *se $N \trianglelefteq G$ e G/N è abeliano, allora $G' \subseteq N$.*
(c) *se $H \leq G$ e $G' \subseteq H$, allora $H \trianglelefteq G$.*

DIMOSTRAZIONE. Procediamo per ordine, partendo dal primo punto.

[a] Siano $x, y \in G$. Per due laterali $xG', yG' \in G/G'$, abbiamo che $[xG', yG'] = [x, y]G' = G'$; infatti, qualunque siano gli elementi x e y di G, il commutatore $[x, y]$ appartiene a G'. Pertanto i laterali xG' e yG' sono permutabili, cioè G/G' è abeliano.

[b] Sia $N \trianglelefteq G$ tale che G/N sia abeliano. $\forall x, y \in G : \ xN$ e yN sono permutabili e quindi $N = [xN, yN] = [x, y]N$, per cui $[x, y] \in N$. Pertanto G', essendo generato dai commutatori di elementi di G, è contenuto in N.

[c] Basta dimostrare che se $g \in G$ e $h \in H$ allora $h^g = g^{-1}hg \in H$. Dato che G/G' è un gruppo abeliano che contiene H/G' come un sottogruppo, allora per ogni $g \in G$ e $h \in H$, vale la seguente relazione

$$h^g G' = (hG')^{gG'} = (gG')^{-1}(hG')gG' = hG'.$$

Allora esiste $g' \in G'$ tale che $h^g = hg' \in H$, da cui segue che H è un sottogruppo normale di G. □

Teorema E2.2 (Schur). *In un gruppo G, se il centro ha indice finito, allora il derivato di G è finito.*

DIMOSTRAZIONE. Denotiamo con Z il centro del gruppo G e consideriamo l'applicazione:

$$\theta : G/Z \times G/Z \longrightarrow G';$$
$$\theta(xZ, yZ) = [x, y] \ \text{ per } \ x, y \in G.$$

È facile verificare che θ è suriettiva. Quindi

$$|G'| \ \leq \ \left|G/Z \times G/Z\right| = [G : Z]^2$$

che significa che G' è finito. □

Per mezzo del teorema appena provato saremo in grado di dare, in seguito, una caratterizzazione dei gruppi risolubili di ordine finito.

Definizione E2.3. *Sia G un gruppo e si ponga $G^{(0)} = G$. Per un numero naturale k, definiamo $G^{(k)}$ per induzione con $G^{(k)} = (G^{(k-1)})'$. Il sottogruppo $G^{(k)}$ si dice* k-esimo derivato *di G.*

In particolare si ha $G^{(1)} = G'$. Possiamo osservare che

$$G' = [G, G], \quad G'' = [G', G'] = \big[[G, G], [G, G]\big], \quad \cdots .$$

Dunque G'' è normale in G perché per ogni $g \in G$ vale la seguente

$$\begin{aligned} (G'')^g &= \big[[G, G], [G, G]\big]^g \\ &= \big[[G, G]^g, [G, G]^g\big] \\ &= \big[[G^g, G^g], [G^g, G^g]\big] \\ &= \big[[G, G], [G, G]\big] = G''. \end{aligned}$$

Secondo il principio di induzione, possiamo concludere che l'insieme $\{G^{(k)} \mid k \in \mathbb{N}_0\}$ risulta essere una serie normale di G; tale serie è chiamata *serie derivata* di G.

E3. Gruppi risolubili

Definizione E3.1. *Un gruppo G si dice* risolubile *se la sequenza*

$$G \supseteq G' \supseteq G'' \supseteq \cdots \supseteq G^{(k)} \supseteq \cdots$$

in cui ogni gruppo $G^{(k)}$ è il derivato del precedente, termina nell'elemento neutro in un numero finito di passi, cioè esiste un intero nonnegativo ℓ tale che $G^{(\ell)} = \{e\}$.

OSSERVAZIONE: Dal Teorema **E2.1** segue che ogni fattore $G^{(k)}/G^{(k+1)}$ è un gruppo quoziente abeliano.

Diamo ora la caratterizzazione dei gruppi risolubili di ordine finito della cui esistenza avevamo accennato nel paragrafo precedente.

Teorema E3.2. *Un gruppo di ordine finito è risolubile se e solo se ogni fattore, in una serie di composizione da G ad $\{e\}$, è ciclico di ordine primo.*

Questo teorema è stato, storicamente, la prima definizione di risolubilità, ma aveva il grosso limite di non essere applicabile ai gruppi infiniti.

DIMOSTRAZIONE. Proviamo separatamente la condizione sufficiente e la condizione necessaria per la validità del teorema.

"$\Longleftarrow$" Supponiamo $G = A_0 \supset A_1 \supset \cdots \supset A_n = \{e\}$, dove A_{i-1}/A_i, $i = 1, 2, \cdots, n$ è ciclico di ordine primo. Dal Teorema **E2.1**, poiché G/A_1 è abeliano, segue che $A_1 \supseteq G'$. Analogamente, $A_2 \supseteq A_1' \supseteq G''$ e, in ultimo $A_n \supseteq G^{(n)}$, quindi $G^{(n)} = \{e\}$ e G è risolubile.

"$\Longrightarrow$" Supponiamo che G sia risolubile e finito. Poiché G/G' è abeliano, nella serie

$$G \supset G' \supset G'' \supset \cdots \supset G^{(n)} = \{e\}$$

esisterà un sottogruppo normale massimale $A_1 \supseteq G'$. Dal fatto che G/A_1 sia abeliano e semplice (cioè non contiene sottogruppi normali propri), segue che G/A_1 è ciclico di ordine primo. Analogamente, poiché A_1 è risolubile, esisterà A_2, sottogruppo normale massimale contenuto in A_1 con $A_1 \supset A_2 \supset A_1' \supseteq G''$, tale che A_1/A_2 è ciclico di ordine primo. Continuando così, avremo

$$G = A_0 \supset A_1 \supset \cdots \supset A_m = \{e\}$$

con A_{i-1}/A_i gruppo ciclico di ordine primo $\forall i = 1, 2, \cdots, m$. Inoltre, secondo il teorema di Jordan-Hölder, date due qualunque serie di composizione di un gruppo finito G, queste sono isomorfe; pertanto vale la tesi. □

Corollario E3.3. *Un gruppo semplice risolubile ha ordine primo.*

DIMOSTRAZIONE. Sia G un gruppo risolubile. Allora $G \neq G'$. Inoltre, dalla semplicità, risulta che $G' = \{e\}$ e $G = G/G'$ è abeliano. Dunque G è un gruppo abeliano semplice, che deve essere un gruppo ciclico di ordine primo. □

Esempio E3.4 (gruppo abeliano). *Ogni gruppo abeliano è risolubile.*

Esempio E3.5. *Il gruppo $\mathbb{Q}_8$ dei quaternioni è risolubile.*

Diamo ora un importante risultato sui p-gruppi finiti.

Teorema E3.6. *Ogni p-gruppo finito è risolubile.*

DIMOSTRAZIONE. Siano p un primo e G un p-gruppo finito di ordine p^n con $n \in \mathbb{N}$. Secondo la Proposizione **D1.4**, possiamo costruire una successione

$$G = G_n \supseteq G_{n-1} \supseteq G_{n-2} \supseteq \cdots \supseteq G_1 \supseteq G_0 = \{e\}$$

dove $\forall k = 0, 1, \cdots, n-1$: G_k è un sottogruppo di G di ordine p^k, pertanto massimale e quindi normale in G_{k+1} grazie alla Proposizione **C5.3**. Allora ogni fattore G_{k+1}/G_k è un gruppo ciclico di ordine p e quindi abeliano. Così la successione è una serie di composizione del gruppo G. Quindi G è risolubile grazie al Teorema **E3.2**. □

Diamo un'ultima caratterizzazione dei gruppi risolubili:

Teorema E3.7. *Sia G un gruppo. Sono equivalenti le seguenti affermazioni:*

(a) *G è risolubile.*

(b) *G ha una serie normale finita*

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_m = \{e\}$$

in cui ogni $A_{i-1}/A_i,\ i = 1, 2, \cdots, m$ è abeliano.

(c) *G ha una serie finita*

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n = \{e\}$$

in cui ogni $B_{j-1}/B_j,\ j = 1, 2, \cdots, n$ è abeliano.

DIMOSTRAZIONE. Proviamo le tre affermazioni ciclicamente.

[a]$\Longrightarrow$[b] Se G è risolubile, allora la sua serie derivata

$$G \supset G' \supset G'' \supset \cdots \supset G^{(m)} = \{e\}$$

è una serie normale finita in cui $G^{(i-1)}/G^{(i)}$ è abeliano per $i = 1, 2, \cdots, m$, quindi vale il punto **[b]**.

[b]$\Longrightarrow$[c] Banale (una serie normale è una serie).

[c]$\Longrightarrow$[a] Se $G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n = \{e\}$ è una serie con B_{j-1}/B_j abeliano per $j = 1, 2, \cdots, n$, allora, poiché $G/B_1 = B_0/B_1$ è abeliano, $B_1 \supseteq G'$. Analogamente, se $B_j \supseteq G^{(j)}$, allora $B_{j+1} \supseteq B_j' \supseteq G^{(j+1)}$. Quindi, in ultimo, $G^{(n)} \subseteq B_n = \{e\}$ e perciò $G^{(n)} = \{e\}$. Pertanto G è risolubile. □

Corollario E3.8. *Un gruppo G è risolubile se ha un sottogruppo normale H tale che sia H che G/H siano risolubili.*

DIMOSTRAZIONE. Consideriamo le due serie

$$G/H \supseteq A_1/H \supseteq \cdots \supseteq A_m/H \supseteq H/H$$

e

$$H \supseteq B_1 \supseteq \cdots \supseteq B_n \supseteq \{e\}$$

rispettivamente per G/H e H, che soddisfano la proprietà **[c]** del teorema precedente. Allora

$$G \supseteq A_1 \supseteq \cdots \supseteq A_m \supseteq H \supseteq B_1 \supseteq \cdots \supseteq B_n \supseteq \{e\}$$

è una serie che soddisfa la stessa suddetta proprietà **[c]** per G; perciò G è risolubile. □

Teorema E3.9. *Tutti i sottogruppi e tutti i gruppi quoziente di un gruppo risolubile sono risolubili.*

DIMOSTRAZIONE. Sia G risolubile e $H \leq G$. Allora dalla definizione di derivato di un gruppo segue che $H' \subseteq G'$, poiché H' è generato da tutti i commutatori di elementi di H e G' è generato da tutti i commutatori di elementi di G. Analogamente, $H'' \subseteq G''$, ecc. Se $G^{(m)} = \{e\}$ per una certa $m \in \mathbb{N}$, allora $H^{(m)} = \{e\}$. Pertanto H è risolubile. Ovviamente può accadere che $H^{(k)} = \{e\}$ già per qualche $k < m$.

Sia ora $W = G/K$ un certo gruppo quoziente di G e consideriamo l'omomorfismo canonico $\varphi : G \longrightarrow W$. Ogni commutatore in W è l'immagine di un commutatore in G, quindi $G' \longrightarrow W'$. Continuando, $G^{(n)} \longrightarrow W^{(n)}$, perciò, se $G^{(n)} = \{e\}$, allora $W^{(n)} = \{e\}$, cioè W è risolubile. Anche in questo caso, naturalmente, può accadere che $W^{(k)} = \{e\}$ già prima per qualche $k < n$. □

Dal confrontando con i teoremi di Sylow possiamo affermare che valgono i seguenti risultati sui gruppi risolubili la cui dimostrazione viene lasciata come esercizio al lettore (si può usare il principio di induzione e l'azione di un gruppo su un insieme).

Teorema E3.10. *Sia G un gruppo risolubile di ordine mn, dove m e n sono numeri naturali coprimi. Allora:*

(a) *G possiede almeno un sottogruppo di ordine m.*
(b) *Due qualunque sottogruppi di ordine m sono coniugati.*
(c) *Un sottogruppo il cui ordine m' divide m è contenuto in un sottogruppo di ordine m.*
(d) *Il numero dei sottogruppi di ordine m può essere espresso come un prodotto in cui ogni fattore*
   - *è congruente a 1 modulo un certo fattore di m;*
   - *è una potenza di un primo.*

Di seguito enunciamo altri tre risultati molto significativi le cui dimostrazioni, tuttavia, sono decisamente complesse e pertanto non possono essere qui riportate.

- Il gruppo simmetrico S_n non è risolubile per $n > 4$.
- Un gruppo di ordine $p^m q^n$, dove p e q sono primi ed m, n interi non negativi, è risolubile (Burnside).
- Ogni gruppo di ordine dispari è risolubile (Feit-Thompson).

E4. Serie centrale inferiore e superiore

Definiamo una serie di sottogruppi di un gruppo G tramite le seguenti regole:

$$\Gamma_1(G) = G \quad \text{e} \quad \Gamma_k(G) = \langle\, [x_1, x_2, \cdots, x_k] \mid \forall x_1, x_2, \cdots, x_k \in G \rangle.$$

Per la proprietà dei commutatori semplici vale che

$$[y_1, y_2, \cdots, y_{k+1}] = \big[[y_1, y_2, \cdots, y_k], y_{k+1}\big].$$

Possiamo notare che per ogni k : $\Gamma_{k+1}(G) \subseteq \Gamma_k(G)$. La serie

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \Gamma_3(G) \supseteq \cdots$$

è detta *serie centrale inferiore* di G.

Teorema E4.1 (Interderivato ricorsivo). $\Gamma_{k+1}(G) = [\Gamma_k(G), G]$.

DIMOSTRAZIONE. Da $[y_1, y_2, \cdots, y_k, y_{k+1}] = \big[[y_1, y_2, \cdots, y_k], y_{k+1}\big]$, abbiamo banalmente la prima inclusione "$\subseteq$". Per provare l'altra inclusione abbiamo bisogno della seguente identità di facilissima verifica:

$$[xy, z] = [x, z]^y\, [y, z] = [x, z]\, [x, z, y]\, [y, z].$$

Ora poniamo

$$\begin{aligned} x &= [a_1, a_2, \cdots, a_k], \\ y &= [a_1, a_2, \cdots, a_k]^{-1}, \\ z &= a_{k+1}. \end{aligned}$$

Allora

$$e = [e, a_{k+1}] = [a_1, a_2, \cdots, a_k, a_{k+1}]^y \, \big[[a_1, a_2, \cdots, a_k]^{-1}, a_{k+1}\big].$$

Così abbiamo l'appartenenza di $\big[[a_1, a_2, \cdots, a_k]^{-1}, a_{k+1}\big]$ a $\Gamma_{k+1}(G)$, conseguenza dell'appartenenza degli altri termini a $\Gamma_{k+1}(G)$. Notiamo che l'interderivato $[\Gamma_k(G), G]$ è generato dagli elementi $[u_1 u_2 \cdots u_n, g]$, dove $u_i = [a_1, a_2, \cdots, a_k]$ oppure $[a_1, a_2, \cdots, a_k]^{-1}$. Abbiamo provato che $[u_i, g] \in \Gamma_{k+1}(G)$. Proviamo per induzione su n che $[u_1 u_2 \cdots u_n, g] \in \Gamma_{k+1}(G)$. Questo si può fare, ponendo nell'identità precedentemente enunciata

$$x = u_1 u_2 \cdots u_{n-1}, \quad y = u_n, \quad z = g;$$

così abbiamo

$$[u_1 u_2 \cdots u_{n-1} u_n, g] = [u_1 u_2 \cdots u_{n-1}, g]^{u_n} [u_n, g].$$

Per l'ipotesi induttiva le due espressioni a destra sono in $\Gamma_{k+1}(G)$. Quindi abbiamo provato l'altra inclusione e, di conseguenza, il teorema. □

Da questo teorema segue un importante corollario.

Corollario E4.2. $\Gamma_k(G)/\Gamma_{k+1}(G)$ *è nel centro di* $G/\Gamma_{k+1}(G)$.

Infatti, presi $\gamma \in \Gamma_k(G)$ e $g \in G$, abbiamo $[\gamma, g] \in \Gamma_{k+1}(G)$. Ne segue

$$[\gamma\Gamma_{k+1}(G), g\Gamma_{k+1}(G)] = \Gamma_{k+1}(G).$$

Quindi effettivamente è valido il corollario.

Possiamo anche definire una *serie centrale superiore* per un gruppo G.

$$Z_0 = \{e\} \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_i(G) \subseteq Z_{i+1}(G) \subseteq \cdots$$

dove definiamo Z_{i+1} tramite la seguente regola: $Z_{i+1}(G)/Z_i(G)$ è il centro di $G/Z_i(G)$. Tra poco spiegheremo il motivo della dicitura *superiore* e *inferiore* applicata alle serie centrali.

Una serie $G = A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \supseteq A_{m+1} = \{e\}$, in cui ogni A_i/A_{i+1} è nel centro di G/A_{i+1} è chiamata *serie centrale.*

Teorema E4.3. *Sia $G = A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \supseteq A_{m+1} = \{e\}$ una serie centrale per G. Allora $A_i \supseteq \Gamma_i(G)$ per $i = 1, \cdots, m+1$ e $A_{1+m-j} \subseteq Z_j(G)$ per $j = 0, 1, 2, \cdots, m$.*

DIMOSTRAZIONE. Abbiamo $A_1 = G = \Gamma_1(G)$. Supponiamo che $A_i \supseteq \Gamma_i(G)$. Dal fatto che A_i/A_{i+1} è nel centro di G/A_{i+1} segue che $[A_i, G] \subseteq A_{i+1}$. Ma allora, ricordando anche il Teorema **E4.1**, si ha che $\Gamma_{i+1}(G) = [\Gamma_i(G), G] \subseteq [A_i, G] \subseteq A_{i+1}$. Per induzione, questo prova che $A_i \supseteq \Gamma_i(G)$ per $i = 0, 1, 2, \cdots, m$.

Evidentemente si ha che $A_{m+1} \subseteq Z_0(G)$ e $A_m \subseteq Z_1(G)$. Supponiamo ora che per una certa j valga che $A_{1+m-j} \subseteq Z_j(G)$. Allora $U = G/Z_j(G)$ è immagine tramite un omomorfismo di $V = G/A_{1+m-j}$ con $\mathrm{Ker} Z_j(G)/A_{1+m-j}$. Ora A_{m-j}/A_{1+m-j} è nel centro di V, quindi la sua immagine omomorfa in U deve essere nel centro di U. Ma questa immagine è $(A_{m-j}Z_j)/Z_j$, mentre il centro di U è Z_{j+1}/Z_j. Quindi $A_{m-j} \subseteq A_{m-j}Z_j \subseteq Z_{j+1}$, provando la tesi per induzione. □

E5. Gruppi nilpotenti

Nelle sezioni precedenti, abbiamo parlato di gruppi risolubili. Ci sono però proprietà più forti della risolubilità; una di queste è la nilpotenza.

Definizione E5.1. *Un gruppo G è nilpotente se possiede una serie normale finita $G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_\ell = \{e\}$, in cui ogni gruppo quoziente A_{i-1}/A_i è nel centro di G/A_i con $i = 1, 2, \cdots, \ell$.*

Ricordando il Teorema **E3.7**, possiamo subito affermare che un gruppo nilpotente è risolubile. Un'altra immediata conseguenza si può evidenziare dal Teorema **E4.3** con il seguente corollario.

Corollario E5.2. *In un gruppo nilpotente G, le serie centrali inferiore e superiore hanno entrambe la medesima lunghezza finita ℓ.*

Infatti, se c'è una serie centrale finita di lunghezza m, il Teorema **E4.3** mostra che le serie centrali inferiore e superiore hanno al più lunghezza m. Inoltre, comparando le due serie, possiamo dedurre che non possono essere di lunghezze differenti, quindi esse hanno la stessa lunghezza ℓ e questo numero ℓ è detto la *classe* del gruppo nilpotente. Un gruppo nilpotente di classe uno è semplicemente un gruppo abeliano.

Possiamo notare che se un gruppo G è nilpotente di classe ℓ, allora ogni commutatore $[a_1, a_2, \cdots, a_{\ell+1}]$ è l'identità, e viceversa, se $[a_1, a_2, \cdots, a_{\ell+1}] = e$, allora G è nilpotente al più di classe ℓ. Indicheremo la proprietà che $[a_1, a_2, \cdots, a_{\ell+1}] = e$ per ogni $a_i \in G$, dicendo che G è *ℓ-nilpotente.*

Teorema E5.3. *Se G è ℓ-nilpotente, allora ogni sottogruppo e ogni gruppo quoziente di G è ℓ-nilpotente.*

DIMOSTRAZIONE. Se G è ℓ-nilpotente, allora necessariamente, per un sottogruppo H, tutti i commutatori $[a_1, a_2, \cdots, a_{\ell+1}]$ con $a_i \in H$, devono essere l'identità. Quindi H è ℓ-nilpotente. Anche se T è un'immagine omomorfa di G, allora ogni commutatore $[b_1, b_2, \cdots, b_{\ell+1}]$ con $b_i \in T$ è immagine di un certo commutatore $[a_1, a_2, \cdots, a_{\ell+1}]$ in G e quindi è l'identità. Perciò T è ℓ-nilpotente. □

Teorema E5.4. *Siano G un gruppo ℓ-nilpotente e $H = H_0$ un sottogruppo. Per $k = 1, 2, \cdots$, si denota con $H_k = N_G(H_{k-1})$, il normalizzante di H_{k-1} in G, allora $H_\ell = G$.*

DIMOSTRAZIONE. $H_0 \supseteq Z_0 = \{e\}$ banalmente. Proviamo ora per induzione che $H_m \supseteq Z_m$ per ogni m. Assumiamo vera l'ipotesi del passo induttivo che $H_i \supseteq Z_i$. Allora, dalla definizione di Z_{i+1}, presi $z_{i+1} \in Z_{i+1}$ e $g \in G$, $z_{i+1}^{-1} g^{-1} z_{i+1} g = z_i \in Z_i$, quindi se $g^{-1} = h_i \in H_i$, abbiamo che $z_{i+1}^{-1} h_i z_{i+1} = z_i h_i \in H_i$, e così Z_{i+1} normalizza H_i, da cui $H_{i+1} \supseteq Z_{i+1}$. Pertanto è provato l'asserto per induzione. Da $Z_\ell = G$, ricaviamo infine $H_\ell = G$. □

Corollario E5.5. *Ogni sottogruppo proprio di un gruppo nilpotente è un sottogruppo proprio del suo normalizzante.*

Altrimenti avremmo $H = H_0 = H_1 = H_2 = \cdots = H_\ell$ con $H_k \subset G$.

Corollario E5.6. *Ogni sottogruppo massimale di un gruppo nilpotente è normale di indice primo e contiene il gruppo derivato.*

Infatti, sia M un sottogruppo massimale del gruppo nilpotente G. $N_G(M)$ contiene propriamente M, perciò abbiamo necessariamente che $N_G(M) = G$, oppure $M \lhd G$. Allora, per la massimalità di M, G/M non contiene sottogruppi propri, quindi deve essere un gruppo ciclico di ordine primo. Così M è di indice primo e G/M è abeliano, perciò M contiene il gruppo derivato G' grazie al Teorema **E2.1**.

Corollario E5.7. *Se G è nilpotente e H è un sottogruppo tale che $G = HG'$, allora $H = G$.*

In questa situazione, infatti, se per assurdo $H \neq G$, allora, per il teorema precedente, esiste una serie

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_{\ell-1} \lhd H_\ell = G \quad \text{con} \quad Z_k(G) \subseteq H_k.$$

Per la definizione di serie centrale superiore, si ha che $G/H_{\ell-1}$ è abeliano; quindi $H_{\ell-1} \supseteq G'$ per il Teorema **E2.1**. Ma allora $HG' \subseteq H_{\ell-1}G' = H_{\ell-1} \neq G$, contrariamente alla nostra ipotesi. Quindi dobbiamo avere $H = G$. Notiamo che non abbiamo supposto che G possedesse sottogruppi massimali.

Torniamo ora a parlare di sottogruppi di Sylow con il prossimo teorema che ci fornisce una caratterizzazione dei gruppi nilpotenti finiti:

Teorema E5.8. *Tutti i p-gruppi finiti sono nilpotenti. Un gruppo finito è nilpotente se e solo se è prodotto diretto dei suoi sottogruppi di Sylow.*

DIMOSTRAZIONE. Ogni p-gruppo finito P ha il centro non banale (differente dall'identità). Quindi la serie centrale superiore per P termina con l'intero gruppo, quindi P è nilpotente. Lo stesso vale per il prodotto diretto di p-gruppi finiti. Supponiamo ora che G sia un gruppo finito nilpotente e sia P un p-sottogruppo di Sylow di G. Allora $N_G(P)$ è il suo stesso normalizzante (vedi il Lemma **D4.1**) e, per il Corollario **E5.5**, $N_G(P)$ non può essere un sottogruppo proprio di G. Quindi $P \lhd G$. Essendo ogni sottogruppo di Sylow di G normale, G risulterà essere prodotto diretto dei suoi sottogruppi di Sylow. Questo è giustificato dal Teorema **D5.1**. □

Corollario E5.9 (Wielandt). *Un gruppo finito è nilpotente se e solo se i suoi sottogruppi massimali sono normali.*

DIMOSTRAZIONE. La condizione necessaria segue immediatamente dal Corollario **E5.6** che afferma che i sottogruppi massimali di un gruppo nilpotente sono normali. Per dimostrare che la condizione è sufficiente, consideriamo

un qualunque p-sottogruppo di Sylow P di G. Vogliamo dimostrare che P è normale in G, cioè il suo normalizzante $N_G(P)$ coincide con G. Se così non fosse, essendo $N_G(P)$ un sottogruppo proprio di G, esisterebbe in G un sottogruppo massimale M contenente $N_G(P)$ come sottogruppo. Dato che M è normale in G, allora $N_G(M) = G$. D'altra parte, risulta $M = N_G(M) < G$ per il Lemma **D4.1**. Questa è una contraddizione. Pertanto $N_G(P) = G$ e P è normale in G. Secondo il Teorema **D5.1**, G è prodotto diretto dei sottogruppi di Sylow e quindi nilpotente. □

E6. Sottogruppo di Frattini

Tratteremo in questo paragrafo di un particolare sottogruppo di un gruppo G, il sottogruppo di *Frattini* che, nel caso di gruppi finiti, risulterà essere nilpotente e che, sotto altre condizioni che vedremo in seguito, ci garantirà la nilpotenza dello stesso gruppo G.

Per ora diamo una definizione del sottogruppo di Frattini:

Definizione E6.1. *Sia G un gruppo. Definiamo il sottogruppo di Frattini F di G nel seguente modo: $F = G \bigcap_M M$, dove M varia sui sottogruppi massimali di G se G ha sottogruppi massimali. Mentre $F = G$ se e solo se G non ha sottogruppi massimali.*

Molto interessante è la relazione del sottogruppo di Frattini F con i generatori di G, infatti F contiene gli elementi di G che non generano G. Formalizziamo meglio questo concetto:

Definizione E6.2. *Un elemento x di un gruppo G è detto un non-generatore di G se, per ogni sottoinsieme T di G tale che $G = \langle T, x\rangle$, risulta $G = \langle T\rangle$.*

Notiamo che se $G \neq \{e\}$, sicuramente e è un non-generatore.

Teorema E6.3. *Se un gruppo G è diverso dall'elemento neutro, allora il suo sottogruppo di Frattini F è l'insieme dei non-generatori di G.*

DIMOSTRAZIONE. Sia x un elemento di G. Se c'è un sottogruppo massimale M che non contiene x, allora il gruppo $\langle M, x\rangle$ contiene propriamente M, ed essendo M massimale, deve risultare che $\langle M, x\rangle = G$. Ma qui $\langle M\rangle = M \neq G$. Così x è un generatore essenziale in $\langle M, x\rangle = G$. Allora i non-generatori di G appartengono ai sottogruppi massimali e così ogni non-generatore è un elemento di $F = G \bigcap_M M$. Viceversa, dobbiamo provare che se $y \in F$, allora y è un non-generatore di G. Per ipotesi $G \neq \{e\}$, quindi "e" è

sicuramente un non-generatore. Ora supponiamo che $G = \langle T, y\rangle$ per un certo sottoinsieme T di G. Proviamo che se $\langle T\rangle = H \neq G$, arriviamo ad un assurdo. Osserviamo intanto che y non può appartenere a H se $H \neq G$. Infatti, se così fosse, avremmo $H = \langle H, y\rangle \supseteq \langle T, y\rangle = G$, contrariamente alla nostra ipotesi. Quindi $y \notin H$. Allora, per il Lemma di Zorn, c'è un sottogruppo $K \supseteq H$ massimale e tale che $y \notin K$. Ora $\langle K, y\rangle \supseteq \langle T, y\rangle = G$, quindi $\langle K, y\rangle = G$. Ma, per come abbiamo scelto K, qualunque gruppo che contenga propriamente K deve contenere y. Quindi $K = M$ è un sottogruppo massimale che non contiene y, in contrasto con il fatto che $y \in F = G \underset{M}{\cap} M$. Quindi dobbiamo avere $\langle T\rangle = G$ e così ogni $y \in F$ risulta essere un non-generatore di G. □

OSSERVAZIONE: Nella dimostrazione abbiamo citato il Lemma di **Zorn**, il cui enunciato è il seguente: "Sia S un insieme parzialmente ordinato. Supponiamo che ogni sottoinsieme ordinato di S abbia estremo superiore in S. Allora S ha massimo".

Teorema E6.4. *Il sottogruppo di Frattini di un gruppo finito è nilpotente.*

DIMOSTRAZIONE. Sia G un gruppo finito e F il suo sottogruppo di Frattini che, come sottogruppo caratteristico di G, è un sottogruppo normale. Sia P un p-sottogruppo di Sylow di F. Dunque ogni coniugato di P in G sta in F e così è coniugato a P in F. Quindi P ha tanti coniugati in F quanti in G e così $[G : N_G(P)] = [F : N_F(P)]$. Ma

$$[G : N_F(P)] = [G : F][F : N_F(P)] = [G : N_G(P)][N_G(P) : N_F(P)]$$

quindi $[G : F] = [N_G(P) : N_F(P)]$. Notando che $N_F(P) = F \cap N_G(P)$ ed applicando la equazione dell'Esempio **C2.7**, troviamo che

$$[G : F] = [N_G(P) : F \cap N_G(P)] = [F \circ N_G(P) : F].$$

Da questo concludiamo che $F \circ N_G(P) = G$. Poiché $G = \langle F, N_G(P)\rangle$, abbiamo anche che, togliendo uno alla volta gli elementi di F, essendo F finito, $G = \langle N_G(P)\rangle = N_G(P)$. Così $P \lhd G$ e chiaramente $P \lhd F$. Poiché ogni sottogruppo di Sylow di F è normale, F deve essere prodotto diretto dei suoi sottogruppi di Sylow e quindi è un gruppo nilpotente. □

Teorema E6.5. *Il sottogruppo di Frattini di un gruppo nilpotente contiene il gruppo derivato.*

DIMOSTRAZIONE. Dal Corollario **E5.7** se G è nilpotente e $G = HG'$, allora $G = H$. Questo significa che G' può essere omesso da un qualunque insieme di generatori di G; segue quindi che $F \supseteq G'$. Inoltre, si nota che il viceversa vale per i gruppi finiti. □

Teorema E6.6 (Wielandt). *Se il sottogruppo di Frattini di un gruppo finito G contiene il gruppo derivato G', allora G è nilpotente.*

DIMOSTRAZIONE. Sia P un sottogruppo di Sylow di G. Se $N_G(P) = H \neq G$, allora H è contenuto in un sottogruppo massimale M di G. Ricordiamo che $F \supseteq G'$ per ipotesi e $M \supseteq F$ perché F è contenuto in ogni sottogruppo massimale di G. Poiché G/G' è abeliano, M è un sottogruppo normale di G (vedi il Teorema **E2.1**). D'altra parte, essendo $M \supseteq N_G(P)$, M è il suo stesso normalizzante grazie al Lemma **D4.1**. Questo è assurdo e possiamo concludere che dobbiamo avere $N_G(P) = G$. Essendo i sottogruppi di Sylow di G normali, possiamo dedurre che G è il loro prodotto diretto e quindi è nilpotente. □

CAPITOLO F

Teoria Enumerativa di Pólya-Redfield

La Teoria di Pólya-Redfield è stata elaborata nel 1937. Essa, attraverso lo studio del concetto algebrico di azione di un gruppo su un insieme, perviene a notevoli risultati nel campo del calcolo combinatorio. La teoria di Pólya-Redfield è nata da un problema inerente la chimica, ma di natura combinatoria, quale quello di conoscere quanti tipi di molecole (o isomeri di posizione) vi siano aventi una data configurazione degli atomi. Questo problema fa parte di una classe molto più vasta , comprendente i problemi riguardanti il numero di modelli distinti di una collezione di oggetti o il numero dei grafi non etichettati. Rielaborando alcune intuizioni di Redfield, Pólya riuscì a costruire una teoria capace di risolvere i problemi sopra esposti.

Questo capitolo è organizzato come segue:

La prima sezione è dedicata al lemma di Cauchy-Frobenius (Burnside). Questo è un importante strumento per la conoscenza del numero delle orbite di un insieme su cui agisce un gruppo finito. È data anche una versione del teorema per gruppi finiti di tipo ciclico. Infine, si dimostra l'utilità del lemma tramite due esempi: problema di codici e permutazioni circolari.

Nella seconda sezione, viene introdotta l'azione di gruppo di permutazioni sulle applicazioni fra due insiemi finiti. Come preparazione per il teorema di Pólya vengono presentati la funzione peso e l'enumaratore di applicazioni.

La terza sezione tratta il risultato centrale della teoria di Pólya-Redfield. Esso ci consente di conoscere il numero di modelli di collezioni di oggetti, di possibili strutture chimiche, di grafi, ecc.. Per fare questo si introduce il concetto di modello. Si identificano gli oggetti da enumerare con oggetti astratti (ad esempio poligoni). Sull'insieme di questi ultimi agisce un gruppo finito (usualmente di simmetrie). Si considera modello una classe di equivalenza degli oggetti astratti sotto l'azione del gruppo. Infine, si espone il teorema di Pólya, che permette di conoscere il numero dei modelli ciascuno con il suo peso, ossia con il numero di oggetti astratti che costituiscono la classe di equivalenza.

Nella quarta sezione viene esaminato l'indice ciclico di un gruppo finito di permutazioni. Questo ci consente di dare un'espressione più semplice alla formula di Pólya. Sono forniti gli indici ciclici dei più importanti gruppi di permutazioni: gruppo simmetrico, gruppo alterno, gruppo ciclico e gruppo diedrale.

La quinta sezione mostra alcune significative applicazioni della teoria di Pólya-Redfield. Vengono enumerati i modelli di cubi colorati, di scacchiere colorate e di molecole organiche aventi una data configurazione atomica ma differenti per il posizionamento degli atomi nello spazio (isomeri di posizione). Infine, partizioni e composizioni dei numeri naturali vengono studiate tramite la teoria di Pólya-Redfield.

F1. Lemma di Cauchy-Frobenius e classi di coniugio

Definizione F1.1. *Sia G un gruppo finito che agisce su un insieme finito Ω. Definiamo una funzione da G ad $\mathbb{N}_0$ come segue:*

$$\chi(g) \;=\; \Big|\big\{\alpha \in \Omega \,\big|\, \alpha^g = \alpha\big\}\Big|$$

cioè χ associa ad ogni $g \in G$ il numero dei membri di Ω fissati da g.

Lemma F1.2 (Cauchy-Frobenius). *Sia G un gruppo finito che agisce su Ω, un insieme anch'esso finito. Indichiamo con $\mathcal{O}$ l'insieme di tutte le orbite di Ω. Allora il numero delle orbite è dato da*

$$|\mathcal{O}| \;=\; \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

DIMOSTRAZIONE. Per ogni $g \in G$, definiamo il sottoinsieme di Ω come segue

$$\Omega_g := \{\alpha \in \Omega \mid \alpha^g = \alpha\}.$$

Allora per le funzioni χ e λ così definite:

$$\chi: \quad G \longrightarrow \mathbb{N}_0 \quad \text{con} \quad g \longmapsto |\Omega_g|;$$

$$\lambda: \quad G\times\Omega \longrightarrow \{0,1\} \;\; \text{con} \;\; (g,\alpha) \longmapsto \begin{cases} 0, & \text{se } \alpha^g \neq \alpha; \\ 1, & \text{se } \alpha^g = \alpha; \end{cases}$$

manipolando la doppia somma

$$\Lambda \quad := \sum_{(g,\alpha)\in G\times\Omega} \lambda(g,\alpha)$$

si ha che

$$\begin{aligned}\Lambda &= \sum_{\alpha\in\Omega}\sum_{g\in G}\lambda(g,\alpha) = \sum_{\alpha\in\Omega}|G_\alpha| \\ &= \sum_{g\in G}\sum_{\alpha\in\Omega}\lambda(g,\alpha) = \sum_{g\in G}\chi(g).\end{aligned}$$

Quindi

$$\sum_{g\in G}\chi(g) = \sum_{\alpha\in\Omega}|G_\alpha|.$$

Ora

$$\Omega = \biguplus_{\alpha\in C}\alpha^G = \biguplus_{T\in\mathcal{O}} T$$

dove C è un sistema di rappresentanti delle orbite. Allora

$$\begin{aligned}\sum_{g\in G}\chi(g) &= \sum_{\alpha\in\Omega}|G_\alpha| = \sum_{T\in\mathcal{O}}\sum_{\alpha\in T}|G_\alpha| = \sum_{T\in\mathcal{O}}\sum_{\alpha\in T}\frac{|G|}{|\alpha^G|} \\ &= \sum_{T\in\mathcal{O}}\sum_{\alpha\in T}\frac{|G|}{|T|} = \sum_{T\in\mathcal{O}}\frac{|G|}{|T|}\sum_{\alpha\in T}1 = |G|\cdot|\mathcal{O}|.\end{aligned}$$

Quindi

$$|\mathcal{O}| = \frac{1}{|G|}\sum_{g\in G}\chi(g). \qquad \square$$

Il seguente lemma fornisce due proprietà della funzione χ definita nel lemma precedente.

Lemma F1.3. *Sia G un gruppo finito che agisce su un insieme Ω. Allora per due elementi $x, y \in G$, valgono le seguenti affermazioni:*

(a) *se x e y sono coniugati, allora $\chi(x) = \chi(y)$.*
(b) *se x e y generano lo stesso sottogruppo ciclico di G, allora $\chi(x) = \chi(y)$.*

DIMOSTRAZIONE. Definiti i seguenti insiemi:

$$\begin{aligned}\Omega_x &= \{\alpha\in\Omega \mid \alpha^x = \alpha\}, \\ \Omega_y &= \{\alpha\in\Omega \mid \alpha^y = \alpha\};\end{aligned}$$

risulta $|\Omega_x| = \chi(x)$ e $|\Omega_y| = \chi(y)$.

[a] Sia $y = g^{-1}xg$ con $g\in G$ e consideriamo la seguente applicazione

$$\begin{aligned}\phi: \quad \Omega_x &\longrightarrow \Omega_y; \\ \beta &\longmapsto \beta^g.\end{aligned}$$

Non è difficile vedere che ϕ è ben definita. Per ogni $\beta \in \Omega_x$ si ha che $\phi(\beta) = \beta^g \in \Omega_y$ perché

$$(\beta^g)^y = \beta^{gy} = \beta^{xg} = (\beta^x)^g = \beta^g.$$

Se ora consideriamo l'applicazione inversa

$$\begin{aligned} \phi^{-1}: \quad \Omega_y &\longrightarrow \Omega_x; \\ \gamma &\longmapsto \gamma^{g^{-1}}. \end{aligned}$$

Si vede che anche ϕ^{-1} è ben definita. Infatti, per ogni $\gamma \in \Omega_y$ si ha che $\phi^{-1}(\gamma) = \gamma^{g^{-1}} \in \Omega_x$ perché

$$(\gamma^{g^{-1}})^x = \gamma^{yg^{-1}} = (\gamma^y)^{g^{-1}} = \gamma^{g^{-1}}.$$

Quindi c'è una corrispondenza biunivoca fra gli insiemi Ω_x e Ω_y, pertanto essi risultano equipotenti e $\chi(x) = \chi(y)$.

[b] Per definizione

$$\begin{aligned} \langle x \rangle &= \{x^i \mid i \in \mathbb{Z}\}, \\ \langle y \rangle &= \{y^j \mid j \in \mathbb{Z}\}. \end{aligned}$$

Se $\langle x \rangle = \langle y \rangle$ allora $x \in \langle y \rangle$ e $y \in \langle x \rangle$ quindi

$$\exists\, i, j \in \mathbb{Z}: \quad x = y^j \quad \text{e} \quad y = x^i.$$

Consideriamo ora gli insiemi Ω_x e Ω_y definiti precedentemente. Allora

$$\begin{aligned} \forall\, \alpha \in \Omega_x: \quad \alpha^x = \alpha &\implies \alpha^{x^2} = \alpha^x = \alpha \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \\ &\implies \alpha^{x^i} = \alpha^y = \alpha \\ &\implies \alpha \in \Omega_y, \end{aligned}$$

$$\begin{aligned} \forall\, \beta \in \Omega_y: \quad \beta^y = \beta &\implies \beta^{y^2} = \beta^y = \beta \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \\ &\implies \beta^{y^j} = \beta^x = \beta \\ &\implies \beta \in \Omega_x; \end{aligned}$$

pertanto

$$\Omega_x = \Omega_y \implies \chi(x) = \chi(y). \qquad \square$$

Proposizione F1.4. *Sia G un gruppo finito che agisce su un insieme Ω, allora*

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in \mathcal{C}} \chi(g) |\mathrm{Cl}(g)|$$

dove $\mathcal{C}$ è un sistema di rappresentanti per le classi di coniugio e $\mathrm{Cl}(g)$ la classe di coniugio a cui g appartiene.

DIMOSTRAZIONE. La relazione di coniugio, essendo un'equivalenza, definisce una partizione su G, quindi risulta $G = \biguplus_{g \in C} \mathrm{Cl}(g)$. Applicando il Lemma **F1.2**, abbiamo

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} \chi(g) = \frac{1}{|G|} \sum_{g \in C} \sum_{g' \in \mathrm{Cl}(g)} \chi(g').$$

Per il primo punto del Lemma **F1.3**, si ha che $\chi(g') = \chi(g)$ per $g' \in \mathrm{Cl}(g)$. Quindi

$$\sum_{g' \in \mathrm{Cl}(g)} \chi(g') = \chi(g)|\mathrm{Cl}(g)| \quad \text{e} \quad |\mathcal{O}| = \frac{1}{|G|} \sum_{g \in C} \chi(g)|\mathrm{Cl}(g)|. \qquad \square$$

Proposizione F1.5. *Sia G un gruppo ciclico di ordine n generato da g che agisce su un insieme Ω. Allora il numero delle orbite*

$$|\mathcal{O}| = \frac{1}{n} \sum_{d|n} \chi(g^d) \varphi(\frac{n}{d})$$

dove φ è la funzione di Eulero.

DIMOSTRAZIONE. Per il teorema di Lagrange, l'ordine di ogni sottogruppo di G è un divisore dell'ordine di G. Inoltre per il Lemma **F1.3** se due elementi di G generano lo stesso sottogruppo, essi hanno la stessa immagine tramite la χ. Proviamo che, per ogni divisore d di n, esiste un sottogruppo di G il cui ordine è proprio d:

$$\langle g^{\frac{n}{d}} \rangle = \{g^{\frac{n}{d}}, g^{\frac{2n}{d}}, \cdots g^{\frac{(n-1)n}{d}}, g^n = e\} \implies |\langle g^{\frac{n}{d}} \rangle| = d.$$

In verità per ogni divisore di $|G|$ esiste un unico sottogruppo. Infatti, se ora consideriamo $\langle g^d \rangle$, questo è un sottogruppo di ordine n/d, quindi, preso un arbitrario $h \in G$ tale che $o(h) = n/d$, necessariamente $h \in \langle g^d \rangle$ in quanto

$$h \in G \implies \exists\, m \in \mathbb{N}_0 : \; h = g^m \implies h^{\frac{n}{d}} = g^{\frac{mn}{d}} = e.$$

Ne segue che

$$\frac{m}{d} \in \mathbb{Z} \implies d \mid m \implies h = g^m = (g^d)^{\frac{m}{d}} \in \langle g^d \rangle.$$

Possiamo allora suddividere G nei sottoinsiemi degli elementi che generano lo stesso sottogruppo. Dimostriamo che per ogni $d \in \mathbb{N}$, tale che $d \,\big|\, |G|$, il numero di generatori di ogni sottogruppo di G del tipo $\langle g^d \rangle$ è $\varphi(\frac{n}{d})$, dove

$$\langle g^d \rangle = \{g^{dk} \mid k = 1, 2, \cdots, n/d\}$$

e

$$\varphi\Big(\frac{n}{d}\Big) = \Big| \Big\{ 1 \le k \le \frac{n}{d} \;\Big|\; \mathrm{mcd}\Big(k, \frac{n}{d}\Big) = 1 \Big\} \Big|.$$

Se g^{dk} è un altro generatore di questo sottogruppo, allora

$$o(g^{dk}) = \frac{n}{d} \qquad \text{e} \qquad \mathrm{mcd}(k, n/d) = 1.$$

Altrimenti, avremmo da $\mathrm{mcd}(k, n/d) > 1$ la seguente espressione:

$$\frac{n}{d} = o(g^{dk}) = \left|\{g^{dk}, g^{2dk}, \cdots, g^{dk \times \frac{n/d}{\mathrm{mcd}(k,n/d)}}\}\right| \leq \frac{n/d}{\mathrm{mcd}(k, n/d)} < \frac{n}{d}$$

che è impossibile. Quindi il numero dei generatori del sottogruppo $\langle g^d \rangle$ è proprio $\varphi(\frac{n}{d})$. □

Mostriamo l'efficacia del teorema con due esempi.

Esempio F1.6 (Problema dei codici). *Il ministero della difesa deve adottare un codice di tre cifre arabe a scelta tra* $0, 1, 2, \cdots, 9$. *Essendo questo codice scritto su un foglio che non contiene del testo, ci potrebbe essere ambiguità nel leggerlo ruotando di* 180^0 *il foglio* (ovvero leggendo lo stesso codice dal basso o dall'alto). *In altre parole, un codice come* 918 *non può essere distinto da* 816. *Quanti codici distinguibili vi sono?*

Indichiamo con Ω l'insieme di tutti i possibili codici che si possono ricavare utilizzando le tre cifre arabe scelte tra $0, 1, \cdots, 9$. Tale insieme ha cardinalità 10^3. I codici capovolgibili sono costituiti esclusivamente da tre cifre scelte tra $0, 1, 6, 8, 9$. Essi sono esattamente 5^3. Pertanto le parole non capovolgibili, che sono in numero di $10^3 - 5^3$, contengono almeno una cifra scelta tra $3, 4, 5, 7$. Cerchiamo ora il gruppo di permutazione dei codici, che crea l'identificazione di alcuni di essi. Consideriamo la funzione

$$\begin{array}{rcl} g : \Omega & \longrightarrow & \Omega; \\ \alpha & \longmapsto & g(\alpha) := \left\{ \begin{array}{ll} \alpha, & \text{se } \alpha \text{ non è capovolgibile;} \\ \alpha^{-1}, & \text{se } \alpha \text{ è capovolgibile;} \end{array} \right. \end{array}$$

dove con α^{-1} si è indicato il codice α letto capovolgendo il foglio. Quindi g è effettivamente una funzione che trasforma ogni codice capovolgibile nel suo inverso, mentre lascia inalterati i codici non capovolgibili. Inoltre $g^{-1} = g$. Consideriamo il gruppo $G := \{g, \mathrm{Id}_\Omega\}$ e definiamo un'azione di G su Ω nel seguente modo:

$$\begin{array}{rcl} G \times \Omega & \longrightarrow & \Omega : \quad (\mathrm{Id}_\Omega, \alpha) \quad \longmapsto \quad \alpha; \\ (g, \alpha) & \longmapsto & \alpha^g := g(\alpha) = \left\{ \begin{array}{ll} \alpha, & \text{se } \alpha \text{ non è capovolgibile;} \\ \alpha^{-1}, & \text{se } \alpha \text{ è capovolgibile.} \end{array} \right. \end{array}$$

I codici distinti, ovvero che non possono essere confusi, sono tanti quante sono le orbite di Ω sotto l'azione di G. Infatti, dato un codice non capovolgibile, esso non può essere equivalente a nessun altro. Se un codice è capovolgibile, il suo inverso è a lui equivalente. Per conoscere il numero di codici distinti sarà sufficiente applicare il Lemma **F1.2**. Ora l'identità su Ω lascia inalterati tutti i codici, capovolgibili o non capovolgibili che essi siano. Le parole non capovolgibili sono lasciate fisse da g, ovvero $g(\alpha) = \alpha$

con α non capovolgibile. Le parole capovolgibili vengono rovesciate da g e restano invariate, ovvero $\alpha = \alpha^{-1}$ con α capovolgibile, se e solo se sono formate da cinque cifre scelte tra $0, 1, 6, 8, 9$ e hanno la cifra centrale scelta tra $0, 1, 8$, che resta fissa, mentre la prima e la terza cifra simmetriche sono scambiate. Allora le parole capovolgibili che restano invariate sotto l'azione di g sono $3 \cdot 5 = 15$. Pertanto il numero dei codici distinguibili è dato da

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{2}\{10^3 + 10^3 - 5^3 + 15\} = 945.$$

Analogamente, si può stabilire che i codici distinguibili composti da quattro cifre sono in numero 9700.

Esempio F1.7 (Problema della collana). *Per la realizzazione di collane, un artigiano ha a disposizione m perline aventi n colori differenti. Se si ipotizza che due collane aventi colorazione differente appartengano allo stesso modello se una può essere ottenuta dall'altra attraverso una rotazione, quanti modelli di collane può realizzare l'artigiano?*

Denotiamo con $[n] = \{1, 2, \cdots, n\}$ gli n colori distinti delle perline e con $a_1, a_2, \cdots, a_m$ le m perline. L'equivalenza delle collane è determinata dal gruppo di rotazioni della struttura circolare della corda di perline. Esso è di fatto un gruppo di permutazioni di m simboli che agisce sulla posizione delle perline. Possiamo rappresentare una collana come una disposizione di perline di lunghezza m, con eventuale ripetizione. Pertanto, se indichiamo con Ω l'insieme di tutte le collane che si possono creare, si ha che

$$\Omega = \{(a_1, a_2, \cdots, a_m) \mid a_i \in [n]\} \quad \text{con} \quad |\Omega| = n^m.$$

Consideriamo, ora la seguente permutazione dell'insieme $\{1, 2, \cdots, m\}$

$$\pi := (12\cdots m).$$

Il gruppo di rotazioni della struttura circolare della corda di perline è quindi generato da π, ovvero $G = \langle\pi\rangle$. Inoltre G è un gruppo finito in quanto $|G| = o(\pi) = m$. Ora, se $(a_1, a_2, \cdots, a_m)$ con $a_i \in \{1, 2, \cdots, n\}$ è un generico membro di Ω e se π^k è una qualsiasi permutazione di G, definiamo un'azione di G su Ω in questo modo:

$$(a_1, a_2, \cdots, a_m)^{\pi^k} = (a_{1+k}, \cdots, a_m, a_1, \cdots, a_k).$$

Ogni orbita di Ω corrisponde ad un modello di collana. Per conoscere il numero $W(m, n)$ dei modelli, sarà sufficiente applicare la Proposizione **F1.5**, per la quale il numero delle orbite distinte di Ω è dato da

$$W(m, n) = \frac{1}{m}\sum_{d|m}\chi(\pi^d)\varphi(\frac{m}{d})$$

dove $W(m, n)$ indica la cardinalità dell'insieme di tutte le orbite di Ω. Resta da trovare $\chi(\pi^d)$, con $d|m$. Poiché d è un divisore di m allora possiamo quindi dividere la m-upla disposizione $(a_1, a_2, \cdots, a_m)$ in m/d pezzi di lunghezza

d in questo modo:

$$\begin{aligned}(a_1,\cdots,a_m) &= (\,a_1,\cdots,a_d \mid a_{d+1},\cdots,a_{2d} \mid \\ &\quad \cdots \mid a_{m-2d+1},\cdots,a_{m-d} \mid a_{m-d+1},\cdots,a_m\,).\end{aligned}$$

Allora

$$\begin{aligned}(a_1,\cdots,a_m)^{\pi^d} &= (a_{1+d},\cdots,a_{2d} \mid a_{2d+1},\cdots,a_{3d} \mid \\ &\quad \cdots \mid a_{1+m-d},\cdots,a_m \mid a_1,\cdots,a_d\,).\end{aligned}$$

Pertanto π^d lascia fisso l'elemento $(a_1,a_2,\cdots,a_m)$ se e solo se $(a_1,a_2,\cdots,a_m)$ è costituito da m/d pezzi identici di lunghezza d, ovvero

$$(a_1,a_2,\cdots,a_m)=(a_1,a_2,\cdots,a_d \mid \cdots \mid a_1,a_2,\cdots,a_d).$$

Poiché vi sono n^d elementi del tipo $(a_1,a_2,\cdots,a_d)$ con $a_i\in\{1,2,\cdots,n\}$ per $i=1,2,\cdots,d$, allora $\chi(\pi^d)=n^d$ e quindi

$$W(m,n)\;=\;\frac{1}{m}\sum_{d\mid m}\varphi(m/d)n^d. \qquad (\star)$$

Invece, se l'artigiano ha a disposizione $m=\sum_{k=1}^{n}m_k$ perline con m_k perline aventi k-esimo colore, allora il numero delle colonne realizzabili è dato da

$$w(m_1,m_2,\cdots,m_n)\;=\;\frac{1}{m}\sum_{d\mid \mathrm{mcd}(m_1,m_2,\cdots,m_n)}\varphi(d)\binom{\frac{m}{d}}{\frac{m_1}{d},\frac{m_2}{d},\cdots,\frac{m_n}{d}} \qquad (\star\star)$$

che enumera anche il numero delle permutazioni circolari del multinsieme $[1^{m_1},2^{m_2},\cdots,n^{m_n}]$.

DIMOSTRAZIONE. Sia $[1^{m_1},2^{m_2},\cdots,n^{m_n}]$ un multinsieme con $\sum_{k=1}^{n}m_k=m$ e calcoliamo il numero delle sue permutazioni. Il numero di modi di distribuire le prime m_1 perle è dato dal coefficiente binomiale $\binom{m}{m_1}$. Ora procedendo analogamente col secondo insieme m_2 per le posizioni vacanti, si hanno $\binom{m-m_1}{m_2}$ modi, e così via fino all'ultimo colore. Quindi

$$\begin{aligned}&\binom{m}{m_1}\binom{m-m_1}{m_2}\cdots\binom{m-m_1-m_2-\cdots-m_{n-1}}{m_n}\\ &=\frac{m!}{m_1!m_2!\cdots m_n!}=\binom{m}{m_1,m_2,\cdots,m_n}.\end{aligned}$$

Allora il numero delle permutazioni del multinsieme $[1^{m_1},2^{m_2},\cdots,n^{m_n}]$ è dato dal coefficiente multinomiale, pertanto

$$|\Omega|=\binom{m}{m_1,m_2,\cdots,m_n}.$$

Se ora vogliamo le permutazioni circolari, considerando l'azione precedente di G su Ω si ha:

$$|\mathcal{O}| = \frac{1}{|G|}\sum_{d|m}\chi(\pi^{\frac{m}{d}})\varphi(d).$$

Per calcolare $\chi(\pi^{\frac{m}{d}})$, notiamo che

$$\begin{aligned}&\pi^{\frac{m}{d}}(a_1\cdots a_{\frac{m}{d}};\ a_{\frac{m}{d}+1}\cdots a_{2\frac{m}{d}};\cdots;a_{(d-1)\frac{m}{d}+1}\cdots a_m)\\ &= (a_{\frac{m}{d}+1}\ \cdots\ a_{2\frac{m}{d}};a_{2\frac{m}{d}+1}\cdots\ a_{3\frac{m}{d}};\ \cdots;\ a_1\cdots\ a_{\frac{m}{d}}).\end{aligned}$$

Se $\pi^{\frac{m}{d}}$ fissa tale permutazione, ne segue che essa è formata da d blocchi uguali, quindi $d|m$ e $d|m_k$ con $1 \le k \le n$, pertanto il numero di membri fissati da $\pi^{\frac{m}{d}}$ è

$$\chi(\pi^{\frac{m}{d}}) = \binom{\frac{m}{d}}{\frac{m_1}{d}, \frac{m_2}{d}, \cdots, \frac{m_n}{d}}$$

ne segue che

$$w(m_1, m_2, \cdots m_n) = \frac{1}{m}\sum_{d|\mathrm{mcd}(m_1,m_2,\cdots,m_n)}\varphi(d)\binom{\frac{m}{d}}{\frac{m_1}{d}, \frac{m_2}{d}, \cdots, \frac{m_n}{d}}.$$

Dalla somma multipla

$$\sum_{m_1+m_2+\cdots+m_n=m} w(m_1, m_2, \cdots, m_n)$$

$$= \sum_{m_1+m_2+\cdots+m_n=m}\frac{1}{m}\sum_{d|\mathrm{mcd}(m_1,m_2,\cdots,m_n)}\varphi(d)\binom{\frac{m}{d}}{\frac{m_1}{d}, \frac{m_2}{d}, \cdots, \frac{m_n}{d}}$$

si ottiene

$$\frac{1}{m}\sum_{d|m}\varphi(d)\sum_{\substack{m_1+m_2+\cdots+m_n=m\\ d|m_k:\,k=1,2,\cdots,n}}\binom{\frac{m}{d}}{\frac{m_1}{d}, \frac{m_2}{d}, \cdots, \frac{m_n}{d}}.$$

Ora se poniamo $m'_k = \frac{m_k}{d}$ si ha

$$\frac{1}{m}\sum_{d|m}\varphi(d)\sum_{m'_1+m'_2+\cdots+m'_n=\frac{m}{d}}\binom{\frac{m}{d}}{m'_1, m'_2, \cdots, m'_n} = \frac{1}{m}\sum_{d|m}\varphi(d)n^{\frac{m}{d}}$$

dove il teorema multinomiale

$$(x_1 + \cdots + x_n)^m = \sum_{m_1+\cdots+m_n=m}\binom{m}{m_1, \cdots, m_n}x_1^{m_1}\cdots x_n^{m_n}$$

è stato applicato nel caso $x_1 = x_2 = \cdots = x_n = 1$, pertanto

$$\sum_{m_1+m_2+\cdots+m_n=m}\binom{m}{m_1, m_2, \cdots, m_n} = n^m.$$

Così abbiamo dimostrato la seguente identità combinatoria:

$$W(m,n) = \sum_{m_1+m_2+\cdots+m_n=m} w(m_1, m_2, \cdots, m_n). \qquad \square$$

F2. Applicazioni fra due insiemi

In questa sezione il concetto di azione di un gruppo G sarà applicato al caso in cui G è il gruppo di permutazioni di un insieme e Ω l'insieme di alcune applicazioni. Si parlerà, pertanto, di funzioni equivalenti e saranno altresì presentati i concetti di *funzione peso* e di *enumeratore*.

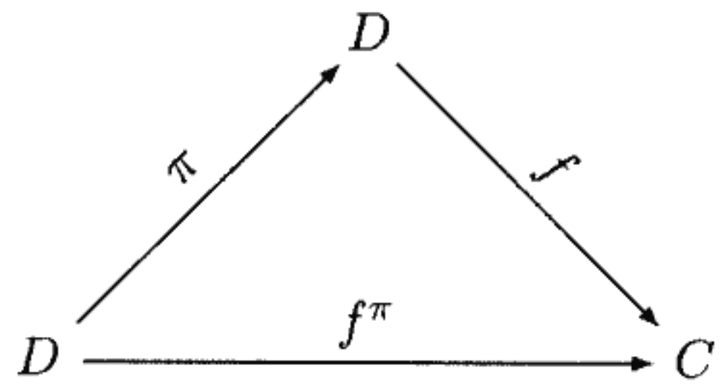
Definizione F2.1 (Azione di un gruppo di permutazioni sulle applicazioni tra due insiemi). *Siano C e D due insiemi e $G \subseteq S_D$ un gruppo di permutazioni di D. L'insieme*

$$\Omega := C^D = \{f : D \to C\}$$

rappresenta tutte le applicazioni da D in C. Se consideriamo la seguente funzione

$$\begin{array}{ccc} G \times \Omega & \longrightarrow & \Omega, \\ (\pi, f) & \longmapsto & f^\pi := f \circ \pi^{-1}; \end{array}$$

possiamo facilmente verificare che essa definisce un'azione del gruppo G di permutazioni sull'insieme delle applicazioni da D a C. Tale azione può essere rappresentata dal seguente diagramma:



Nota F2.2. *In questo caso l'orbita di una qualunque funzione f è*

$$f^G = \{f^\pi \mid \pi \in G\}$$

mentre il suo stabilizzatore risulta in

$$G_f = \{\pi \in G \mid f^\pi = f\}.$$

Nell'insieme Ω definiamo la relazione di Pólya-Redfield al modo seguente:

$$f \sim g \iff \exists \pi \in G \text{ tale che } f \circ \pi = g$$

dove "$\sim$" è un'equivalenza che partiziona l'insieme Ω in classi di equivalenza. Queste sono le orbite di (G, Ω).

Esempio F2.3. *Per colorazione dei lati di un quadrato intendiamo una funzione dall'insieme* $D = \{1, 2, 3, 4\}$ *dei lati del quadrato nell'insieme* $C = \{b, n\}$ *dei colori* (bianco e nero) *disponibili. Così due colorazioni* f *e* g *saranno equivalenti se esisterà* π*, una permutazione dei lati del quadrato, per la quale* $f \circ \pi = g$*. Pertanto il gruppo* G *che agisce sull'insieme* C^D *e che determina l'equivalenza tra le colorazioni è il gruppo delle permutazioni dei lati del quadrato.*

Definizione F2.4 (Funzione peso). *Sia* A *un anello commutativo. Una funzione*

$$\begin{aligned} w : C &\longrightarrow A, \\ c &\longmapsto w(c); \end{aligned}$$

si chiama funzione peso *e se* c *è un elemento di* C*,* $w(c)$ *è il peso di* c*. Solitamente* A *è l'anello dei polinomi in un numero finito di variabili a coefficienti reali. La somma*

$$W(C) = \sum_{c \in C} w(c)$$

è chiamata enumeratore *di* C*. Essa è stata definita per* C*, ma evidentemente può essere estesa ad ogni insieme sul quale sia stata assegnata una funzione peso. Per ogni* $f \in \Omega = C^D$*, definiamo il peso di questa funzione ponendo*

$$w(f) := \prod_{d \in D} w(f(d)).$$

Lemma F2.5. *Funzioni appartenenti alla stessa orbita hanno lo stesso peso:*

$$\forall f_1,\, f_2 \in f^G : \quad w(f_1) = w(f_2).$$

DIMOSTRAZIONE. Dal momento che f_1 ed f_2 appartengono alla stessa orbita, per quanto detto nella Nota ***F2.2*** esse sono equivalenti, ovvero esiste una permutazione π di G per la quale

$$f_1 = f_2 \circ \pi.$$

Allora

$$\begin{aligned} w(f_1) &= \prod_{d \in D} w(f_1(d)) = \prod_{d \in D} w(f_2 \circ \pi(d)) \\ &= \prod_{d \in D} w(f_2(d)) = w(f_2). \end{aligned}$$

Nel penultimo segno di uguaglianza è avvenuta semplicemente una permutazione degli elementi di D tramite π e nel prodotto sono stati riordinati i fattori. □

Definizione F2.6 (Peso di un'orbita). *Il lemma precedente consente di definire il peso di un'orbita dell'insieme $\Omega = C^D$ sotto l'azione del gruppo $G \subseteq S_D$, come il peso di un suo rappresentante, ponendo*

$$w(f^G) := w(g) \quad \textit{per qualunque} \quad g \in f^G.$$

F3. Teorema di Pólya

In questa sezione sarà ampiamente illustrato il teorema di Pólya. Esso fornisce un metodo alquanto comodo e veloce, capace di stabilire non solo il numero delle orbite dell'insieme Ω (sotto l'azione di G), ma anche il peso di ciascuna di esse.

Nota F3.1. *Consideriamo l'enumeratore*

$$W(\Omega) := \sum_{f \in \Omega} w(f).$$

Dal momento che abbiamo supposto D e C insiemi finiti, possiamo ipotizzare $D = \{d_1, d_2, \cdots, d_n\}$ e $C = \{c_1, c_2, \cdots, c_m\}$ per $m, n \in \mathbb{N}$. Siano w la funzione peso su C a valori nell'anello commutativo A e $x_i = w(c_i) \in A$ per $i = 1, 2, \cdots, m$. Poiché

$$\forall f \in C^D : \quad w(f) = \prod_{j=1}^{n} w(f(d_j))$$

allora $w(f)$ sarà un monomio della forma $x_1^{j_1} x_2^{j_2} \cdots x_m^{j_m}$ con $j_i \in \{0, \cdots, n\}$. Quindi l'enumeratore $W(\Omega)$ risulta essere un polinomio nelle indeterminate $x_1, x_2, \cdots, x_m$ nel quale il coefficiente di ciascun monomio indica il numero delle funzioni di Ω aventi peso pari a quel monomio.

Lemma F3.2. *Siano C e D due insiemi finiti e w una funzione peso definita in C a valori in un anello commutativo. L'enumeratore dell'insieme delle applicazioni $\Omega = C^D$ è dato da*

$$W(\Omega) = W^{|D|}(C).$$

DIMOSTRAZIONE. Gli insiemi C e D sono, per ipotesi, finiti. Poniamo $m := |C|$ ed $n := |D|$, allora $C = \{c_1, \cdots, c_m\}$ e $D = \{d_1, \cdots, d_n\}$. Ora

$$\begin{aligned} W(C)^{|D|} &= \Big\{ \sum_{c \in C} w(c) \Big\}^{|D|} = \Big\{ \sum_{k=1}^{m} w(c_k) \Big\}^{n} \\ &= \sum_{\substack{n_1 + n_2 + \cdots + n_m = n \\ n_1, n_2, \cdots, n_m \geq 0}} \binom{n}{n_1, n_2, \cdots, n_m} \prod_{k=1}^{m} w^{n_k}(c_k). \end{aligned}$$

Sia $X_k := \{f^{-1}(c_k)\}$ con $k = 1, 2, \cdots, m$. Osserviamo che

$$D = \biguplus_{k=1}^{m} X_k \quad \text{e} \quad w(f) = \prod_{k=1}^{m} w(c_k)^{|X_k|}.$$

Allora per $n_k := |X_k|$ con $n = n_1 + n_2 + \cdots + n_m$, si ha che

$$w(f) = \prod_{k=1}^{m} w(c_k)^{|X_k|} = \prod_{k=1}^{m} w(c_k)^{n_k}.$$

Considerando tutte le funzioni che inducono la stessa partizione su D si ha:

$$W(\Omega) = \sum_{\substack{n_1+n_2+\cdots+n_m=n \\ n_1,n_2,\cdots,n_m \geq 0}} \binom{n}{n_1, n_2, \cdots, n_m} \prod_{k=1}^{m} w^{n_k}(c_k). \qquad \square$$

Lemma F3.3. *Dati due insiemi finiti C e D con $C = m$ e $D = n$, sia $D = \biguplus_{k=1}^{\ell} X_k$ una partizione di D con $n_k := |X_k|$ per $k = 1, 2, \cdots, \ell$. Consideriamo l'insieme delle funzioni*

$$\Lambda := \left\{ f \in C^D \;\middle|\; |f(X_k)| = 1 \right\}$$

che sono costanti negli X_k per $k = 1, 2, \cdots, \ell$. Allora il suo enumeratore è

$$W(\Lambda) = \prod_{i=1}^{\ell} \sum_{c \in C} w^{n_k}(c) \quad con \quad n = \sum_{k=1}^{\ell} n_k$$

dove w è la funzione peso definita su C.

DIMOSTRAZIONE. Sia f una funzione in Λ e consideriamone il peso

$$w(f) = \prod_{d \in D} w(f(d)) = \prod_{k=1}^{\ell} \prod_{d \in X_k} w(f(d)) = \prod_{k=1}^{\ell} w^{|X_k|}(f(x_k))$$

dove con x_k si indica un rappresentante dell'insieme X_k per $k = 1, 2, \cdots, \ell$. Supponendo $C = \{c_1, c_2, \cdots, c_m\}$ e per ogni $k \in \{1, 2, \cdots, \ell\}$ considerando $c_{i_k} := f(x_k)$ con $i_k \in \{1, 2, \cdots, m\}$, l'equazione diventa:

$$w(f) = \prod_{k=1}^{\ell} w^{n_k}(c_{i_k}).$$

Considerando tutte le possibili immagini in C per ogni blocco X_k, possiamo calcolare l'enumeratore dell'insieme Λ come segue:

$$\begin{aligned} W(\Lambda) &= \sum_{f \in \Lambda} w(f) = \sum_{f \in \Lambda} \prod_{k=1}^{\ell} w^{|X_k|}(f(x_k)) \\ &= \sum_{\substack{1 \leq i_k \leq m \\ 1 \leq k \leq \ell}} \prod_{k=1}^{\ell} w^{n_k}(c_{i_k}) = \prod_{k=1}^{\ell} \sum_{c \in C} w^{n_k}(c). \end{aligned} \qquad \square$$

Per illustrare questo lemma consideriamo il seguente esempio.

Esempio F3.4. *Sia* $D = \{a, b, c, d, e, f, g\}$ *un insieme costituito da sette persone che vogliono visitare le tre città* c_1, c_2, c_3. *Supponiamo che le persone* a, b, c *siano della stessa famiglia,* d *ed* e *siano una coppia di sposi,* f *e* g *altre persone che viaggiano da sole. Poniamo*

$$X_1 = \{a,\ b,\ c\}, \quad X_2 = \{d, e\}, \quad X_3 = \{f\}, \quad X_4 = \{g\};$$

$$C = \{c_1, c_2, c_3\}, \quad x := w(c_1), \quad y := w(c_2), \quad z := w(c_3).$$

In questo caso il codominio della funzione peso è l'anello dei polinomi a coefficienti reali nelle indeterminate x, y *e* z. *Allora l'enumeratore risulta* $W(C) = x + y + z$ *e* Λ *è l'insieme dei viaggi che possono fare le sette persone nelle tre città, con la ovvia condizione che i membri della stessa famiglia debbano andare nella stessa città. Ad esempio, la funzione*

$$\psi = \begin{pmatrix} a & b & c & d & e & f & g \\ c_1 & c_1 & c_1 & c_3 & c_3 & c_2 & c_1 \end{pmatrix}$$

indica che la famiglia X_1 *ed il signor* g *vanno nella città* c_1, *la famiglia* X_2 *va nella città* c_3 *ed il signor* f *va nella città* c_2. *La funzione* ψ *ha peso*

$$w(\psi) = \prod_{d \in D} w(\psi(d)) = x^4 y z^2$$

e l'enumeratore dei viaggi, per il lemma precedente, è dato da

$$W(\Lambda) = \prod_{k=1}^{4} \sum_{c \in C} w^{|X_k|}(c) = (x^3 + y^3 + z^3)(x^2 + y^2 + z^2)(x + y + z)^2.$$

Sia D un insieme finito con $n := |D|$ e consideriamo il gruppo simmetrico S_D. Ogni elemento $\pi \in S_D$ può essere decomposto nel prodotto di cicli disgiunti e tale decomposizione è unica. Indicheremo la struttura ciclica della permutazione π con $[1^{m_1(\pi)} 2^{m_2(\pi)} \cdots n^{m_n(\pi)}]$ in cui m_k indica il numero dei cicli di lunghezza k, chiamati anche k-cicli per $k = 1, 2, \cdots, n$.

Teorema F3.5 (Pólya, 1937). *Siano* C *e* D *due insiemi finiti con* $n := |D|$ *e* $G \subseteq S_D$ *un gruppo di permutazioni dell'insieme* D *che agisce su* $\Omega := C^D$. *Allora l'enumeratore di* $\mathcal{O}$, *l'insieme delle orbite determinate da* (G, Ω), *è*

$$W(\mathcal{O}) = \frac{1}{|G|} \sum_{\pi \in G} \prod_{k=1}^{n} \Big\{ \sum_{c \in C} w^k(c) \Big\}^{m_k(\pi)}$$

dove $[1^{m_1(\pi)} 2^{m_2(\pi)} \cdots n^{m_n(\pi)}]$ *è la struttura ciclica della permutazione* π *nel gruppo* G. *Il coefficiente del monomio*

$$\prod_{c \in C} w^{n_c}(c) \quad con \quad \sum_{c \in C} n_c = n$$

nel polinomio $W(\mathcal{O})$ *fornisce il numero delle orbite aventi il peso uguale a questo monomio.*

DIMOSTRAZIONE. Siano $|C| = m$ e $|D| = n$ con $D = \{1, 2, \cdots, n\}$ per semplicità. Allora $\Omega = C^D$.

- **Classificazione:** Consideriamo la funzione peso

$$\begin{aligned} w : \Omega &\longrightarrow A, \\ f &\longmapsto w(f); \end{aligned}$$

con $\Omega := C^D$ ed A anello commutativo. Poiché Ω è un insieme finito, diverso dall'insieme vuoto, allora il codominio della funzione peso

$$\mathcal{P} := \Big\{ w(\beta) \mid \beta \in \mathcal{O} \Big\} = \bigcup_{f \in \Omega} \{w(f)\}$$

è anch'esso un insieme finito e diverso dall'insieme vuoto. Per ogni peso $\omega \in \mathcal{P}$, considerando

$$\Omega_\omega := \{ f \in \Omega \mid w(f) = \omega \} \quad \Longrightarrow \quad \Omega = \biguplus_{\omega} \Omega_\omega$$

possiamo allora classificare le orbite di Ω sotto l'azione di G secondo la funzione peso. Indicando con $\mathcal{O}_\omega$ l'insieme di tutte le orbite costituite da funzioni aventi peso ω, allora si ha che

$$\Omega_\omega = \Big\{ f \in \Omega \mid w(f) = \omega \Big\} \quad \Longrightarrow \quad \mathcal{O} = \biguplus_{\omega} \mathcal{O}_\omega.$$

- **Lemma di Cauchy-Frobenius (Burnside):** Sulla base dell'azione del gruppo G su Ω, è facile verificare che induce un'azione di G anche su Ω_ω. Applicando il lemma **F1.2** a (G, Ω_ω), si ha che

$$|\mathcal{O}_\omega| = \frac{1}{|G|} \sum_{\pi \in G} \chi(\pi | \Omega_\omega)$$

dove con $\chi(\pi|\Omega_\omega)$ si denota il numero delle funzioni in Ω_ω fissate da π. Allora possiamo calcolare l'enumeratore delle orbite come segue:

$$\begin{aligned} W(\mathcal{O}) &= \sum_{\omega \in \mathcal{P}} w(\mathcal{O}_\omega) = \sum_{\omega \in \mathcal{P}} \omega \cdot |\mathcal{O}_\omega| \\ &= \sum_{\omega \in \mathcal{P}} \frac{\omega}{|G|} \sum_{\pi \in G} \chi(\pi | \Omega_\omega) \\ &= \frac{1}{|G|} \sum_{\pi \in G} \sum_{\omega \in \mathcal{P}} \omega \cdot \chi(\pi | \Omega_\omega). \end{aligned}$$

- **Classe di Ω fissata da $\pi \in G$:** Se, per ogni $\pi \in G$, poniamo

$$\Lambda(\pi) = \Big\{ f \in \Omega \mid f^\pi = f \Big\}$$

allora il suo enumeratore è uguale alla somma interna appena mostrata:

$$W(\Lambda(\pi)) = \sum_{f \in \Omega:\, f^\pi = f} w(f) = \sum_{\omega \in \mathcal{P}} \omega \cdot \chi(\pi \mid \Omega_\omega).$$

- **Struttura ciclica di $\pi \in G$:** Se la struttura ciclica di π è

$$[\pi] := [1^{m_1(\pi)} 2^{m_2(\pi)} \cdots n^{m_n(\pi)}] \quad \text{con} \quad \sum_{k=1}^{n} k\, m_k(\pi) = n$$

allora, dalla decomposizione ciclica di π, deriviamo la seguente partizione dell'insieme D:

$$\begin{aligned} \pi &= \prod_{k=1}^{n} \prod_{j=1}^{m_k} \big({}_1x_{kj}\, {}_2x_{kj} \cdots {}_kx_{kj} \big); \\ D &= \biguplus_{k=1}^{n} \biguplus_{j=1}^{m_k} X_{kj}, \quad \text{dove} \quad X_{kj} = \Big\{ {}_ix_{kj} \mid 1 \le i \le k \Big\}. \end{aligned}$$

Dunque, $f \in \Lambda(\pi)$ se e solo se f è costante su ciascun X_{kj}.

- **Enumeratore della classe $\Lambda(\pi)$:** Dato che $\Lambda(\pi) \subseteq \Omega$ è un sottoinsieme delle funzioni costanti negli X_{kj}, possiamo ricavare il suo enumeratore tramite la formula mostrata nel Lemma **F3.3**:

$$W(\Lambda(\pi)) = \prod_{k=1}^{n} \prod_{j=1}^{m_k} \sum_{c \in C} w^k(c) = \prod_{k=1}^{n} \Big\{ \sum_{c \in C} w^k(c) \Big\}^{m_k(\pi)}.$$

Ricapitolando abbiamo stabilito la seguente:

$$W(\mathcal{O}) = \frac{1}{|G|} \sum_{\pi \in G} \prod_{k=1}^{n} \Big\{ \sum_{c \in C} w^k(c) \Big\}^{m_k(\pi)}$$

così la dimostrazione del teorema è conclusa. □

Il teorema dimostrato è dovuto a Pólya, il quale nel 1937 risolse il problema di contare le strutture algebriche e combinatorie sotto l'azione di gruppi di permutazioni, detti gruppi di simmetria.

F4. Indice ciclico di gruppo finito

In questa sezione esamineremo l'indice ciclico di un gruppo finito di permutazioni che ci consentirà di dare un'espressione più semplice alla formula di Pólya. Il concetto di indice ciclico venne introdotto da Redfield nel 1927, ma esso rimase pressocché sconosciuto fino al 1937 quando Pólya ne diede la definizione seguente e ne fece un uso sistematico come strumento centrale nella sua teoria di conteggio.

Definizione F4.1 (Indice ciclico). *Siano G un gruppo finito di permutazioni su un insieme finito D avente cardinalità n e $x_1, x_2, \cdots, x_n$ delle indeterminate. Se $\pi \in G$ e $[1^{m_1(\pi)} 2^{m_2(\pi)} \cdots n^{m_n(\pi)}]$ ne è la struttura*

ciclica, assoceremo a π *il seguente monomio* $x_1^{m_1(\pi)} x_2^{m_2(\pi)} \cdots x_n^{m_n(\pi)}$. *Allora il polinomio formale:*

$$\mathcal{Z}(G|x_1, x_2, \cdots, x_n) := \frac{1}{|G|} \sum_{\pi \in G} \prod_{k=1}^{n} x_k^{m_k(\pi)}$$

nelle variabili x_k *con* $k = 1, 2, \cdots, n$, *indicato anche con* $\mathcal{Z}_n(G)$ *per semplicità, è chiamato* l'indice ciclico di G.

Se C e D sono due insiemi finiti e G è un gruppo di permutazioni dell'insieme D, allora dall'indice ciclico di G si ottiene l'enumeratore delle orbite di C^D sotto l'azione di G, sostituendo x_k con $p_k[W(C)]$, dove

$$p_k[W(C)] \quad = \quad \sum_{c \in C} w^k(c) \quad \text{per} \quad k = 1, 2, \cdots, n.$$

Pertanto possiamo riformulare il teorema di Pólya come segue.

Teorema F4.2. *L'enumeratore* $W(\mathcal{O})$ *delle orbite di* C^D *sotto l'azione di* G *è dato da:*

$$W(\mathcal{O}) \;=\; \mathcal{Z}\big(G|\, p_1[W(C)], p_2[W(C)], \cdots, p_n[W(C)]\big). \qquad \square$$

Nota F4.3. *Se poniamo* $w(c) := 1$ *per ogni* $c \in C$, *si ha*

$$p_k[W(C)] = |C| = m \quad \textit{con} \quad k = 1, 2, \cdots, n.$$

La somma dei coefficienti dell'enumeratore è ovviamente il numero delle orbite e quindi

$$|\mathcal{O}| = \mathcal{Z}(G|m, m, \cdots, m).$$

Esempio F4.4. *Calcoliamo l'indice ciclico di alcuni semplici gruppi di permutazioni:*

$$[A] \qquad \mathcal{Z}(I_n|x_1, x_2, \cdots, x_n) = x_1^n,$$

$$[B] \qquad \mathcal{Z}(S_2|x_1, x_2) = \frac{1}{2}(x_1^2 + x_2),$$

$$[C] \qquad \mathcal{Z}(S_3|x_1, x_2, x_3) = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3).$$

Ricerchiamo ora gli indici ciclici di alcuni gruppi più noti di permutazioni.

F4.1. Gruppo simmetrico S_n.

Lemma F4.5 (Formula di Cauchy). *Consideriamo il gruppo simmetrico* S_n *ed* n *numeri naturali* $m_1, m_2, \cdots, m_n \in \mathbb{N}$ *tali che* $m_1 + 2m_2 + \cdots + nm_n = n$. *Allora le permutazioni di* S_n *aventi struttura ciclica* $[1^{m_1} 2^{m_2} \cdots n^{m_n}]$ *sono in numero di*

$$\frac{n!}{\prod_{k=1}^{n} m_k! k^{m_k}} = \frac{n!}{1^{m_1} 2^{m_2} \cdots n^{m_n} \times m_1! m_2! \cdots m_n!}.$$

DIMOSTRAZIONE. Tutte le permutazioni di S_n aventi la struttura ciclica richiesta si possono scrivere nella forma seguente:

$$\prod_{k=1}^{n}\prod_{i=1}^{m_k} \mathcal{C}_{ki}$$

dove $\mathcal{C}_{ki}$, è il i-esimo ciclo di lunghezza k che compare nella decomposizione ciclica delle suddette permutazioni. Poiché ciascun ciclo $\mathcal{C}_{ki}$ contiene k-elementi distinti scelti tra $\{1, 2, \cdots, n\}$, abbiamo $n!$ modi di scegliere gli elementi di tutti i cicli. Tuttavia le permutazioni che ne risultano non sono tutte distinte perché gli m_k cicli $\{\mathcal{C}_{ki}\}$ di lunghezza k possono essere tra loro permutati senza cambiare la permutazione e ciò si può fare in $m_k!$ modi. Per di più, poiché il numero iniziale in ciascun ciclo di lunghezza k si può scegliere in k modi, ogni ciclo di lunghezza k può essere scritto in k differenti modi senza cambiare la permutazione. Ciò si può fare in k^{m_k} modi diversi e quindi, dividendo $n!$ per $m_k!k^{m_k}$ con $k \in [n]$, otteniamo il numero di permutazioni di S_n aventi la struttura ciclica $[1^{m_1}2^{m_2}\cdots n^{m_n}]$. □

Classificando ora tutte le permutazioni di S_n secondo le strutture cicliche, si stabilisce subito l'indice del gruppo simmetrico come segue:

Teorema F4.6. *L'indice ciclico del gruppo simmetrico S_n è*

$$\mathcal{Z}(S_n) = \sum_{\substack{m_1,m_2,\cdots,m_n\geq 0\\ m_1+2m_2+\cdots+nm_n=n}} \prod_{k=1}^{n} \frac{x_k^{m_k}}{m_k!k^{m_k}}.$$

F4.2. Gruppo alterno A_n. Ricordando che una permutazione ciclica di lunghezza k è pari se e solo se k è dispari, si deduce che una permutazione di S_n con la struttura ciclica $[1^{m_1}2^{m_2}\cdots n^{m_n}]$, risulta pari se e solo se il numero $\sigma(m)$ è pari, dove

$$\sigma(m) \quad = \sum_{1\leq k\leq n/2} m_{2k}.$$

Adesso osserviamo la somma

$$\begin{aligned}\mathcal{Z}\big(S_n|x_1,x_2,\cdots,x_n\big) \quad &+ \quad \mathcal{Z}\big(S_n|x_1,-x_2,\cdots,(-1)^{n-1}x_n\big)\\ &= \sum_{\substack{m_1,m_2,\cdots,m_n\geq 0\\ m_1+2m_2+\cdots+nm_n=n}} \{1+(-1)^{\sigma(m)}\}\prod_{k=1}^{n}\frac{x_k^{m_k}}{k^{m_k}m_k!}.\end{aligned}$$

Quando $\sigma(m)$ è dispari, il fattore $\{1 + (-1)^{\sigma(m)}\}$ nella somma annulla il termine corrispondente; altrimenti, il fattore diventa 2. Questo risulta dal fatto che il gruppo alterno A_n è composto dalle permutazioni pari di S_n e

l'inverso dell'ordine soddisfa l'uguaglianza $1/|A_n| = 2/|S_n|$. In conclusione, abbiamo stabilito il seguente teorema.

Teorema F4.7. *L'indice ciclico del gruppo alterno A_n è*

$$\mathcal{Z}(A_n) = \sum_{\substack{m_1,m_2,\cdots,m_n\geq 0 \\ m_1+2m_2+\cdots+nm_n=n}} \{1+(-1)^{\sigma(m)}\} \prod_{k=1}^{n} \frac{x_k^{m_k}}{k^{m_k} m_k!}.$$

F4.3. Gruppo ciclico C_n.

Teorema F4.8. *Detto C_n il gruppo ciclico generato da $(12\cdots n)$ si ha*

$$\mathcal{Z}(C_n) = \frac{1}{n}\sum_{d|n} \varphi(d) x_d^{n/d}$$

dove con φ si è indicata la funzione di Eulero.

DIMOSTRAZIONE. Consideriamo per ipotesi il gruppo $C_n = \langle \pi \rangle$, dove $\pi = (12\cdots n)$ e l'ordine $o(\pi) = n$. Ragionando in modo analogo a quanto fatto per la Proposizione **F1.5**, ripartiamo C_n in classi di equivalenza costituite dai generatori di uno stesso sottogruppo. Per ogni $d|n$ con $n \in \mathbb{N}$, il numero dei generatori del sottogruppo di ordine d è $\varphi(d)$ con ciascun generatore avente la struttura ciclica $[d^{n/d}]$ associato al monomio $x_d^{n/d}$. Quindi l'indice del gruppo ciclico C_n è dato da

$$\mathcal{Z}(C_n) = \frac{1}{|C_n|}\sum_{\sigma\in C_n} x_1^{m_1(\sigma)} x_2^{m_2(\sigma)} \cdots x_n^{m_n(\sigma)} = \frac{1}{n}\sum_{d|n} \varphi(d) x_d^{n/d}. \qquad \square$$

F4.4. Gruppo diedrale D_n. Tutte le simmetrie del poligono regolare di n vertici costituiscono un gruppo D_n, chiamato *gruppo diedrale*. Si evidenzia che D_n ha ordine $2n$ composto da n rotazioni e n riflessioni risulta essere un sottogruppo di S_n.

Teorema F4.9. *L'indice ciclico del gruppo diedrale D_n, con $n > 2$, è:*

$$\mathcal{Z}(D_n) = \begin{cases} \frac{1}{2}\mathcal{Z}(C_n) + \frac{1}{4}\{x_2^{n/2} + x_1^2 x_2^{(n-2)/2}\}, & \text{se } n \text{ è pari;} \\ \frac{1}{2}\mathcal{Z}(C_n) + \frac{1}{2}x_1 x_2^{(n-1)/2}, & \text{se } n \text{ è dispari.} \end{cases}$$

DIMOSTRAZIONE. Quando n è dispari, non è difficile verificare che

$$\begin{aligned} D_n &= \langle \pi, \eta \rangle = \{\pi^k, \pi^k\eta \mid k = 1, 2, \cdots, n\} \\ &= C_n \biguplus \{\pi^k\eta \mid k = 1, 2, \cdots, n\} \end{aligned}$$

dove π e η sono rispettivamente una rotazione $\pi = (1, 2, \cdots, n)$ ed una riflessione $\eta = (n)(1, n-1)(2, n-2)\cdots(\frac{n-1}{2}, \frac{n+1}{2})$. Allora l'indice ciclico

segue dal fatto che tutte le riflessioni $\pi^k\eta$ hanno la stessa struttura ciclica $[1^1 \times 2^{(n-1)/2}]$ per $k = 1, 2, \cdots, n$.

Invece, quando n è pari, abbiamo che

$$\begin{aligned} D_n &= \langle \pi, \sigma, \tau \rangle = \left\{ \pi^k, \pi^\ell\sigma, \pi^\ell\tau \;\middle|\; \begin{smallmatrix} k=1,2,\cdots,n \\ \ell=1,2,\cdots,n/2 \end{smallmatrix} \right\} \\ &= C_n \biguplus \{\pi^\ell\sigma, \pi^\ell\tau \mid \ell = 1, 2, \cdots, n/2\} \end{aligned}$$

dove σ e τ sono rispettivamente due riflessioni date da

$$\begin{aligned} \sigma &= (1,n)(2,n-1)(3,n-2)\cdots(\tfrac{n}{2}, \tfrac{n+2}{2}); \\ \tau &= (n)(\tfrac{n}{2})(1,n-1)(2,n-2)(3,n-3)\cdots(\tfrac{n-2}{2}, \tfrac{n+2}{2}). \end{aligned}$$

È facile vedere che per $\ell = 1, 2, \cdots, n/2$, le riflessioni $\pi^\ell\sigma$ e $\pi^\ell\tau$ hanno le strutture cicliche $[2^{n/2}]$ e $[1^2 \times 2^{(n-2)/2}]$ rispettivamente. Questo conferma l'indice del gruppo D_n evidenziato dal teorema. □

F5. Applicazioni

Il gruppo delle simmetrie viene frequentemente utilizzato nella teoria dell'enumerazione. Mostreremo in questa sezione alcune significative applicazioni della Teoria di Pólya-Redfield.

F5.1. Simmetrie di poligono regolare. Dato un poligono regolare avente n vertici, vogliamo colorare tutti gli n lati con gli m colori. Se consideriamo appartenenti allo stesso modello due poligoni aventi colorazioni distinte ma coincidenti in seguito a rotazioni e/o a riflessioni, quanti modelli dei poligoni si ottengono?

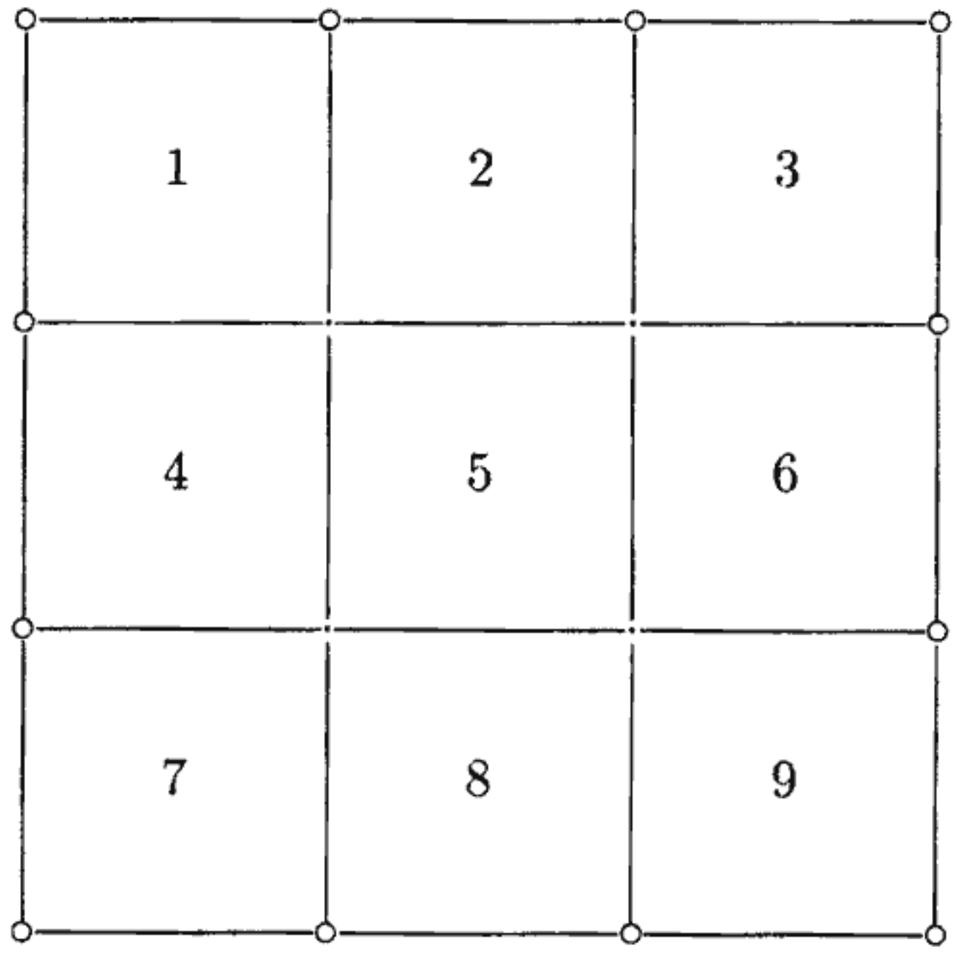
In questo caso, consideriamo gli n lati del poligono come dominio $D = \{1, 2, \cdots, n\}$ e gli m colori come codominio $C = \{1, 2, \cdots, m\}$. Allora tutte le colorazioni sono le applicazioni $\Omega = C^D$. Il numero delle colorazioni non equivalenti sotto rotazioni e riflessioni è quello delle orbite di Ω sotto l'azione del gruppo diedrale D_n. Ricordando l'indice del gruppo diedrale

$$\mathcal{Z}(D_n) = \begin{cases} \frac{1}{2}\mathcal{Z}(C_n) + \frac{1}{2}x_1x_2^{(n-1)/2}, & n - \text{dispari}; \\ \frac{1}{2}\mathcal{Z}(C_n) + \frac{1}{4}\left\{x_2^{n/2} + x_1^2x_2^{(n-2)/2}\right\}, & n - \text{pari}; \end{cases}$$

e poi applicando il teorema di Pólya, otteniamo il numero delle colorazioni non equivalenti del poligono come segue:

$$|\mathcal{O}| = \mathcal{Z}(D_n|m, m, \cdots, m) = \frac{1}{2n}\sum_{d|n}\varphi(d)m^{n/d} + \begin{cases} \frac{1}{2}m^{(n+1)/2}, & n - \text{dispari}; \\ \frac{1+m}{4}m^{n/2}, & n - \text{pari}. \end{cases}$$

F5.2. Colorazione di una scacchiera. Consideriamo una scacchiera di dimensione 3×3 come in figura:



Siano dati tre colori, bianco, nero e verde. In quanti modi si possono colorare *le nove caselle della scacchiera con tre colori? Inoltre, in quanti modi si* possono colorare le caselle della scacchiera sapendo che due sono bianche, tre nere e quattro verdi?

Sia $D = \{1, 2, \cdots, 9\}$ l'insieme delle nove caselle e $C = \{bianco, nero, verve\}$. Definiamo la funzione peso con

$$w(bianco) = b, \quad w(nero) = n, \quad w(verde) = v.$$

Il gruppo G di permutazioni di nove caselle è composto da otto simmetrie (una identica, tre rotazioni e quattro riflessioni). È facile stabilire le strutture cicliche delle permutazioni come segue:

e	a_1	a_2	a_3	b_1	b_2	c_1	c_2
x_1^9	$x_1x_4^2$	$x_1x_2^4$	$x_1x_4^2$	$x_1^3x_2^3$	$x_1^3x_2^3$	$x_1^3x_2^3$	$x_1^3x_2^3$

L'indice ciclico del gruppo G è

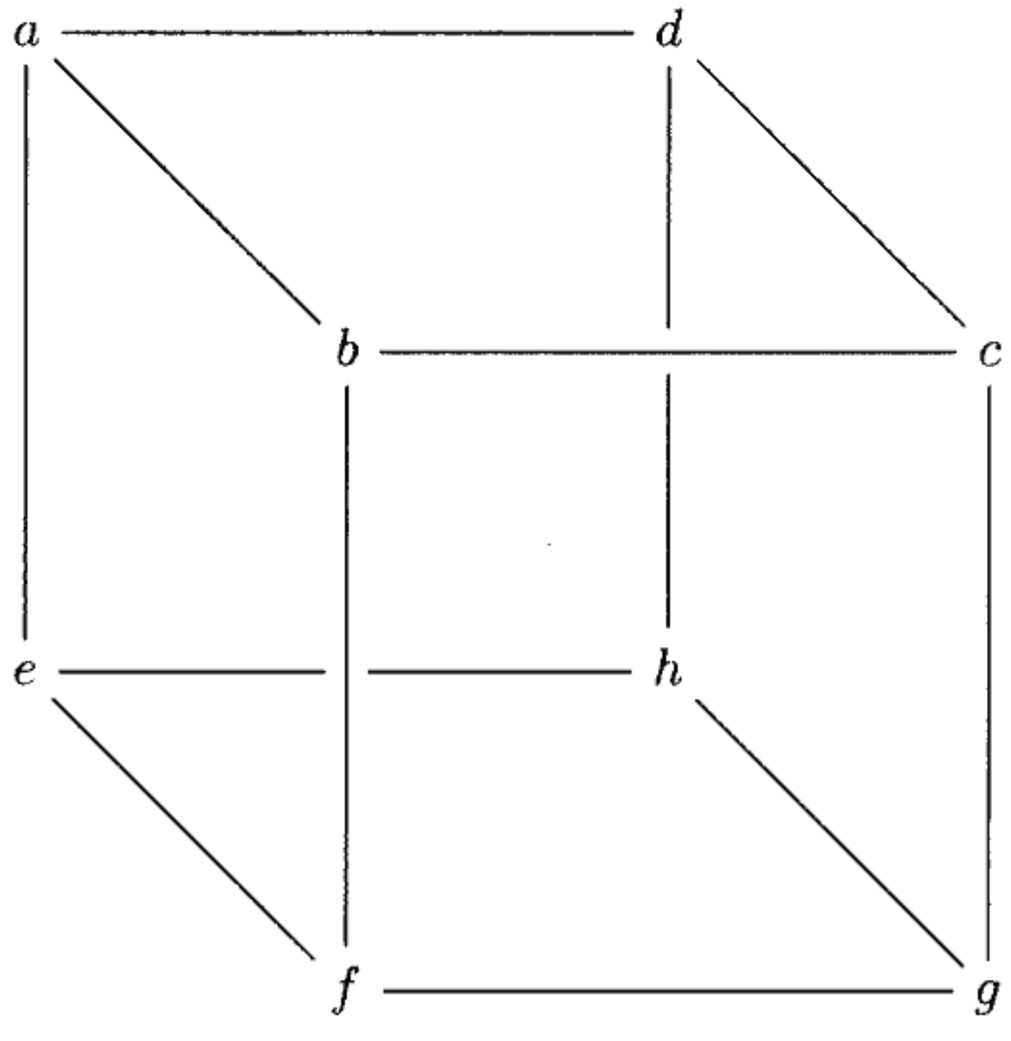
$$\mathcal{Z}(G \mid x_1, x_2, x_4) = \frac{1}{8}\Big\{x_1^9 + x_1x_2^4 + 2x_1x_4^2 + 4x_1^3x_2^3\Big\}.$$

L'enumeratore delle colorazioni è uguale al polinomio

$$\begin{aligned}\mathcal{Z}(G \mid p_1, p_2, p_4) \;=\; &(b+n+v)^9 + (b+n+v)(b^2+n^2+v^2)^4 \\ &+2(b+n+v)(b^4+n^4+v^4)^2 + 4(b+n+v)^3(b^2+n^2+v^2)^3.\end{aligned}$$

Ponendo $b = n = v = 1$, otteniamo il numero totale delle colorazioni [$2862 = 2 \times 3^3 \times 53$]. Invece, le colorazioni con $[b^2n^3v^4]$ sono in numero 174.

F5.3. Colorazione di un cubo. Supponiamo di voler colorare le facce di un cubo con i colori *bianco* e *nero.* Quanti modelli di cubi colorati otteniamo?



Indichiamo con $D = \{1, 2, 3, 4, 5, 6\}$ l'insieme delle 6 facce del cubo e con $C = \{bianco, nero\}$ l'insieme dei due colori disponibili per la colorazione del cubo. I modi di colorare il cubo sono in tutto $|C^D| = 64$. Ciascuna colorazione corrisponde ad una funzione $f \in C^D$ e due colorazioni sono equivalenti se esiste una opportuna permutazione dell'insieme D che porti l'una nell'altra.

Due cubi colorati appartengono allo stesso modello se, ruotando opportunamente uno di essi, questi coincidono. Di conseguenza, il gruppo delle

rotazioni del cubo, agendo sull'insieme dei cubi colorati, determina una equivalenza tra quest'ultimi e i modelli di cubi colorati altro non sono che le orbite di quest'azione.

Osserviamo, ora, che ciascuna rotazione del cubo individua una particolare permutazione delle facce. Precisamente esiste un monomorfismo tra il gruppo G delle rotazioni del cubo ed il gruppo S_6 delle permutazioni delle facce del cubo. Allora l'equivalenza tra cubi colorati, prodotta dal gruppo delle rotazioni, induce un'equivalenza tra le colorazioni attraverso il gruppo G. Pertanto i modelli di cubi colorati altro non sono che le orbite di C^D sotto l'azione di G. Infatti due colorazioni f e g sono equivalenti se esiste un'*opportuna* permutazione delle facce del cubo che porti una colorazione nell'altra.

Nella tabella seguente sono riportati gli assi rispetto ai quali ruota il cubo, le permutazioni indotte e le relative strutture cicliche.

Rotazioni	Permutazioni	Strutture cicliche
abcd-efgh	(2645); (24)(56); (2546)	$x_1^2x_4; x_1^2x_2^2; x_1^2x_4$
bcfg-adhe	(1536); (13)(56); (1635)	$x_1^2x_4; x_1^2x_2^2; x_1^2x_4$
abfe-dcgh	(1234); (13)(24); (1432)	$x_1^2x_4; x_1^2x_2^2; x_1^2x_4$
a-g	(145)(632); (154)(623)	$x_3^2; x_3^2$
b-h	(152)(643); (125)(634)	$x_3^2; x_3^2$
c-e	(126)(345); (162)(345)	$x_3^2; x_3^2$
d-f	(164)(352); (146)(325)	$x_3^2; x_3^2$
ab-hg	(15)(36)(24)	x_2^3
bc-eh	(12)(34)(56)	x_2^3
cd-ef	(16)(35)(24)	x_2^3
ad-fg	(14)(23)(56)	x_2^3
bf-dh	(13)(25)(46)	x_2^3
ae-gc	(13)(26)(45)	x_2^3
Id	(1)(2)(3)(4)(5)(6)	x_1^6

dove le 6 facce sono segnate come segue:

$$1 = \{abcd\} \quad 2 = \{bcfg\} \quad 3 = \{efgh\};$$
$$4 = \{adeh\} \quad 5 = \{abef\} \quad 6 = \{cdgh\}.$$

Pertanto l'indice ciclico del gruppo G *è:*

$$\mathcal{Z}_6(G) = \frac{1}{24}(x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2).$$

Definiamo la funzione peso su C ponendo $w(bianco) = b$ e $w(nero) = n$. Allora $W(C) = (b + n)$ e quindi, per il Teorema **F4.2**, l'enumeratore delle

orbite risulta come segue:

$$\begin{aligned} W(\mathcal{O}) &= \frac{1}{24}\Big\{(b+n)^6 + 6(b^2+n^2)^3 + 8(b^3+n^3)^2 \\ &\qquad + 3(b+n)^2(b^2+n^2)^2 + 6(b+n)^2(b^4+n^4)\Big\} \\ &= b^6 + b^5n + 2b^4n^2 + 2b^3n^3 + 2b^2n^4 + bn^5 + n^6. \end{aligned}$$

Così ci sono due orbite (e quindi due modelli) con 4 facce bianche e 2 facce nere. Pertanto il numero delle orbite è

$$|\mathcal{O}| = \mathcal{Z}(H; 2, \cdots, 2) = 10.$$

Se invece delle facce si vogliono colorare i vertici o gli spigoli del cubo, dobbiamo considerare le permutazioni indotte dal gruppo delle rotazioni rispettivamente sull'insieme dei vertici e sull'insieme degli spigoli. Ragionando analogamente al caso della colorazione delle facce, si ricavano i seguenti indici ciclici.

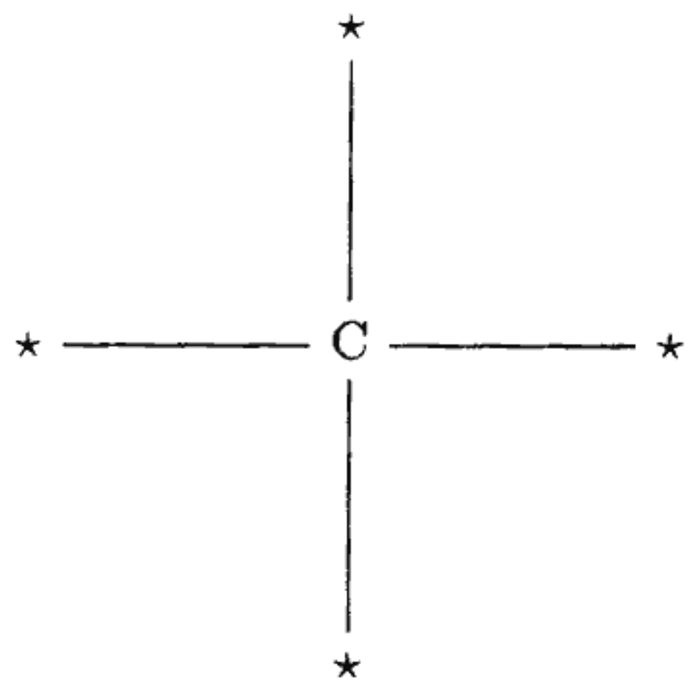
$$\begin{aligned} \mathcal{Z}_v &= \frac{1}{24}(x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2) \quad \text{per i } \textit{vertici}; \\ \mathcal{Z}_s &= \frac{1}{24}(x_1^{12} + 3x_2^6 + 6x_4^3 + 6x_1^2x_2^5 + 8x_3^4) \quad \text{per gli } \textit{spigoli}. \end{aligned}$$

Se invece di due colori se ne usano m, le orbite che si ottengono nei tre casi sono rispettivamente:

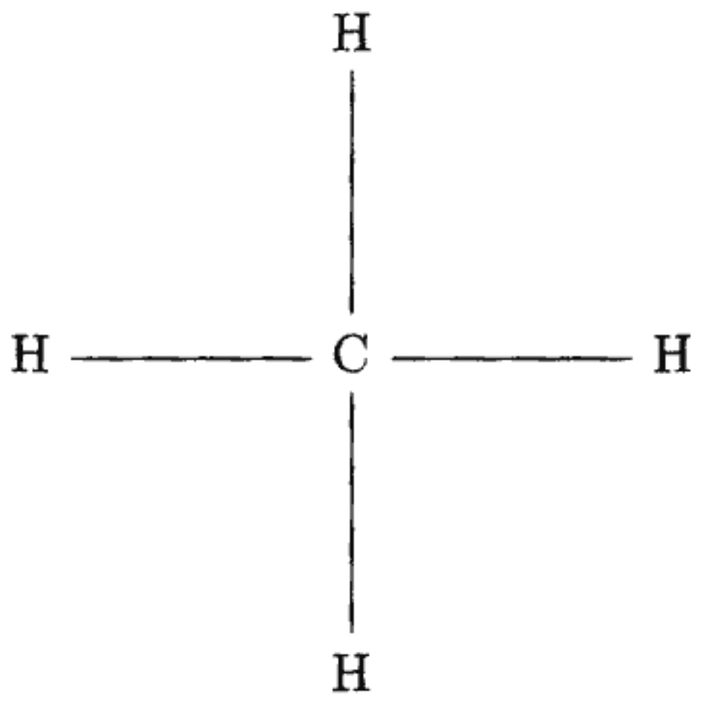
$$\begin{aligned} f_m &= \frac{1}{24}(m^6 + 3m^4 + 12m^3 + 8m^2) \quad \text{per le } \textit{facce}; \\ v_m &= \frac{1}{24}(m^8 + 17m^4 + 6m^2) \quad \text{per i } \textit{vertici}; \\ s_m &= \frac{1}{24}(m^{12} + 6m^7 + 3m^6 + 8m^4 + 6m^3) \quad \text{per gli } \textit{spigoli}. \end{aligned}$$

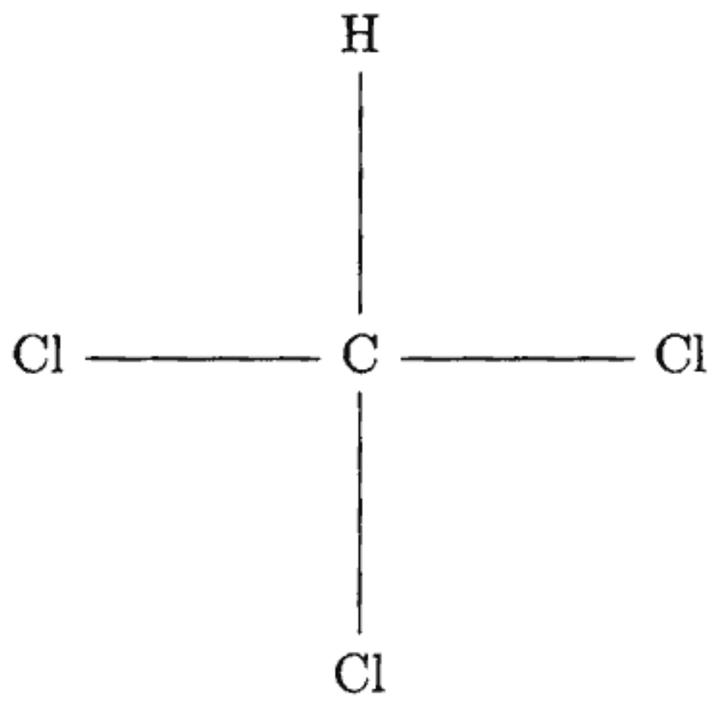
F5.4. Problema di enumerazione in chimica. Presentiamo adesso un problema di natura chimica che è fondamentalmente combinatorio. In realtà furono proprio i problemi di questo tipo a far nascere la teoria di enumerazione di Pólya-Redfield.

Consideriamo la classe delle molecole organiche della forma:



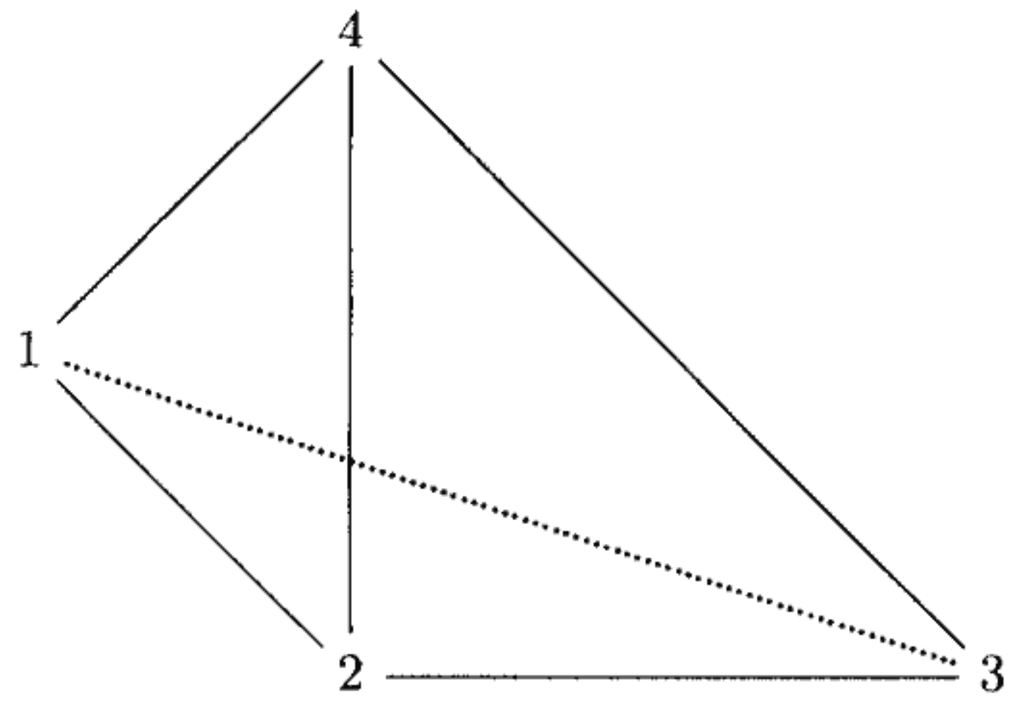
dove C è un atomo di carbonio e ciascun "$\star$" denota uno qualsiasi dei componenti CH_3(metile), C_2H_5(etile), H(idrogeno), Cl(cloro). Per esempio, le seguenti molecole di *Metano* e di *Cloroformio* sono della forma considerata.





Ciascuna molecola può essere rappresentata come un tetraedro regolare con l'atomo di carbonio nel centro ed i componenti segnati con "$\star$" nei vertici. Il problema è quello di contare le differenti molecole di questa forma.

Denotiamo con $D = \{1, 2, 3, 4\}$ e $C = \{CH_3, C_2H_5, H, Cl\}$ rispettivamente l'insieme dei vertici del tetraedro e l'insieme delle molecole da legare. Il problema consiste nel contare i modelli di così fatte molecole.



Ciascuna molecola organica corrisponde ad una funzione $f \in C^D$ e due molecole sono equivalenti se esiste un'opportuna permutazione dei vertici del tetraedro che porti l'una nell'altra. Il gruppo G delle rotazioni del tetraedro, agendo sull'insieme delle $|C^D|$ molecole organiche del tipo descritto, determina un'equivalenza tra molecole.

Le rotazioni del tetraedro sono 12 e precisamente:

π_1 : rotazione di 120^0 attorno all'asse passante per 1 ed il centro della faccia opposta;
σ_1 : rotazione di 240^0 attorno all'asse passante per 1 ed il centro della faccia opposta;
π_2 : rotazione di 120^0 attorno all'asse passante per 2 ed il centro della faccia opposta;
σ_2 : rotazione di 240^0 attorno all'asse passante per 2 ed il centro della faccia opposta;
π_3 : rotazione di 120^0 attorno all'asse passante per 3 ed il centro della faccia opposta;
σ_3 : rotazione di 240^0 attorno all'asse passante per 3 ed il centro della faccia opposta;
π_4 : rotazione di 120^0 attorno all'asse passante per 4 ed il centro della faccia opposta;
σ_4 : rotazione di 240^0 attorno all'asse passante per 4 ed il centro della faccia opposta;
τ_1 : rotazione di 180^0 attorno alla retta che unisce i punti medi degli spigoli [12] e [43];
τ_2 : rotazione di 180^0 attorno alla retta che unisce i punti medi degli spigoli [23] e [14];
τ_3 : rotazione di 180^0 attorno alla retta che unisce i punti medi degli spigoli [13] e [24].

Osserviamo che ciascuna rotazione del tetraedro determina una permutazione dei vertici, come descritto nella tabella seguente.

Rotazioni	Permutazioni dei vertici	Strutture cicliche
Id	(1)(2)(3)(4)	x_1^4
π_1	(243)(1)	x_1x_3
σ_1	(234)(1)	x_1x_3
π_2	(143)(2)	x_1x_3
σ_2	(134)(2)	x_1x_3
π_3	(421)(3)	x_1x_3
σ_3	(412)(3)	x_1x_3
π_4	(132)(4)	x_1x_3
σ_4	(123)(4)	x_1x_3
τ_1	(21)(34)	x_2^2
τ_2	(23)(14)	x_2^2
τ_3	(13)(24)	x_2^2

Allora l'equivalenza tra molecole (ovvero tra le funzioni dell'insieme C^D) è determinata dalle permutazioni descritte in tabella. Queste, assieme alla permutazione identica, costituiscono un gruppo che sarà denotato con G.

Ad esempio se consideriamo le molecole:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \mathrm{Cl} & \mathrm{C_2H_5} & \mathrm{Cl} & \mathrm{CH_3} \end{pmatrix} \quad \text{e} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \mathrm{Cl} & \mathrm{Cl} & \mathrm{C_2H_5} & \mathrm{CH_3} \end{pmatrix}$$

queste sono equivalenti perché la permutazione $\sigma_4 = (123)(4)$ muta la molecola g in f. Tenendo conto della tabella precedente l'indice ciclico del gruppo G è:

$$\mathcal{Z}(G; x_1, x_2, x_3, x_4) = \frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2).$$

Pertanto vi sono

$$\mathcal{Z}(G; 4, 4, 4, 4) = 36$$

orbite, ovvero vi sono 36 possibili molecole del tipo richiesto. Ponendo $w(\mathrm{H}) = w$, $w(\mathrm{Cl}) = x$, $w(\mathrm{CH_3}) = y$, $w(\mathrm{C_2H_5}) = z$ si ottiene l'enumeratore delle orbite (ovvero delle molecole) sostituendo x_k con $w^k + x^k + y^k + z^k$, con $k = 1, 2, 3, 4$, che però ha uno sviluppo piuttosto lungo. Per semplicità poniamo $x = y = z = 1$, allora:

$$\begin{aligned} W(\mathcal{O}) &= \frac{1}{12}\Big\{(w+3)^4 + 3(w^2+3)^2 + 8(w+3)(w^3+3)\Big\} \\ &= 15 + 11w + 6w^2 + 3w^3 + w^4. \end{aligned}$$

Questo polinomio in w afferma che vi sono 15 molecole senza atomi di idrogeno, 11 molecole con 1 atomo di idrogeno, eccetera, infine una sola molecola con 4 atomi di idrogeno. Complessivamente le molecole sono 36.

F5.5. Partizioni e composizioni. Dato un intero non negativo m, il numero delle soluzioni dell'equazione diofantina

$$x_1 + x_2 + \cdots + x_n = m$$

si chiama numero di composizioni di m in n-parti. Quando le soluzioni sono ordinate

$$x_1 \geq x_2 \geq \cdots \geq x_n$$

il numero delle soluzioni corrispondenti viene denominato numero delle partizioni di m. Adesso, studiamo composizioni e le partizioni mediante la teoria di Pólya-Redfield.

Poniamo $D = \{1, 2, \cdots, n\}$ e $C = \{0, 1, 2, \cdots, m\}$. Sia G un gruppo di permutazioni di D. Evidentemente ogni applicazione $f \in \Omega = C^D$ rappresenta una composizione di qualche numero naturale. Per una variabile complessa q, definiamo la funzione peso $w(x) = q^x$, $\forall x \in C$. Abbiamo subito che

$$\eta(q) = W(C) = \frac{1 - q^{m+1}}{1 - q} = \sum_{k=0}^{m} q^k.$$

Secondo il teorema di Pólya, l'enumeratore delle orbite (o funzione generatrice delle orbite $\mathcal{O}_G$ di Ω sotto l'azione di G) viene fornito da

$$W(\mathcal{O}_G) = \mathcal{Z}\big(G \,|\, \eta(q), \eta(q^2), \eta(q^n)\big).$$

- $G = E_n$, gruppo identico: si ha l'enumeratore delle composizioni:

$$W(\mathcal{O}_E) = \eta^n(q) = \left\{ \frac{1 - q^{m+1}}{1 - q} \right\}^n.$$

  Calcolando il limite per $m \to \infty$, otteniamo la funzione generatrice delle composizioni senza restrizione

$$\frac{1}{(1-q)^n} = \sum_{m=0}^{\infty} \binom{m+n-1}{m} q^m.$$

- $G = S_n$, gruppo simmetrico: Possiamo stabilire la funzione generatrice delle orbite delle partizioni:

$$W(\mathcal{O}_S) = \sum_{1 \cdot m_1 + 2 \cdot m_2 + \cdots + n \cdot m_n = n} \prod_{k=1}^{n} \frac{\eta^{m_k}(q^k)}{k^{m_k} \cdot m_k!}.$$

  Per semplificare la multisomma sulla destra, notiamo che

$$W(\mathcal{O}_S) \;=\; [x^n] \prod_{k=1}^{n} \exp\left\{ \frac{x^k}{k} \eta(q^k) \right\} \;=\; [x^n] \exp\left\{ \sum_{k=1}^{\infty} \frac{x^k}{k} \eta(q^k) \right\}.$$

L'esponente della funzione esponenziale si riduce a una forma chiusa:

$$\sum_{k=1}^{\infty} \frac{x^k}{k} \eta(q^k) \;=\; \sum_{k=1}^{\infty} \frac{x^k}{k} \sum_{i=0}^{m} q^{ik} \;=\; \sum_{i=0}^{m} \sum_{k=1}^{\infty} \frac{(q^i x)^k}{k}$$

$$= \; -\sum_{i=0}^{m} \ln(1-q^i x) \;=\; -\ln\left\{(1-x)(1-qx)\cdots(1-q^m x)\right\}.$$

Allora si ha la funzione generatrice delle partizioni

$$\begin{aligned} W(\mathcal{O}_S) &= [x^n] \frac{1}{(1-x)(1-qx)\cdots(1-q^m x)} \\ &= \frac{(1-q^{m+1})(1-q^{m+2})\cdots(1-q^{m+n})}{(1-q)(1-q^2)\cdots(1-q^n)} \end{aligned}$$

che risulta noto come coefficiente binomiale gaussiano.

CAPITOLO G

Teoria dell'Inversione di Möbius-Rota

L'obiettivo di questo capitolo è di presentare la teoria dell'inversione basata su *insiemi parzialmente ordinati*, con particolare riferimento alle applicazioni algebriche e combinatorie.

G1. Insiemi parzialmente ordinati ed inversione di Möbius

La parte teorica dell'inversione di Möbius costituisce l'argomento di questa sezione. Partendo dai concetti fondamentali di *insiemi parzialmente ordinati*, *reticoli* e di *algebra di incidenza*, si stabiliscono la funzione di Möbius e le proprietà (ortogonalità e relazione ricorrente), le quali sono indispensabili per costruire la teoria centrale dell'inversione, cioè il teorema dell'inversione. Tale teorema ci permette di determinare una funzione, definita su un insieme finito parzialmente ordinato, quando si conoscono le sue somme parziali e la funzione di Möbius corrispondente. Per facilitare il calcolo delle funzioni di Möbius, sono state incluse due formule concernenti il prodotto diretto e l'isomorfismo di insiemi parzialmente ordinati.

G1.1. Insiemi parzialmente ordinati. Il concetto più generale che considereremo in questa sezione è quello di un insieme parzialmente ordinato.

Ricordiamo che una relazione binaria su un insieme S è un sottoinsieme R dell'insieme prodotto $S \times S$. Diciamo che $a \in S$ è in relazione R con $b \in S$ e scriviamo $a\,R\,b$ se e solo se $(a, b) \in R$.

Definizione G1.1 (Poset). *Sia S un insieme su cui è definita una relazione binaria denotata con $\leq$* (oppure con $\leq_S$ quando c'è possibilità di confusione) *soddisfacente i seguenti tre assiomi:*

- *riflessività:* $\forall a \in S: \quad a \leq a.$
- *antisimmetria:* $\forall a, b \in S: \quad a \leq b,\ b \leq a \ \Rightarrow\ a = b.$
- *transitività:* $\forall a, b, c \in S: \quad a \leq b,\ b \leq c \ \Rightarrow\ a \leq c.$

La coppia $(S, \leq)$ *si chiama* insieme parzialmente ordinato *o semplicemente* "poset" (partially ordered set).

- Due elementi a e b di S, distinti ($a \neq b$), si dicono incomparabili se $a \not\leq b$ e $b \not\leq a$. Se $a \leq b$ e $a \neq b$, allora scriviamo $a < b$.
- Inoltre scriviamo $a \geq b$ in alternativa di $b \leq a$ e $a > b$ per $b < a$.
- In generale, se $(S, \leq_S)$ è un insieme parzialmente ordinato, allora ogni sottoinsieme T di S è parzialmente ordinato attraverso la stessa relazione $\leq_S$ di S ristretta a T ($\leq_T$), così definita:

$$\forall a, b \in T: \quad a \leq_T b \quad \Longleftrightarrow \quad a \leq_S b.$$

Così, se $(S, \leq_S)$ è un insieme finito parzialmente ordinato, allora esso ha esattamente $2^{|S|}$ sottoinsiemi parzialmente ordinati attraverso la relazione sopra definita.

Definizione G1.2 (Poset localmente finito). *Sia* $(S, \leq)$ *un insieme parzialmente ordinato:*

- *Un intervallo* (chiuso) *è un sottoinsieme parzialmente ordinato così definito*

$$[a, b] := \Big\{ s \in S \mid a \leq s \leq b \Big\} \quad con \quad a \leq b.$$

- *Analogamente definiamo l'intervallo* (aperto)

$$(a, b) := \{ s \in S \mid a < s < b \} \quad con \quad a \leq b.$$

- *In particolare, si ha* $[a, a] = \{a\}$ *e* $(a, a) = \emptyset$.

Allora, $(S, \leq)$ *si dice* localmente finito *se* $\forall a, b \in S : [a, b]$ *è finito.*

Definizione G1.3 (Cover). *Siano* $(S, \leq)$ *un insieme parzialmente ordinato con* a *e* b *due elementi di* S. *Diciamo che* b è un cover di a *se* $b > a$ *e non esiste* $s \in S$ *tale che* $b > s > a$. *Così,* b *è un "cover" di* a *se* $b > a$ *e* $[a, b] = \{a, b\}$.

Un poset localmente finito $(S, \leq)$ è completamente determinato attraverso le sue relazioni di "covers".

La nozione di "cover" suggerisce un modo di rappresentare un insieme finito parzialmente ordinato $(S, \leq)$ attraverso un *diagramma di Hasse.*

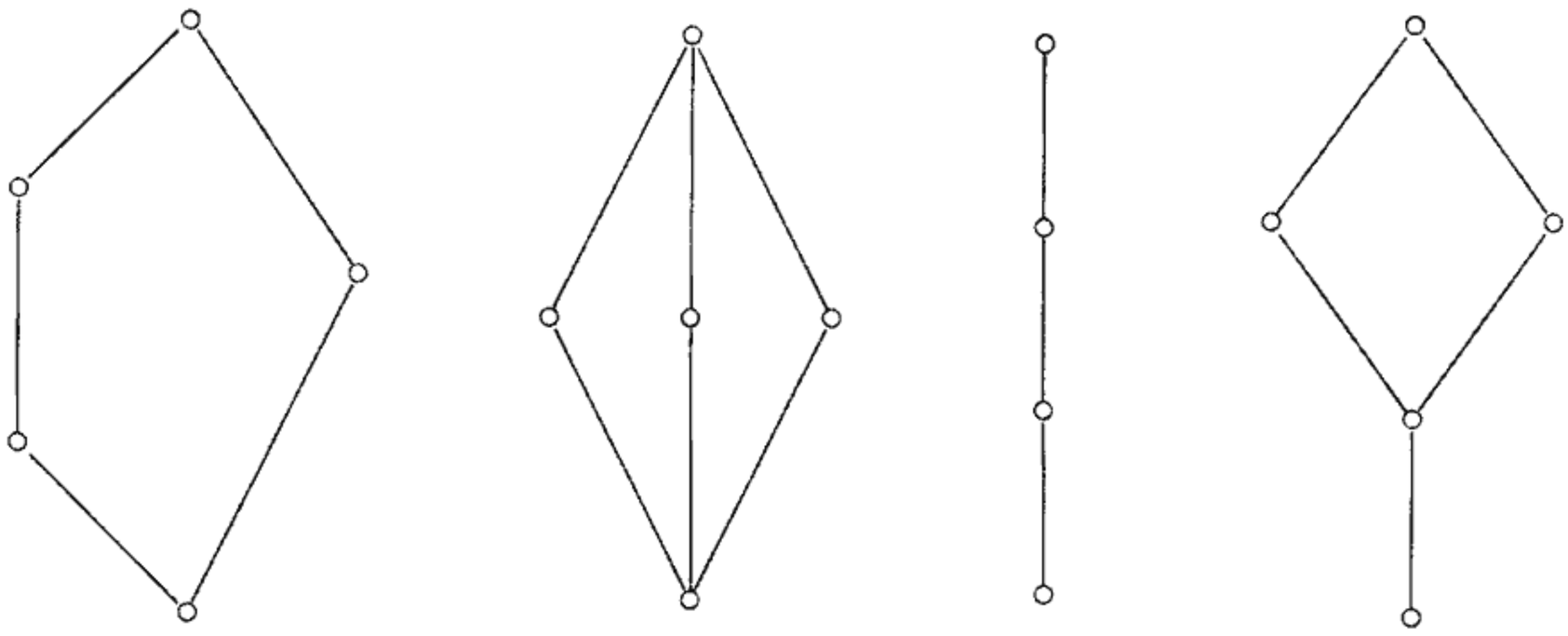
È chiaro che $b > a$ in un insieme finito S se e solo se esiste una sequenza

$$a = s_0, s_1, \cdots, s_n = b$$

tale che ogni s_i è un "cover" di s_{i-1} per $i = 1, 2, \cdots, n$.

Rappresentiamo gli elementi di S nel diagramma di Hasse attraverso punti. Se s_i è un "cover" di $s_{i-1}\,(i = 1, 2, \cdots, n)$, allora collochiamo nel diagramma di Hasse s_i al di sopra di s_{i-1} e congiungiamo i due punti con una linea retta. Allora $b > a$ se e solo se esiste una spezzata discendente che congiunge b ad a. Se nessuna spezzata congiunge b ad $a \neq b$, allora a e b sono incomparabili.

Riportiamo, di seguito, alcuni esempi di diagrammi di Hasse di insiemi finiti parzialmente ordinati.



Definizione G1.4 (Poset totalmente ordinato). *Un insieme parzialmente ordinato* $(S, \leq)$ *si dice* totalmente ordinato *o* catena *se tutti i suoi elementi sono comparabili, cioè se* $\forall a, b \in S : a \neq b \Longleftrightarrow a < b$ *oppure* $b < a$.

- Il terzo diagramma di Hasse sopra riportato rappresenta un insieme finito totalmente ordinato.
- Se $(S, \leq)$ è una catena (insieme finito totalmente ordinato), possiamo immaginarla nella forma $s_0 < s_1 < \cdots < s_n$. In tal caso n è la lunghezza della catena.
- Un'anticatena è un insieme parzialmente ordinato $(S, \leq)$ con tutti gli elementi incomparabili.
- Se un insieme parzialmente ordinato $(S, \leq)$ possiede un minimo (cioè esiste $u \in S$ tale che $\forall s \in S : u \leq s$) e un massimo (cioè esiste $v \in S$ tale che $\forall s \in S : s \leq v$), o soltanto uno di essi, questi vengono indicati usualmente con i simboli 0 e 1 rispettivamente. Gli elementi di S che sono "covers" di 0 si chiamano *atomi*, mentre quelli per i quali 1 è "cover" di quest'ultimi si dicono *coatomi*.

G1.2. Reticoli e proprietà. Un elemento u di un insieme parzialmente ordinato $(S, \leq)$ è un "upper bound" di un sottoinsieme T di S se $\forall t \in T : u \geq t$. L'elemento u è un "least upper bound" oppure $\sup T$ se u è un "upper bound" di T e per ogni "upper bound" v di T: $u \leq v$. È

chiaro che se esiste sup T, allora è unico, grazie all'antisimmetria dell'insieme parzialmente ordinato.

In maniera simile si definiscono i "lower bounds" e i "greatest lower bounds" oppure "infs" di un insieme T. Inoltre, se esiste inf T, allora è unico.

Adesso introduciamo la seguente definizione:

Definizione G1.5 (Lattice). *Un* reticolo *o* "lattice" *è un insieme parzialmente ordinato $(L, \leq)$ nel quale due elementi a e b qualunque hanno il "least upper bound" $a \vee b$ e il "greatest lower bound" $a \wedge b$. Per specificare le due operazioni $\vee$ e $\wedge$, il reticolo L viene denotato con $(L, \vee, \wedge)$.*

- Se a, b e c sono elementi di un reticolo L, allora $(a \vee b) \vee c \geq a, b, c$ e se $v \geq a, b, c$ allora $v \geq (a \vee b)$ e c; così $v \geq (a \vee b) \vee c$. Quindi $(a \vee b) \vee c$ è il sup di a, b e c. Per induzione, si dimostra che qualunque insieme finito di elementi di un reticolo L ha sup.
- Analogamente, qualunque sottoinsieme finito di un reticolo L ha inf. Denotiamo il sup e l'inf di $s_0, s_1, \cdots, s_n$, elementi di un reticolo, L con $s_0 \vee s_1 \vee \cdots \vee s_n$ e $s_0 \wedge s_1 \wedge \cdots \wedge s_n$ rispettivamente.
- Ogni insieme totalmente ordinato è un reticolo; infatti se a e b sono due qualunque elementi di un insieme di questo tipo, abbiamo $a \leq b$ oppure $b \leq a$.

$$\text{Nel } 1^\circ \text{ caso } (a \leq b): \quad a \vee b = b \quad \text{e} \quad a \wedge b = a;$$
$$\text{Nel } 2^\circ \text{ caso } (b \leq a): \quad a \vee b = a \quad \text{e} \quad a \wedge b = b.$$

Per un reticolo $(L, \vee, \wedge)$, le operazioni $\vee$ e $\wedge$ soddisfano le seguenti proprietà:

Associativa	$\forall a, b, c \in L:$	$(a \vee b) \vee c = a \vee (b \vee c)$,
		$(a \wedge b) \wedge c = a \wedge (b \wedge c)$;
Commutativa	$\forall a, b \in L:$	$a \vee b = b \vee a$ e $a \wedge b = b \wedge a$;
Idempotente	$\forall a \in L:$	$a \vee a = a \quad \text{e} \quad a \wedge a = a.$

Inoltre, entrambe le leggi di assorbimento sono valide, ossia:

$$\forall a, b \in L: \quad a \wedge (a \vee b) = a \quad \text{e} \quad a \vee (a \wedge b) = a.$$

Definizione G1.6 (Complete lattice). *Un insieme parzialmente ordinato è detto un* reticolo completo *o* "complete lattice" *se ogni sottoinsieme T di S ha* sup *e* inf. *Denotiamo questi rispettivamente con*

$$\bigvee_{t \in T} t \qquad e \qquad \bigwedge_{t \in T} t.$$

G1.3. Esempi di "lattices". Diamo alcuni esempi importanti di reticoli:

Esempio G1.7 $(\mathbb{Z}, \leq)$. *L'insieme* $\mathbb{Z}$ *dei numeri interi relativi con la relazione d'ordine per grandezza è un reticolo. Infatti* $(\mathbb{Z}, \leq)$ *è un poset totalmente ordinato poiché*

$$\forall a, b \in \mathbb{Z} \quad con \quad a \neq b: \quad a < b \quad oppure \quad b < a.$$

Notando che l'insieme dei numeri naturali $\mathbb{N}$ *è incluso in* $\mathbb{Z}$*, si ha che* $\mathbb{N}$ *è un reticolo sotto la stessa relazione d'ordine "*$\leq$*".*

Esempio G1.8 $(\mathbb{N}, \mid)$. *L'insieme* $\mathbb{N}$ *dei numeri naturali con la relazione di divisibilità, che indicheremo con "*$\mid$*", così definita:*

$$\forall a, b \in \mathbb{N}: \quad a \mid b \iff a \text{ divide } b$$

è un reticolo dove

$$\forall a, b \in \mathbb{N}: \quad a \wedge b = \mathrm{mcd}(a, b) \quad e \quad a \vee b = \mathrm{mcm}(a, b).$$

Lo 0 *del reticolo coincide col numero naturale* 1 *e gli atomi sono i primi.*

Esempio G1.9 $(\mathcal{P}(S), \subseteq)$. *L'insieme* $\mathcal{P}(S)$ *delle parti di un insieme finito* S *con la relazione di inclusione, così definita:*

$$\forall A, B \in \mathcal{P}(S): \quad A \subseteq B \iff A \text{ è una parte di } B$$

è un reticolo dove le operazioni $\wedge$ *e* $\vee$ *corrispondono all'intersezione e all'unione rispettivamente. Gli insiemi* $\emptyset$ (vuoto) *e* S *sono rispettivamente* 0 *e* 1 *del reticolo.*

G1.4. Funzioni su insiemi parzialmente ordinati.

Definizione G1.10 (L'algebra di incidenza). *Siano* $(S, \leq)$ *un poset localmente finito e* K *un campo* (si pensi in pratica ai reali). *Indicheremo con* $\mathfrak{F}(S)$ *l'insieme delle funzioni* $f : S \times S \to K$ *tali che*

$$\forall a, b \in S: \quad a \not\leq b \implies f(a, b) = 0.$$

In $\mathfrak{F}(S)$ definiamo l'operazione di *convoluzione* "$\star$" come segue:

$$\forall f,\ g \in \mathfrak{F}(S): \quad f \star g(a, b) := \sum_{a \leq t \leq b} f(a, t)\, g(t, b).$$

L'insieme $\mathfrak{F}(S)$ con la convoluzione, con le ordinarie operazioni di addizione e moltiplicazione scalare tra funzioni, diventa una K-algebra associativa, ma in generale non commutativa. Essa è chiamata *algebra d'incidenza* di $(S, \leq)$ in K.

Si verifica facilmente che la funzione di Kronecker

$$\begin{aligned} \delta : S \times S &\longrightarrow K; \\ (a,b) &\longmapsto \delta(a,b) := \begin{cases} 1, & \text{se} \quad a = b; \\ 0, & \text{se} \quad a \neq b; \end{cases} \end{aligned}$$

è l'elemento neutro per l'operazione "$\star$", ciò significa che

$$\forall f \in \mathfrak{F}(S): \quad f \star \delta = \delta \star f = f.$$

Infatti, siano $a,\ b \in S$; allora si vede facilmente

$$\begin{aligned} f \star \delta\,(a,b) &= \sum_{a \le t \le b} f(a,t)\,\delta(t,b) \;=\; f(a,b); \\ \delta \star\ f(a,b) &= \sum_{a \le t \le b} \delta(a,t)\,f(t,b) \;=\; f(a,b). \end{aligned}$$

Per quanto riguarda l'inversa di una funzione rispetto all'operazione di convoluzione "$\star$", bisogna tener presente il seguente risultato.

Lemma G1.11. *Sia $f \in \mathfrak{F}(S)$, con $f(a,a) \neq 0$ per ogni $a \in S$. Allora esiste l'unica inversa g di f tale che $f \star g = g \star f = \delta$. Per due elementi $a,\ b \in S$ l'inversa g è definita per induzione come segue:*

$$g(a,b) = \begin{cases} \dfrac{1}{f(a,a)}, & \textit{se} \quad a = b; \\ -\displaystyle\sum_{a \le t < b} \frac{f(t,b)}{f(b,b)} g(a,t), & \textit{se} \quad a < b. \end{cases}$$

Inoltre, vale anche la seguente formula duale:

$$g(a,b) = \begin{cases} \dfrac{1}{f(a,a)}, & \textit{se} \quad a = b; \\ -\displaystyle\sum_{a < t \le b} \frac{f(a,t)}{f(a,a)} g(t,b), & \textit{se} \quad a < b. \end{cases}$$

Dimostrazione. Se $a = b$, risulta

$$g \star f(a,a) = g(a,a) f(a,a) = 1.$$

Invece se $a < b$, abbiamo che

$$\begin{aligned} 0 &= \delta(a,b) \;=\; g \star f(a,b) \\ &= g(a,b)\, f(b,b) + \sum_{a \le t < b} g(a,t) f(t,b). \end{aligned}$$

Così abbiamo dimostrato che $g \star f = \delta$, cioè che g è un'inversa sinistra di f. Analogamente, possiamo provare l'esistenza di un'inversa destra h di f.

Ora si verifica facilmente che $g = h$. Infatti, multiplicando $g \star f = \delta$ alla destra per h ed richiamando la proprietà associativa, si ha che

$$h = \delta \star h = (g \star f) \star h = g \star (f \star h) = g \star \delta = g.$$

Inoltre, supponendo che g e g' siano le inverse sinistre di f, multiplicando $\delta = g \star f = g' \star f$ alla destra per h si conferma $g = g'$ come segue:

$$\begin{aligned} h = \delta \star h &= (g \star f) \star h = g \star (f \star h) = g \star \delta = g \\ &= (g' \star f) \star h = g' \star (f \star h) = g' \star \delta = g'. \end{aligned}$$

Invece, supponendo che sia h che h' sono le inverse destre di f, si dimostra ugualmente che $g = h = h'$. Quindi f ammette l'unica inversa (sinistra e destra). Dall'equazione $f \star g = \delta$, segue la formula duale esplicitamente. □

G1.5. Funzione di Möbius μ. Prima di definire la funzione di Möbius, abbiamo bisogno di introdurre delle funzioni ξ, η, λ.

Una delle funzioni più importanti in $\mathfrak{F}(S)$ è la *zeta* (o *funzione d'incidenza*) così definita:

$$\xi : \ S \times S \longrightarrow K;$$

$$(a,b) \longmapsto \xi(a,b) := \begin{cases} 1, & \text{se} \quad a \leq b; \\ 0, & \text{altrimenti.} \end{cases}$$

Essa infatti caratterizza la relazione d'ordine parziale.

Altre due funzioni interessanti dell'algebra d'incidenza sono:

$$\eta : \ S \times S \longrightarrow K;$$

$$(a,b) \longmapsto \eta(a,b) := \begin{cases} 1, & \text{se} \quad a < b; \\ 0, & \text{altrimenti.} \end{cases}$$

ovvero $\eta = \xi - \delta$; la funzione di ricoprimento

$$\lambda : \ S \times S \longrightarrow K$$

$$(a,b) \longmapsto \lambda(a,b) := \begin{cases} 1, & \text{se } b \text{ è un "cover" di } a; \\ 0, & \text{altrimenti.} \end{cases}$$

Le funzioni ξ e λ hanno un significato combinatorio derivante dalla loro definizione. Esse danno alcune informazioni sugli intervalli dell'insieme parzialmente ordinato $(S, \leq)$ espresse nel seguente:

Teorema G1.12. *Sia $(S, \leq)$ un poset localmente finito. Per ogni intervallo chiuso $[a, b]$ con $a \leq b$, risulta:*

$$\begin{aligned}
&\text{(a)} \quad \xi^2(a,b) = \textit{cardinalità di } [a,b].\\
&\text{(b)} \quad \lambda \star \xi(a,b) = \textit{numero di atomi in } [a,b].\\
&\text{(c)} \quad \xi \star \lambda(a,b) = \textit{numero di coatomi in } [a,b].
\end{aligned}$$

DIMOSTRAZIONE. Procediamo con la dimostrazione caso per caso.

[a] La prima formula si dimostra osservando i seguenti passaggi:

$$\xi^2(a,b) = \xi \star \xi(a,b) = \sum_{a \leq t \leq b} \xi(a,t)\xi(t,b) = \sum_{t \in [a,b]} 1 = \Big|[a,b]\Big|.$$

[b] La seconda formula segue dalla definizione dell'operazione "$\star$":

$$\begin{aligned}
\lambda \star \xi(a,b) &= \sum_{a \leq t \leq b} \lambda(a,t)\xi(t,b) = \sum_{t \in (a,b]:\ |[a,t]|=2} 1\\
&= \text{numero di atomi in } [a,b].
\end{aligned}$$

[c] Per la terza ed ultima formula si ha:

$$\begin{aligned}
\xi \star \lambda(a,b) &= \sum_{a \leq t \leq b} \xi(a,t)\lambda(t,b) = \sum_{t \in [a,b):\ |[t,b]|=2} 1\\
&= \text{numero di coatomi in } [a,b].
\end{aligned}$$

Così tutte le affermazioni del teorema sono verificate. □

La *funzione di Möbius* viene definita come l'inversa della funzione zeta (o funzione d'incidenza) $\mu = \xi^{-1}$. In virtù del Lemma **G1.11** si può esprimere per ricorrenza nel modo seguente:

$$\mu : S \times S \longrightarrow K;$$

$$(a,b) \longmapsto \mu(a,b) := \xi^{-1}(a,b) = \begin{cases} 1, & \text{se} \quad a = b;\\ -\sum_{a \leq t < b} \mu(a,t), & \text{se} \quad a < b. \end{cases}$$

Evidentemente abbiamo le seguenti ortogonalità:

$$\begin{aligned}
\xi \star \mu = \delta \quad &\Longleftrightarrow \quad \sum_{a \leq t \leq b} \mu(t,b) = \delta(a,b);\\
\mu \star \xi = \delta \quad &\Longleftrightarrow \quad \sum_{a \leq t \leq b} \mu(a,t) = \delta(a,b).
\end{aligned}$$

Per poter enunciare altre proprietà delle funzioni ξ, η e λ bisogna dare ulteriori definizioni.

G1.6. Catene. Gli elementi $s_0, s_1, \cdots, s_n$ non necessariamente distinti di un insieme parzialmente ordinato $(S, \leq)$ formano una multicatena di lunghezza n quando $s_0 \leq s_1 \leq \cdots \leq s_n$ (così una multicatena è ovviamente una catena con elementi ripetuti).

Una catena (multicatena) con primo elemento a ed ultimo elemento b si denota con $\langle a, b\rangle$-catena (multicatena). Una $\langle a, b\rangle$-catena è massimale se non esiste alcun elemento dell'insieme parzialmente ordinato $(S, \leq)$ da poter aggiungere per ottenere una catena più lunga.

Ecco allora come le precedenti funzioni permettono di rispondere a problemi combinatori riguardanti catene e multicatene.

Teorema G1.13. *Sia $(S, \leq)$ un poset localmente finito. Per ogni a, $b \in S$, valgono le seguenti identità:*

(a) $\eta^k(a, b)$ – *numero di $\langle a, b\rangle$-catene lunghe k.*
(b) $\lambda^k(a, b)$ – *numero di $\langle a, b\rangle$-catene massimali lunghe k.*
(c) $\xi^k(a, b)$ – *numero di $\langle a, b\rangle$-multicatene lunghe k.*

Le formule elencate nel teorema sono ovvie. □

La prima identità ci permette di dare un significato combinatorio alla funzione di Möbius. Infatti $\xi = \delta + \eta$, mentre si può dimostrare che nell'algebra d'incidenza, vale la relazione

$$\mu = \xi^{-1} = (\delta + \eta)^{-1} = \sum_{k \geq 0} (-1)^k \eta^k.$$

Quindi, per ogni intervallo $[a, b]$ di S con $a \leq b$, risulta

$$\mu(a, b) = 1 - \eta(a, b) + \eta^2(a, b) - \cdots$$

dove $\eta^k(a, b)$ è il numero di $\langle a, b\rangle$-catene lunghe k. Questa formula, in alcuni casi, permette di ricavare $\mu(a, b)$ una volta noti i numeri $\eta^k(a, b)$.

G1.7. Formula di inversione. Presentiamo il risultato più importante della teoria delle algebre di incidenza che è fondamentale nella combinatoria enumerativa e nell'algebra quantitativa.

Teorema G1.14. *Siano $(S, \leq)$ un poset finito, f e g funzioni definite da S a valori in un campo K con $f, g : S \longrightarrow K$. Allora per ogni $a \in S$ vale*

l'equivalenza:

$$f(a) = \sum_{t \le a} g(t) \iff g(a) = \sum_{t \le a} \mu(t,a)\, f(t)$$

dove μ è la funzione di Möbius dell'algebra $\mathfrak{F}(S)$.

DIMOSTRAZIONE. Osserviamo che

$$f(a) = \sum_{t \le a} g(t) \quad \text{per tutti} \quad a \in S$$

è un sistema di equazioni; allora il teorema afferma che questo sistema è equivalente al sistema delle equazioni

$$g(a) = \sum_{t \le a} \mu(t,a)\, f(t) \quad \text{per tutti} \quad a \in S.$$

Supponiamo che il primo sistema sia valido; dimostriamo, allora, che il secondo è vero. Sostituendo $f(t)$ nel secondo sistema, possiamo riscrivere il membro destro dell'equivalenza come segue:

$$\begin{aligned} \sum_{t \le a} \mu(t,a)\, f(t) &= \sum_{t \le a} \mu(t,a) \sum_{c \le t} g(c) \\ &= \sum_{c \le a} g(c) \sum_{c \le t \le a} \mu(t,a). \end{aligned}$$

Questa somma si riduce alla funzione $g(a)$ poiché

$$\sum_{c \le t \le a} \mu(t,a) = \delta(c,a)$$

in virtù delle ortogonalità della funzione di Möbius. □

In modo analogo si può dimostrare la seguente forma duale:

Teorema G1.15. *Siano $(S, \le)$ un poset finito, f e g funzioni definite da S a valori in un campo K con $f, g : S \to K$. Allora per ogni $a \in S$ vale l'equivalenza:*

$$f(a) = \sum_{t \ge a} g(t) \iff g(a) = \sum_{t \ge a} \mu(a,t)\, f(t)$$

dove μ è la funzione di Möbius dell'algebra $\mathfrak{F}(S)$. □

L'utilità del teorema di inversione consiste principalmente nel fatto seguente: permette di determinare la funzione g quando si conoscono le sue somme parziali, cioè la funzione f e la funzione μ di Möbius corrispondente.

Introduciamo ora i concetti di prodotto diretto e di isomorfismo di insiemi parzialmente ordinati per dare vari esempi di applicazione del teorema.

G1.8. Prodotto diretto di posets. Siano $(S_1, \leq_{S_1})$ e $(S_2, \leq_{S_2})$ due insiemi parzialmente ordinati. Il loro *prodotto diretto* $(S_1 \otimes S_2, \leq)$ è costituito dalle coppie ordinate di elementi di S_1 e S_2 con la relazione d'ordine seguente:

$$(a,b) \leq (c,d) \iff \begin{cases} a \leq_{S_1} c, & \forall a, c \in S_1; \\ b \leq_{S_2} d, & \forall b, d \in S_2. \end{cases}$$

Il prodotto diretto di un numero finito, o numerabilmente infinito, di insiemi parzialmente ordinati è introdotto in maniera analoga.

Teorema G1.16. *Siano μ_{S_1} e μ_{S_2} le funzioni di Möbius per gli insiemi parzialmente ordinati $(S_1, \leq_{S_1})$ e $(S_2, \leq_{S_2})$ rispettivamente, allora per ogni $a, c \in S_1$ e $b, d \in S_2$, la funzione di Möbius $\mu_{S_1 \otimes S_2}$ del loro prodotto diretto $(S_1 \otimes S_2, \leq)$ è data dalla formula:*

$$\mu_{S_1 \otimes S_2}\big((a,b),(c,d)\big) = \mu_{S_1}(a,c)\,\mu_{S_2}(b,d).$$

DIMOSTRAZIONE. Per $f = \delta$ e $f = \xi$ vale ovviamente l'identità:

$$f_{S_1 \otimes S_2}\big((a,b),(c,d)\big) = f_{S_1}(a,c) f_{S_2}(b,d)$$

dove $a, c \in S_1$ e $b, d \in S_2$. Pertanto si può scrivere:

$$\begin{aligned} & \sum_{\substack{a \leq c \leq e \\ b \leq d \leq f}} \mu_{S_1 \otimes S_2}\big((a,b),(c,d)\big) \xi_{S_1 \otimes S_2}\big((c,d),(e,f)\big) \\ = \quad & \delta_{S_1 \otimes S_2}\big((a,b),(e,f)\big) = \delta_{S_1}(a,e)\delta_{S_2}(b,f) \\ = \quad & \sum_{a \leq c \leq e} \mu_{S_1}(a,c)\,\xi_{S_1}(c,e) \sum_{b \leq d \leq f} \mu_{S_2}(b,d)\,\xi_{S_2}(d,f) \\ = \quad & \sum_{\substack{a \leq c \leq e \\ b \leq d \leq f}} \mu_{S_1}(a,c)\,\mu_{S_2}(b,d)\,\xi_{S_1 \otimes S_2}\big((c,d)(e,f)\big) \end{aligned}$$

che conferma la tesi del teorema. □

G1.9. Isomorfismo di poset. Siano $(S_1, \leq_{S_1})$ e $(S_2, \leq_{S_2})$ due insiemi parzialmente ordinati. Essi sono *isomorfi* se esiste una biiezione $\psi : S_1 \to S_2$ tale che per ogni a e b di S_1 risulti:

$$a \leq_{S_1} b \implies \psi(a) \leq_{S_2} \psi(b).$$

Teorema G1.17. *Se ψ è un isomorfismo tra $(S_1, \leq_{S_1})$ e $(S_2, \leq_{S_2})$ allora per ogni $a, b \in S_1$, vale*

$$\mu_{S_1}(a,b) = \mu_{S_2}\big(\psi(a), \psi(b)\big).$$

DIMOSTRAZIONE. Denotiamo per ogni $a, b \in S_1$ con

$$\begin{aligned} f(a,b) &:= \mu_{S_1}(a,b), \\ g(a,b) &:= \mu_{S_2}\big(\psi(a),\psi(b)\big). \end{aligned}$$

Allora sia $f(a,b)$ che $g(a,b)$ sono funzioni su $S_1 \otimes S_1$. Entrambe le funzioni hanno i seguenti valori particolari:

$$f(a,b) = g(a,b) = 1, \quad \text{se} \quad a = b;$$
$$f(a,b) = g(a,b) = 0, \quad \text{se} \quad a \not\leq b.$$

Inoltre, le due funzioni soddisfano le stesse relazioni ricorrenti

$$\begin{aligned} \delta(a,b) &= \sum_{a\leq t\leq b} f(a,t) = \sum_{a\leq t\leq b} g(a,t), \\ \delta(a,b) &= \sum_{a\leq t\leq b} f(t,b) = \sum_{a\leq t\leq b} g(t,b); \end{aligned}$$

grazie all'isomorfismo tra $(S_1, \leq_{S_1})$ e $(S_2, \leq_{S_2})$ e alle ortogonalità della funzione di Möbius mostrate nella sezione **G1.5**. Per induzione matematica, f e g coincidono; cioè la tesi. □

Esempio G1.18 (Funzione di Möbius su $(\mathbb{N}_0, \leq)$). *Denotiamo con* $(\mathbb{N}_0, \leq)$ *l'insieme dei numeri interi relativi ordinati per grandezza. La funzione di Möbius* μ *per* $(\mathbb{N}_0, \leq)$ *dell'Esempio* **G1.7** *è chiaramente data da:*

$$\forall a, b \in \mathbb{N}_0: \quad \mu(a,b) = \begin{cases} 1, & \textit{se} \quad b = a; \\ -1, & \textit{se} \quad b = a+1; \\ 0, & \textit{altrimenti.} \end{cases}$$

Allora la inversione di Möbius si esprime come segue:

$$\left.\begin{aligned} f(n) = \sum_{k=0}^{n} g(k) &= g(0) + g(1) + \cdots + g(n) \\ g(n) = \nabla f(n) &= f(n) - f(n-1) \end{aligned}\right\} \quad (n \in \mathbb{N}_0).$$

Più in generale, l'insieme composto da una catena $(n_0 < n_1 < n_2 < \cdots)$ con $n_k \in \mathbb{N}_0$ ha la seguente funzione di Möbius:

$$\mu(n_i, n_j) = \begin{cases} +1, & j = i; \\ -1, & j = i+1; \\ 0, & \text{altrimenti.} \end{cases}$$

Ricordando il Teorema **G1.16** del prodotto diretto, possiamo ottenere la funzione di Möbius per $(\mathbb{N}_0^\ell, \leq)$ come segue:

$$\mu\big((n_1, n_2, \cdots, n_\ell), (m_1, m_2, \cdots, m_\ell)\big) = \begin{cases} (-1)^{\sum_{k=1}^{\ell}(m_k - n_k)}, & \substack{m_k - n_k = 0,\,1 \\ \text{per } 1\leq k\leq \ell;} \\ 0, & \text{altrimenti;} \end{cases}$$

dove $(m_1, m_2, \cdots, m_\ell)$ e $(n_1, n_2, \cdots, n_\ell)$ sono due ℓ-uple di $\mathbb{N}_0^\ell$.

G2. Funzioni aritmetiche ed applicazione

Per l'insieme $(\mathbb{N}, |)$ dei numeri naturali ordinati per divisibilità, la funzione di Möbius coincide con quella classica. In questa sezione, studieremo due funzioni aritmetiche, la classica funzione di Möbius e la funzione di Eulero, utili per le applicazioni relative all'inversione di Möbius nella teoria dei numeri. Esporremo la proprietà moltiplicativa di entrambe e le relazioni che le legano. Successivamente, verrà trattato il problema enumerativo delle permutazioni circolari.

G2.1. Funzione classica μ di Möbius e proprietà. La funzione di Möbius μ per $(\mathbb{N}, |)$, l'insieme dei numeri naturali ordinati per divisibilità, dell'Esempio **G1.8** è data da:

$$\forall a, b \in \mathbb{N}: \quad \mu(a,b) = \begin{cases} (-1)^k, & \text{se } b/a \text{ è un prodotto di } k \text{ primi distinti;} \\ 0, & \text{se } b/a \text{ ha un primo fattore quadrato.} \end{cases}$$

OSSERVAZIONE: Per $n \in \mathbb{N}$ il teorema fondamentale dell'aritmetica afferma che n ammette una scomposizione unica in fattori primi. Quindi $n = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$ dove i p_i sono primi distinti e gli $n_i > 0$ con $i = 1, 2, \cdots, \ell$.

Indichiamo con D_n il reticolo dei divisori interi positivi di n ordinato con la relazione di divisibilità. D_n è isomorfo al prodotto diretto $C_1 \otimes C_2 \otimes \cdots \otimes C_\ell$ dove C_i è la catena $C_i = \{0, 1, \cdots, n_i\}$ con $i = 1, 2, \cdots, \ell$. Per $b|n$ con $b = p_1^{b_1} p_2^{b_2} \cdots p_\ell^{b_\ell}$, quest'isomorfismo è così definito:

$$\begin{array}{ccc} D_n & \longrightarrow & C_1 \otimes C_2 \otimes \cdots \otimes C_\ell; \\ b & \longmapsto & (b_1, b_2, \cdots, b_\ell). \end{array}$$

Se $a|b$ con $a = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}$, si ha che $a_i \leq b_i$ per ogni $i = 1, 2, \cdots, \ell$; allora combinando i Teoremi **G1.16** e **G1.17**, ne segue che:

$$\begin{aligned} \mu(a,b) &= \prod_{i=1}^{\ell} \mu(a_i, b_i) \\ &= \begin{cases} (-1)^k, & \text{se } b/a \text{ è un prodotto dei } k \text{ primi distinti;} \\ 0, & \text{se } b/a \text{ ha un primo fattore quadrato.} \end{cases} \end{aligned}$$

Ponendo $\mu(b/a) = \mu(a,b)$, otteniamo la classica funzione di Möbius, che è una delle notevoli funzioni dell'aritmetica introdotta da Möbius nel 1832 per lo studio della distribuzione dei numeri primi.

Infatti, per ogni $n \in \mathbb{N}$ avente la scomposizione in primi $n = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$, possiamo tradurre $\mu(n) = \mu(1,n)$ come segue:

$$\mu(n) := \begin{cases} 1, & \text{se } n = 1; \\ (-1)^k, & \text{se } e_k = 1 \text{ per } 1 \le k \le \ell; \\ 0, & \text{se esiste } k \text{ con } 1 \le k \le \ell \text{ tale che } e_k > 1. \end{cases}$$

Questa espressione è esattamente quella classica per definire la funzione di Möbius μ.

Teorema G2.1. *La funzione μ è moltiplicativa; cioè per ogni n ed $m \in \mathbb{N}$ tale che* $\mathrm{mcd}(n,m) = 1$ *si ha*

$$\mu(n \cdot m) \quad = \quad \mu(n) \cdot \mu(m).$$

Dimostrazione. Siano $n, m \in \mathbb{N}$ tali che $\mathrm{mcd}(n,m) = 1$. L'equazione viene dimostrata distinguendo i tre casi:

- $n = 1$ o $m = 1$: Senza perdere di generalità supponiamo che $n = 1$. In tale caso risulta
$$\mu(n \cdot m) = \mu(1 \cdot m) = \mu(m) = \mu(n) \cdot \mu(m).$$
- n o m contiene un fattore primo quadrato: Assumendo che la decomposizione di n ha un fattore primo quadrato, allora anche $n \cdot m$ contiene tale fattore primo quadrato; perciò
$$\mu(n \cdot m) = 0 = \mu(n) = \mu(n) \cdot \mu(m).$$
- $n > 1$, $m > 1$ e nessuno dei due contiene un fattore primo quadrato: Sia n che m sono prodotti di primi distinti
$$n = p_1 p_2 \cdots p_k \quad \text{e} \quad m = q_1 q_2 \cdots q_\ell.$$
Allora
$$n \cdot m = p_1 p_2 \cdots p_k \, q_1 q_2 \cdots q_\ell$$
costituisce la decomposizione di $n \cdot m$ in primi distinti poiché per ipotesi $\mathrm{mcd}(n,m) = 1$. Secondo la definizione di funzione di Möbius, si conclude che
$$\mu(n \cdot m) = (-1)^{k+\ell} = (-1)^k \cdot (-1)^\ell = \mu(n) \cdot \mu(m).$$

Così abbiamo provato il teorema. □

Teorema G2.2. *Sia $n \in \mathbb{N}$. Abbiamo:*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & se \quad n = 1; \\ 0, & se \quad n > 1. \end{cases}$$

DIMOSTRAZIONE. La formula è chiaramente vera se $n = 1$.

Assumiamo, allora, che $n > 1$ e scriviamo $n = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$ con p_i primi distinti e $n_i > 0$ per ogni $i = 1, 2, \cdots, \ell$. Tutti i divisori d di n saranno del tipo: $p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$ dove $0 \leq e_i \leq n_i$ con $i = 1, 2, \cdots, \ell$. Quando d contiene una potenza di un primo, si ha $\mu(d) = 0$. Si noti che in questo caso tali divisori danno contributo nullo alla somma del problema.

Invece se d è un prodotto di primi distinti, $d = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_\ell^{\epsilon_\ell}$, dove $\epsilon_i \in \{0, 1\}$ con $i = 1, 2, \cdots, \ell$, indichiamo con r il numero di potenze diverse da zero, cioè

$$k := \Big|\{i : \ 1 \leq i \leq \ell \mid \epsilon_i = 1\}\Big|.$$

Allora, ricordando che il numero di modi per scegliere gli k fattori tra ℓ fattori è $\binom{\ell}{k}$, si ha:

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{\ell} (-1)^k \binom{\ell}{k} = (1-1)^\ell = 0$$

dove l'ultimo passaggio è stato giustificato dal teorema binomiale. □

Sulla base del teorema appena dimostrato, possiamo stabilire facilmente la versione classica del Teorema **G1.14**.

Teorema G2.3. *Siano f e g due sequenze complesse. Allora il sistema delle equazioni*

$$f(n) = \sum_{d|n} g(d) \quad per \quad n = 1, 2, \cdots$$

è equivalente al sistema

$$g(n) = \sum_{d|n} \mu(\frac{n}{d})\, f(d) \quad per \quad n = 1, 2, \cdots$$

dove μ è la funzione classica di Möbius. □

G2.2. Funzione φ di Eulero e proprietà. Ricordiamo che la funzione di Eulero $\varphi(n)$ indica il numero di interi positivi $k \leq n$ coprimi con n:

$$\varphi(n) = \sum_{\substack{1 \leq k \leq n \\ \text{mcd}(k,n)=1}} 1.$$

Come nel caso della funzione di Möbius $\mu(n)$, esiste una formula semplice per la somma di questa funzione su tutti i divisori d di n.

Teorema G2.4. *Per $n \in \mathbb{N}$, vale la seguente identità:*

$$\sum_{d|n} \varphi(d) = n.$$

Questa formula è stata già provata nella sezione A5.3 e verrà ridimostrata tramite partizione insiemistica. .

DIMOSTRAZIONE. Ripartiamo l'insieme $\{1, 2, \cdots, n\}$ considerando per ogni divisore d di n il seguente insieme:

$$\Phi_d := \Big\{ k \in \{1, 2, \cdots, n\} \mid \text{mcd}(k, n) = d \Big\}.$$

Allora

$$\{1, 2, \cdots, n\} = \biguplus_{d|n} \Phi_d$$

è un'unione disgiunta. D'altra parte

$$\Phi_d = \Big\{ kd : \ k \in \big\{1, 2, \cdots, n/d\big\} \mid \text{mcd}(k, n/d) = 1 \Big\}.$$

Quindi, per la definizione di funzione di Eulero, risulta $|\Phi_d| = \varphi(\frac{n}{d})$, pertanto

$$\begin{aligned} n &= \Big|\{1, 2, \cdots, n\}\Big| = \Big|\biguplus_{d|n} \Phi_d\Big| \\ &= \sum_{d|n} |\ \Phi_d\ | = \sum_{d|n} \varphi(n/d) \end{aligned}$$

la quale è equivalente all'espressione $\sum_{d|n} \varphi(d) = n$, invertendo l'ordine della somma. □

La funzione di Eulero è in relazione con la funzione di Möbius attraverso la seguente formula:

Teorema G2.5. *Per $n \in \mathbb{N}$, vale la seguente formula:*

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

DIMOSTRAZIONE. La definizione di $\varphi(n)$ può essere riformulata nella forma

$$\varphi(n) = \sum_{k=1}^{n} \Big\lfloor \frac{1}{\text{mcd}(k, n)} \Big\rfloor$$

dove con $\lfloor x \rfloor$ denotiamo la parte intera di un numero reale x. Adesso usiamo il Teorema **G2.2** sostituendo ad n il $\mathrm{mcd}(k,n)$ per ottenere

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d \mid \mathrm{mcd}(k,n)} \mu(d) = \sum_{d \mid n} \mu(d) \sum_{\substack{k=1 \\ d \mid k}}^{n} 1 = \sum_{d \mid n} \mu(d) \frac{n}{d}.$$

Ciò completa la dimostrazione. □

La somma per $\varphi(n)$ nel teorema precedente può essere espressa anche come un prodotto esteso ai divisori primi distinti di n.

Teorema G2.6. *Per $n \in \mathbb{N}$, vale la seguente formula:*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

dove p corre su tutti i fattori primi di n.

DIMOSTRAZIONE. Per $n = 1$ il prodotto è nullo poiché non esistono primi che dividano 1. In questo caso assegnamo per convenzione $\varphi(n) = 1$.

Supponiamo allora che $n > 1$ e siano $p_1, p_2, \cdots, p_k$ divisori primi distinti di n. Il prodotto può essere riscritto come:

$$\begin{aligned} n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\ &= n + \sum_{\iota=1}^{k} \sum_{1 \le i_1 < i_2 < \cdots < i_\iota \le k} \frac{(-1)^\iota \, n}{p_{i_1} p_{i_2} \cdots p_{i_\iota}}. \end{aligned}$$

Notiamo che ogni termine dell'ultima espressione è della forma $\pm n/d$ dove d è un divisore di n che è un primo o un prodotto di primi distinti. Il numeratore $\pm n$ è esattamente $n \cdot \mu(d)$. Poiché $\mu(d) = 0$ se d è divisibile dal quadrato di qualche p_i, si conclude che l'ultima espressione è esattamente $\sum_{d \mid n} \mu(d) \, \frac{n}{d}$; cioè la tesi grazie al teorema precedente. □

Molte proprietà di $\varphi(n)$ possono essere dedotte da quest'ultimo teorema.

Teorema G2.7. *La funzione di Eulero soddisfa le seguenti proprietà:*

(a) *Per ogni primo p e per ogni $e \ge 1$, risulta*

$$\varphi(p^e) = p^e - p^{e-1}.$$

(b) *Per ogni $m, n \in \mathbb{N}$ tale che $d = \mathrm{mcd}(m,n)$ si ha*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \frac{d}{\varphi(d)}.$$

(c) *La funzione φ è moltiplicativa; cioè per ogni $m, n \in \mathbb{N}$ si ha*

$$\mathrm{mcd}(m,n) = 1 \quad \Longleftrightarrow \quad \varphi(m \cdot n) \;=\; \varphi(m) \cdot \varphi(n).$$

(d) *Per ogni $m, n \in \mathbb{N}$ si ha*

$$m \mid n \qquad \Longleftrightarrow \qquad \varphi(m) \mid \varphi(n).$$

DIMOSTRAZIONE. La prima parte segue ponendo $n = p^e$ nel teorema precedente. Per provare la seconda parte scriviamo:

$$\frac{\varphi(n)}{n} = \prod_{p|n} \Big(1 - \frac{1}{p}\Big).$$

Notiamo che ogni divisore primo di $m \cdot n$ è un divisore primo di m o di n o di ambedue, e questi primi che dividono sia m che n dividono anche il $\mathrm{mcd}(m,n)$. Donde:

$$\frac{\varphi(m \cdot n)}{m \cdot n} = \prod_{p|m\cdot n} \Big(1 - \frac{1}{p}\Big)$$

$$= \quad \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|\mathrm{mcd}(m,n)} \left(1 - \frac{1}{p}\right)}$$

$$= \quad \left\{ \frac{\varphi(m)}{m} \times \frac{\varphi(n)}{n} \right\} \Big/ \left\{ \frac{\varphi(d)}{d} \right\}$$

e quindi vale la seconda formula.

La terza parte è un caso speciale della seconda. L'ultima parte segue dalla formula esplicita nel Teorema **G2.6**. □

G2.3. Permutazioni circolari e conteggio. Adesso rivediamo il problema di collane trattato nell'Esempio **F1.7**. Denotiamo la permutazione ciclica con $\pi := (1\,2 \cdots m)$. Nell'insieme delle parole lineari di lunghezza m su un alfabeto di n lettere, definiamo la seguente relazione di equivalenza: le parole $a_1\,a_2 \cdots a_m$ e $b_1\,b_2 \cdots b_m$ sono equivalenti se esiste una permutazione σ, potenza del ciclo π tale che

$$a_{\sigma(1)}\; a_{\sigma(2)} \cdots a_{\sigma(m)} = b_1\; b_2 \cdots b_m.$$

Una classe di equivalenza sarà chiamata *parola circolare.*

Sia d un divisore di m; se la parola circolare $\mathcal{C}$ è una sequenza di altre m/d parole circolari di lunghezza d, uguali tra loro, $\mathcal{C}$ è detta *periodica.* Si definisce *periodo* di $\mathcal{C}$ la più piccola delle lunghezze delle parole circolari che rendono $\mathcal{C}$ periodica.

Teorema G2.8. *Il numero di parole circolari aperiodiche di lunghezza m su n lettere è:*

$$w(m,n) \;=\; \frac{1}{m}\sum_{d|m}\mu(d)\,n^{m/d}$$

mentre il numero di parole circolari di lunghezza m su n lettere è:

$$W(m,n) \;=\; \frac{1}{m}\sum\varphi(d)\,n^{m/d}.$$
$$d|m$$

DIMOSTRAZIONE. Sia $w(d,n)$ il numero di parole circolari aperiodiche di lunghezza d, a ciascuna delle quali corrispondono d parole lineari distinte. Tutte le parole lineari di lunghezza m che si possono formare con n lettere sono in numero n^m, come sappiamo. Classificandole secondo il periodo "d", otteniamo l'identità seguente:

$$n^m \;=\; \sum_{d|m} d\,w(d,n) \qquad (\#)$$

dove d varia su tutti i divisori di m.

Da questa relazione si può ricavare $w(d,n)$ utilizzando la formula dell'inversione di Möbius nel Teorema **G2.3**. Infatti, se poniamo

$$\begin{aligned} f(m) &:= n^m, \\ g(d) &:= d\,w(d,n); \end{aligned}$$

si ottiene, invertendo la relazione (#):

$$w(m,n) \;=\; \frac{1}{m}\sum_{d|m}\mu(d)\,n^{m/d}$$

cioè la prima formula desiderata del teorema.

Classificando tutte le parole circolari di lunghezza n secondo il periodo, otteniamo immediatamente

$$W(m,n) = \sum_{d|m} w(d,n)$$

da cui procediamo come segue:

$$W(m,n) = \sum_{d|m}\frac{1}{d}\sum_{c|d} n^c\,\mu(d/c) = \sum_{c|m}\frac{n^c}{m}\sum_{\frac{d}{c}\,|\,\frac{m}{c}}\frac{m/c}{d/c}\,\mu(d/c).$$

L'ultima somma interna si riduce alla funzione di Eulero $\varphi(m/c)$ in virtù del Teorema **G2.5**. Così abbiamo completato la dimostrazione del teorema. □

G3. Principio di inclusione ed esclusione

In questa sezione vogliamo studiare una generalizzazione della formula sulla cardinalità degli insiemi finiti A e B:

$$\mid A \cup B \mid = \mid A \mid + \mid B \mid - \mid A \cap B \mid .$$

Per il reticolo $(P(S), \subseteq)$ dell'insieme delle parti (ordinate per inclusione) di un insieme finito S, vengono determinata la funzione di Möbius e presentata il principio di inclusione-esclusione (come conseguenza del teorema di inversione). Come applicazioni, vengono affrontati tre problemi:

- le permutazioni senza punti fissi, viene cioè determinato il numero delle permutazioni di un insieme finito senza punti fissi.
- il problema dei Ménages (Lucas, 1891) nel quale si chiede il numero di modi di assegnare i posti intorno ad un tavolo rotondo a n coppie in modo alternato, tale che nessun marito abbia al proprio fianco la moglie.
- la presentazione di una soluzione al problema 10770 di *American Mathematical Monthly*, riguardante la divisibilità di una somma binomiale.

G3.1. Funzione di Möbius su $(\mathcal{P}(S), \subseteq)$. Per S insieme finito, la funzione di Möbius μ per $(\mathcal{P}(S), \subseteq)$, l'insieme delle parti di S dell'Esempio **G1.9**, è data da:

$$\forall A, B \in \mathcal{P}(S): \quad \mu(A,B) = \begin{cases} (-1)^{|B\backslash A|}, & \text{se } A \subseteq B; \\ 0, & \text{se } A \not\subseteq B. \end{cases}$$

dove $B\backslash A = B \cap A^c$ (A^c è il complementare di A in S). Osserviamo che: $\mathcal{P}(S)$ è isomorfo, quando $|S| = n$, al prodotto diretto $C^n := C \otimes C \otimes \cdots \otimes C$ per n volte, dove C è la catena $C = \{0, 1\}$. Infatti, se A è un sottoinsieme di S, allora associamo ad A la sua funzione caratteristica χ_A così definita:

$$\chi_A(s) = \begin{cases} 1, & \text{se } s \in A; \\ 0, & \text{se } s \notin A. \end{cases}$$

La funzione

$$\begin{array}{rcl} \mathcal{P}(S) & \longrightarrow & C^n = C \otimes C \otimes \cdots \otimes C, \\ A & \longmapsto & \big(\chi_A(s_1), \chi_A(s_2), \cdots, \chi_A(s_n)\big); \end{array}$$

è un isomorfismo. Allora, combinando i Teoremi **G1.16** e **G1.17**, ne segue che:

$$\mu(A,B) = \prod_{i=1}^{n} \mu(\chi_A(s_i), \chi_B(s_i)) = \begin{cases} (-1)^{|B\backslash A|}, & \text{se } A \subseteq B; \\ 0, & \text{se } A \not\subseteq B. \end{cases}$$

G3.2. Principio di inclusione-esclusione. Per un numero naturale n ed $[n] = \{1, 2, \cdots, n\}$, siano Ω un insieme finito e $\Phi = \{A_1, A_2, \cdots, A_n\}$ una classe di sottoinsiemi di Ω. Definiamo i coefficienti

$$S_m := \sum_{\substack{\sigma \subset [n] \\ |\sigma| = m}} \Big| \bigcap_{j \in \sigma} A_j \Big| \quad \text{con} \quad S_0 := |\ \Omega\ | \ .$$

Inoltre, denotiamo con ω_m la cardinalità del sottoinsieme di Ω definito da

$$\Omega_m = \big\{ x \in \Omega \big| x \text{ appartiene esattamente a } m \text{ sottoinsiemi di } \{A_k\}_{k=1}^n \big\}.$$

Allora abbiamo le seguenti formule:

Teorema G3.1 (Principio di inclusione-esclusione).

(a) **Formula di Sylvester**:

$$\Big| \bigcap_{i=1}^n A_i^c \Big| \ = \ \omega_0 \ = \ \sum_{k=0}^n (-1)^k S_k.$$

(b) **Formula di Da Silva**:

$$\Big| \bigcup_{i=1}^n A_i \Big| \ = \ |\Omega| - \omega_0 \ = \ \sum_{k=1}^n (-1)^{k-1} S_k.$$

(c) **Formula di Jordan**:

$$\omega_m \ = \ \sum_{k=m}^n (-1)^{k+m} \binom{k}{m} S_k.$$

DIMOSTRAZIONE Il principio di inclusione ed esclusione si può ricavare come caso particolare del teorema dell'inversione **G1.15**. Sull'insieme delle parti di $[n]$ definiamo la funzione g nel modo seguente:

$$\forall \sigma \subseteq [n]: \quad g(\sigma) := \Big| \Big(\bigcap_{i \in \sigma} A_i \Big) \bigcap \Big(\bigcap_{i \notin \sigma} A_i^c \Big) \Big|.$$

Per come è definita, $g(\sigma)$ è il numero di elementi di Ω che appartengono agli insiemi A_i aventi indice in σ e in nessun altro. Per ogni $\sigma \subseteq [n]$, determiniamo

$$f(\sigma) \ = \ \Big| \bigcap_{i \in \sigma} A_i \Big| \ = \ \sum_{\sigma \subseteq \tau \subseteq [n]} g(\tau).$$

Il teorema d'inversione **G1.15**, costruito sull'insieme parzialmente ordinato $(\mathcal{P}([n]), \subseteq)$ ci dà:

$$\begin{aligned} g(\sigma) &= \sum_{\sigma \subseteq \tau \subseteq [n]} \mu(\sigma, \tau) f(\tau) \\ &= \sum_{\sigma \subseteq \tau \subseteq [n]} (-1)^{|\tau \setminus \sigma|} \ | \ (\cap_{i \in \tau} A_i) \ | \ . \end{aligned}$$

Per $\sigma = \emptyset$ si ha:

$$\begin{aligned} g(\emptyset) &= \left|A_1^c \cap A_2^c \cap \cdots \cap A_n^c\right| = \sum_{\emptyset\subseteq\tau\subseteq[n]} (-1)^{|\tau|}\left|(\cap_{i\in\tau} A_i)\right| \\ &= \sum_{k=0}^{n}(-1)^k \sum_{|\tau|=k} |\ (\cap_{i\in\tau} A_i)\ | = \sum_{k=0}^{n}(-1)^k S_k \end{aligned}$$

che è la formula di Sylvester.

Notando la relazione insiemistica

$$\left|A_1 \cup A_2 \cup \cdots \cup A_n\right| = |\Omega| - \left|A_1^c \cap A_2^c \cap \cdots \cap A_n^c\right|$$

otteniamo subito, dalla formula di Sylvester, la formula di Da Silva.

Se vogliamo, invece, il numero ω_m di elementi di Ω che si trovano in esattamente m degli insiemi A_k con $1 \le k \le n$, bisogna manipolare la seguente somma:

$$\begin{aligned} \omega_m &= \sum_{|\sigma|=m} g(\sigma) = \sum_{|\sigma|=m}\sum_{\sigma\subseteq\tau\subseteq[n]} (-1)^{|\tau\setminus\sigma|}\left|(\cap_{i\in\tau} A_i)\right| \\ &= \sum_{\substack{\tau\subseteq[n]\\|\tau|\ge m}}\sum_{\substack{\sigma\subseteq\tau\\|\sigma|=m}} (-1)^{|\tau|-m}\left|(\cap_{i\in\tau} A_i)\right| \\ &= \sum_{k=m}^{n}(-1)^{k-m}\binom{k}{m}\sum_{|\tau|=k}\left|(\cap_{i\in\tau} A_i)\right| \\ &= \sum_{k=m}^{n}(-1)^{k-m}\binom{k}{m} S_k \end{aligned}$$

che è la formula di Charles Jordan.

OSSERVAZIONE: La formula di Jordan è in effetti duale alla seguente:

$$S_m = \sum_{\sigma\subset[n]} \left|\bigcap_{j\in\sigma} A_j\right| = \sum_{k=m}^{n}\binom{k}{m}\omega_k$$
$$|\sigma|=m$$

che può essere stabilita tramite ragionamento combinatorio. □

Teorema G3.2 (Principio di inclusione-esclusione con funzione peso). *Introducendo una* funzione peso *su* Ω*:*

$$\begin{aligned} w : \Omega &\longrightarrow A, \\ x &\longmapsto w(c); \end{aligned}$$

dove A un anello commutativo. Per ogni sottoinsieme $X \subseteq \Omega$, definiamo il suo enumeratore *come segue:*

$$\mathcal{W}(X) = \sum_{x \in X} w(x).$$

Allora il principio d'inclusione ed esclusione ha una forma pesata con la funzione w:

$$\mathcal{W}(\omega_m) \;=\; \sum_{k=m}^{n} (-1)^{k+m} \binom{k}{m} \sum_{\substack{\sigma \subset [n] \\ |\sigma|=k}} \mathcal{W}\Big(\bigcap_{j \in \sigma} A_j \Big). \qquad \square$$

G3.3. Permutazioni senza punti fissi. Un'applicazione della formula di Sylvester si ha risolvendo il seguente problema: vogliamo calcolare il numero di permutazioni su n elementi, tra le $n!$ possibili, che non abbiano punti fissi.

Sia Ω l'insieme di tutte le permutazioni di $[n]$ con $|\Omega| = n!$. Una permutazione π di Ω ha un punto fisso $j \in [n]$ se $\pi(j) = j$. Indichiamo con $\mathcal{D}_n$ il numero delle permutazioni di $[n]$ senza elementi fissi, cioè

$$\mathcal{D}_n := \Big| \{ \pi \in \Omega \mid \forall j \in [n] : \pi(j) \neq j \} \Big|.$$

Per calcolare $\mathcal{D}_n$, consideriamo gli insiemi A_i definiti per ogni $i \in [n]$ come segue:

$$A_i := \{ \pi \in \Omega \mid \pi(i) = i \}.$$

Così dovrà essere

$$\mathcal{D}_n = \Big| A_1^c \cap A_2^c \cap \cdots \cap A_n^c \Big|$$

e possiamo applicare la formula di Sylvester.

Per definizione $S_0 := |\Omega| = n!$, mentre per ogni parte σ di $[n]$ si ha

$$\Big| \bigcap_{i \in \sigma} A_i \Big| = (n - |\sigma|)!$$

che conta il numero delle permutazioni di Ω che lasciano fissi gli elementi appartenenti a σ. Allora

$$S_k := \sum_{\substack{\sigma \subseteq [n] \\ |\sigma|=k}} \Big| \bigcap_{i \in \sigma} A_i \Big| \;=\; \binom{n}{k} (n-k)! \;=\; \frac{n!}{k!}$$

e quindi per la formula di Sylvester, si ha:

$$\mathcal{D}_n \;=\; \sum_{k=0}^{n} (-1)^k \, \frac{n!}{k!} \;=\; n! \sum_{k=0}^{n} (-1)^k \, \frac{1}{k!} \;\approx\; \frac{n!}{e}.$$

I numeri $\mathcal{D}_n$ al variare di $n \in \mathbb{N}$ sono detti *subfattoriali* in quanto verificano la ricorrenza

$$\mathcal{D}_n \;=\; n\,\mathcal{D}_{n-1} + (-1)^n$$

che è una conseguenza immediata della formula esplicita appena stabilita.

G3.4. Problema dei Ménages. Questo problema ci chiede il numero di modi di assegnare i posti intorno ad un tavolo rotondo di n signori numerati da 1 a n e delle loro rispettive consorti numerate da $1'$ a n' in modo alternato tale che nessun marito abbia al proprio fianco la moglie.

Supponiamo gli uomini già seduti; con questa ipotesi stiamo considerando il *problema dei Ménages ridotto*. Una disposizione al tavolo si può descrivere con una biiezione

$$f : [n] \;\longrightarrow\; \{1', 2', \cdots, n'\}.$$

L'uomo numero 1 si siede e alla sua destra sta la donna $f(1)$; a destra della donna $f(1)$ si siede l'uomo numero 2 alla cui destra si siede la donna $f(2)$ e così via. Poniamo

$$\begin{aligned}
1 \le i \le n: \quad & A_{2i-1} := \big\{f : [n] \to \{1', 2', \cdots, n'\} \mid f(i) = i'\big\};\\
1 \le i < n: \quad & A_{2i} \quad := \big\{f : [n] \to \{1', 2', \cdots, n'\} \mid f(i) = (i+1)'\big\};\\
i = n: \quad & A_{2n} \quad := \big\{f : [n] \to \{1', 2', \cdots, n'\} \mid f(n) = 1'\big\}.
\end{aligned}$$

Per un fissato $\sigma \subseteq [n]$, denotiamo

$$\theta(\sigma) \quad = \quad \Big|\bigcap_{i\in\sigma} A_i\Big|.$$

Se $\sigma \subseteq [n]$ non contiene due interi consecutivi della successione circolare $(1, 2, \cdots, 2n)$, abbiamo che

$$\theta(\sigma) \quad = \quad (n - |\sigma|)!$$

altrimenti $\theta(\sigma)$ si riduce allo zero.

È noto che le k-parti non contenenti due interi consecutivi della successione circolare $(1, 2, \cdots, m)$ sono in numero $\frac{m}{m-k}\binom{m-k}{k}$. Applicando la formula di Sylvester, si ha la formula di *Touchard* come segue:

$$\begin{aligned}
\big|A_1^c \cap A_2^c \cap \cdots \cap A_{2n}^c\big| &= \sum_{\sigma\subseteq[2n]}^{*} (-1)^{|\sigma|}\,\theta(\sigma) \;=\; \sum_{\sigma\subseteq[2n]}^{*} (-1)^{|\sigma|}\,\Big|\big(\bigcap_{i\in\sigma} A_i\big)\Big|\\
&= \sum_{k=0}^{n} (-1)^k \frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!
\end{aligned}$$

dove l'indice della somma condizionata da "$*$" varia nei sottoinsiemi compatibili in $[n]$; cioè, σ non contiene due interi consecutivi della successione circolare $(1, 2, \cdots, 2n)$.

Quindi la soluzione finale dei Ménages risulta

$$2 \cdot n! \sum_{k=0}^{n} (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k} (n-k)!.$$

G3.5. Problema 10770 in American Mathematical Monthly. Siano $m, n \in \mathbb{N}$ tali che $1 < m < n + \varphi(m)$, dove φ è la funzione di Eulero. Il problema 10770 di *American Mathematical Monthly* chiede di dimostrare che m divide la somma binomiale definita da

$$\sum_{k=1}^{n} (-1)^k \binom{n}{k} k^m.$$

Forniamo una soluzione utilizzando il principio di inclusione-esclusione.

La somma binomiale nel problema può essere trasformata nella somma multipla definita da

$$T(m,n) := \sum_{\substack{i_1+i_2+\cdots+i_n=m \\ i_k>0:\, k=1,2,\cdots,n}} \binom{m}{i_1, i_2, \cdots, i_n}$$

dove l'argomento della sommatoria è l'usuale coefficiente multinomiale.

Per l'equazione $x_1 + x_2 + \cdots + x_n = m$ con due numeri naturali fissati m ed n, sia Ω l'insieme delle sue soluzioni intere non negative, cioè:

$$\Omega = \Big\{ (i_1, i_2, \cdots, i_n) \in \mathbb{N}_0^n \mid i_1 + i_2 + \cdots + i_n = m \Big\}.$$

Definiamo la funzione peso $\mathcal{W}$ su Ω attraverso

$$\mathcal{W}\left[(i_1, i_2, \cdots, i_n)\right] := \binom{m}{i_1, i_2, \cdots, i_n} \quad \text{per} \quad (i_1, i_2, \cdots, i_n) \in \Omega.$$

Per $k \in [n]$, sia S_k il sottoinsieme delle n-uple di Ω nelle quali la k-esima coordinata è uguale a zero. Per il Teorema **G3.2** del principio di inclusione-esclusione con funzione di peso, abbiamo

$$T(m,n) = \mathcal{W}\Big[\bigcap_{k=1}^{n} S_k^c\Big] = \sum_{\sigma \subset [n]} (-1)^{|\sigma|}\, \mathcal{W}\Big[\bigcap_{i \in \sigma} S_i\Big]$$

dove con $|\sigma|$ denotiamo la cardinalità di $\sigma \subset [n]$.

Con $|\sigma| = n - k$ specificato da $[n] \backslash \sigma = \{\nu_1, \nu_2, \cdots, \nu_k\}$, possiamo valutare $\mathcal{W}\left[\cap_{i \in \sigma} S_i\right]$ grazie al teorema multinomiale, come segue:

$$\mathcal{W}\left[\cap_{i \in \sigma} S_i\right] = \sum_{\substack{j_1+j_2+\cdots+j_k=m \\ j_i>0:\, i=1,2,\cdots,k}} \binom{m}{j_1, j_2, \cdots, j_k} = k^m$$

che dipende solo dalla cardinalità di σ.

Classificando la multisomma rispettando la cardinalità di $\sigma \subset [n]$, abbiamo:

$$T(m,n) \;=\; \mathcal{W}\Big[\bigcap_{k=1}^{n} S_k^c\Big] \;=\; (-1)^n \sum_{k=1}^{n} (-1)^k \binom{n}{k} k^m$$

che è esattamente la trasformazione anticipata all'inizio.

In base al teorema fondamentale dell'aritmetica, possiamo scrivere:

$$m = p_1^{m_1}\, p_2^{m_2} \cdots p_\ell^{m_\ell}$$

dove i p_i sono primi distinti e gli m_i interi positivi per $i = 1, 2, \cdots, \ell$. Se possiamo mostrare che per ogni p_k della decomposizione di m, l'argomento della sommatoria (coefficiente multinomiale) di $T(m,n)$ è un multiplo di $p_k^{m_k}$, allora esso è anche un multiplo di m. Segue immediatamente che $T(m,n)$ è divisibile per m come desiderato.

Per m fissato come prima, richiamando la funzione di Eulero

$$\varphi(m) \;=\; m \prod_{k=1}^{\ell} \Big(1 - \frac{1}{p_k}\Big) \le m\, \frac{p_k - 1}{p_k} \quad \text{per} \quad k = 1, 2, \cdots, \ell$$

possiamo riformulare $m < n + \varphi(m)$ come

$$m < n\, p_k \quad \text{per} \quad k = 1, 2, \cdots, \ell$$

Allora per ogni p_k assegnato, osserviamo che esiste un indice di $\{i_1, i_2, \cdots, i_n\}$ nell'argomento della sommatoria di $T(m,n)$ il quale è più piccolo di p_k. Altrimenti, dovremmo avere

$$m = i_1 + i_2 + \cdots + i_n \ge n p_k$$

che ci induce in contraddizione con $m < n\, p_k$ già stabilito. Senza perdere di generalità, supponiamo che l'indice specificato sia i_1 con $0 < i_1 < p_k$. È facile vedere che $\binom{m}{i_1}$ è divisibile per $p_k^{m_k}$ per $m = \prod_{i=1}^{\ell} p_i^{m_i}$. Come conseguenza, l'argomento della sommatoria

$$\binom{m}{i_1, i_2, \cdots, i_n} = \binom{m}{i_1}\binom{m}{i_2, \cdots, i_n}$$

è un multiplo di $p_k^{m_k}$.

Questo conferma che $T(m,n)$ è divisibile per m con $m < n + \varphi(m)$, il quale fornisce una soluzione al problema.

G4. Spazi vettoriali e coefficiente Gaussiano

Lo scopo di questa sezione è lo studio del reticolo degli spazi vettoriali di dimensione finita su un campo finito. Si dimostra che il numero di sottospazi

è uguale al coefficiente Gaussiano. Si valuta la funzione di Möbius per il reticolo di tutti i sottospazi. Infine viene calcolato il numero delle trasformazioni lineari (iniettive, suriettive e biettive) tra due spazi vettoriali di dimensione finita, che risulta conseguentemente in due identità q-binomiali.

G4.1. Spazi vettoriali finiti su campi finiti. Di seguito riportiamo un teorema che ci permette di determinare il numero di tutti i sottospazi di uno spazio vettoriale finito.

Teorema G4.1. *Denotiamo con $V_n(q)$ lo spazio vettoriale di dimensione finita n sul campo finito $K(q)$ di q elementi* (dove q è una potenza di un primo). *Allora, per ogni k con $0 < k \leq n$, il numero dei sottospazi di $V_n(q)$ di dimensione k è il coefficiente Gaussiano:*

$$\begin{bmatrix} n \\ k \end{bmatrix} := \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q^k)(1-q^{k-1})(1-q)}.$$

DIMOSTRAZIONE. Dalle ipotesi segue che $V_n(q)$ ha q^n vettori distinti. Per determinare i sottospazi k-dimensionali di $V_n(q)$, prima determiniamo tutti i possibili insiemi $\{v_1, v_2, \cdots, v_k\}$ di k vettori linearmente indipendenti.

Tali insiemi possono essere scelti come segue: v_1 può essere qualunque dei $q^n - 1$ non zero elementi di $V_n(q)$; v_2 può essere qualunque dei $q^n - q$ vettori situato al di fuori del sottospazio generato da v_1; v_3 può essere qualunque dei $q^n - q^2$ vettori situato al di fuori del sottospazio generato da $\{v_1, v_2\}$; e così via. Donde il numero di modi in cui può essere scelto l'insieme $\{v_1, v_2, \cdots, v_k\}$ è $(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$. Adesso, ognuna di tali k-uple $\{v_1, v_2, \cdots, v_k\}$ genera un sottospazio k-dimensionale di $V_n(q)$; tuttavia, diverse k-uple possono generare lo stesso sottospazio. Infatti, più precisamente

$$(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})$$

è il numero di modi di scegliere un sottoinsieme di k elementi linearmente indipendenti di $V_k(q)$ che genera lo stesso sottospazio k-dimensionale.

Donde il numero di sottospazi k-dimensionali di $V_n(q)$ è

$$\begin{aligned} & \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} \\ = \quad & \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q^k)(1-q^{k-1})\cdots(1-q)} \end{aligned}$$

che è quanto volevamo dimostrare. □

- Il numero $\begin{bmatrix} n \\ k \end{bmatrix}$ è detto *coefficiente Gaussiano* che si riduce, quando $q \to 1$, al coefficiente binomiale ordinario.
- Dal Teorema **G4.1** segue che il numero di tutti i sottospazi di $V_n(q)$ è

$$G_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}$$

che è denominato numero di Galois.
- Indichiamo con $(L(V_n), \subseteq)$ il reticolo costituito da tutti i sottospazi dello spazio vettoriale $V_n(q)$ di dimensione finita n sul campo finito $K(q)$ con la relazione di inclusione tra sottospazi.

G4.2. Funzione di Möbius sugli spazi vettoriali. Introduciamo il lemma di Weisner (1935) per determinare la funzione di Möbius degli spazi vettoriali finiti.

Lemma G4.2 (Weisner, 1935). *Sia μ la funzione di Möbius di un "lattice" finito L con $0_L := \inf L$ e $1_L := \sup L$. Per ogni elemento $a \in L$ con $a > 0_L$ si ha*

$$\sum_{x \in L:\, x \vee a = 1_L} \mu(0_L, x) = 0.$$

DIMOSTRAZIONE. Per $a \in L$, consideriamo una doppia somma formale

$$S := \sum_{x,\, y \in L} \mu(0_L, x)\xi(x, y)\xi(a, y)\mu(y, 1_L).$$

Manipoliamo questa doppia somma in due modi diversi per arrivare al risultato desiderato.

Fissando $x \in L$ possiamo riscriverla nel modo seguente:

$$S = \sum_{x \in L} \mu(0_L, x) \sum_{a,\, x \le y \le 1_L} \mu(y, 1_L)$$

ma $y \geq a$ e $y \geq x$ se e solo se $y \geq x \vee a$ e la somma interna si riduce:

$$\sum_{a \vee x \le y \le 1_L} \mu(y, 1_L) = \begin{cases} 1, & \text{se } x \vee a = 1; \\ 0, & \text{se } x \vee a < 1. \end{cases}$$

Così S diventa la somma nell'espressione del teorema.

Invece, fissando $y \in L$ riformuliamo la doppia somma come segue:

$$S = \sum_{a \le y \le 1_L} \mu(y, 1_L) \sum_{0_L \le x \le y} \mu(0_L, x)$$

e la somma interna viene annullata poiché $y > 0_L$. Perciò $S = 0$ grazie alla condizione $0_L < a \leq y$. Confrontando le due espressioni ottenute, abbiamo il risultato di Weisner. □

Ora siamo in grado di dimostrare il seguente teorema che ci dà una formula esplicita per la funzione di Möbius sul reticolo degli spazi vettoriali finiti.

Teorema G4.3 (Funzioni di Möbius). *Sia $(L(V_n), \subseteq)$ il reticolo di tutti i sottospazi dello spazio vettoriale $V_n(q)$ di dimensione finita n sul campo finito $K(q)$ con la relazione di inclusione tra sottospazi. Per $U, W \in L(V_n)$, si ha la funzione di Möbius:*

$$\mu(U,W) = \begin{cases} (-1)^k\, q^{\binom{k}{2}}, & \text{se } U \subseteq W \text{ e } \dim(W) - \dim(U) = k; \\ 0, & \text{se } U \not\subseteq W. \end{cases}$$

DIMOSTRAZIONE. Per l'isomorfismo tra lo spazio vettoriale V_k di dimensione k e lo spazio quoziente W/U, sarà sufficiente mostrare che, per uno spazio vettoriale V di dimensione n, vale

$$\mu(0,V) = (-1)^n\, q^{\binom{n}{2}}.$$

Procediamo per induzione sulla dimensione n dello spazio vettoriale V.

Sia P un sottospazio unidimensionale di V. Per il lemma di Weisner risulta

$$\mu(0,V) = -\sum_{U \subset V:\, U \vee P = V} \mu(0,U).$$

Dall'ipotesi induttiva, il termine generale nella somma uguaglia

$$\mu(0,U) = (-1)^{\dim U}\, q^{\binom{\dim U}{2}} = (-1)^{n-1}\, q^{\binom{n-1}{2}}.$$

I soli sottospazi U oltre a V tali che $U \vee P = V$ sono quelli U di dimensione $n-1$ che non contengono P; il loro numero è uguale a

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} - \begin{bmatrix} n-1 \\ n-2 \end{bmatrix} = q^{n-1}.$$

Quest'espressione ci porta alla formula

$$\begin{aligned} \mu(0,V) &= -\sum_{U \subset V:\, U \vee P = V} \mu(0,U) \\ &= -q^{n-1} \times (-1)^{n-1}\, q^{\binom{n-1}{2}}. \end{aligned}$$

Ciò completa la dimostrazione. □

G4.3. Teorema q-binomiale. Sia $V_n(q)$ uno spazio vettoriale di dimensione finita n sul campo finito $K(q)$ di q elementi (q potenza di un primo); così $V_n(q)$ ha complessivamente q^n vettori distinti.

Sia $X(q)$ uno spazio vettoriale sullo stesso campo avente x vettori. Conteremo in due modi l'insieme di tutte le trasformazioni lineari da $V_n(q)$ a $X(q)$, ottenendo in questo modo un'identità.

Sia $T : V_n(q) \to X(q)$ una tale trasformazione lineare e sia $\{v_1, v_2, \cdots, v_n\}$ una base per lo spazio vettoriale $V_n(q)$. La trasformazione lineare T è univocamente determinata una volta che le immagini dei v_i con $i = 1, 2, \cdots, n$ sono assegnate. L' immagine di ogni v_i $(i = 1, 2, \cdots, n)$ può essere uno degli x vettori di $X(q)$, donde ci sono x^n scelte per T.

Adesso contiamo l'insieme di tutte le trasformazioni lineari T, in accordo con la dimensione dei loro nuclei. Avendo scelto un sottospazio N di dimensione k, $k \leq n$ di $V_n(q)$, l'insieme delle trasformazioni lineari T in $X(q)$ il cui nucleo è N viene contato come segue.

Siano $\{v_1, v_2, \cdots, v_n\}$ una base per $V_n(q)$ e $\{v_1, v_2, \cdots, v_k\}$ una base per il sottospazio N. Una trasformazione lineare T ha N come suo nucleo se e solo se le immagini dei vettori $\{v_1, v_2, \cdots, v_k\}$ sono nulle e nessun'altra combinazione lineare non banale dei v_i $(i = 1 + k, \cdots, n)$ viene annullata da T. Questo dà, per l'immagine di v_{k+1}, la scelta di $x - 1$ vettori, tutti appartenenti a $X(q)$ tranne il vettore nullo; per l'immagine di v_{k+2}, la scelta di $x - q$ vettori, tutti appartenenti a $X(q)$ tranne quelli della combinazione lineare ottenuta dall'immagine di v_{k+1}; per l'immagine di v_{k+3}, la scelta di $x - q^2$ vettori, tutti appartenenti a $X(q)$ tranne quelli della combinazione lineare ottenuta dalle immagini di v_{k+1} e di v_{k+2}; e così via.

Allora le trasformazioni lineari T con nucleo N sono in numero

$$(x-1)(x-q)\cdots(x-q^{n-k-1}).$$

Per il Teorema **G4.1** sappiamo che il numero di sottospazi k-dimensionali di $V_n(q)$ è $\begin{bmatrix} n \\ k \end{bmatrix}$; quindi, combinando i due conti, otteniamo l'identità cercata.

Teorema G4.4 (Teorema q-binomiale).

$$x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} (x-1)(x-q)\cdots(x-q^{n-k-1}). \qquad \square$$

Applicando la formula esplicita per la funzione di Möbius sul reticolo degli spazi vettoriali finiti, possiamo ora determinare il numero delle trasformazioni fra due spazi vettoriali di dimensioni finite.

Teorema G4.5. *Il numero delle trasformazioni lineari suriettive da uno spazio n-dimensionale V_n ad uno spazio m-dimensionale V_m sullo stesso campo finito $K(q)$ è:*

$$\sum_{k=0}^{m}(-1)^{m-k}\begin{bmatrix} m \\ k \end{bmatrix} q^{nk+\binom{m-k}{2}}.$$

DIMOSTRAZIONE. Per un sottospazio $U \subseteq V_m$ denotiamo con $g(U)$ il numero delle trasformazioni lineari da V_n a V_m, la cui immagine è U, e con $f(U)$ il numero delle trasformazioni lineari da V_n a V_m, la cui immagine è contenuta in U. Chiaramente

$$f(U) = q^{n \dim U} \qquad \text{e} \qquad f(U) = \sum_{W \subseteq U} g(W).$$

Per il Teorema di inversione di Möbius **G1.14** risulta:

$$g(U) = \sum_{W \subseteq U} \mu(W, U)\, q^{n\, dim(W)}.$$

Prendiamo $U = V_m$ e usiamo i Teoremi **G4.1** e **G4.3** per avere la tesi. □

Ricordando che i sottospazi di dimensione ℓ in V_m sono in numero $\begin{bmatrix} m \\ \ell \end{bmatrix}$, si ha subito il seguente risultato.

Corollario G4.6. *Il numero delle matrici $n \times m$ sul campo finito $K(q)$ di rango ℓ ugualia*

$$\begin{bmatrix} m \\ \ell \end{bmatrix} \sum_{k=0}^{\ell}(-1)^{\ell-k}\begin{bmatrix} \ell \\ k \end{bmatrix} q^{nk+\binom{\ell-k}{2}}.$$

Notiamo che il numero delle trasformazioni lineari iniettive ha una forma relativamente semplice. Se fissiamo una base per V_n e consideriamo le iniezioni in V_m, l'immagine dell'i-esimo vettore base ($i = 1, 2, \cdots, n$) deve essere scelto come uno fra i $(q^m - q^{i-1})$ vettori che non appartengono allo spazio delle immagini dei precedenti vettori base. In conclusione ci sono

$$(q^m - 1)(q^m - q) \cdots (q^m - q^{n-1})$$

trasformazioni lineari iniettive. Poiché il corollario precedente con $\ell = n$ dà anche un'espressione per questo numero, abbiamo provato la seguente identità:

$$(q^m - 1)(q^m - q) \cdots (q^m - q^{n-1}) = q^{n^2}\begin{bmatrix} m \\ n \end{bmatrix} \sum_{k=0}^{n}(-1)^k\begin{bmatrix} n \\ k \end{bmatrix} q^{\binom{k}{2}-kn}.$$

G5. Funzione di Möbius del reticolo delle partizioni

Sulla base del reticolo $(\mathbb{P}(X), \leq)$ delle partizioni dell'insieme finito X, studiamo, in questa sezione, la funzione di Möbius e un'applicazione al calcolo del permanente per una matrice rettangolare.

G5.1. Funzione di Möbius su $(\mathbb{P}(X), \leq)$. Sia $(\mathbb{P}(X), \leq)$ il reticolo delle partizioni dell'insieme finito X, ordinato per rifinitezza. Se due partizioni $\mathcal{B}, \mathcal{F} \in \mathbb{P}(X)$ sono ordinate come $\mathcal{B} \leq \mathcal{F}$, allora per ogni parte $F \in \mathcal{F}$, si ha per rifinitezza che $\{B \in \mathcal{B} | B \subseteq F\} \in \mathbb{P}(F)$. Questa partizione viene chiamata la restrizione di $\mathcal{B}$ a F e denotata con $\mathcal{B}(F)$.

Proposizione G5.1 (Funzione di Möbius delle partizioni). *La funzione di Möbius per il reticolo $(\mathbb{P}(X), \leq)$ è data da*

$$\mu(\mathcal{B}, \mathcal{F}) = \prod_{F \in \mathcal{F}} (-1)^{\ell(\mathcal{B}(F))-1} (\ell(\mathcal{B}(F)) - 1)!$$

dove con $\ell(\mathcal{B}(F))$ si denota il numero delle parti della partizione $\mathcal{B}(F)$.

DIMOSTRAZIONE. Data $\mathcal{F} = \{F_1, F_2, \cdots, F_\ell\} \in \mathbb{P}(X)$, supponiamo che $\mathcal{B} \leq \mathcal{F}$. Per ogni $k = 1, 2, \cdots, \ell$, si definisce $\mathcal{B}_k = \mathcal{B}(F_k)$. Si verifica facilmente che l'intervallo $[\mathcal{B}, \mathcal{F}]$ nel $(\mathbb{P}(X), \leq)$ è isomorfo al prodotto diretto:

$$[\mathcal{B}_1, F_1] \otimes [\mathcal{B}_2, F_2] \otimes \cdots \otimes [\mathcal{B}_\ell, F_\ell]$$

che è a sua volta un intervallo del reticolo

$$(\mathbb{P}(F_1), \leq) \otimes (\mathbb{P}(F_2), \leq) \otimes \cdots \otimes (\mathbb{P}(F_\ell), \leq).$$

Notiamo che ogni intervallo $[\mathcal{B}_k, F_k]$ nel $(\mathbb{P}(F_k), \leq)$ è isomorfo all'intervallo $[\mathfrak{B}_k, \mathcal{B}_k]$ del reticolo $(\mathbb{P}(\mathcal{B}_k), \leq)$, dove $\mathfrak{B}_k$ è la partizione minima (ogni parte è composta da un solo membro) dell'insieme $\mathcal{B}_k$ (delle parti di $\mathcal{B}_k$ come membri). Allora l'intervallo $[\mathcal{B}, \mathcal{F}]$ nel $(\mathbb{P}(X), \leq)$ è isomorfo al prodotto diretto:

$$[\mathfrak{B}_1, \mathcal{B}_1] \otimes [\mathfrak{B}_2, \mathcal{B}_2] \otimes \cdots \otimes [\mathfrak{B}_\ell, \mathcal{B}_\ell].$$

Quindi si ha che

$$\mu(\mathcal{B}, \mathcal{F}) = \prod_{k=1}^{\ell} \mu_k(\mathfrak{B}_k, \mathcal{B}_k)$$

dove μ_k è la funzione di Möbius del reticolo $(\mathbb{P}(\mathcal{B}_k), \leq)$ per $k = 1, 2, \cdots, \ell$. Dunque la dimostrazione si riduce a confermare che, per ogni insieme finito B, la funzione di Möbius μ_o del reticolo $(\mathbb{P}(B), \leq)$ soddisfa la relazione:

$$\mu_o(\mathfrak{B}, B) = (-1)^{|B|-1}(|B| - 1)!. \qquad \text{(A)}$$

Possiamo procedere tramite il principio di induzione su $|B|$. Quando $|B| = 1$, sia sinistra che destra di (A) si riduce ovviamente a uno. Ora sia B con

$|B| > 1$. Supponiamo, come l'ipotesi dell'induzione, che vale (A) per tutti i sottoinsiemi $F \subset B$ con $|F| < |B|$.

Sia $\mathcal{F}$ una partizione di B con $\mathfrak{B} \leq \mathcal{F} < B$. Seguendo lo stesso ragionamento di prima, possiamo verificare che l'intervallo $[\mathfrak{B}, \mathcal{F}]$ nel $(\mathbb{P}(B), \leq)$ è isomorfo al prodotto cartesiano degli intervalli $[\mathfrak{F}, F]$ per $F \in \mathcal{F}$. Allora per l'ipotesi dell'induzione, si ha che

$$\mu_o(\mathfrak{F}, \mathcal{F}) = \prod_{F \in \mathcal{F}} (-1)^{|F|-1}(|F| - 1)!. \qquad \text{(B)}$$

Ricordiamo che la funzione di Möbius soddisfa la seguente proprietà:

$$\sum_{\mathcal{F} \in \mathbb{P}(B)} \mu(\mathfrak{B}, \mathcal{F}) = 0 \quad per \quad |B| > 1. \qquad \text{(C)}$$

Fissando $x \in B$, ogni partizione $\mathcal{F}$ di B può essere considerata come un'unione della parte D contenente x con una partizione del complemento di D in B. Allora (C) equivale alla seguente ($|B| > 1$):

$$\mu_o(\mathfrak{B}, B) = - \sum_{x \in D \subset B} \mu_o(\mathfrak{D}, D) \sum_{\mathcal{F} \in \mathbb{P}(B \setminus D)} \mu_o(\mathfrak{B} \setminus \mathfrak{D}, \mathcal{F}). \qquad \text{(D)}$$

Se $|B \setminus D| > 1$, l'ipotesi dell'induzione implica che la seconda somma in (D) si riduce a zero. Qulla somma è uguale a uno se $|B \setminus D| = 1$. A questo punto, possiamo riformulare (D) come segue:

$$\begin{aligned} \mu_o(\mathfrak{B}, B) &= - \sum_{\substack{x \in D \subset B \\ |B \setminus D| = 1}} (-1)^{|D|-1}(|D| - 1)! \\ &= - \sum_{\substack{x \in D \subset B \\ |B \setminus D| = 1}} (-1)^{|B|-2}(|B| - 2)! \\ &= (-1)^{|B|-1}(|B| - 2)!\,(|B| - 1) \end{aligned}$$

che è equivalente a (A). Secondo il principio dell'induzione, abbiamo completato la dimostrazione della Proposizione. □

G5.2. Permanente. Armati con la funzione di Möbius delle partizioni, procediamo a calcolare il permanente $\mathrm{per}(A)$ per una matrice $A = [a_{ij}]$ di ordine $n \times m$ su campo complesso $\mathbb{C}$.

Denotiamo con $(\mathbb{P}[n], \leq)$ il reticolo delle partizioni di $[n] := \{1, 2, \cdots, n\}$ con la minima partizione $\mathfrak{N} = \uplus_{k=1}^{n} \{k\}$. Per ogni partizione $\mathcal{D} \in \mathbb{P}[n])$, indichiamo con $\Omega(\mathcal{D})$ tutte le applicazioni da $[n]$ a $[m]$ che sono costanti in ogni parte $D \in \mathcal{D}$ e hanno valori distinti in tutte le parti di $\mathcal{D}$. Consideriamo

la somma definita da

$$\alpha(\mathcal{D}) = \sum_{\sigma\in\Omega(\mathcal{D})}\prod_{i=1}^{n} a_{i\sigma(i)}.$$

Osservando che $\Omega(\mathfrak{N})$ consiste di tutte le n-permutazioni di $[m]$, allora vale $\mathrm{per}(A) = \alpha(\mathfrak{N})$.

Introduciamo un'altra funzione di $\mathbb{P}[n]$ tramite la matrice A:

$$\beta(\mathcal{D}) = \prod_{D\in\mathcal{D}}\sum_{j=1}^{m}\prod_{i\in D} a_{ij}.$$

Se $|D| = 2$ con $D = \{i, i\}$, allora la somma $\sum_{j=1}^{m}\prod_{i\in D} a_{ij}$ si riduce al prodotto scalare delle due righe di A indicizzate con $\imath$ e i rispettivamente.

Per ogni partizione $\mathcal{B} \in \mathbb{P}[n]$, è possibile verificare le seguenti relazioni:

$$\beta(\mathcal{B}) = \sum_{\mathcal{B}\leq\mathcal{D}} \alpha(\mathcal{D}), \tag{$\triangle$}$$

$$\alpha(\mathcal{B}) = \sum_{\mathcal{B}\leq\mathcal{D}} \beta(\mathcal{D})\mu(\mathcal{B},\mathcal{D}). \tag{∇}$$

Secondo il teorema di inversione di Möbius, (∇) è la conseguenza immediata di $(\triangle)$. Quindi dobbiamo solo stabilire $(\triangle)$.

Data una partizione $\mathcal{B} = \{B_1, B_2, \cdots, B_\ell\} \in \mathbb{P}[n]$, possiamo riscrivere la funzione $\beta(\mathcal{B})$ come segue:

$$\begin{aligned}
\beta(\mathcal{B}) &= \prod_{B\in\mathcal{B}}\sum_{j=1}^{m}\prod_{i\in B} a_{ij}\\
&= \prod_{k=1}^{\ell}\sum_{j_k=1}^{m}\prod_{i\in B_k} a_{ij_k}\\
&= \sum_{\sigma\in\Lambda(\mathcal{B})}\prod_{i=1}^{n} a_{i\sigma(i)}
\end{aligned}$$

dove $\Lambda(\mathcal{B})$ è l'insieme delle applicazioni da $[n]$ ad $[m]$ che sono costanti in ogni parte B_k della partizione $\mathcal{B} \in \mathbb{P}[n]$.

Per ogni funzione $f \in \Lambda(\mathcal{B})$, la sua immagine induce una partizione $\mathcal{D}$ del dominio, cioè un raggruppamento delle parti di $\mathcal{B}$. Si ha ovviamente che $\mathcal{B} \leq \mathcal{D}$ in $\mathbb{P}[n]$ e $f \in \Omega(\mathcal{D})$. Classificando $\Lambda(\mathcal{B})$ secondo le partizioni $\mathcal{D}$ con $\mathcal{B} \leq \mathcal{D}$:

$$\Lambda(\mathcal{B}) = \biguplus_{\mathcal{B}\leq\mathcal{D}} \Omega(\mathcal{D})$$

otteniamo la seguente relazione:

$$\beta(\mathcal{B}) = \sum_{\sigma\in\Lambda(\mathcal{B})}\prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\mathcal{B}\le\mathcal{D}}\sum_{\sigma\in\Omega(\mathcal{D})}\prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\mathcal{B}\le\mathcal{D}}\alpha(\mathcal{D}).$$

Questa è esattamente $(\triangle)$ che volevamo dimostrare. □

Sostituendo $\alpha(A)$, $\beta(A)$ e $\mu(\mathcal{B},\mathcal{D})$ con le loro espressioni esplicite, ricaviamo da (∇) la seguente formule per il calcolo del permanente.

Teorema G5.2 (Permanente). *Per una matrice $A = [a_{ij}]$ di ordine $n \times m$ su campo complesso $\mathbb{C}$, il permanente* $\mathrm{per}(A)$ *è uguale alla seguente:*

$$\mathrm{per}(A) = \sum_{\mathcal{D}\in\mathbb{P}[n]}\prod_{D\in\mathcal{D}}(-1)^{|D|-1}(|D|-1)!\sum_{j=1}^{m}\prod_{i\in D} a_{ij}.$$

G5.3. Formula di Ryser. Possiamo trattare il permanente anche per mezzo del principio d'inclusione ed esclusione.

Sia $A = (a_{ij})$ una matrice $n \times m$ su un anello commutativo. Il *permanente* di A, scritto $\mathrm{per}(A)$, è definito dalla formula

$$\mathrm{per}(A) = \sum_{\pi}\prod_{i=1}^{n} a_{i\pi(i)}$$

dove la somma è estesa a tutte le applicazioni iniettive da $[n]$ ad $[m]$ (o tutte le n-permutazioni di $[m]$). Quando $m = n$, $\mathrm{per}(A)$ è la somma dei termini (a parte il fattore alternato) che compaiono nello sviluppo del determinante di A. Inoltre, definiamo una funzione sulla matrice

$$\rho(A) = \prod_{i=1}^{n}\sum_{j=1}^{m} a_{ij}$$

che è data dal prodotto delle somme di ogni riga della matrice A.

Per $\Omega = [m]^{[n]}$, introduciamo la funzione peso

$$w(\pi) = \prod_{i=1}^{n} a_{i\pi(i)} \quad \text{per ogni} \quad \pi\in\Omega.$$

Fissando $\kappa \in [m]$, consideriamo il sottoinsieme

$$B_\kappa = \{\pi\in\Omega \mid \pi^{-1}(\kappa) = \emptyset\}.$$

Per $\sigma \subseteq [m]$, indichiamo con σ^c il complemento di σ in $[m]$. Allora non è difficile verificare che

$$\mathcal{W}\Big(\bigcap_{\kappa\in\sigma} B_\kappa\Big) = \rho(A_{\sigma^c})$$

dove A_σ è la sottomatrice di A avente gli indici delle colonne in σ; perciò, A_{σ^c} è la sottomatrice di A senza le colonne indicizzate con σ.

Per l'insieme Ω e la classe dei sottoinsiemi $\{B_1, B_2, \cdots, B_m\}$, notiamo che tutte le applicazioni iniettive da $[n]$ ad $[m]$ costituiscono Ω_{m-n}. Secondo la formula pesata del principio d'inclusione ed esclusione (vedi il Teorema **G3.2**), si ha che

$$\begin{aligned}
\mathrm{per}(A) = \mathcal{W}(\Omega_{m-n}) &= \sum_{k=m-n}^{m} (-1)^{m-n+k} \binom{k}{m-n} \sum_{\substack{\sigma\subseteq[m]\\|\sigma|=k}} \mathcal{W}\Big(\bigcap_{\kappa\in\sigma} B_\kappa\Big) \\
&= \sum_{k=m-n}^{m} (-1)^{m-n+k} \binom{k}{m-n} \sum_{\substack{\sigma\subseteq[m]\\|\sigma|=k}} \rho(A_{\sigma^c}) \\
&= \sum_{k=1}^{n} (-1)^{n-k} \binom{m-k}{m-n} \sum_{\substack{\sigma\subseteq[m]\\|\sigma|=k}} \rho(A_\sigma)
\end{aligned}$$

dove l'ultimo passaggio viene giustificato dal fatto che $\rho(A_\emptyset) = 0$ e dalla sostituzione $k \to m-k$ sull'indice della somma. Così abbiamo stabilito il seguente importante risultato.

Teorema G5.3 (Formula di Ryser). *Sia $A = (a_{ij})$ una matrice $n \times m$ su un anello commutativo. Vale la seguente formula:*

$$\mathrm{per}(A) = \sum_{\sigma\subseteq[m]} (-1)^{n+|\sigma|} \binom{m-|\sigma|}{m-n} \rho(A_\sigma).$$

Esempio G5.4. *Sia $J[n\times m]$ la matrice $n\times m$ con tutti gli elementi uguali ad uno e $I[n\times m]$ la matrice con gli elementi diagonali uguali ad uno ed altri a zero. Allora*

$$\begin{aligned}
&\mathrm{per}\,(I[n\times m]) = 1; \\
&\mathrm{per}\,(J[n\times m]) = \langle m\rangle_n = m(m-1)\cdots(m-n+1); \\
&\mathrm{per}\,(J[n\times n] - I[n\times n]) = D_n.
\end{aligned}$$

Secondo il Teorema **G5.3** e l'espressione

$$\rho(J_\sigma[n\times m]) = |\sigma|^n$$

abbiamo la seguente formula

$$\begin{aligned}\mathrm{per}(J[n\times m]) &= \sum_{k=1}^{n}(-1)^{n-k}\binom{m-k}{m-n}\sum_{\substack{\sigma\subseteq[m]\\|\sigma|=k}}\rho(A_\sigma)\\ &= \sum_{k=1}^{n}(-1)^{n-k}\binom{m}{k}\binom{m-k}{m-n}k^n\\ &= \binom{m}{n}\sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k}k^n\end{aligned}$$

che ci porta conseguentemente all'identità combinatoria:

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^n = n!.$$

□

Bibliografia

[A] G. E. Andrews, *The Theory of Partitions,* Cambridge University Press, 1976.

[B] M. Hall, *The Theory of Groups,* AMS Chelsea Publishing, 1999.

[C] G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, 1979.

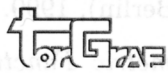
[D] N. Jacobson, *Basic Algebra* I & II (Second Edition), W. H. Freeman (New York), 1989.

[E] A. Kerber, *Applied Finite Group Actions* (Second Edition), Springer-Verlag (Berlin), 1999.

[F] I. G. Macdonald, *Symmetric Functions and Hall Polynomials* (Second Edition), Clarendon/Oxford, 1995.

[G] G. Pólya – R. C. Read, *Combinatorial Enumeration of Groups, Graghs and Chemical Compounds,* Springer–Verlag (New York/Berlin), 1987.

[H] R. P. Stanley, *Enumerative Combinatorics* I & II, Cambridge University Press, 1997/1999.



Finito di stampare nel mese di ottobre 2007
presso lo stabilimento tipolitografico della **TorGraf**
S.P. 362 km. 15,300 - Zona Industriale • 73013 **GALATINA** (Lecce)
Telefono +39 0836.561417 • Fax +39 0836.569901
e-mail: **stampa@torgraf.it**