Alma Mater Studiorum
Università di Bologna

facoltà di scienze matematiche, fisiche e naturali
Corso di Laurea in Matematica

Il teorema di Lagrange e i suoi inversi parziali

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
Verardi Libero

Presentata da:
Pasquale Franco

II Sessione
Anno Accademico 2010-2011

Introduzione

In algebra, più precisamente in teoria dei gruppi, è di fondamentale importanza il Teorema di Lagrange, il quale asserisce che, dato un gruppo finito, cioè costituito da un numero finito di elementi e quindi di *ordine finito*, l'ordine di ogni suo sottogruppo è un divisore dell'ordine del gruppo. In generale non esiste una inversione totale di questo teorema, cioè non è vero che ogni divisore dell'ordine di un gruppo è ordine di un suo sottogruppo.
Il seguente lavoro di tesi approfondisce quindi questo discorso.
Dimostreremo immediatamente la non totale invertibilità del Teorema di Lagrange fornendo a controesempio il gruppo alterno A_4, per poi elencare alcuni risultati a sostegno dell'inversione parziale del teorema. Faremo esempi più forti (è il caso dei gruppi ciclici finiti per i quali non solo esiste un sottogruppo per ogni divisore del gruppo, ma possiamo anche dimostrarne l'unicità) e meno forti (è il caso dei gruppi abeliani e dei p-gruppi) di classi di gruppi per i quali il suddetto teorema è invertibile.
Proporremo infine risultati che offrono una maggiore generalizzazione del problema, invertendo il teorema per particolari divisori. A tal proposito enunceremo e dimostreremo il Teorema di Sylow, il quale assicura l'esistenza di un sottogruppo per ogni divisore dell'ordine del gruppo che sia potenza di un primo. Per concludere enunceremo il Teorema di Hall, a sua volta generalizzazione del Teorema di Sylow, il quale dimostra l'esistenza, nel caso di gruppi risolubili, di sottogruppi di ordine un qualsiasi intero che costituisca uno spezzamento dell'ordine del gruppo in interi relativamente primi.
Ogni risultato sarà opportunamente preceduto dalle dovute premesse.

Indice

Capitolo 1

Il Teorema di Lagrange e la sua non totale invertibiltà

In questo primo capitolo riporteremo la dimostrazione del Teorema di Lagrange per i gruppi finiti e faremo vedere, attraverso un controesempio, che il teorema non è sempre invertibile.

1.1 Classi laterali e indice di un sottogruppo

Prima di enunciare il teorema di Lagrange per i gruppi finiti è bene dare le definizioni e le nozioni utili. In questa sezione definiamo le classi laterali, l'insieme quoziente e l'indice di un sottogruppo, strumenti necessari per parlare del Teorema di Lagrange.

Definizione 1.1. Siano G un gruppo ed H un suo sottogruppo. Presi $x, y \in G$, denotiamo con $\equiv_H$ la relazione binaria in G definita ponendo $x \equiv_H y \Leftrightarrow xy^{-1} \in H$.

Facciamo vedere che questa è una relazione d'equivalenza.

(i) Innanzitutto $xx^{-1}=1 \in H$ per cui $x \equiv_H x \; \forall \; x \in G$, quindi la relazione è riflessiva;

(ii) se $x \equiv_H y \Rightarrow xy^{-1} \in H$, ma $(xy^{-1})^{-1} = yx^{-1} \in H$, quindi la relazione è simmetrica;

(iii) infine, se $x \equiv_H y$ e $y \equiv_H z$ allora $xz^{-1} = (xy^{-1})(yz^{-1}) \in H \Rightarrow x \equiv_H z$ cioè la relazione è transitiva.

Abbiamo visto che la relazione $\equiv_H$ è una relazione d'equivalenza.
Le classi d'equivalenza rispetto a tale relazione sono descritte dal seguente lemma.

Lemma 1.1.1. *Siano G un gruppo e H un sottogruppo di G. Allora $\forall x \in G$ risulta: $[x]_{\equiv_H} = \{hx \mid h \in H\}$.*

Dimostrazione. Sia $y \in [x]_{\equiv_H}$. Allora $x \equiv_H y$ cioè $xy^{-1} \in H$ pertanto $y = (xy^{-1})^{-1}x \in \{hx \mid h \in H\}$.
Reciprocamente, sia $y = hx$, con $h \in H$. Allora $xy^{-1} = h^{-1} \in H \Rightarrow x \equiv_H y$ pertanto $y \in [x]_{\equiv_H}$.

□

Definizione 1.2. La classe di equivalenza $[x]_{\equiv_H}$ si dice *laterale destro* di H in G determinato da x, e si denota con Hx.
Ovviamente laterali destri distinti di H in G sono disgiunti e il loro insieme costituisce una partizione di G.

Lo stesso discorso si può fare sulla relazione d'equivalenza ${}_H\equiv$ ottenuta ponendo $x_H \equiv y \Leftrightarrow x^{-1}y \in H$ per definire i *laterali sinistri* xH di H in G.
Si dimostra che i laterali xH e Hx sono equipotenti ad H, cioè esistono due relazioni biettive $H \longmapsto Hx$ e $H \longmapsto xH$ per cui i laterali destri e sinistri hanno lo stesso numero di elementi di H.

Definizione 1.3. Sia G un gruppo e $\Re$ una relazione d'equivalenza in G. Si dice *insieme quoziente* di G rispetto ad $\Re$, e si indica con $G/\Re$, l'insieme delle classi di equivalenza su G rispetto ad $\Re$.

Lemma 1.1.2. *Siano G un gruppo e H un sottogruppo di G. Allora gli insiemi quozienti $G/\equiv_H$ e $G/_H\equiv$ sono equipotenti.*

Dimostrazione. Per la dimostrazione si veda [2], pag. 99.

□

Abbiamo quindi dimostrato che l'insieme dei laterali destri ha la stessa cardinalità dell'insieme dei laterali sinistri.

Definizione 1.4. Sia G un gruppo e H un sottogruppo di G. Si dice *indice* di H in G e si denota con $|G:H|$ il numero di laterali destri (o sinistri) di H in G.

Adesso siamo pronti ad enunciare e dimostrare il teorema di Lagrange.

1.2 Il teorema di Lagrange e il suo inverso

Teorema 1.2.1 (Lagrange)**.** *Se G è un gruppo finito e H un sottogruppo di G, allora l'ordine di H divide l'ordine di G.*
In particolare $|G| = |H| \cdot |G:H|$.

Dimostrazione. Siano $Hx_1, \ldots, Hx_t$ i laterali destri di H in G; abbiamo che $|G:H|$=t. Poiché l'insieme $\{Hx_1, \ldots, Hx_t\}$ dei laterali destri è una partizione di G, si ha $|G| = |Hx_1| + \ldots + |Hx_t|$. Ma sappiamo che $|Hx_i| = |H|$ $\forall i \leq t$ perché si può dimostrare che l'applicazione $f : H \longmapsto Hx$, definita da $f(h) = hx$ è biettiva, quindi Hx è equipotente ad H.
Allora $|G| = |H| + \ldots + |H|$ t volte, cioè $|G| = |H| \cdot t = |H| \cdot |G:H|$. Questo risultato mostra innanzitutto che $|G|$ è multiplo di $|H|$ e poi, in particolare, che vale sempre $|G| = |H| \cdot |G:H|$.

□

Abbiamo dimostrato che dato un gruppo finito G di ordine n, ogni suo sottogruppo H ha ordine un divisore di n.
Ci si può chiedere se vale il viceversa. Cioè se ogni divisore di n è ordine di

un sottogruppo di G. In generale non è così.
Possiamo dimostrare che il teorema di Lagrange non è totalmente invertibile mostrando un controesempio. Esiste un gruppo di ordine 12 che non ha sottogruppi di ordine 6: il gruppo alterno A_4.

Facciamo alcune premesse.

Definizione 1.5. Sia n un numero intero positivo. Si chiama *gruppo simmetrico* su n lettere il gruppo $S_n = S(\{1, \ldots, n\})$, cioè il gruppo costituito dall'insieme delle permutazioni di $\{1, \ldots, n\}$ con l'operazione di composizione.

Definizione 1.6. Sia $i_1, \ldots, i_l$ una successione non ordinata di l elementi distinti di $\{1, \ldots, n\}$, con $2 \leq l \leq n$. La permutazione $\gamma \in S_n$ definita da $\gamma(i_k) = i_{k+1}$ per $k = 1, \ldots, l-1$ con $\gamma(i_l) = i_1$ e $\gamma(j) = j$ se $j \notin \{i_1, \ldots, i_l\}$ è detta *ciclo di lunghezza* l e viene denotata con $(i_1, \ldots, i_l)$.

Definizione 1.7. Due cicli $(i_1, \ldots, i_l)$ e $(j_1, \ldots, j_h)$ si dicono *disgiunti* se $\{i_1, \ldots, i_l\}$ e $\{j_1, \ldots, j_h\}$ sono insiemi disgiunti.
Cicli disgiunti commutano. (Si veda [5], 8.2.5)

Teorema 1.2.2. *Ogni permutazione di S_n si può scrivere come prodotto di cicli disgiunti. La sua fattorizzazione in cicli disgiunti è unica a meno dell'ordine dei fattori.*

Dimostrazione. Per la dimostrazione si veda [5], 8.2.7.

□

Definizione 1.8. Si dice *ordine di un ciclo* in S_n la lunghezza del ciclo stesso.
Si dice *ordine di una permutazione* in S_n il minimo comune multiplo delle lunghezze di tutti i cicli che intervengono in una scomposizione della permutazione come prodotto di cicli disgiunti.

Definizione 1.9. Una *trasposizione* è un ciclo di lunghezza 2, ossia una permutazione della forma $(i\ j)$, dove $i, j \in \{1, \ldots, n\}$, ma $i \neq j$.

Si può mostrare facilmente che ogni ciclo di lunghezza l è prodotto di $l-1$ trasposizioni in questa forma: $(i_1 \ \ldots, i_l) = (i_1 \ i_l)\cdot(i_1 \ i_{l-1})\cdot\ldots\cdot(i_1 \ i_3)\cdot(i_1 \ i_2)$.

Ne viene immediatamente il seguente risultato.

Proposizione 1.2.3. *Ogni permutazione è prodotto di trasposizioni.*

Contrariamente al caso del prodotto di cicli disgiunti, in un prodotto di trasposizioni queste non sono in generale permutabili.
Ad esempio $(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3) = (1\ 3\ 2)$.
Inoltre la decomposizione di una permutazione in trasposizioni non è unica:
$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 2)(1\ 3)(1\ 2)(1\ 3)$.
C'è però una cosa che non varia al variare di questi prodotti, ed è l'essere pari o dispari il numero di trasposizioni che vi compaiono.
Infatti:

Teorema 1.2.4. *Se una permutazione è prodotto di r trasposizioni, e anche prodotto di s trasposizioni, allora $r \equiv s \pmod 2$, cioè $r - s$ è un numero pari.*

Dimostrazione. Per la dimostrazione si veda [5], 8.3.3.

□

La parità di una permutazione, cioè l'essere pari o dispari il numero di trasposizioni in cui è scomponibile, è quindi ben definita, e ciò ci permette la seguente definizione.

Definizione 1.10. Una permutazione si dice *pari* se è prodotto di un numero pari di trasposizioni. Si dice invece *dispari* se è prodotto di un numero dispari di trasposizioni.

L'applicazione tra gruppi $S_n \longrightarrow \{-1, 1\}$ ottenuta associando 1 ad una permutazione σ se questa è pari e -1 se è dispari, è quindi ben definita, e poiché un prodotto di due permutazioni σ e γ è pari se e solo se le permutazioni sono entrambe pari oppure entrambe dispari, mentre è dispari se una permutazione è pari e l'altra è dispari, la suddetta applicazione è un

omomorfismo suriettivo il cui *nucleo* è l'insieme delle permutazioni pari, che costituisce quindi un sottogruppo di S_n.

Definizione 1.11. Si chiama *gruppo alterno* A_n il sottogruppo di S_n costituito dalle permutazioni pari.

Abbiamo adesso tutti gli strumenti e le nozioni che ci sono necessari per mostrare il nostro controesempio all'inversione totale del teorema di Lagrange:

Esempio 1.1. Il gruppo alterno A_4 non ha sottogruppi di ordine 6.

Dimostrazione. A_4, il gruppo costruito sull'insieme delle permutazioni pari di S_4, ha $\left(\frac{n!}{2}\right) = 12$ elementi di cui tre elementi di periodo 2 $\big((1\ 2)(2\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)\big)$ ed otto elementi di periodo 3 $\big((1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(2\ 3\ 4)$, $(2\ 4\ 3)\big)$.
Allora $A_4 = \{$Id, $(1\ 2)(2\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$, $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(2\ 3\ 4)$, $(2\ 4\ 3)\}$
Vediamo come dovrebbe essere fatto un ipotetico sottogruppo H di A_4 di ordine $|H| = 6$.
Innanzitutto osserviamo che $V_4 = \{Id,\ (1\ 2)(2\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$, detto *sottogruppo di Klein*, è l'unico sottogruppo di A_4 che ha ordine 4. Allora H sicuramente non conterrà V_4 perché questo, essendo sottogruppo di A_4, deve esserlo anche di H, ma 4 non divide 6, quindi per V_4 non è soddisfatto il teorema di Lagrange.
Perciò H avrà al più due elementi di ordine 2. In tal caso, perché H abbia 6 elementi, è necessario aggiungere altri tre elementi e prenderli tra quelli di ordine 3. Per ognuno di questi però, portiamo nel gruppo anche il suo inverso, perciò non riusciamo a prenderne tre, che è numero dispari. Notiamo infatti che $(1\ 2\ 3)^{-1} = (1\ 2\ 4)$, $(1\ 3\ 4)^{-1} = (1\ 4\ 3)$, $(1\ 2\ 4)^{-1} = (1\ 4\ 2)$ e $(2\ 3\ 4)^{-1} = (2\ 3\ 4)$. Cioè possiamo scrivere: $A_4 = \{$Id, $(1\ 2)(2\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$, $< (1\ 2\ 3) >, < (1\ 3\ 4) >, < (1\ 2\ 4) >, < (2\ 3\ 4) >\}$. (Ad ogni modo, se H avesse due elementi di ordine 2, avrebbe anche il terzo, che è il loro prodotto, e avremmo di nuovo V_4 contenuto in H).

A questo punto è evidente che l'unico modo per costruire H è prendere un solo elemento di ordine 2 e due elementi di ordine 3, ognuno col suo inverso. Cioè prendiamo un $h \in A_4$ con $|h| = 2$ nel gruppo di Klein e due elementi $< \alpha >$ e $< \beta >$ tra i sottogruppi $< (1\ 2\ 3) >$, $< (1\ 3\ 4) >$, $< (1\ 2\ 4) >$, $< (2\ 3\ 4) >$. Ma basta fare un po' di semplici calcoli per vedere che $< \{\alpha, \beta\} >= A_4$ e che $h \neq \alpha \cdot h \cdot \alpha^{-1}$. Ma $h \in H$ e $\alpha \cdot h \cdot \alpha^{-1} \in H$ ed hanno entrambi periodo 2. Questo è assurdo perché abbiamo detto che deve esserci al massimo un elemento di periodo 2.

□

Dimostrando che A_4, gruppo di ordine 12, non ha sottogruppi di ordine 6, abbiamo provato che, in generale, non è vero che ogni divisore dell'ordine di un gruppo è ordine di un suo sottogruppo.
Il teorema di Lagrange non è totalmente invertibile.

Capitolo 2

L'inversione del Teorema di Lagrange per classi di gruppi

In questo secondo capitolo analizzeremo delle classi di gruppi per le quali il teorema di Lagrange è invertibile.
Il primo esempio, i *gruppi ciclici*, è il più forte, perché se è vero che ogni divisore dell'ordine di un gruppo ciclico finito è ordine di un suo sottogruppo, è anche vero che questo sottogruppo è unico.
Negli altri due esempi, quello dei *gruppi abeliani* e quello dei *p-gruppi* non vale l'unicità e per ogni divisore dell'ordine di un gruppo esiste più di un sottogruppo.

2.1 I gruppi ciclici

Prima di dimostrare che i gruppi ciclici sono una delle classi di gruppi per cui il teorema di Lagrange è invertibile, introduciamoli brevemente.

Definizione 2.1. Sia G un gruppo e $a \in G$ un suo elemento.
Il *sottogruppo generato da a in G* è l'insieme $< a >= \{a^n | n \in \mathbb{Z}\}$ di tutte le potenze di a.

Definizione 2.2. Un gruppo G si dice *ciclico* se esiste un elemento $x \in G$ tale che $< x >= G$

Definizione 2.3. Se il gruppo $< x >$ è finito di ordine n si dice che l'elemento x ha *periodo* (o ordine) finito n.

Si dimostra che, a meno di isomorfismi, gli unici esempi di gruppi ciclici sono $\mathbb{Z}_n$ (a cui sono isomorfi tutti i gruppi ciclici finiti di ordine n) e $\mathbb{Z}$ (a cui sono isomorfi tutti i gruppi ciclici non finiti).
Un gruppo isomorfo ad un gruppo ciclico è anch'esso ciclico. Ad esempio i gruppi delle *radici n-esime dell'unità* e quello delle *rotazioni* sono, in quanto isomorfi a $\mathbb{Z}_n$, gruppi ciclici.

Lemma 2.1.1. *Un gruppo ciclico $G =< x >$ è finito se e solo se esiste un numero intero positivo m tale che $x^m = 1$.*

Dimostrazione. Se G è finito, esistono due numeri interi relativi h e k tali che $x^h = x^k$. Supposto per fissare le idee $h > k$, si ha $m = h - k > 0$ e $x^m = x^{h-k} = x^h(x^k)^{-1} = 1$.
Reciprocamente, esista un numero intero positivo m tale che $x^m = 1$. Qualunque sia il numero intero relativo n, si ha $n = mq + r$, con q ed r numeri interi tali che $0 \leq r < m$. Allora $x^n = x^{mq+r} = (x^m)^q x^r = x^r$, per cui $G = \{x^0, x^1, \cdots, x^{m-1}\}$ è finito.

□

Teorema 2.1.2. *Sia $G =< x >$ gruppo ciclico finito di ordine m. Allora $G = \{x^0, x^1, \ldots, x^{m-1}\}$ e m è il minimo intero positivo tale che $x^m = 1$.*

Dimostrazione. Per il lemma precendente l'insieme I dei numeri interi positivi i tali che $x^i = 1$ non è vuoto, e quindi è dotato di un minimo t. Poiché $x^t = 1$, come nella dimostrazione precedente si ottiene che G è l'insieme $\{x^0, x^1, \ldots, x^{t-1}\}$. D'altra parte, se $0 \leq i \leq j < t$ e $x^i = x^j$, risulta $x^{j-i} = x^j(x^i)^{-1} = 1$, con $0 \leq j - i < t$, per cui $j - i = 0$ e $i = j$. Pertanto gli elementi $x^0, x^1, \ldots, x^{t-1}$ sono a due a due distinti. Poichè G ha ordine m, si ha $t = m$, sicchè $G = \{x^0, x^1, \ldots, x^{m-1}\}$ e m è il minimo intero positivo per

cui $x^m = 1$.

□

Possiamo adesso dimostrare il risultato che ci interessa, cioè che un divisore dell'ordine di un gruppo ciclico finito è sempre ordine di un suo sottogruppo, e che questo sottogruppo è unico.

Teorema 2.1.3. *Sia G un gruppo ciclico di ordine m e sia d un divisore positivo di m. Allora G possiede un unico sottogruppo di ordine d.*

Dimostrazione. Se x è un generatore di G allora per il teorema precedente m è il più piccolo intero positivo tale che $x^m = 1$. Essendo d un divisore di m allora esiste un n tale che $m = n \cdot d$. Consideriamo il sottogruppo $H =< x^n >$ di G. Si ha che $(x^n)^d = x^m = 1$, e se prendiamo un intero h tale che $1 \leq h < d$ abbiamo che $n \cdot h < m$. Quindi $(x^n)^h = x^{n \cdot h} \neq 1$. Questo vuol dire che d è il più piccolo intero positivo tale che $(x^n)^d = 1$ e, per il teorema precedente, H ha ordine d.
Ogni divisore d dell'ordine di G è ordine di un sottogruppo di G.
Sia ora K un qualsiasi altro sottogruppo di G di ordine $|K| = d$. Allora esisterà un intero k tale che $K =< x^k >$. Abbiamo così che $x^{k \cdot d} = (x^k)^d = 1 = x^0$. Questo vuol dire che $k \cdot d \equiv 0 \pmod{m}$, cioè che $k \cdot d$ è multiplo di m. Esisterà perciò un intero q tale che $k \cdot d = m \cdot q$, ovvero $k = \frac{m}{d} \cdot q \Rightarrow k = n \cdot q$. Quindi $x^k = x^{nq} = (x^n)^q$ appartiene ad H.
Ne segue che K è contenuto in H, ma essendo $|H| = |K| = d$, risulta che $K = H$.

□

2.2 I gruppi abeliani

In questa sezione faremo vedere che anche per i gruppi abeliani il teorema di Lagrange è invertibile, cioè che un divisore dell'ordine di un gruppo abeliano finito è sempre ordine di un sottogruppo del gruppo.
Prima però bisogna fare delle premesse su alcune caratteristiche particolari

dei sottogruppi di gruppi abeliani e dare l'importante definizione di gruppo quoziente, consequenzialmente legata a quella di insieme quoziente proposta nella prima sezione del primo capitolo.

Definizione 2.4. Un sottogruppo H di un gruppo G si dice *normale in* G, e si scrive $H \lhd G$, se $aHa^{-1} = H \ \forall \ a \in G$.

Questo equivale a dire che $aH = Ha \ \forall \ a \in G$, cioè che laterali sinistri e destri di ogni elemento a di G coincidono.
È ovvio che in un gruppo abeliano questo risultato, che i laterali destri e sinistri coincidano, si ottiene sempre, il che dimostra che in un gruppo abeliano ogni sottogruppo è normale.
In definitiva è facile dimostrare che se H è un sottogruppo normale di un gruppo G allora sono equivalenti le seguenti condizioni:

1. $xHx^{-1} = H \ \forall \ x \in G$;
2. $xHx^{-1} \subseteq H \ \forall \ x \in G$;
3. $\forall \ x \in G \ \exists \ y \in G$ tale che $xH = Hy$;
4. $xH = Hx$;
5. ${}_H\equiv = \equiv_H$, cioè le due relazioni coincidono. (Si veda [3], 2.2)

Se $H \lhd G$, e quindi $xH = Hx \ \forall \ x \in G$, allora la relazione $\equiv_H$ (che coincide con ${}_H\equiv$) si denota con $\equiv \pmod H$.
La classe di x in $G/_{\equiv \pmod H}$ è $[x]_{\equiv \pmod H} = xH = Hx$ e prende il nome di *classe bilaterale*.
Osserviamo che il prodotto di due classi bilaterali è ancora una classe bilaterale, infatti se prendiamo $x, x', y, y' \in G$ tali che $Hx = Hx'$, cioè $x \equiv x' \pmod H$ cioè $xx'^{-1} \in H$, e $Hy = Hy'$, cioè $y \equiv y' \pmod H$ cioè $yy'^{-1} \in H$, abbiamo che $xy(x'y')^{-1} = x(yy'^{-1})x'^{-1} \in xHx'^{-1} = Hxx'^{-1} = H$.
Questo vuol dire che la relazione $\equiv \pmod H$ è compatibile con il prodotto

definito come $Hx \cdot Hy = H \cdot xy$, il quale, adottando $H = H \cdot 1$ come elemento neutro, soddisfa anche gli altri assiomi di gruppo; in particolare vale che $(Hx)^{-1} = Hx^{-1}$.
Pertanto $G/_{\equiv \pmod H}$ possiede la struttura di un gruppo che prende il nome di *gruppo quoziente* di G rispetto ad H e si denota con G/H.
È chiaro che, in relazione ad un sottogruppo normale, il gruppo quoziente è sempre ben definito. Questo ci consente di dire che un gruppo abeliano si può quozientare con qualsiasi suo sottogruppo.
Infine è utile notare che il Teorema di Lagrange ci assicura che

$$|G/H| = |G : H| = \frac{|G|}{|H|}.$$

Torniamo ora al nostro interesse primario di dimostrare che esiste una inversione parziale del Teorema di Lagrange per il caso particolare dei gruppi abeliani finiti.
Per dimostrare il teorema che, dato un gruppo abeliano finito, ci assicura l'esistenza, per ogni divisore dell'ordine del gruppo, di un sottogruppo di ordine quel divisore, abbiamo bisogno di un paio di lemma di carattere meno generale. Entrambi assicurano l'esistenza di un sottogruppo di ordine primo, ma uno lo fa per un qualsiasi tipo di gruppo finito, mentre il secondo, il Lemma di Cauchy-Galois, lo fa per i gruppi abeliani di ordine un multiplo di quel numero primo.

Lemma 2.2.1. *Sia G un gruppo finito non identico. Allora G possiede un sottogruppo di ordine primo.*

Dimostrazione. Sia x un elemento di $G \setminus \{1\}$. Allora $< x >$ è un gruppo ciclico finito di ordine $n > 1$. Ora, se p è un divisore primo di n, per il Teorema 2.1.3 si ha che $< x >$ possiede un sottogruppo di ordine p, che ovviamente è sottogruppo anche di G.

□

Lemma 2.2.2 (Cauchy-Galois)**.** *Sia G un gruppo abeliano finito di ordine m, e sia p un divisore primo di m. Allora G possiede un sottogruppo di ordine p.*

Dimostrazione. L'asserto è banale se m è un numero primo. Infatti, poiché un gruppo abeliano di ordine primo è sempre ciclico (si veda [5], 3.5.7), con m primo ci ricondurremmo al caso trattato nella sezione precedente riguardante i gruppi ciclici.
Allora procediamo per induzione sull'ordine m di G.
Per il lemma precedente il gruppo G contiene un sottogruppo H di ordine un primo q, e si può ovviamente supporre $q \neq p$. Allora p, che divide m, divide anche l'ordine $|G/H|$ del gruppo quoziente G/H. Ma $|G/H| = |G : H| = \frac{|G|}{|H|} = \frac{m}{q}$ per il Teorema di Lagrange.
Abbiamo quindi che p divide $\frac{m}{q}$.
Per ipotesi induttiva G/H possiede un sottogruppo K/H di ordine p. Cioè $|K/H| = \frac{|K|}{|H|} = p$ e si ha $|K| = p \cdot |H| = p \cdot q$.
Pertanto K è un gruppo abeliano di ordine pq.
Allora K è ciclico, perchè un gruppo abeliano di ordine pq con p e q numeri primi distinti è sempre ciclico (si veda [2], Corollario 4.12.9, pag. 135).
Sempre il teorema 2.1.3 ci assicura infine che K possiede un sottogruppo di ordine p, che è ovviamente anche sottogruppo di G.

□

Giungiamo adesso al teorema che ci interessa.

Teorema 2.2.3. *Sia G un gruppo abeliano finito di ordine m, e sia d un divisore positivo di m. Allora G possiede un sottogruppo di ordine d.*

Dimostrazione. L'enunciato è ovvio per $d = 1$.
Supponiamo $d > 1$ e procediamo per induzione su d.
Sia p un divisore primo di d. Per il Lemma di Cauchy-Galois il gruppo G possiede sicuramente un sottogruppo H di ordine p. Poichè $\frac{d}{p}$ è un numero intero che divide l'ordine $\frac{m}{p}$ di G/H, l'ipotesi induttiva ci assicura che G/H possiede un sottogruppo K/H di ordine $\frac{d}{p}$.

È chiaro allora che K è un sottogruppo di ordine d di G.

□

Con questo teorema abbiamo dimostrato che, limitatamente al caso dei gruppo abeliani, esiste un'inversione parziale del Teorema di Lagrange.
Ma questo dei gruppi abeliani è un esempio più debole di quello dei gruppi ciclici precedentemente esposto. Infatti il teorema 2.2.3 non assicura l'unicità del sottogruppo di ordine un divisore del gruppo.
Quindi, diversamente da quanto avviene per i gruppi ciclici finiti, un gruppo abeliano può ammettere sottogruppi dello stesso ordine. Ad esempio $V_4 = \{Id,\ (1\ 2)(2\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$, il gruppo di Klein citato nell'esempio 1.1, contiene ben tre sottogruppi di ordine 2.

2.3 I p-gruppi

Analizzeremo adesso un terzo ed ultimo esempio di classe di gruppi per i quali è possibile invertire il Teorema di Lagrange: i *p-gruppi*.
Sono gruppi il cui ordine è una potenza di un numero primo, ad esempio gruppi di ordine $25 = 5^2$ oppure $27 = 3^3$ o $169 = 13^2$.
In generale un gruppo G è un *p-gruppo* se $|G| = p^n$ con p primo e $n \in \mathbb{N}$.

Facciamo alcune premesse.

Definizione 2.5. Dati un gruppo G ed un insieme X, chiamiamo *azione di gruppo* di G su X (o semplicemente azione di G su X) ogni applicazione $\mu : X \times G \longrightarrow X$ tale che, $\forall g, h \in G$ e $\forall x \in X$, valgano le seguenti proprietà:

a) $\mu(x, gh) = \mu(\mu(x, g), h)$;

b) $\mu(x, 1_G) = x$.

Denotando con x^g l'immagine $\mu(x, g)$ della coppia (x, g), le due proprietà a) e b) diventano rispettivamente:

a) $x^{gh} = (x^g)^h$;

b) $x^{1_G} = x$.

Si dice allora che G *agisce su* X o che X è un $G-$*insieme*.

La nozione di gruppo che agisce su un insieme generalizza quella di gruppo di permutazioni di un insieme, cioè nelle azioni di gruppi su un insieme può accadere che esista qualche elemento $g \in G$, $g \neq 1_G$, tale che $x^g = x \ \forall x \in X$ (se G è un gruppo di permutazioni, questo fatto implica $g = 1$).

Teorema 2.3.1. *Se un gruppo G agisce su un insieme X, ogni elemento di G dà luogo ad una permutazione di X. Più precisamente, la corrispondenza*

$$\tau_g : X \longrightarrow X$$

$$x \longmapsto x^g$$

è, per ogni fissato $g \in G$, una permutazione di X. Cioè $\tau_g \in S_X$.

Dimostrazione. Una permutazione su un generico insieme X è una biezione da X su X, cioè un'applicazione iniettiva e suriettiva. Dobbiamo quindi dimostrare che $\tau_g : X \longrightarrow X$, con $\tau_g(x) = x^g$ è una funzione iniettiva e suriettiva $\forall g \in G$.
Siano $g \in G$ e $x, y \in X$ tali che $x^g = y^g$. Allora:
$x^g = y^g \Rightarrow (x^g)^{g^{-1}} = (y^g)^{g^{-1}} \Rightarrow x^{gg^{-1}} = y^{gg^{-1}} \Rightarrow x^{1_G} = y^{1_G} \Rightarrow x = y$ quindi τ_g è iniettiva.
Inoltre, se $x \in X$, sia $y = x^{g^{-1}}$. Allora $y^g = (x^{g^{-1}})^g = x^{g^{-1}g} = x^{1_G} = x$, cioè x proviene da y e quindi τ_g è suriettiva.
Dunque $\tau_g : X \longrightarrow X$ è biettiva.

□

Siano ora S_X il gruppo simmetrico su $X = \{x_1, x_2, x_3, \ldots\}$ e G un gruppo che agisce su X.

In base al teorema precedente possiamo prendere in considerazione l'applicazione $\tau : G \longrightarrow S_X$ ottenuta associando ad ogni elemento $g \in G$ la permutazione τ_g di X:

$$\tau : G \longrightarrow S_X$$

$$g \longmapsto \tau_g$$

cioè

$$g \longmapsto \begin{pmatrix} x_1 & x_2 & x_3 & \dots \\ {x_1}^g & {x_2}^g & {x_3}^g & \dots \end{pmatrix}.$$

Questa applicazione è detta *rappresentazione di G come gruppo di permutazioni su X* ed è un omomorfismo di gruppi (è facile vedere che al prodotto di due elementi di G corrisponde il prodotto delle due permutazioni che li rappresentano, cioè $\tau(g \cdot h) = \tau(g) \cdot \tau(h)$).
Il nucleo di τ, che si chiama *nucleo dell'azione*, è dato da

$$K = \{g \in G \mid x^g = x \ \forall \ x \in X\}$$

e, per il teorema d'omomorfismo, risulta essere un sottogruppo normale di G.

Esempio 2.1 (Azione per moltiplicazione a destra)**.** Fissiamo X uguale all'insieme degli elementi del gruppo G (cioè il suo insieme sostegno) e definiamo un'azione di G su X in questo modo:

$$\forall x, g \in G : x^g = x \cdot g.$$

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

- Per ogni $x \in X$ e $g, h \in G$, vale $(x^g)^h = (xg)^h = (xg)h = x(gh) = x^{gh}$;
- Per ogni $x \in X$ e dato l'elemento neutro 1_G di G, si ha che $x^{1_G} = x \cdot 1_G = x$.

Quella qui definita è quindi un'azione di gruppo che prende il nome di *azione per moltiplicazione a destra* dal momento che si ottiene moltiplicando a destra gli elementi di G per un elemento fissato. Il nucleo dell'azione è l'identità 1_G di G quindi l'omomorfismo $G \longrightarrow S_X$ è un isomorfismo tra G e un sottogruppo del gruppo simmetrico S_G. Tale isomorfismo prende il nome di *rappresentazione regolare destra di G*.

Definizione 2.6. Se G agisce su un insieme X e $x \in X$, si chiama *orbita di* x sotto l'azione di G, e si indica con x^G, il sottoinsieme di X così definito:

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

cioè l'insieme degli elementi di X in cui x è portato dai vari elementi di G. Allora si deduce che

$$X = \bigcup_{x \in X} x^G.$$

Definizione 2.7. Il numero cardinale $|x^G|$ di x^G si dice *lunghezza dell'orbita* di x.

Definizione 2.8. Siano G un gruppo e X un insieme. Prendiamo $x, y \in X$ e consideriamo la relazione binaria $\backsim$ definita in X ponendo $x \backsim y \Leftrightarrow \exists\ g \in G$ tale che $y = x^g$.
Si prova facilmente che questa è una relazione di equivalenza in X, e si nota che le sue classi d'equivalenza altro non sono che le orbite degli elementi di X sopra definite.

L'azione di un gruppo G su un insieme X induce, quindi, una partizione su X, dunque

$$X = \bigcup_{x \in T} x^G.$$

dove T è un insieme di rappresentanti delle orbite di X.
In particolare, se X è finito, si ottiene

$$|X| = \sum_{x \in T} |x^G|.$$

Definizione 2.9. Sia G un gruppo che agisce su un insieme X. Dato $x \in X$, si chiama *stabilizzatore di* x, e si indica con $St_G(x)$, il sottoinsieme di G così definito:

$$St_G(x) = \{g \in G \mid x^g = x\}.$$

Si tratta cioè dell'insieme degli elementi di G che fissano x.

Si dimostra che lo stabilizzatore è un sottogruppo di G.
Osserviamo che se un elemento di G appartiane allo stabilizzatore di ogni elemento di X, allora appartiene al nucleo dell'azione, e viceversa.
Pertanto, il nucleo dell'azione è l'intersezione degli stabilizzatori di tutti gli elementi di X:

$$\bigcap_{x \in X} St_G(x).$$

Ora possiamo fare lo stesso tipo di discorso con un altro tipo di relazione d'equivalenza: il coniugio.

Definizione 2.10. Sia G un gruppo e siano x, y elementi di G. Denotiamo con C_G la relazione binaria definita in G ponendo $xC_Gy \Leftrightarrow \exists g \in G$ tale che $y = g^{-1}xg$.
Si prova facilmente che questa è una relazione d'equivalenza in G, che chiamiamo *relazione di coniugio*, le cui classi di equivalenza si dicono *classi di coniugio* e si denotano con $[x]_{C_G}$.

Definizione 2.11. Dato un gruppo G si chiama *azione per coniugio* in G l'azione di G sul suo insieme sostegno definita come $\rho : G \times G \longrightarrow G$ tale che $\rho(g, x) = x^g = g^{-1} \cdot x \cdot g \ \forall \ g, x \in G$.
Vale infatti $x^{gh} = (gh)^{-1}x(gh) = h^{-1}(g^{-1}xg)h = h^{-1}x^g h = (x^g)^h$.

È evidente che le orbite dell'azione di coniugio altro non sono che le classi di coniugio, mentre abbiamo una nuova definizione per lo stabilizzatore:

Definizione 2.12. Sia G un gruppo che agisce per coniugio sul suo insieme sostegno G. Dato $x \in G$, Lo stabilizzatore di x,

$$St_G(x) = \{g \in G \mid g^{-1}xg = x\}$$

prende il nome di *centralizzante di x in G* e si denota con $C_G(x)$.
Si tratta cioè dell'insieme degli elementi di G che commutano con x. Infatti $g^{-1}xg = x \Leftrightarrow xg = gx$.

Si dimostra che il centralizzante è un sottogruppo di G. (Si veda [2], pag. 107).

Definizione 2.13. Dato un gruppo G si chiama *centro di G* il suo sottoinsieme così definito:

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

Si tratta cioè del sottoinsieme composto dagli elementi di G che commutano con tutti gli elementi di G.

Si dimostra che $Z(G)$ è un sottogruppo abeliano ed anche un sottogruppo normale di G.
È evidente che si ha

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

e quindi in questo caso il nucleo dell'azione coincide con il centro del gruppo.

Riportiamo ora la dimostrazione di una proposizione che ci sarà molto utile per provare una importante proprietà del centro dei p-gruppi finiti non identici.

Proposizione 2.3.2. *Siano G un gruppo e a un elemento di G. Allora la classe di coniugio $[a]_{C_G}$ di a è equipotente all'insieme $G/\equiv_{C_G(a)}$ dei laterali destri di $C_G(a)$ in G.*

Dimostrazione. Siano $x, y \in G$. Si ha $x \equiv_{C_G(a)} y \Leftrightarrow xy^{-1} \in C_G(a)$.
Cioè $C_G(a)x = C_G(a)y \Leftrightarrow xy^{-1} \in C_G(a)$, ma questo avviene se e solo se $axy^{-1}a^{-1} = xy^{-1} \Leftrightarrow axy^{-1} = xy^{-1}a \Leftrightarrow ax = xy^{-1}ay \Leftrightarrow x^{-1}ax = y^{-1}ay$.
Allora l'applicazione

$$\phi : G/\equiv_{C_G(a)} \longrightarrow [a]_{C_G}$$

$$C_G(a)x \longrightarrow x^{-1}ax$$

è ben definita e risulta iniettiva.
ϕ è poi suriettiva, perchè se prendiamo b coniugato di a, si ha sempre $b = x^{-1}ax = \phi(C_G(a)x)$ per qualche x in G. Allora ϕ è biettiva e gli insiemi $[a]_{C_G}$ e $G/\equiv_{C_G(a)}$ sono equipotenti.

□

Ovviamente questo risultato è valido anche in generale per qualsiasi azione di gruppo. Cioè la cardinalità dell'orbita di un elemento x è sempre uguale all'indice dello stabilizzatore di x nel gruppo.
Inoltre per il Teorema di Lagrange vale che l'ordine di G è uguale per ogni elemento dell'insieme al prodotto dell'indice dello stabilizzatore per l'ordine dello stabilizzatore stesso. Essendo la cardinalità dell'orbita di un elemento x sempre uguale all'indice dello stabilizzatore di x, si ha infine che

$$|G| = |x^G| \cdot |St_g(x)| \ \forall x \in X.$$

Adesso passiamo a parlare strettamente di p-gruppi e della parziale invertibilità del teorema di Lagrange, dimostrando una particolare proprietà del centro di un p-gruppo finito.

Proposizione 2.3.3. *Sia p un numero primo e sia G un p-gruppo finito non identico. Allora $Z(G) \neq 1$.*

Dimostrazione. Abbiamo che $|G| = p^n$ con p primo, $n \in \mathbb{N}$ e p^n finito.
Sia x$\in G$. Per la proposizione 2.3.2 la classe di coniugio $[x]_{C_G}$ è equipotente all'insieme dei laterali destri di $C_G(a)$ in G. Poiché G è finito risulta $|[x]_{C_G}| = |G : C_G(x)|$ quindi $|G| = |C_G(x)| \cdot |[x]_{C_G}|$ per il Teorema di Lagrange, il che vuol dire che $|[x]_{C_G}|$ divide $|G| = p^n$.
Allora esiste un $k \in \mathbb{N}$ tale che $|[x]_{C_G}| = p^k$.
Essendo le classi di coniugio una partizione di G, si ha che

$$G = \bigcup_{i=1}^{r} [x_i]_{C_G} \Rightarrow p^n = |G| = \sum_{i=1}^{r} |[x_i]_{C_G}| = p^{k_1} + \ldots + p^{k_r}.$$

Ma tra le classi di coniugio di cui G è unione disgiunta, c'è anche $[1_G]_{C_G}$ che ha ordine $|[1_G]_{C_G}| = 1 = p^0$. Allora $p^n = 1 + p^{k_2} + \ldots + p^{k_r}$, ma deve esserci almeno un altro $p^{k_i} = 1$ altrimenti p dividerebbe 1. Questo vuol dire che almeno un altro elemento appartiene a $Z(G)$ perché $|[x_i]_{C_G}| = 1 \Leftrightarrow x \in Z(G)$. Infatti se $x \in Z(G) \Rightarrow xg = gx \; \forall \; g \in G$ e la sua classe di coniugio è composta soltanto da x stesso.
Possiamo quindi concludere che $Z(G) \neq 1$.

□

A questo punto possiamo esporre il risultato che ci interessa.

Proposizione 2.3.4. *Sia G un p-gruppo, cioè tale che $|G| = p^n$ con p primo ed $n \in \mathbb{N}$. Allora $\forall \; 0 \leq k \leq n$ esiste un sottogruppo K di ordine p^k.*
Cioè $\forall \; p^k$ divisore di p^n esiste un sottogruppo di G di ordine p^k.

Dimostrazione. Se $n = 0$ abbiamo il gruppo identico $G = \{1_G\}$ di ordine $|\{1_G\}| = 1 = p^0$ e l'asserto è vero.
Procediamo allora per induzione su n.
Se $k = 0$, si ha $K = \{1_G\}$. Consideriamo quindi il caso $k > 0$.
Dal momento che $Z(G)$ è sottogruppo di G, per il Teorema di Lagrange l'ordine di $Z(G)$ divide l'ordine di G, cioè $|Z(G)| \;\Big|\; p^n = |G|$.
Allora $|Z(G)| = p^t$ per qualche $t \neq 0$ perchè $Z(G) \neq 1$. Ora, essendo $Z(G)$ abeliano si ha, per il teorema 2.2.3, che un sottogruppo H di $Z(G)$ con $|H| = h$ che divida p^t esiste $\forall \; h$ che divide p^t.
Siccome $p \;\Big|\; p^t$ allora esiste anche un sottogruppo H_p di $Z(G)$ con $|H_p| = p$.
Ma $H_p \lhd G$ e possiamo quindi considerare G/H_p che ha ordine

$$|G/H_p| = \frac{|G|}{|H_p|} = \frac{p^n}{p} = p^{n-1}.$$

Per ipotesi induttiva esiste in G/H_p un sottogruppo K/H_p di ordine $\frac{p^k}{p} = p^{k-1}$. Questo significa che $\forall \; 0 \leq k \leq n$ esiste K sottogruppo di ordine p^k di G.

□

Per i p-gruppi finiti il Teorema di Lagrange è chiaramente invertibile.
Ma anche in questo caso, come abbiamo visto per i gruppi abeliani, non vale l'unicità, come mostra ancora lo stesso gruppo di Klein di ordine $4 = 2^2$.
Anzi, possiamo dimostrare che c'è l'unicità se e solo se il p-gruppo è ciclico.
Infatti, se G non è ciclico allora esistono due elementi $x, y \in G$ tali che $< x > \subsetneq < y >$ e $< x > \supsetneq < y >$.
Ora sia $|x| = p^h$ e $|y| = p^k$. Se $h = k$ siamo a posto perché si ottiene $< x > \neq < y >$. Se invece ad esempio $h > k$, allora $< x^{p^{h-k}} >$ ha ordine p^k, ma è diverso da $< y >$ perché è sottogruppo di $< x >$ mentre $< y >$ non lo è.
Quindi se il p-gruppo non è ciclico non vale l'unicità.

Lo stesso accade per i gruppi abeliani finiti:
Sia A un gruppo abeliano per il quale valga l'unicità. Sia $|A| = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$, con $p_i \neq p_j$ primi. Sia poi P_i il sottogruppo di A con $|P_i| = p_i^{k_i}$, allora P_i è un $p_i - gruppo$ con l'unicità $\Rightarrow P_i$ è ciclico: $P_i =< x_i >$.
Pertanto A è prodotto diretto di sottogruppi ciclici con gli ordini coprimi, ed è quindi ciclico: $A =< x >$ con $x = x_1 \cdot \ldots \cdot x_r$.

Ovviamente, come si è gia detto, quelli trattati in questo capitolo non sono che esempi di classi di gruppi per i quali il Teorema di Lagrange è invertibile. Ci sono altri gruppi che soddisfano l'inverso del teorema senza essere né abeliani né p-gruppi né tantomeno ciclici: due semplici esempi sono il gruppo S_3 ed S_4. S_3 ha ordine $|S_3| = 3! = 6$ ed ha sottogruppi di ordine 1, 2, 3 e 6, mentre S_4 ha ordine $|S_4| = 4! = 24$ ed ha sottogruppi di ordine 1, 2, 3, 4, 6, 8, 12 e 24.
In particolare per quest'ultimo gruppo si ha:
di ordine 1: $< Id >$;
di ordine 2: $< (1\ 2) >$;
di ordine 3: $< (1\ 2\ 3) >$;
di ordine 4: $< 1\ 2\ 3\ 4 >$;

di ordine 6: $\{\alpha \in S_4 \mid \alpha(4) = 4\} \cong S_3$;
di ordine 8: il gruppo diedrale D_4 delle simmetrie di un quadrato, come gruppo di permutazioni sui 4 vertici;
di ordine 12: A_4;
di ordine 24: S_4.
Questo non deve assolutamente lasciarci pensare che il Teorema di Lagrange si inverta per tutti gli S_n. Infatti i gruppi S_n, per $n > 4$ non hanno questa proprietà. Ad esempio, S_5, d'ordine $5! = 120$, non ha sottogruppi d'ordine 30 o 40. Più in generale, S_n non ha sottogruppi d'ordine $\frac{n!}{3}$ $\forall$ $n > 4$.

Capitolo 3

L'inversione del Teorema di Lagrange per particolari divisori

Guarderemo adesso il problema dell'inversione del Teorema di Lagrange da un altro punto di vista. Nel secondo capitolo abbiamo cercato dei casi in cui il teorema risultava invertibile per particolari classi di gruppi e ne abbiamo analizzate tre: i gruppi ciclici per primi, che assicurano oltre l'esistenza anche l'unicità del sottogruppo, poi i gruppi abeliani ed infine i p-gruppi.
In questo capitolo invece saliamo ad un livello maggiore di generalizzazione, cercando parziali inversioni del Teorema di Lagrange senza fare restrizioni sul gruppo in questione.
Di teoremi che asseriscano l'esistenza di un sottogruppo di ordine assegnato in un gruppo finito arbitrario ve ne sono pochi. Ne vedremo due tra i più importanti: il Teorema di Sylow e il Teorema di Hall.

3.1 Il Teorema di Sylow

Quello a cui ci siamo riferiti fino ad adesso col nome di Teorema di Sylow, in realtà è soltanto la prima di tre parti di un teorema più ampio. Le chia-

meremo per chiarezza *Primo Teorema di Sylow*, *Secondo Teorema di Sylow* e *Terzo Teorema di Sylow*. Quello che a noi interessa, e al quale ci siamo precedentemente riferiti, è il primo, cioè quello che assicura l'esistenza di sottogruppi di un gruppo finito arbitrario, aventi ordine una potenza di un numero primo. Delle altre due parti daremo solo l'enunciato.

Teorema 3.1.1 (Primo Teorema di Sylow)**.** *Sia G un gruppo finito di ordine n, e sia p^r la massima potenza di p che divide n, con p primo. Allora G possiede un sottogruppo di ordine p^r.*

Prima di dare la dimostrazione del Teorema di Sylow forniamo una nozione di calcolo combinatorio che ci sarà estremamente utile.
Il numero di modi di scegliere un sottoinsieme di k elementi da un insieme di n elementi si chiama *coefficiente binomiale*, e si indica con:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Procediamo ora con la dimostrazione del teorema.

Dimostrazione. Per ipotesi su p^r, possiamo scrivere $|G| = p^r \cdot m$, dove m è un intero positivo non divisibile per p.
Dimostriamo che esiste un sottogruppo di G di ordine p^r.
Denotiamo con X l'insieme di tutti i sottoinsiemi di G formati da p^r elementi:

$$X = \{S \subseteq G \mid |S| = p^r\}.$$

Considerando la definizione di coefficiente binomiale all'uopo fornita poco fa, si ha che:

$$|X| = \binom{n}{p^r} = \binom{p^r m}{p^r}$$

dove

$$\binom{p^r m}{p^r} = \frac{p^r m \cdot (p^r m - 1) \cdot \ldots \cdot (p^r m - i) \cdot \ldots \cdot (p^r m - p^r + 1)}{p^r \cdot (p^r - 1) \cdot \ldots \cdot (p^r - i) \cdot \ldots \cdot (p^r - p^r + 1)}.$$

Ora, se una potenza p^k divide $p^r - i$ allora p^k divide i e quindi anche $p^r m - i$, e viceversa. Nel quoziente scompaiono quindi tutte le potenze di p. Si conclude

che è possibile semplificare il numeratore ed il denominatore dell'espressione, in modo da ottenere un'espressione che deve fornire un intero positivo il quale non è divisibile per p.
Ora definiamo su X un'azione di G:

$$X \times G \longrightarrow X$$

$$(S, g) \longmapsto S \cdot g$$

dove $S \cdot g = \{sg \mid s \in S\}$.
(Notiamo che questa è un'azione per moltiplicazione a destra come quella definita nell'esempio 2.1 del capitolo precedente.)
Si ha che

$$X = \bigcup_{S \in T} S^G$$

dove T è un sistema di rappresentanti per le orbite dei membri di X.
Ora, per quanto visto nel capitolo precedente, si ha che $|G| = |S^G| \cdot |St_G(S)|$ e, dal momento che $|X|$ non è multiplo di p e che le orbite formano una partizione di X, allora esiste sicuramente un S in particolare la cui orbita S^G ha cardinalità non divisibile per p.
Perciò essendo p^r divisore di $|G|$, ma non di $|S^G|$, abbiamo che p^r divide $|St_G(S)| \Longrightarrow |St_G(S)| \geq p^r$.
D'altra parte, fissato un elemento $s \in S$, $\forall g \in St_G(S)$ l'applicazione

$$St_G(S) \longrightarrow S$$

$$g \longmapsto s \cdot g$$

è iniettiva.
Quindi vale anche $|St_G(S)| \leq p^r$.
Cioè $|St_G(S)| = p^r$.
Abbiamo pertanto trovato un sottogruppo di G di ordine p^r proprio nello stabilizzatore di un sottoinsieme che appartiene ad un'orbita di cardinalità non divisibile per p.

□

Ci sono in realtà altre dimostrazioni del Primo Teorema di Sylow, ma questa qui proposta ha l'enorme vantaggio, oltre l'eleganza e la semplicità, di esibire concretamente il sottogruppo cercato.
Combinando il Primo Teorema di Sylow col teorema sui p-gruppi, possiamo concludere che per ogni k tale che p^k divide $|G|$ esiste un sottogruppo di G di ordine p^k. Infatti, sia P un sottogruppo di ordine p^r, allora $k \leq r$ e P ha un sottogruppo di ordine p^k.

Ora enunciamo il secondo e il terzo teorema di Sylow, chiamando *p-sottogruppi di Sylow* i sottogruppi di ordine la massima potenza di p, con p primo, che divide l'ordine di un gruppo finito G.

Teorema 3.1.2 (Secondo Teorema di Sylow)**.** *Siano G un gruppo finito e p un numero primo. Allora due qualunque p-sottogruppi di Sylow di G sono coniugati.*

Dimostrazione. (Per la dimostrazione si veda [2], 4.14.14)

□

Teorema 3.1.3 (Terzo Teorema di Sylow)**.** *Siano G un gruppo finito e p un numero primo. Allora il numero dei p-sottogruppi di Sylow di G è del tipo 1+kp, con k numero intero non negativo.*

Dimostrazione. (Per la dimostrazione si veda [2], 4.14.18)

□

3.2 Il Teorema di Hall

Il teorema di cui qui daremo soltanto l'enunciato può essere visto come una generalizzazione del Teorema di Sylow nel caso dei gruppi risolubili. Infatti se $|G| = p^n m$, con p che non divide m e dunque $(p^n, m) = 1$, il Teorema di Sylow assicura l'esistenza di un sottogruppo di ordine p^n. Se però consideriamo un altro spezzamento dell'ordine di G in interi relativamente primi,

$|G| = ab$, con $(a, b) = 1$, nulla si può dire sull'esistenza o meno di un sottogruppo di ordine a. Ad esempio, il gruppo A_5 ha ordine $60 = 15 \cdot 4$, con $(15, 4) = 1$, ma A_5 non ha sottogruppi di ordine 15. Se però il gruppo è risolubile, allora tale sottogruppo esiste sempre, e si hanno anche opportune generalizzazioni delle altre parti del Teorema di Sylow.
Prima di passare al Teorema di Hall introduciamo i concetti di *commutatore*, di *sottogruppo derivato* e di *serie derivata*, essenziali per giungere alla definizione di risolubilità. (Per una trattazione più esaustiva dei gruppi risolubili si rimanda a [2], 4.17)

Definizione 3.1. Sia G un gruppo e siano $x, y \in G$. Si dice *commutatore* della coppia (x, y) e si denota con $[x, y]$, l'elemento $x^{-1}y^{-1}xy$.

Notiamo che $yx[x, y] = yxx^{-1}y^{-1}xy = xy$. Da questa uguaglianza si vede chiaramente che due elementi x e y del gruppo G sono permutabili se e solo se $[x, y] = 1_G$.
In particolare $\forall\ x \in G : [x, x] = 1_G$, quindi l'unità di G è un commutatore. Si dimostra poi che anche l'inverso di un commutatore è un commutatore, infatti: $[x, y]^{-1} = (x^{-1}y^{-1}xy) = y^{-1}x^{-1}yx = [y, x]$.
Tuttavia non è assolutamente detto che il prodotto di due commutatori sia un commutatore, perciò l'insieme dei commutatori di un gruppo G, in generale, non è un sottogruppo di G.

Definizione 3.2. 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 $\{[h, k] \big|\ h \in H, k \in K\}$.

Poichè, come abbiamo visto, $\forall\ h \in H$ e $\forall\ k \in K$ si ha $[h, k]^{-1} = [k, h]$, allora vale che $[H, K] = [K, H]$. Si dimostra che se H e K sono normali in G, anche il loro interderivato $[H, K]$ è normale in G. (Si veda [2], 4.17.4, pag.173).

Definizione 3.3. Sia G un gruppo. Si dice *derivato di G* e si denota col simbolo G' l'interderivato $[G, G]$, cioè il sottogruppo generato da tutti i commutatori di elementi di G.

Anche il derivato è un sottogruppo normale di G. (Si veda [2], 4.17.6, pag.173).

Definizione 3.4. Sia G un gruppo e si ponga $G^{(0)} = G$. Per un numero naturale k, definiamo per induzione $G^{(k)} = (G^{(k-1)})'$. Il sottogruppo $G^{(k)}$ di G si chiama *k-esimo derivato di G.*
In particolare si ha $G^{(1)} = G'$, e si osserva che

$$G^{(1)} = [G, G] \ \ , \ G^{(2)} = [G', G'] = \big[[G, G], [G, G]\big] \ \ , \ \ldots .$$

Otteniamo dunque la sequenza

$$G \supseteq G' \supseteq G'' \supseteq \cdots \supseteq G^{(k)} \supseteq \cdots$$

che chiamiamo *serie derivata* di G.

Giungiamo ora alla definizione di gruppo risolubile.

Definizione 3.5. Un gruppo G si dice *risolubile* se la sua serie derivata termina nell'elemento neutro in un numero finito di passi, cioè se esiste un intero non negativo l tale che $G^{(l)} = 1_G$, e si abbia

$$G \supseteq G' \supseteq G'' \supseteq \cdots \supseteq G^{(l-1)} \supseteq G^{(l)} = \{1_G\}$$

Adesso possiamo enunciare il Teorema di Hall.

Teorema 3.2.1 (Hall)**.** *Sia G un gruppo finito risolubile di ordine $|G| = ab$ con $(a, b) = 1$. Allora:*

(i) esiste in G un sottogruppo di ordine a;

(ii) due sottogruppi di ordine a sono coniugati;

(iii) se A è un sottogruppo il cui ordine divide a, allora A è contenuto in un sottogruppo di ordine a.

Dimostrazione. (Per la dimostrazione si veda [3], 5.103) □

Se il gruppo non è risolubile, vi sono controesempi per tutte e tre le parti del teorema.:

(i) Per la prima parte del teorema abbiamo già visto un controesempio: $|A_5| = 60 = 4 \cdot 15$, ma A_5 non ha sottogruppi di ordine 15.

(ii) Nel gruppo semplice $GL(3, 2)$ di ordine $168 = 24 \cdot 7$ vi sono sottogruppi di ordine 24 non coniugati.

(iii) Sempre in A_5 vi sono sottogruppi di ordine 6 $\big($ad esempio il gruppo S_3 generato da (1 2 3) e (1 2)(4 5)$\big)$ non contenuti in sottogruppi di ordine 12 (che sono tutti degli A_4).

Osserviamo infine che la risolubilità per i gruppi finiti non è un'ipotesi molto restrittiva. Infatti, alcuni importanti teoremi assicurano la risolubilità a partire dall'ordine del gruppo:

a) (*Teorema di Burnside*) Se $|G| = p^n q^m$, con p e q primi, allora G è risolubile.

b) (*Teorema di Feit-Thompson*) Se G è un gruppo finito di ordine dispari, allora G è risolubile.

c) Se $|G| = 2m$, con m dispari, allora G è risolubile.

d) Se $|G| = 4m$, con m dispari e $(3, m) = 1$, allora G è risolubile.

Ossia, per avere un gruppo G *non* risolubile occorre che $|G|$ sia multiplo di almeno tre primi distinti, e che sia multiplo di 8 o di 12.
Il piu piccolo esempio è proprio il gruppo alterno A_5, di ordine $60 = 2^2 \cdot 3 \cdot 5$.

Bibliografia

[1] W.Chu, *Teoria dei Gruppi finiti ed applicazioni combinatorie*, Quaderni del Dipartimento di Matematica dell'Università del Salento, 1 / 2007.

[2] S.Franciosi, F.De Giovanni, *Elementi di Algebra*, Aracne, Roma 1992.

[3] A.Machì, *Gruppi. Una introduzione a idee e metodi della Teoria dei Gruppi.*, Springer-Verlag, Milano 2007.

[4] L.Verardi, *Appunti di Algebra Superiore.*

[5] A.Vistoli, *Note di Algebra*, Bologna, 1993/94.