Note per il corso di Teoria dei Gruppi.

Sandro Mattarei

Queste Note raccolgono scarni appunti su alcuni argomenti per il corso di Teoria dei gruppi alla Facoltà di Scienze MFN dell'Università di Trento. La versione iniziale risale all'anno 2007/08. Sono quindi state leggermente ampliate durante gli anni successivi. A partire dal corso del 2009/10 la notazione per la composizione di mappe è stata convertita nell'opposta (composizione da sinistra a destra), che meglio si adatta ad indicare concetti quali il coniugio e le azioni. Questa versione è essenzialmente quella di fine corso 2011/12, ma continua a subire piccoli aggiornamenti. [1]

Le Note comunque contengono (per ora) poco piú che una traccia degli argomenti, che viene espansa a lezione. Buona parte degli argomenti dei Capitoli 1-4 si trovano nella maggior parte dei testi di Algebra, ad esempio in [**Her64**].

Nota importante sulla notazione. In questo corso scriviamo le mappe a destra del loro argomento (con qualche eccezione classica, quale la funzione di Eulero). Coerentemente, le componiamo da sinistra a destra. Questa è la convenzione che va per la maggiore nella teoria dei gruppi astratti, ed in particolare dei gruppi finiti. In teorie con aspetti analitici, quali la teoria dei gruppi di Lie, si tende invece ad usare la convenzione tradizionale di comporre le mappe da destra a sinistra. Usiamo anche noi questa convenzione nel breve capitolo introduttivo sui gruppi di Lie, che per ora contiene solo una piccola selezione di concetti di quella teoria.

[1] Ultimo aggiornamento: 9 maggio 2014.

Indice

CAPITOLO 1

Gruppi di permutazioni e gruppi astratti

1.1. Nozioni fondamentali sui gruppi

Sottogruppi. Sottogruppi, laterali, indice, teorema di Lagrange, trasversali, l'esempio di S_3. [Vedi lezioni.]

Omomorfismi. Omomorfismi, nucleo, gruppo quoziente. Le notazioni $H \leq G$ allora G/H e $H\backslash G$ indicano, rispettivamente, l'insieme dei laterali sinistri di H in G, e l'insieme dei laterali destri di H in G. Essi coincidono se e solo se $N \trianglelefteq G$, e solo in quel caso si può costruire il gruppo quoziente G/H.

[Vedi lezioni.]

Ci sono tre teoremi importanti sugli omomorfismi, detti spesso *i teoremi di isomorfismo* (talvolta detti il Primo, il Secondo ed il Terzo, ma in certe trattazioni gli ultimi due vengono scambiati di ordine...).

Teorema (Teorema fondamentale sugli omomorfismi). *Sia $\varphi : g \to H$ un omomorfismo di gruppi, con nucleo $K = \ker(\varphi)$. Allora K è un sottogruppo normale di G e $G/K \cong G\varphi$.*

Teorema. *Siano G un gruppo, H e N suoi sottogruppi, con N normale. Allora $HN = NH$ è un sottogruppo di G (contenente N come sottogruppo normale), $H \cap N$ è un sottogruppo normale di H, e la mappa $hN \mapsto h(H \cap N)$ è un isomorfismo di gruppi $HN/N \cong H/(H \cap N)$.*

(Si noti che per dimostrarlo conviene usare la mappa inversa.)

Teorema (Teorema di corrispondenza). *Siano G un gruppo e N un suo sottogruppo normale. Se $N \leq H \leq G$ allora $\overline{H} = H/N$ è un sottogruppo di $\overline{G} = G/N$. Inoltre la corrispondenza $H \mapsto \overline{H}$ è una biiezione fra l'insieme dei sottogruppi di G contenenti N, e l'insieme dei sottogruppi di $\overline{G}$. In tale corrispondenza, H è normale in G se e solo se $\overline{H}$ è normale in $\overline{G}$, ed in tal caso vale $G/H \cong \overline{G}/\overline{H}$.*

Prodotto diretto di gruppi. Se H e K sono gruppi, il loro *prodotto diretto (esterno)* è il prodotto cartesiano $H \times K = \{(h, k) : h \in H, k \in K\}$ dotato dell'operazione "componente per componente", cioè $(h_1, k_1) \cdot (h_2, k_2) := (h_1h_2, k_1k_2)$. Notate che il gruppo prodotto diretto $H \times K$ contiene sottogruppi $\bar{H} = H \times 1$ e $\bar{K} = 1 \times K$ isomorfi ad H e K, rispettivamente. Anzi, essi sono sottogruppi normali con $H \times K = \bar{H}\bar{K}$ e $\bar{H} \cap \bar{K} = 1$.

Viceversa, si mostra facilmente che se un gruppo G ha sottogruppi normali H e K tali che $G = HK$ e $H \cap K = 1$ cioè, come si dice, G è *prodotto diretto interno* dei suoi sottogruppi H e K, allora G è isomorfo al prodotto diretto (esterno) $H \times K$.

Gruppi ciclici. Ordine di un elemento e di una sua potenza, classificazione dei gruppi ciclici, automorfismi dei gruppi ciclici. [Vedi lezioni.]

1.2. Gruppi di permutazioni

Permutazioni. I vari modi di rappresentare una permutazione, in particolare la scrittura come prodotto di cicli disgiunti. Ordine di un ciclo e ordine di un prodotto di cicli disgiunti. [Vedi lezioni.]

Segno di una permutazione. Un k-ciclo, e di conseguenza ogni permutazione, si scrive come prodotto di trasposizioni:

$$(i_1, i_2, \dots, i_k) = (i_1, i_2)(i_1, i_3) \cdots (i_1, i_k) = (i_{k-1}, i_k) \cdots (i_2, i_3)(i_1, i_2).$$

Una permutazione si può scrivere come prodotto di trasposizioni in tanti modi diversi, usando numeri diversi di trasposizioni: ciò che non può cambiare è la *parità* del numero di trasposizioni usate. Se $g \in S_n$ è una permutazione che si scrive come prodotto di r cicli disgiunti (includendo nel conto quelli di lunghezza uno), applicando la formula appena vista a ciascun ciclo possiamo scrivere g come prodotto di $n - r$ trasposizioni. Definiamo allora il *segno* di g come $\operatorname{sgn}(g) := (-1)^{n-r}$, e diciamo g *pari* o *dispari* a seconda che il segno sia 1 o -1. Notate che questa definizione dipende solo dalla scrittura di g come prodotto di cicli disgiunti (cioè dal numero delle sue orbite nell'azione naturale), che è unica. (Non dipende invece dalla particolare scrittura di g come prodotto di trasposizioni, che abbiamo usato finora solo come motivazione.) Ora mostriamo che se g si scrive come prodotto di m trasposizioni, allora m è pari o dispari a seconda che g sia pari o dispari.[1]

Dimostrazione. Il punto cruciale è mostrare che se g è una permutazione e t è una trasposizione allora $\operatorname{sgn}(gt) = -\operatorname{sgn}(g)$; infatti da ciò segue induttivamente che un prodotto di k trasposizioni ha segno $(-1)^k$. Per verificare la formula, scriviamo g come prodotto di cicli disgiunti e distinguiamo due casi a seconda che i simboli scambiati dalla trasposizione t appartengano allo stesso ciclo di g, o a due cicli diversi. Riordinando i cicli disgiunti e rinominando eventualmente i vari simboli, possiamo sempre supporre che il prodotto gt finisca, nei due casi, nei modi seguenti: [2]

$$(1, \dots, i, i+1, \dots, j)(1, i+1) = (1, \dots, i)(i+1, \dots, j),$$
$$(1, \dots, i)(i+1, \dots, j)(1, i+1) = (1, \dots, i, i+1, \dots, j);$$

ciascuna segue dall'altra componendola a destra con la trasposizione $(1, i+1)$. Le due formule mostrano che gt, scritta come prodotto di cicli disgiunti, ha un ciclo in

[1] Questa sembrerebbe la definizione piú naturale di parità di una permutazione; naturalmente se si sceglie di adottarla è necessario verificare che si tratti di una buona definizione.

[2] Infatti rinominando i simboli possiamo supporre che 1 sia uno dei simboli scambiati da t. Se nel ciclo di g in cui appare 1 appare anche l'altro simbolo di t, rinominando i simboli rimanenti (escluso 1) possiamo assumere che tale ciclo sia $(1, \dots, i, i+1, \dots, j)$, e che $t = (1, i+1)$, per qualche $0 < i < j$. Nel caso opposto, rinominando man mano i simboli possiamo assumere che il ciclo di g in cui appare 1 sia $(1, \dots, i)$, quindi che $t = (1, i+1)$, ed infine che il ciclo di g in cui appare $i+1$ sia $(i+1, \dots, j)$.

piú o in meno di g, rispettivamente, e quindi $\mathrm{sgn}(gt) = -\mathrm{sgn}(g)$ vale in entrambi i casi. □

A questo punto segue che vale $\mathrm{sgn}(gh) = \mathrm{sgn}(g)\mathrm{sgn}(h)$ per due permutazioni qualsiasi g, h, cioè che la mappa $\mathrm{sgn} : S_n \to \{\pm 1\}$ è un omomorfismo di gruppi. Il suo nucleo è un sottogruppo normale di S_n di indice 2, il *gruppo alterno* A_n, costituito quindi dalle permutazioni pari di n simboli.

Esercizio. Mostrate che per $g \in S_n$ vale

$$\prod_{1 \le i < j \le n} (jg - ig) = \mathrm{sgn}(g) \prod_{1 \le i < j \le n} (j - i).$$

(Notate che è sufficiente verificare la formula nel caso in cui g è una trasposizione; determinate allora quali differenze $jg - ig$ sono negative, e verificate che esse sono in numero dispari.) Questo suggerisce un altro modo di definire il segno di una permutazione, come $\mathrm{sgn}(g) = \prod_{1 \le i < j \le n}(jg - ig)/(j - i)$ (si veda [**CUD02**, Exercise 2.3.6]).

Applicazione: il "gioco del 15". [Si vedano le lezioni, una trattazione semplificata rispetto a [**CUD02**, Section 2.3], piú meno corrispondente a [**CUD02**, Exercise 2.3.8].] Come descritto in [**CUD02**, Section 2.3], numeriamo le posizioni da 1 a 16. Possiamo considerare ciascuna "mossa elementare" come lo scambio fra due posizioni adiacenti, che però è possibile solo se al momento considerato una delle due posizioni è vuota. Quindi tali mosse elementari *non* formano un gruppo (perché non si possono comporre arbitrariamente), ma possono comunque essere pensate come elementi di S_{16}, e precisamente trasposizioni. Ad una determinata configurazione si possono applicare solo quattro, tre o due mosse legali, a seconda di dove si trova la casella vuota.

Il gioco consiste nel partire da una configurazione con la casella vuota in basso a destra ed applicare una sequenza di mosse fino a raggiungere la configurazione standard contenente 1, 2, 3, 4 nella prima riga, ecc., fino a 13, 14, 15 e la casella vuota nell'ultima riga. Tale sequenza, avendo riportato la casella vuota in basso a destra, consiste di un numero pari di mosse elementari. Dato che queste sono trasposizioni, la permutazione complessivamente realizzata può soltanto essere pari.

Ne segue che, rimuovendo dal puzzle due quadratini e rimettendoli nelle loro posizioni scambiati fra loro (e quindi applicando, in modo illegale, una trasposizione), lo si porta in una posizione da cui non si può legalmente raggiungere la posizione standard.

1.3. Il coniugio

Elementi coniugati in un gruppo. Se g, h sono elementi di un gruppo G, allora $g^h = h^{-1}gh$ è detto un *coniugato* di h e, se si vuole specificare, *il coniugato di h sotto g*. Per $x, h, k \in G$ vale $(x^h)^k = x^{hk}$. Segue che essere coniugati in un gruppo è una relazione di equivalenza.

Si noti che $g^h = g$ se e solo se $gh = hg$.

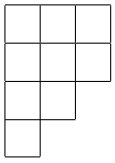
Per $x, y, h \in G$ vale anche $(xy)^h = x^h y^h$. Essa esprime il fatto che la mappa $x \mapsto x^h$ associata ad un certo h è un omomorfismo di gruppi; anzi, essa è un automorfismo, l'*automorfismo interno* associato a h. Ne segue anche che se $n \in \mathbb{N}$, e piú in generale se $n \in \mathbb{Z}$, vale $(x^h)^n = (x^n)^h$. In particolare, elementi coniugati hanno lo stesso ordine. Se $H \leq G$ allora anche $H^g \leq G$; essi sono *sottogruppi coniugati*.

Coniugio in S_n. Grazie a una delle proprietà del coniugio (il fatto che coniugare sotto un dato elemento è un automorfismo), se α e β sono permutazioni, per calcolare β^α basta scrivere β come prodotto di cicli (qui non necessariamente disgiunti), e imparare come si trova il coniugato di un ciclo. Questo si fa con la formula

$$(i_1, i_2, \ldots, i_r)^\alpha := \alpha^{-1}(i_1, i_2, \ldots, i_r)\alpha = (i_1\alpha, i_2\alpha, \ldots, i_r\alpha);$$

per dimostrarla basta verificare che i due membri danno lo stesso risultato se applicati a $i_j\alpha$, mentre lasciano invariato ogni k che non sia di questa forma per qualche j.

Struttura ciclica di una permutazione. Due permutazioni sono coniugate in S_n se e solo se hanno la stessa struttura ciclica. Dunque le classi di coniugio di S_n corrispondono biiettivamente alle *partizioni* del numero naturale n. Una partizione di n è una sequenza non crescente $\alpha = (\alpha_1, \ldots, \alpha_k)$ di interi positivi aventi somma n, e si scrive $\alpha \vdash n$. Spesso una partizione si indica mediante il corrispondente *diagramma di Young*, che si ottiene disegnando una riga di α_1 caselle quadrate affiancate, poi sotto di e essa una riga di α_2 caselle quadrate affiancate, eccetera, con tutte le righe allineate a sinistra. (Lo scopo di disegnare un tale diagramma è di riempire successivamente le caselle con dei numeri, ma per ora a noi ciò non interessa.) Ad esempio, la classe di coniugio di S_9 costituita da $(1,2,3)(4,5,6)(7,8)(9)$ (dove potremmo anche non scrivere l'1-ciclo (9)) e dai suoi coniugati è costituita da tutte le permutazioni di S_9 di struttura ciclica $(\cdot,\cdot,\cdot)(\cdot,\cdot,\cdot)(\cdot,\cdot)(\cdot)$, e tale struttura ciclica si può rappresentare con la partizione $(3,3,2,1)$ di S_9, ovvero, in notazione compatta (ma è solo una notazione, non un prodotto di numeri), $3^2\,2^1\,1^1$, o anche $3^2\,2\,1$, o mediante il diagramma di Young



CAPITOLO 2

Le azioni

2.1. Azione di un gruppo su un insieme

Siano G un gruppo e Ω un insieme. Un'*azione* di G su Ω è una mappa $\alpha : \Omega \times G \to \Omega, \quad (\omega, g) \mapsto \omega \cdot g$ (scritto spesso semplicemente ωg) tale che

(1) $\omega \cdot (gh) = (\omega \cdot g) \cdot h$ per ogni $g, h \in G$ e $\omega \in \Omega$;
(2) $\omega \cdot e = \omega$ per ogni $\omega \in \Omega$.

Ad un'azione corrisponde in modo naturale un omomorfismo di gruppi $G \to \mathrm{Sym}(\Omega)$, dato da $g \mapsto (\omega \mapsto \omega \cdot g)$. Il nucleo di tale omomorfismo è detto il *nucleo* dell'azione: $\{g \in G : \omega \cdot g = \omega \text{ per ogni } \omega \in \Omega\}$. Per ogni $\omega \in \Omega$ definiamo lo *stabilizzatore* di ω come $G_\omega = \mathrm{Stab}_G(\omega) := \{g \in G : \omega \cdot g = \omega\}$. Il nucleo dell'azione è l'intersezione di tutti gli stabilizzatori: $\bigcap_{\omega \in \Omega} G_\omega$. L'azione è *fedele* se il nucleo è il sottogruppo banale $1 = \{e\}$.

Viceversa, dato un omomorfismo $\psi : G \to \mathrm{Sym}(\Omega)$, vi è associata in modo naturale un'azione di G su Ω ponendo $\omega \cdot g := \omega(g\psi)$. Perciò, azioni di G su Ω e omomorfismi $G \to \mathrm{Sym}(\Omega)$ sono concetti equivalenti.

Data un'azione di G su Ω, l'*orbita* di un elemento $\omega \in \Omega$ è $\omega \cdot G := \{\omega \cdot g : g \in G\}$. Talvolta è utile scrivere $\omega \sim_G \omega'$ per dire che i punti ω e ω' di Ω appartengono alla stessa orbita sotto l'azione di G, cioè che $\omega' = \omega \cdot g$ per qualche $g \in G$. L'azione è *transitiva* (o si dice talvolta che Ω è uno *spazio omogeneo per* G) se $\omega \cdot G = \Omega$ per almeno un ω, e quindi per ogni $\omega \in \Omega$; in altre parole, se c'è una sola orbita.

Esempio. Se V è uno spazio vettoriale sul campo K, la moltiplicazione di vettori per scalari (restringendo l'attenzione a scalari non nulli) è un'azione di K^* su V.

Gli stabilizzatori dei punti di un'orbita sono fra loro coniugati (e viceversa, qualsiasi sottogruppo coniugato allo stabilizzatore di un punto è esso stesso lo stabilizzatore di un punto della stessa orbita); precisamente, $G_{\omega \cdot g} = g^{-1} G_\omega g = {G_\omega}^g$.

Esempio. Un'ottimo esempio concreto della relazione appena vista sono gli stabilizzatori dei punti nel gruppo dei movimenti rigidi del piano (diciamo quelli *propri*, cioè rotazioni e traslazioni).

Esempio. Nell'azione *naturale* di S_n su $\{1, \ldots, n\}$ lo stabilizzatore G_i della cifra i è costituito dalle permutazioni che fissano i. Ad esempio, se j e k sono altre due cifre avremo $(ijk)^{-1} G_i (ijk) = (ikj) G_i (ijk) = G_{j \cdot (ijk)} = G_j$.

TEOREMA (orbita-stabilizzatore). [1] *Data un'azione di G su Ω, fissiamo $\omega \in \Omega$. Allora la mappa*

$$G_\omega \backslash G \to \omega \cdot G \qquad G_\omega\, g \mapsto \omega \cdot g$$

è ben definita e biiettiva. In particolare, $|G| = |\omega \cdot G| \cdot |G_\omega|$ se G è finito, e quindi la lunghezza di ogni orbita $\omega \cdot G$ divide $|G|$.

DIMOSTRAZIONE. Abbiamo

$$\omega \cdot g = \omega \cdot h \iff \omega \cdot gh^{-1} = \omega \iff gh^{-1} \in G_\omega \iff G_\omega g = G_\omega h.$$

Quindi la mappa è ben definita e biiettiva. □

ESEMPIO. L'azione naturale di S_n. Nell'azione indotta di S_n sull'insieme delle parti di $\Omega = \{1, \dots, n\}$, ogni orbita consiste esattamente di tutti i sottoinsiemi di una data cardinalità k, che possiamo indicare con $\binom{\Omega}{k}$. Lo stabilizzatore del sottoinsieme $\{1, \dots, k\}$ di Ω è isomorfo al prodotto diretto $S_k \times S_{n-k}$, perciò grazie al teorema orbita-stabilizzatore il numero di sottoinsiemi di Ω di cardinalità k è il coefficiente binmiale $n!/k!(n-k)!$, cioè $\left|\binom{\Omega}{k}\right| = \binom{|\Omega|}{k}$, il che giustifica la notazione $\binom{\Omega}{k}$.

ESEMPIO. Il *gruppo lineare generale* $\mathrm{GL}(n, F)$ è il gruppo delle matrici $n \times n$ invertibili a coefficienti nel campo F. L'azione naturale di $\mathrm{GL}(n, F)$ sullo spazio (dei vettori riga) F^n induce un'azione sull'insieme delle basi di tale spazio; tale azione è transitiva e ogni stabilizzatore è 1, quindi l'azione è regolare. In particolare, se F è il campo $\mathbb{F}_q$ con q elementi, abbiamo che l'ordine di $\mathrm{GL}(n, F)$ è uguale al numero di basi di $\mathbb{F}_q^n$, perciò[2]

$$\begin{aligned} |\mathrm{GL}(n, \mathbb{F}_q)| &= (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \\ &= q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1). \end{aligned}$$

Il fattore $q^{n(n-1)/2}$ nella formula è in effetti l'ordine di un sottogruppo di $\mathrm{GL}(n, \mathbb{F}_q)$, il gruppo delle matrici *unitriangolari inferiori* (o di quelle unitriangolari superiori, se si preferisce), di cui l'altro fattore è l'indice. Diciamolo U. È interessante anche un altro sottogruppo T di $\mathrm{GL}(n, \mathbb{F}_q)$, contenente U, che consiste delle matrici triangolari inferiori invertibili (necessariamente), cioè con entrate tutte non nulle sulla diagonale. Il gruppo T ha ordine $q^{n(n-1)/2}(q-1)^n$, in quanto $|T : U| = (q-1)^n$. (Anzi, U è un sottogruppo normale di T, e il gruppo quoziente è

[1] Per i gruppi di Lie, sotto opportune condizioni vale un teorema analogo, con $|G| = |\omega \cdot G| \cdot |G_\omega|$ rimpiazzata da $\dim(G) = \dim(\omega \cdot G) + \dim(G_\omega)$. Ciò sarà esemplificato in varie successive note a pié di pagina.

[2] La formula per l'ordine è un polinomio in q. Sul campo reale o quello complesso al posto di $\mathbb{F}_q$ l'ordine del gruppo è infinito, ma il grado n^2 di quel polinomio, diciamolo $f(q)$, conserva un significato: è la dimensione del gruppo (come gruppo di Lie o come gruppo algebrico, reale o complesso, a seconda). In vista della corretta estensione dai polinomi alle funzioni razionali, piuttosto che come il grado del polinomio $f(q)$ il numero n^2 va interpretato come *l'ordine di polo del polinomio al punto* ∞, cioè l'unico intero s tale che $\lim_{q\to\infty} f(q)/q^s$ sia finito e non nullo; nel caso generale di una funzione razionale esso si trova sottraendo in grado del denominatore a quello del numeratore. Un'interpretazione analoga varrà allora per tutti i sottogruppi di $\mathrm{GL}(n, F)$ che introdurremo.

isomorfo al gruppo D delle matrici diagonali invertibili. Ancora più precisamente, T è il prodotto semidiretto di U e D.) Quindi

$$|\mathrm{GL}(n,\mathbb{F}_q) : T| = [n]_q \cdot [n-1]_q \cdots [2]_q \cdot [1]_q,$$

dove

$$[n]_q := \frac{1-q^n}{1-q} = 1 + q + q^2 + \cdots + q^{n-1}$$

è un *q-numero*, o il *q-analogo* di un intero positivo (la ragione del nome è che $\lim_{q\to 1}[n]_q = 1$).[3] Dunque $|\mathrm{GL}(n,\mathbb{F}_q) : T| = [n]_q!$, il *q-fattoriale* di $[n]_q$.

L'azione naturale di $\mathrm{GL}(n,\mathbb{F}_q)$ induce varie azioni, quali sull'insieme $\mathcal{P}(F^n)$ dei sottoinsiemi di $\mathbb{F}^n$, su $\mathcal{P}(\mathcal{P}(F^n))$, ecc. In particolare, consideriamo l'azione indotta di $\mathrm{GL}(n,\mathbb{F}_q)$ sull'insieme dei sottospazi di $\mathbb{F}^n$. Essa ha esattamente $n+1$ orbite, ciascuna consistente di tutti i sottospazi di un'assegnata dimensione k. È quindi sufficiente considerare lo stabilizzatore del particolare sottospazio $W = \langle e_1, \ldots, e_k\rangle$, che consiste di tutte le matrici in $\mathrm{GL}(n,\mathbb{F}_q)$ della forma $\left[\begin{smallmatrix} A & 0 \\ B & C \end{smallmatrix}\right]$, dove $A \in \mathrm{GL}(k,\mathbb{F}_q)$, $C \in \mathrm{GL}(n-k,\mathbb{F}_q)$, e $B \in \mathrm{M}_{n-k,k}(\mathbb{F}_q)$. Perciò, grazie al teorema orbita-stabilizzatore, il numero di $\mathbb{F}_q$-sottospazi di uno spazio vettoriale di dimensione n sul campo $\mathbb{F}_q$, è

$$\frac{|\mathrm{GL}(n,\mathbb{F}_q)|}{q^{k(n-k)} \cdot |\mathrm{GL}(k,\mathbb{F}_q)| \cdot |\mathrm{GL}(n-k,\mathbb{F}_q)|} = \frac{[n]_q!}{[k]_q! \cdot [n-k]_q!} =: \begin{bmatrix} n \\ k \end{bmatrix}_q,$$

detto un *coefficiente binomiale Gaussiano*.[4] [5]

Come ulteriore esercizio analizziamo meglio lo stabilizzatore visto, diciamolo S. Essendo $\left[\begin{smallmatrix} A & 0 \\ B & C \end{smallmatrix}\right] = \left[\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1 & 0 \\ B & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1 & 0 \\ 0 & C \end{smallmatrix}\right]$, con notazione ovvia, S è il prodotto $\mathcal{ABC}$ di tre sottogruppi $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$. Chiaramente il primo ed il terzo sono isomorfi a $\mathrm{GL}(k,\mathbb{F}_q)$ e $\mathrm{GL}(n-k,\mathbb{F}_q)$, ma si noti che il secondo è isomorfo al gruppo additivo $\mathrm{M}_{n-k,k}(\mathbb{F}_q)$.

---

[3] Se dividiamo l'ordine di $|\mathrm{GL}(n,\mathbb{F}_q)|$ per $(q-1)^n$ otteniamo una funzione razionale in q, che prende valore $n!$ quando $q = 1$. Si noti che $n!$ è l'ordine del gruppo simmetrico S_n. Esiste un concetto di *campo* $\mathbb{F}_1$ *con un elemento* (che non è per niente facile da costruire, non si tratta semplicemente di $\mathbb{Z}/\mathbb{Z}$, che è l'anello nullo, si veda ad esempio Wikipedia), secondo il quale uno spazio vettoriale di dimensione n su $\mathbb{F}_1$ è semplicemente un insieme con n elementi e, conseguentemente, il suo gruppo degli automorfismi è il gruppo simmetrico S_n. Questo punto di vista estende ad un'interpretazione di un forte parallelismo fra $|\mathrm{GL}(n,\mathbb{F}_q)|$ e il gruppo simmetrico come suo *caso speciale*. Provate ad interpretare anche le parti successive di questo esempio per $q \to 1$ e confrontatele con quelle corrispondenti per S_n dell'esempio precedente.

[4] L'insieme dei sottospazi di dimensione k di $\mathbb{R}^n$ (o di $\mathbb{C}^n$ come spazio vettoriale su $\mathbb{C}$) ha una struttura di varietà differenziabile (o algebrica). La sua dimensione si ottiene sottraendo il grado in q del denominatore da quello del numeratore nella formula del binomiale Gaussiano, ed è quindi $k(n-k)$.

[5] I coefficienti binomiali Gaussiani soddisfano generalizzazioni di note identità per i coefficienti binomiali, quali $(1+t)^n = \sum_{k=0}^n \binom{n}{k} t^k$, e $(1-t)^{-n} = \sum_{k=0}^\infty \binom{n+k-1}{k} t^k$, che diventano

$$\prod_{k=1}^{n}(1+q^k t) = \sum_{k=0}^{n} q^{k(k+1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q t^k, \qquad \prod_{k=0}^{n-1}(1-q^k t) = \sum_{k=0}^{\infty} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q t^k.$$

In effetti

$$\mathcal{BC} = \{g \in \mathrm{GL}(n, \mathbb{F}_q) : wg = g \text{ per ogni } w \in W\}$$

agisce sullo spazio quoziente V/W, dove $V = \mathbb{F}_q^n$, e

$$\mathcal{B} = \{g \in \mathcal{BC} : vg = g \text{ per ogni } v \in V/W\}.$$

Il fatto che $\mathcal{B} \cong \mathrm{M}_{n-k,k}(\mathbb{F}_q)$ (e quindi è, in particolare, abeliano elementare) si vede anche notando che la mappa $\mathrm{Hom}_{\mathbb{F}_q}(V/W, W) \to \mathcal{B}$ data da $h \mapsto g = 1 + h$ è ben definita, biiettiva, e un omomorfismo di gruppi (quest'ultimo fatto in quanto $hh' = 0$ per ogni $h, h' \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^n/W, W)$, e quindi $(1 + h)(1 + h') = 1 + hh'$). Notate anche che $\mathcal{B}$ è un sottogruppo normale di S, per verifica diretta, o in quanto nucleo dell'omomorfismo $S \to \mathrm{Aut}_{\mathbb{F}_q}(W) \times \mathrm{Aut}_{\mathbb{F}_q}(V/W)$ che manda $g \in S$ nella coppia $(g_{|W}, g_{|V/W})$, e che $\mathcal{AC}$ è un prodotto diretto interno. Perciò

$$S = \mathcal{ABC} \cong \mathcal{B} \rtimes (\mathcal{A} \times \mathcal{C}) \cong \mathrm{M}_{n-k,k}(\mathbb{F}_q) \rtimes \big(\mathrm{GL}(k, \mathbb{F}_q) \times \mathrm{GL}(n-k, \mathbb{F}_q)\big),$$

un prododotto semidiretto (rispetto alla particolare azione considerata di quel prodotto diretto su $\mathrm{M}_{n-k,k}(\mathbb{F}_q)$).

Infine, il sottogruppo T è uno stabilizzatore nell'azione di $\mathrm{GL}(n, \mathbb{F}_q)$ sull'insieme dei *full flags* $0 < V_1 < V_2 < \cdots < V_{n-1} < \mathbb{R}^n$ (cioè catene propriamente ascendenti di sottospazi di $\mathbb{R}^n$, e l'aggettivo *full,* o equivalentemente *complete,* indica la presenza di un sottospazio di ciascuna possibile dimensione). È facile vedere che i full flags formano un'unica orbita sotto l'azione di $\mathrm{GL}(n, \mathbb{F}_q)$, e T è lo stabilizzatore del full flag con $V_i = \langle e_1, \ldots, e_i \rangle$, dove $e_1, \ldots, e_n$ è la base canonica di $\mathbb{R}^n$. Grazie al teorema orbita-stabilizzatore concludiamo che in $\mathbb{R}^n$ (o in qualsiasi spazio vettoriale di dimensione n su $\mathbb{F}_q$) ci sono esattamente $[n]_q!$ full flags distinti.[6]

2.2. L'azione per moltiplicazione

Il gruppo G agisce su $\Omega = G$, cioè su se stesso, per *moltiplicazione (a destra),* detta anche *traslazione (a destra),* ponendo $\omega \cdot g := \omega g$ (il loro prodotto) per $\omega, g \in G$. L'azione è transitiva, e fedele, cioè il nucleo è 1. Anzi, lo stabilizzatore di un punto (e quindi tutti gli stabilizzatori) è 1. Questa azione è anche detta *l'azione regolare.*

Vi è associato un omomorfismo iniettivo $G \to \mathrm{Sym}(G)$. In particolare, se G è finito, di ordine n, ne otteniamo un omomorfismo $G \mapsto S_n$, e quindi abbiamo il seguente risultato.

Teorema (di Cayley). *Ogni gruppo (finito) è isomorfo ad un gruppo di permutazioni (di un insieme finito).*

Naturalmente il teorema di Cayley non pretende di essere efficiente: applicato a S_n ne produce una rappresentazione come gruppo di permutazioni su $n!$ elementi, che sono molti piú degli n che sono sufficienti a rappresentare S_n fedelmente come gruppo di permutazioni.

[6] Lavorando su $\mathbb{R}$ o su $\mathbb{C}$, i full flags formano una varietà differenziabile (o algebrica), una *flag variety.* La sua dimensione è il grado in q di $[n]_q!$, che vale $n(n-1)$.

Il teorema di Cayley implica anche che ogni gruppo finito G è isomorfo a un gruppo di matrici su un campo F (o anche un anello, arbitrariamente assegnato). Basta comporre l'omomorfismo iniettivo $G \to S_n$ dato dall'azione regolare con l'omomorfismo iniettivo $S_n \to \mathrm{GL}(n, F)$ che manda una permutazione $g \in S_n$ nella corrispondente *matrice di permutazione,* con entrate $a_{ij} = \delta(ig, j)$. Naturalmente anche questa rappresentazione di G è molto inefficiente, ancor più della precedente, in quanto rappresenta gli elementi di G come matrici $n \times n$, dove $n = |G|$.

Ecco un'applicazione del teorema di Cayley (o meglio della sua dimostrazione, cioè dell'azione regolare):

LEMMA 2.1. *Sia G un gruppo di ordine $2r$, con $r > 1$ dispari. Allora G ha un sottogruppo di indice due. In particolare, G non è un gruppo semplice.*

DIMOSTRAZIONE. Identifichiamo G con la sua immagine isomorfa in S_{2r} data dall'azione regolare. Come ogni gruppo di ordine pari, si vede facilmente (accoppiando g con g^{-1}) che G ha almeno un elemento di ordine due (cioè *un'involuzione*). Un tale elemento t è il prodotto di r trasposizioni (tutte della forma (g, gt)), e quindi è una permutazione dispari. Dunque $G \not\leq A_{2r}$, perciò $GA_{2r} = S_{2r}$, quindi $|G : G \cap A_{2r}| = |GA_{2r} : A_{2r}| = 2$. □

Se $H \leq G$, ponendo $Hx \cdot g := Hxg$ per $x, g \in G$ otteniamo un'azione, anch'essa detta per *moltiplicazione (a destra),* di G sull'insieme $H\backslash G$ (che non è un gruppo se H non è normale!) dei laterali destri di H. Qui gli stabilizzatori sono i coniugati di H. Il nucleo, cioè la loro intersezione, è $H_G = \cap_{x \in G} H^x$, detto il *cuore* di H in G, che è il piú grande sottogruppo normale di G contenuto in H (nel senso che $H_G \trianglelefteq G$, e che da $N \trianglelefteq G$ e $N \leq H$ segue $N \leq H$). In particolare, $H_G = H$ se e solo se H è normale in G.

Nel caso di indice finito $|G : H| = n$, a questa azione è associato un omomorfismo $G \to S_n$, con nucleo $H_G = \cap_{x \in G} H^x$, e quindi un omomorfismo iniettivo $G/H_G \to S_n$. Ne segue che se G ha un sottogruppo H (eventualmente anche infinito, ma) di indice n allora H contiene un sottogruppo normale di G, il cui indice in $|G|$ divide $n!$.

Una conseguenza di questo fatto è la seguente: se un gruppo finito G ha un sottogruppo H di indice primo p, e p è il piú piccolo primo che divide $|G|$, allora $H \trianglelefteq G$. Questo generalizza il fatto che un sottogruppo di indice 2 è sempre normale. Infatti l'indice $|G : H_G|$ divide $p!$, ma dividendo anche $|G|$ per Lagrange esso può solo valere 1 o p; dato che $H_G \leq H$ concludiamo che $H = H_G \trianglelefteq G$.

ESERCIZIO. Notate che il gruppo simmetrico $G = S_n$ ha un sottogruppo isomorfo a S_{n-1}, ad esempio lo stabilizzatore della cifra n nell'azione naturale. Tale sottogruppo ha indice n.

Ora assumete $n \geq 5$ e considerate un arbitrario sottogruppo H di S_n, diverso da S_n ed dal sottogruppo alterno A_n (che ha indice due). Dando per buono il fatto che i soli sottogruppi normali di S_n (per $n \geq 5$) sono 1, A_n e S_n, ed usando l'azione di G per moltiplicazione a destra su $H\backslash G$, dimostrate che $|G : H| \geq n$.

Il significato di questa conclusione è il seguente: sappiamo già che S_n ha almeno un sottogruppo isomorfo a S_{n-1}, e quindi di ordine $(n-1)!$; ora abbiamo scoperto che S_n non ha sottogruppi propri piú grandi di esso.

Ogni azione transitiva di G è *equivalente* all'azione di G per moltiplicazione a destra su $H\backslash G$, per un opportuno sottogruppo H. Infatti, fissando $\omega \in \Omega$ e prendendo come H lo stabilizzatore di ω, la mappa $\varphi : H\backslash G \to \Omega$ definita da $Hx \mapsto \omega x$ è ben definita e una biiezione, e soddisfa $(Hx \cdot g)\varphi = (Hx)\varphi \cdot g$.

Segue che due azioni transitive sono equivalenti se e solo se esse hanno gli stessi stabilizzatori (che come sappiamo formano una classe di coniugio di sottogruppi). Dunque le possibili azioni transitive di un gruppo corrispondono alle sue classi di coniugio di sottogruppi.

2.3. L'azione per coniugio

Un gruppo G agisce su se stesso per coniugio, ponendo $\omega \cdot g := \omega^g = g^{-1}\omega g$ per $\omega, g \in G$. Le orbite sono le classi di coniugio. Lo stabilizzatore di un elemento h è $\mathbf{C}_G(h) := \{g \in G : gh = hg\}$, il *centralizzante* di h in G. Dunque la lunghezza della classe di coniugio h^G è data da $|h^G| = |G : \mathbf{C}_G(h)|$ e, in particolare, divide $|G|$. Il nucleo dell'azione è il centro $\mathbf{Z}(G)$.

L'equazione delle classi. Talvolta si chiama *equazione delle classi* l'uguaglianza

$$|G| = |G : \mathbf{C}_G(g_1)| + \cdots + |G : \mathbf{C}_G(g_r)|,$$

dove $g_1, \ldots, g_r$ sono rappresentanti per le classi di coniugio di G. Eccone un paio di applicazioni.

Lemma. *Ogni gruppo non banale di ordine una potenza di un primo p ha centro non banale.*

Per mostrarlo basta notare che ogni classe ha lunghezza un divisore di $|G| = p^n$, quindi una potenza di p, ed ogni elemento del centro forma da solo una classe di lunghezza 1; dato che p divide sia $|G|$ che la lunghezza di ogni classe fuori del centro, per differenza p deve dividere il numero di classi di lunghezza 1, cioè l'ordine del centro.

Una conseguenza di questo fatto è che un gruppo di ordine p^2 è necessariamente abeliano: infatti il suo centro $\mathbf{Z}(G)$ avrà ordine p o p^2, e quindi $G/\mathbf{Z}(G)$ sarà ciclico, da cui segue facilmente che G stesso è ciclico.

Lemma (di Cauchy). *Se un primo p divide $|G|$, allora G ha (almeno) un elemento di ordine p.*

La dimostrazione [vedi lezioni per i dettagli], si fa per induzione, dimostrando prima il caso G abeliano, ragionando su un eventuale sottogruppo proprio H ed il corrisponde quoziente G/H (uno dei due ha un elemento di ordine p per induzione); nel caso di G non abeliano, allora o $\mathbf{Z}(G)$ ha un elemento di ordine p, oppure qualche $\mathbf{C}_G(g_i)$ lo ha, grazie all'equazione delle classi.

Una conseguenza importante del Lemma di Cauchy è che ogni p-gruppo (cioè un gruppo in cui ogni elemento abbia ordine una potenza del primo fissato p) finito ha ordine una potenza di p. (Infatti se qualche primo $q \neq p$ dividesse l'ordine del gruppo, il Lemma di Cauchy fornirebbe almeno un elemento di ordine q, contraddizione.) Il verso contrario, che ogni gruppo di ordine una potenza di p è un p-gruppo, segue semplicemente dal Teorema di Lagrange.

Automorfismi interni. Una particolarità dell'azione per coniugio è che G agisce su se stesso *per automorfismi* (a differenza che nell'azione per traslazione, ad esempio), cioè l'omomorfismo associato $G \to \mathrm{Sym}(G)$ ha in realtà immagine contenuta in $\mathrm{Aut}(G)$. L'immagine di questa mappa è un sottogruppo normale di $\mathrm{Aut}(G)$, indicato con $\mathrm{Inn}(G)$, il *gruppo degli automorfismi interni* di G, cioè quelli della forma $\gamma_g : x \mapsto g^{-1}xg$ per qualche $g \in G$. Grazie al teorema fondamentale sugli omomorfismi, $\mathrm{Inn}(G)$ è isomorfo al gruppo quoziente $G/\mathbf{Z}(G)$.

Sia ora N un sottogruppo normale di G. Allora G agisce per coniugio su N (in quanto N è unione di classi di coniugio di G, pertanto possiamo restringere l'azione di G per coniugio su G all'unione di orbite N). Anche in questo caso si tratta di un'azione per automorfismi, e quindi abbiamo un omomorfismo $G \to \mathrm{Aut}(N)$, di nucleo $\mathbf{C}_G(N) = \bigcap_{n\in N} \mathbf{C}_G(n)$.

Si noti che se N ha un complemento H, cioè un sottogruppo H di G tale che $HN = G$ e $H \cap N = 1$, e si dice che G è il prodotto semidiretto interno di N e H, l'omomorfismo descritto restringe ad un omomorfismo $H \to \mathrm{Aut}(N)$. Esso diventa un ingrediente nella definizione del (corrispondente) prodotto semidiretto esterno.

Prodotti semidiretti. Se un gruppo G ha un sottogruppo H e un sottogruppo normale N tali che $G = HN$ e $H \cap N = 1$, diciamo che G è il *prodotto semidiretto (interno)* di H e N, e scriviamo $G = H \ltimes N$ (o anche $G = N \rtimes H$, se preferiamo). (Si tratta poi di un prodotto diretto se anche H è normale in G.) Ogni elemento di G si scrive in modo unico come hn con $h \in H$ e $n \in N$.

Notando che $(h_1n_1)(h_2n_2) = (h_1h_2)(n_1^{h_2}n_2)$, dove $n_1^{h_2} \in N$, e che la mappa $h \mapsto (n \mapsto n^h)$ è omomorfismo di H in $\mathrm{Aut}(N)$, siamo portati a dare la seguente definizione. Dati due gruppi N e H, ed un omomorfismo $\alpha : H \to \mathrm{Aut}(N)$, il *prodotto semidiretto (esterno)* di H e N rispetto all'omomorfismo α, indicato con $H \ltimes_\alpha N$ (o semplicemente $H \ltimes N$, purché sia chiaro quale sia α) è l'insieme prodotto cartesiano $H \times N$ con l'operazione

$$(h_1, n_1)(h_2, n_2) = \big(h_1h_2, n_1^{h_2\alpha}n_2\big).$$

(Solo per maggiore chiarezza in questo caso abbiamo apposto l'automorfismo $h_2\alpha \in \mathrm{Aut}(N)$ ad esponente del suo argomento n_1, piuttosto che semplicemente a destra di esso come facciamo di solito.) Si verifica (esercizio) che $H \ltimes_\alpha N$ è un gruppo, e che è il prodotto semidiretto interno di $\bar{H} = \{(h, 1) : h \in H\}$ e $\bar{N} = \{(1, n) : n \in N\}$.

Orbite di un sottogruppo. Supponiamo che il gruppo G agisca sull'insieme Ω. Se H è un sottogruppo di G, possiamo restringere questa azione ad un'azione di H su Ω. Chiaramente ogni orbita di G su Ω è unione di orbite di H su Ω, cioè $\omega G = \dot{\bigcup}\omega_i H$ per certi ω_i (perché se $\omega \sim_H \omega'$ allora $\omega \sim_G \omega'$). In generale queste orbite di H (e le corrispondenti azioni di H) possono essere molto diverse fra loro, ad esempio nel caso in cui G è finito possono avere lunghezze diverse. Un modo piú esplicito di trovare le orbite $\omega_i H$ è il seguente. Se $\{g_j\}$ è un insieme di rappresentanti per i laterali sinistri di H in G, cioè se $G = \dot{\bigcup} g_j H$, avremo $\omega G = \bigcup \omega g_j H$, e quindi da esso possiamo estrarre un sottoinsieme $\{g_i'\}$ tale che

$\{\omega g_i'\}$ sia un insieme di rappresentanti per le orbite di H su ωG, cioè tale che $\omega G = \dot{\bigcup} \omega g_j' H$. In particolare, ωG è unione di al piú $|G : H|$ orbite di H, se questo indice è finito. Notate che la lunghezza di una certa orbita $\omega g H$ è calcolabile grazie al teorema orbita-stabilizzatore, ed è quindi uguale all'indice in G dello stabilizzatore $H_{\omega g} = H \cap G_{\omega g} = H \cap (G_\omega)^g$.

Un caso speciale importante di questa situazione si ottiene prendendo come H lo stabilizzatore in G di un punto ω, cioè $H = G_\omega$. Naturalmente G_ω ha almeno un'orbita di lunghezza uno su ωG, e cioè $\{\omega\}$. Le altre orbite di G_ω su ωG avranno in generale varie lunghezze. Anzi, saranno tutte di lunghezza uno se e solo se $G_\omega \trianglelefteq G$ Infatti gli stabilizzatori in G_ω di altri punti di ωG sono dati da $G_{\omega g} = G_\omega \cap (G_\omega)^g$, e quindi coincidono tutti con G_ω se e solo se questo è un sottogruppo normale di G. (All'estremo opposto è il caso in cui G_ω ha esattamente due orbite su gG, precisamente $\{\omega\}$ e $\omega G \setminus \{\omega\}$; questo avviene se e solo se l'azione di G su ωG è 2-transitiva.)

Orbite di un sottogruppo normale. Piú in generale, se H è un sottogruppo normale di G, chiamiamolo piuttosto N per ricordarcelo, allora $N_{\omega g} = N \cap G_{\omega g} = N^g \cap (G_\omega)^g = (N \cap G_\omega)^g = (N_\omega)^g$, che generalizza una formula nota. Dunque in questo caso gli stabilizzatori in N di punti di una G-orbita ωG sono coniugati in G (anche se non necessariamente in N). In particolare, le orbite di N su ωG hanno tutte la stessa lunghezza $|N : N_\omega|$ (finita se questo indice è finito), che possiamo anche riscrivere come $|N : N \cap G_\omega| = |NG_\omega : G_\omega|$. In particolare, se G è finito vediamo che la G-orbita ωG è l'unione di esattamente $|G : G_\omega|/|NG_\omega : G_\omega| = |G : NG_\omega|$ orbite di N. In particolare, la G-orbita ωG è anche una N-orbita se e solo se $NG_\omega = G$. Vedremo subito che quelle fra queste affermazioni che continuano ad aver senso anche se G non è finito, continuano in effetti a valere.

Infatti le orbite di N su ωG vengono permutate da G, infatti $g \in G$ manda una N-orbita ωN in $\omega N g = \omega g\, N^g = \omega g N$, che è un'altra N-orbita. (In generale $g \in G$ manda una H-orbita ωH in $\omega g H^g$, che è un'orbita per H^g, ma non necessariamente per H se questo non è normale in G.) Chiaramente G permuta queste N-orbite transitivamente, e il nucleo di questa azione contiene N, pertanto queste orbite sono in realtà permutate dal gruppo quoziente G/N. È facile vedere (esercizio) che nell'azione di G sull'insieme delle N-orbite su ωG, lo stabilizzatore di ωN è NG_ω. Ne riotteniamo la conclusione che N ha esattamente $|G : NG_\omega|$ orbite su ωG, e quindi una sola se e solo se $NG_\omega = G$, come abbiamo appena visto in un caso speciale.

Ricapitolando nel caso speciale in cui ωG è un'orbita finita, essa è l'unione di $|G : NG_\omega|$ orbite di N, tutte della stessa lunghezza $|NG_\omega : G_\omega| = |N : N \cap G_\omega|$. In particolare, entrambi questi numeri sono divisori della lunghezza dell'orbita ωG. Notate che nel caso speciale in cui $|G : N|$ è un numero primo sono possibile solo due alternative: o $\omega G = \omega N$, il che avviene se $NG_\omega = G$ (cioè se $G_\omega \not\leq N$), oppure ωG è l'unione di $|G : N|$ distinte N-orbite di uguale lunghezza, il che avviene se $NG_\omega = N$ (cioè se $G_\omega \leq N$).

Classi di coniugio di un sottogruppo normale. Applicando quanto visto all'azione per coniugio di un gruppo finito G su un suo sottogruppo normale N, e

restringendo l'azione a N, concludiamo quanto segue: una classe di coniugio g^G di G, che sia contenuta in N, si spezza nell'unione di $|G : N\mathbf{C}_G(g)|$ classi di coniugio di N, tutte della stessa lunghezza.

In particolare, se $G = S_n$ e $N = A_n$, abbiamo che una classe di coniugio g^{S_n} di S_n contenuta in A_n, cioè fatta di permutazioni pari, o è anche una classe di coniugio di A_n, o si spezza nell'unione di due classi di coniugio di A_n. Questa seconda alternativa avviene e solo se $\mathbf{C}_{S_n}(g) \leq A_n$, cioè se e solo se il centralizzante di g non contiene alcuna permutazione dispari. Ciò avviene se e solo se nella decomposizione di g come prodotto di cicli disgiunti (inclusi quelli di lunghezza uno) le lunghezze dei cicli sono tutte dispari e tutte distinte.

Esempio. Si vede facilmente che il gruppo simmetrico S_5 ha sette classi di coniugio (pari al numero di partizioni di 5), con rappresentanti 1, (12)(34), (123), (12345), (12), (1234), (123)(45), e corrispondenti classi di coniugio lunghe 1, 15, 20, 24, 10, 30, 20. Le prime quattro sono contenute in A_5, e si verifica che solo la quarta si spezza in due classi di coniugio di A_5, con rappresentanti (12345) e (12354), ad esempio. (Che questa classe di S_5 non possa formare una classe di coniugio di A_5 si vede anche dal fatto che la sua lunghezza, 24, non divide $|A_5|$.)

In particolare, se ne deduce che il gruppo alterno A_5 è semplice. Infatti ogni suo sottogruppo normale deve essere unione di certe classi di coniugio, e quindi il suo ordine deve essere uguale alla somma di alcune fra le lunghezze 1, 15, 20, 12, 12 delle classi. Ma grazie al teorema di Lagrange tale ordine deve anche dividere $|A_5| = 60$, e se ne conclude che esso può essere solo 1 o 60.

CAPITOLO 3

Esempi e costruzioni di gruppi; applicazioni delle azioni

3.1. Isometrie del piano Euclideo

Il gruppo $O_2(\mathbb{R})$. Il *gruppo ortogonale* $O_2(\mathbb{R})$ è il gruppo delle isometrie del piano Euclideo che fissano un punto assegnato O. Si dividono in *proprie* ed *improprie* a seconda che conservino o rovescino un orientamento del piano (e che quindi corrispondano o meno a *movimenti rigidi* all'interno del piano). Si verifica geometricamente che le isometrie proprie sono rotazioni intorno ad O, mentre quelle improprie sono riflessioni rispetto ad un asse passante per O.

Il sottogruppo delle isometrie proprie, cioè delle rotazioni, che avendo indice due è normale, è il *gruppo ortogonale speciale* $SO_2(\mathbb{R})$. Poiché arbitrarie rotazioni del piano attorno llo stesso punto O commutano, si tratta di un gruppo abeliano. Più precisamente, essendo le rotazioni parametrizzate da un angolo $\alpha \in \mathbb{R}$, abbiamo un omomorfismo suriettivo $\mathbb{R} \to SO_2(\mathbb{R})$, di nucleo $2\pi\mathbb{Z}$. Pertanto $SO_2(\mathbb{R})$ è isomorfo a $\mathbb{R}/2\pi\mathbb{Z}$.

Il gruppo $O_2(\mathbb{R})$ è il prodotto semidiretto del sottogruppo normale $SO_2(\mathbb{R})$ con il sottogruppo generato da una qualsiasi riflessione B (di asse passante per O). Se A è una rotazione, diciamo di angolo α, allora il suo centralizzante in $O_2(\mathbb{R})$ contiene $SO_2(\mathbb{R})$, pertanto la classe di coniugio di A può solo essere lunga 1 o 2. In effetti i coniugati di A sono la stessa A, e $A^B = B^{-1}AB = A^{-1}$, che è la rotazione di angolo $-\alpha$. Quindi A appartiene al centro di $O_2(\mathbb{R})$ se e solo se $\alpha \equiv -\alpha \pmod{2\pi}$, cioè se e solo se $\alpha \equiv 0, \pi \pmod{2\pi}$. Pertanto il centro di $SO_2(\mathbb{R})$ è formato dalle rotazioni di angolo 0 (l'identità) e π, mentre tutte le altre rotazioni formano classi di coniugio $\{A, A^{-1}\}$ di lunghezza due.

Si vede anche facilmente che le riflessioni di asse passante per O, cioè gli elementi di $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$, formano un'unica classe di coniugio in $O_2(\mathbb{R})$. Infatti se B e B' sono due riflessioni avremo $B' = B^A$, dove A è una delle due rotazioni che portano l'asse di B sull'asse di B'.

Fissato un sistema di riferimento ortonormale centrato in O, gli elementi di $O_2(\mathbb{R})$ risultano rappresentati dalle matrici A *ortogonali,* cioè che soddisfano $AA^\intercal = I$. Le matrici

$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \qquad \text{e} \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix}$$

rappresentano, rispettivamente, la rotazione di angolo α, e la riflessione con asse che forma un angolo $\alpha/2$ rispetto all'asse delle ordinate. Notate che due rotazioni sono coniugate se e solo se esse hanno la stessa traccia $2\cos\alpha$; pertanto le classi di coniugio di rotazioni in $O_2(\mathbb{R})$ sono *parametrizzate* dagli elementi dell'intervallo chiuso $[-2, 2]$ (e gli estremi dell'intervallo corrispondono alle classi centrali).

I gruppi diedrali. Il gruppo D_n (talvolta indicato invece con D_{2n}, per via del suo ordine) è definito come il gruppo delle simmetrie di un poligono regolare di n lati. Si vede che tali simmetrie sono o rotazioni, intorno al centro del poligono, di un angolo pari ad un multiplo intero di $2\pi/n$, e quindi n distinte, o riflessioni rispetto ad uno degli n assi di simmetria del poligono. Dunque D_n ha ordine $2n$, e contiene un sottogruppo ciclico di indice due, che consiste delle sole rotazioni (cioè le simmetrie *proprie,* mentre le riflessioni sono quelle *improprie*).

Numerando ciclicamente i vertici del poligono, e fissato un sistema di riferimento ortonormale nel piano con origine nel centro del poligono, possiamo assumere che il vertice k abbia coordinate $(\cos 2\pi k/n,\ \sin 2\pi k/n)$. Ponendo

$$a = \begin{bmatrix} \cos 2\pi/n & \sin 2\pi/n \\ -\sin 2\pi/n & \cos 2\pi/n \end{bmatrix} \qquad \text{e} \qquad b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

avremo che $\langle a \rangle$ è il gruppo delle rotazioni del poligono, e quindi il suo laterale $b\langle a \rangle = \langle a \rangle b$ consiste delle riflessioni. Dunque

$$D_n = \{1, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$$

In effetti ba^j è la riflessione rispetto alla retta per l'origine di direzione $\pi j/n$.

Il gruppo D_n agisce transitivamente e fedelmente sull'insieme $V = \{1, 2, \dots, n\}$ dei vertici del poligono. Ad esempio a agisce come $(1, 2, \dots, n)$, mentre b agisce come

$$\begin{cases} (1, n-1)(2, n-2)\cdots(r-1, r+1) & \text{se } n = 2r \\ (1, n-1)(2, n-2)\cdots(r, r+1) & \text{se } n = 2r+1. \end{cases}$$

In particolare a non ha punti fissi su V, mentre b ne ha due (i vertici n e r) se n è pari, e uno (il vertice n) se n è dispari. L'azione sui vertici dà luogo ad un omomorfismo iniettivo $D_n \to S_n$.

Se A è un'arbitraria rotazione del piano, attorno ad un punto O, e B una riflessione rispetto ad un asse passante per O, allora vale $B^{-1}AB = A^{-1}$ (ovvero $BAB = A^{-1}$ visto che $B^2 = 1$), che si scrive anche $AB = BA^{-1}$, o ancora $BABA = 1$ (o l'equivalente $ABAB = 1$). In particolare, i generatori a e b di D_n soddisfano $a^n = 1$, $b^2 = 1$ e $(ba)^2 = 1$. In effetti queste tre regole sono completamente sufficienti per eseguire qualsiasi calcolo in D_n (a partire da elementi scritti nella forma a^j o ba^j, ed esprimendo il risultato finale nuovamente nella forma a^j o ba^j). In modo piú formale,

$$D_n = \langle x, y \colon x^n = 1, y^2 = 1, (xy)^2 = 1 \rangle$$

è una *presentazione* di D_n. (Discuteremo le presentazioni piú avanti.)

Per determinare le classi di coniugio di D_n dobbiamo distinguere due casi, a seconda della parità di n. Infatti per cominciare D_n ha centro banale se n è dispari, ma ha centro $\{1, a^{n/2}\}$ se n è pari. Ciascuna rotazione a^j poi forma una classe di coniugio insieme alla sua inversa $a^{-j} = a^{n-j}$, purché queste siano distinte, cioè $n \nmid 2j$. Per quanto riguarda le n riflessioni, esse formano un'unica classe di coniugio se n è dispari, ma due classi coniugio di lunghezza $n/2$ se n è pari. Quest'ultimo fatto si spiega geometricamente con l'esistenza di due tipi

diversi di assi di simmetria per n pari, quelli passanti per due vertici opposti e quelli passanti per i punti medi di due lati opposti.

È comunque un buon esercizio la verifica di queste affermazioni in modo indipendente dalla geometria. Ad esempio, i coniugati della rotazione a^j si trovano calcolando $(a^j)^{a^k} = a^j$ (le rotazioni commutano tutte fra loro) e $(a^j)^{ba^k} = (a^{-j})^{a^k} = a^{-j}$ (coniugando una rotazione sotto una qualsiasi riflessione si ottiene la rotazione inversa, come spiegato prima).

Si noti che il gruppo D_n è il prodotto semidiretto (interno) del sottogruppo normale $\langle a \rangle$ delle rotazioni (che è isomorfo a C_n) ed il sottogruppo generato da una particolare riflessione, diciamo $\langle b \rangle$. Conseguentemente, lo possiamo anche costruire come il prodotto semidiretto esterno $C_2 \ltimes_\alpha C_2$, dove $\alpha : C_2 \to \mathrm{Aut}(C_n)$ è l'omomorfismo tale che $b \mapsto (a \mapsto a^{-1})$.

3.2. Gruppi liberi e presentazioni

(Questo argomento non è un'applicazione delle azioni, quanto uno strumento utile per costruire o descrivere gruppi.)

Gruppi liberi. Sia F un gruppo e X un suo sottoinsieme. Si dice che F è un *gruppo libero* con *insieme libero di generatori* X (o piú semplicemente *sui generatori* X) se per ogni gruppo G ogni mappa $X \to G$ estende in modo unico ad un omomorfismo $F \to G$. (Il fatto che X generi F non è esplicitato perché si può mostrare che segue dalla richiesta di unicità dell'estensione.) Da questa *proprietà universale* dei gruppi liberi segue la loro unicità (per insiemi X di una data cardinalità): due gruppi liberi su insiemi di generatori X, e rispettivamente Y, della stessa cardinalità, sono isomorfi. (Vale anche il viceversa: se i due gruppi liberi sono isomorfi, allora X e Y hanno la stessa cardinalità; pertanto questa è determinata dal gruppo, e si dice il *rango* del gruppo libero.) Rimane da vedere l'esistenza dei gruppi liberi, che si fa con la seguente costruzione esplicita.

Dato X consideriamo anche un insieme $X^{-1} = \{x^{-1} : x \in X\}$, disgiunto da X ed in biiezione con esso. (Qui x^{-1} è solo un simbolo per un elemento di X^{-1}, che alla fine giocherà il ruolo dell'inverso di x.) Una *parola* nei generatori X e i loro inversi (formali) X^{-1} è una sequenza finita $y_1 y_2 \cdots y_n$ di elementi di $X \cup X^{-1}$. Definiamo il prodotto di due parole come la parola ottenuta giustapponendole (cioè scrivendole di seguito), e consideriamo due parole equivalenti se una delle due si può ottenere dall'altra cancellando due simboli x e x^{-1} che compaiono in posizioni adiacenti, per qualche $x \in X$. Piú in generale, consideriamo equivalenti parole che si possano ottenere l'una dall'altra applicando una sequenza delle cancellazioni appena descritte o delle operazioni inverse. In tal modo si ottiene una relazione di equivalenza sull'insieme delle parole in $X \cup X^{-1}$. Si verifica che l'insieme quoziente F ne ricava una struttura di gruppo, e che soddisfa la definizione di gruppo libero sull'insieme X.

Esempio. Il gruppo libero su un solo generatore x è il gruppo ciclico infinito $\{x^n : n \in \mathbb{Z}\}$. (In generale si scrive x^2 e x^{-2} al posto di xx e $x^{-1}x^{-1}$, ecc., quando compaiono adiacenti all'interno di una parola.) In topologia, esso appare come il gruppo fondamentale del "piano bucato" $\mathbb{C} \setminus \{0\}$ (o di un disco bucato,

se preferiamo). Piú in generale, il gruppo fondamentale del piano a cui abbiamo tolto k punti distinti è il gruppo libero su k generatori. Si può mostrare che il sottogruppo di $\mathrm{GL}(2,\mathbb{Q})$ generato dalle matrici $A = \left[\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right]$ e $B = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$ è libero di rango due, sui generatori liberi A e B.

Presentazioni di gruppi. Formalmente, una *presentazione libera* di un gruppo G è un omomorfismo suriettivo $F \to G$, dove F è un gruppo libero: avremo allora $G \cong F/R$, dove R è il nucleo dell'omomorfismo. Piú concretamente, la situazione si descrive esplicitando un insieme di generatori liberi di F, ed un sottoinsieme di R che lo generi come sottogruppo normale di F (cioè tale che R sia il piú piccolo sottogruppo normale di F che contiene quel sottoinsieme). Si scrive $G = \langle X \mid S \rangle$. Un po' informalmente, X è un insieme di simboli che rappresenta un insieme di generatori di G, mentre S è un insieme di parole in $X \cup X^{-1}$. Piú spesso gli elementi di S sono scritti come *relazioni* piuttosto che relatori, cioè come uguaglianze fra parole del tipo $w_1 = w_2$, che rappresenta il relatore $w_1 w_2^{-1}$ (cioè è equivalente all'uguaglianza $w_1 w_2^{-1} = 1$). Ancora piú informalmente, la presentazione ci dice che calcolare nel gruppo G, equivale a calcolare con i generatori assegnati X di G come fossimo in un gruppo libero, ma dove l'equivalenza di parole che ci permette di cancellare xx^{-1}, o $x^{-1}x$, è estesa ad includere le relazioni assegnate e le loro conseguenze. Dunque se una parola contiene un segmento w_1, e $w_1 = w_2$ è una forma equivalente di uno dei relatori o relazioni assegnate, la parola ottenuta rimpiazzando w_1 con w_2 rappresenta lo stesso elemento di G.

Esempio. $G = \langle x, a \mid x^2 = a^n = 1,\ x^{-1}ax = a^{-1} \rangle$ è una presentazione del gruppo diedrale D_n di ordine $2n$. Una presentazione equivalente è $G = \langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle$, come si vede sostituendo $a = yx$ nella prima (e notando che $(xy)^n = 1$ è una scrittura equivalente di $(yx)^n = 1$), e l'equivalente $y = x^{-1}a$ nella seconda. Le presentazioni $G = \langle x, a \mid x^2 = 1,\ x^{-1}ax = a^{-1} \rangle = \langle x, y \mid x^2 = y^2 = 1 \rangle$, definiscono invece il *gruppo diedrale infinito* D_∞. Ogni gruppo diedrale D_n è isomorfo ad un quoziente di D_∞.

Esempio. Consideriamo la presentazione $G = \langle x, y \mid x^7 = y^6 = 1,\ xy = yx^3 \rangle$. Notate che la terza relazione si può anche riscrivere come $x^y = x^3$.

Usando le relazioni si mostra che ogni parola in x e y è equivalente ad una parola della forma $y^j x^i$, con $0 \le i < 7$ e $0 \le j < 6$. Infatti, data una parola arbitraria $x^a y^b x^c y^d \cdots$ possiamo far diventare tutti gli esponenti positivi usando le prime due relazioni; poi ogni volta che nella parola compaiono xy (adiacenti) li possiamo rimpiazzare con yx^3; essendoci un numero finito di y nella parola, dopo un numero finito di passi li avremo portati tutti all'inizio, facendola diventare $y^j x^i$; applicando le prime due relazioni possiamo far cadere gli esponenti i e j negli intervalli specificati.

Dunque abbiamo mostrato che G ha al massimo $7 \cdot 6 = 42$ elementi. In effetti G ha proprio ordine 42. Informalmente è perché *le relazioni non permettono ulteriori semplificazioni*. Attenzione però, questo va dimostrato rigorosamente. Ad esempio, se avessimo avuto invece la presentazione $\langle x, y \mid x^7 = y^4 = 1,\ xy = yx^3 \rangle$, avremmo mostrato in modo analogo che definisce un gruppo di ordine al massimo $7 \cdot 4 = 28$, ma in realtà essa definisce un gruppo di ordine 4; infatti dalla terza

relazione nella forma $x^y = x^2$ otteniamo $x^{y^2} = (x^y)^y = (x^2)^y = (x^y)^2 = (x^2)^2 = x^4$, e iterando troviamo $x^{y^i} = x^{2^i}$, e in particolare $x^{y^4} = x^{16}$; ma essendo $y^4 = 1$ ne otteniamo $x = x^{16}$; perciò x ha ordine un divisore di 15, ed anche un divisore di 7 grazie alla prima relazione, quindi x ha ordine 1, cioè $x = 1$; in definitiva la presentazione data è equivalente a $\langle x, y \mid x = 1,\ y^4 = 1,\ y = y\rangle$, perciò definisce un gruppo ciclico di ordine 4.

Un modo per mostrare che G ha proprio ordine 42 è trovare un gruppo $\bar{G}$, di ordine noto 42, generato da due elementi X e Y che soddisfino relazioni analoghe a quelle che definiscono G. Siamo fortunati a conoscere già un tale gruppo, è il gruppo affine $\mathrm{AGL}(1, \mathbb{F}_7)$. Prendendo come X una qualunque traslazione non banale, ad esempio $X : z \mapsto z + 1$, e come Y una mappa affine con coefficiente di dilatazione 3 (oppure 5), diciamo $Y : z \mapsto 3z$, sono soddisfatte le relazioni $X^7 = Y^6 = 1$ e $X^Y = X^3$, e $\mathrm{AGL}(1, \mathbb{F}_7)$ è generato da X e Y. (Attenzione a questo ultimo punto, rimpiazzando Y con $Y' : z \mapsto 2z$ le relazioni rimarrebbero soddisfatte, ma $\langle X, Y\rangle$ sarebbe un sottogruppo proprio di $\mathrm{AGL}(1, \mathbb{F}_7)$, di indice 2 in quanto $Y' = Y^2$.)

Esempio. Modifichiamo leggermente la presentazione del gruppo G dell'esempio precedente, considerando $H = \langle x, y \mid x^7 = y^6 = 1,\ xy = yx^2\rangle$.

Come nell'esempio precedente vediamo che H ha ordine al massimo 42. Anche in questo caso, *dovrebbe* essere proprio 42 perché pare che *le relazioni non permettano ulteriori semplificazioni*. Il modo più semplice per dimostrarlo è, nuovamente, trovare un gruppo $\bar{H}$, di ordine noto 42, generato da due elementi X e Y che soddisfino relazioni analoghe a quelle che definiscono H. Stavolta però non conosciamo già un tale gruppo, perciò bisogna costruirlo. Ma ce lo suggerisce la presentazione: consideriamo il prodotto semidiretto di un gruppo di ordine 7 generato da X, con un gruppo ciclico di ordine 6 generato da un elemento Y. La definizione di prodotto semidiretto ci richiede di scegliere un omomorfismo $\alpha : \langle Y\rangle \to \langle \mathrm{Aut}(\langle X\rangle)$. Essendo $\langle Y\rangle$ ciclico basta assegnare $Y\alpha$, e poiché Y ha ordine 6 siamo autorizzati a mandare Y in qualsiasi elemento di ordine un divisore di 6. Decidiamo che α mandi Y nell'automorfismo di $\langle X\rangle$ che manda X in X^2 (e di conseguenza X^i in X^{2i}, un automorfismo di un gruppo ciclico basta specificarlo mandando un generatore in un altro), che ha ordine 3 in quanto $((X^2)^2)^2 = X$.

A questo punto il prodotto semidiretto $\bar{H} := \langle Y\rangle \ltimes \langle X\rangle$ soddisfa $X^7 = 1$, $Y^6 = 1$ e $X^Y = X^{Y\alpha} = X^2$, come volevamo, e quindi è isomorfo ad un quoziente di H (essendoci un omomorfismo suriettivo di H su $\bar{H}$, dato assegnando $x \mapsto X$ e $y \mapsto Y$). Avendo mostrato in precedenza che H ha al massimo ordine 42, concludiamo che $H \cong \bar{H}$.

Per concludere, H non è isomorfo a G perché a differenza di G ha centro non banale: vi appartiene (l'immagine di) y^3, anzi lo genera.

Esempio. Una presentazione del gruppo simmetrico S_n, per $n > 1$, è data da generatori $x_1, \ldots, x_{n-1}$ e dalle relazioni

$$1 = x_i^2 = (x_j x_{j+1})^3 = (x_k x_\ell)^2,$$

dove $1 \leq i \leq n-1$, $1 \leq j \leq n-2$, $1 \leq k < \ell - 1 \leq n-2$. È chiaro che tali relazioni sono soddisfatte in S_n prendendo come x_i la trasposizione $(i, i+1)$: quindi il gruppo definito dalla presentazione ha un quoziente isomorfo a S_n. Si può poi dimostrare (ma non lo facciamo) che le relazioni sono anche sufficienti a definire S_n.

3.3. I gruppi di ordine pq

Determineremo la struttura dei gruppi il cui ordine è il prodotto di due primi.[1] Se i primi non sono distinti l'ordine è il quadrato di un numero primo, e sappiamo che un tale gruppo è abeliano, e quindi è ciclico o il prodotto diretto di due gruppi ciclici. Quindi possiamo assumere i due primi distinti.

Sia G un gruppo di ordine pq, dove p e q sono primi distinti, diciamo con $p < q$. Mostreremo che allora G è prodotto semidiretto di un sottogruppo normale di ordine q e un sottogruppo di ordine p. Grazie al Lemma di Cauchy, G ha almeno un elemento di ordine p ed uno di ordine q. Siano P e Q i sottogruppi generati da questi due elementi.

Si può vedere in almeno due modi che Q è un sottogruppo normale di G. Quello piú elementare è che se Q non fosse normale, e $Q^g \neq Q$ fosse un suo coniugato distinto, avremmo $Q \cap Q^g = 1$ e quindi $|G| \geq |QQ^g| = |Q|^2 > |G|$, una contraddizione. (Piú in generale, se $H \leq G$ e $|H| > |G : H|$ allora $H \cap H^g \neq 1$ per ogni $g \in G$.) Il secondo modo dipende da un fatto mostrato studiando le azioni per moltiplicazione a destra: l'indice di Q in G è il piú piccolo divisore primo di G, quindi $Q \trianglelefteq G$.

A questo punto, essendo chiaramente $P \cap Q = 1$, concludiamo che $G = P \ltimes Q$, un prodotto semidiretto, come volevamo dimostrare. Però possiamo anche dire di piú. Nell'azione di P su Q per coniugio, le orbite possono solo essere lunghe 1 o p. Ma l'insieme delle orbite di lunghezza 1 è $\mathbf{C}_Q(P)$, un sottogruppo di Q, che essendo q primo può solo essere Q o 1. Nel primo caso G è il prodotto diretto di Q e P, e quindi è ciclico. Nel secondo caso abbiamo che $|Q \setminus \{1\}|$ è multiplo di p. In conclusione, un gruppo di ordine pq può non essere ciclico solo se $q \equiv 1 \pmod{p}$. Ad esempio, l'unico gruppo di ordine 15 è quello ciclico.

Un approccio alternativo a quest'ultimo ragionamento è il seguente, che in realtà produrrà una conclusione piú forte. Il gruppo G avrà una presentazione della forma

$$G = \langle x, y \colon x^q = 1, y^p = 1, x^y = x^a \rangle,$$

dove a è un opportuno intero, e poichè $x^{a^p} = x^{y^p} = x$ dovrà essere $a^p \equiv 1 \pmod{q}$. Viceversa si vede facilmente che se a soddisfa questa condizione allora la presentazione definisce proprio un gruppo di ordine pq. Notate che di a importa realmente solo il resto modulo q. Nel caso $a \equiv 1 \pmod{p}$ avremo $x^y = x$, e quindi si tratterà in effetti di un prodotto diretto, e quindi G sarà ciclico. Poichè grazie al Piccolo Teorema di Fermat vale anche $a^{q-1} \equiv 1 \pmod{q}$, se p non divide q segue che $a \equiv 1 \pmod{q}$, e quindi G è ciclico, come avevamo già concluso in altro modo.

[1] Alcuni passaggi del ragionamento sarebbero piú rapidi se già conoscessimo i Teoremi di Sylow.

Se invece p divide $q-1$, oltre al caso $a \equiv 1 \pmod q$ avremo altre $p-1$ possibilità diverse per a modulo q, corrispondenti agli elementi di ordine p nel gruppo $\mathbb{F}_q^*$, che sappiamo essere ciclico. Ma se rimpiazziamo y con $\bar{y} = y^k$ nella presentazione, dove k è un intero primo con p, otteniamo per G la nuova presentazione

$$G = \langle x, \bar{y} \colon x^q = 1, \bar{y}^p = 1, x^{\bar{y}} = x^{a^k} \rangle.$$

Fissato $a \not\equiv 1 \pmod p$, al variare di k primo con p il resto modulo q dell'esponente a^k nella presentazione varia proprio su tutti gli elementi di ordine p in $\mathbb{F}_q$. Ne concludiamo che tutte queste scelte per a danno luogo allo stesso gruppo G. Perciò se p divide $q-1$ ci sono esattamente due gruppi di ordine pq a meno di isomorfismo: quello ciclico e quello appena descritto.

3.4. Altri esempi di gruppi di origine *geometrica*

I solidi platonici e i loro gruppi di simmetrie. [Vedi lezioni e documento separato.]

Alcuni gruppi lineari. Il *gruppo lineare generale* $\mathrm{GL}(n, F)$ è il gruppo delle matrici $n \times n$ invertibili a coefficienti nel campo F, ed il *gruppo lineare speciale* $\mathrm{SL}(n, F)$ è il sottogruppo normale costituito da quelle di determinante 1 (cioè il nucleo dell'omomorfismo $\det : \mathrm{GL}(n, F) \to F^*$). L'azione naturale di $\mathrm{GL}(n, F)$ sullo spazio (dei vettori riga) F^n induce un'azione sull'insieme delle basi di tale spazio; tale azione è transitiva e ogni stabilizzatore è 1, quindi l'azione è regolare. In particolare, se F è il campo $\mathbb{F}_q$ con q elementi, abbiamo che l'ordine di $\mathrm{GL}(n, F)$ è uguale al numero di basi di $\mathbb{F}_q^n$, perciò

$$\begin{aligned} |\mathrm{GL}(n, \mathbb{F}_q)| &= (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \\ &= q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1). \end{aligned}$$

Grazie al teorema fondamentale sugli omomorfismi abbiamo poi

$$|\mathrm{SL}(n, \mathbb{F}_q)| = |\mathrm{GL}(n, \mathbb{F}_q)|/(q - 1).$$

Il centro di $\mathrm{GL}(n, F)$ e del suo sottogruppo $\mathrm{SL}(n, F)$ consistono delle sole matrici scalari (invertibili nel primo caso, e di determinante uno nel secondo). Entrambe le affermazioni sono conseguenze della seguente affermazione leggermente piú forte: il centralizzante di $\mathrm{SL}(n, F)$ in $\mathrm{GL}(n, F)$ consiste delle sole matrici scalari invertibili. È infatti chiaro che le matrici scalari commutano con tutte le altre. Per il viceversa è sufficiente che verifichiate che se una matrice A commuta con tutte le matrici della forma $1 + E_{ij}$ con $i \neq j$, allora A deve essere scalare.[2]

[2]Ecco una dimostrazione con le mappe lineari al posto delle matrici. Oltre che essere più elegante ha il vantaggio di essere valida anche in dimensione infinita. Sia L una mappa lineare invertibile da V in se stesso, e assumiamo che essa commuti con ogni mappa lineare se $\dim(V) = \infty$, ma solo quelle di determinante uno in caso $\dim(V) > \infty$. È sufficiente mostrare che allora ogni $v \in V$ è un autovettore per L, da cui seguirà subito che L è la moltiplicazione per uno scalare. Infatti supponendo per assurdo che $uL = v$, per certi $u, v \in V$ linearmente indipendenti, notiamo che esiste una mappa lineare M, di determinante 1 in caso $\dim(V) > \infty$, tale che $uM = u$ e $vM = u + v$. Ma allora $uML = u$ mentre $uLM = u + v$, il che contraddice le ipotesi.

Indicando con Z il centro di $\mathrm{GL}(n,F)$, il gruppo quoziente $\mathrm{PGL}(n,F) := \mathrm{GL}(n,F)/Z$ è il *gruppo lineare generale proiettivo*. Sul campo $\mathbb{F}_q$ ha perciò anche lui ordine

$$|\mathrm{PGL}(n,\mathbb{F}_q)| = |\mathrm{GL}(n,\mathbb{F}_q)|/(q-1).$$

(Attenzione però: $\mathrm{SL}(n,\mathbb{F}_q)$ e $\mathrm{PGL}(n,\mathbb{F}_q)$ hanno lo stesso ordine, ma in generale non sono isomorfi.)[3] Come abbiamo visto, il centro di $\mathrm{SL}(n,F)$ consiste delle matrici scalari di determinante 1, cioè è $Z \cap \mathrm{SL}(n,F)$, dove come sopra Z indica il centro di $\mathrm{GL}(n,F)$. Il gruppo quoziente $\mathrm{PSL}(n,F) := \mathrm{SL}(n,F)/(Z \cap \mathrm{SL}(n,F))$ è il *gruppo lineare speciale proiettivo*. Le matrici scalari $\mathrm{diag}(\alpha,\cdots,\alpha)$ di determinante 1 sono tante quante le soluzioni di $\alpha^n = 1$ in F, e quindi al massimo n, in generale. Ad esempio, $\mathrm{SL}(n,\mathbb{R})$ ha centro di ordine 2 se n è pari, mentre ha centro banale se n è dispari. Se poi F è il campo finito $\mathbb{F}_q$, il numero di tali soluzioni, e quindi l'ordine del centro di $\mathrm{SL}(n,\mathbb{F}_q)$, è il massimo comun divisore $(n, q-1)$ (poiché $\mathbb{F}_q$ è ciclico di ordine $q-1$). Avremo quindi

$$|\mathrm{PSL}(n,\mathbb{F}_q)| = |\mathrm{SL}(n,\mathbb{F}_q)|/(n,q-1).$$

In particolare, per $n = 2$ abbiamo

$$|\mathrm{GL}(2,\mathbb{F}_q)| = q(q-1)(q^2-1), \quad |\mathrm{SL}(2,\mathbb{F}_q)| = |\mathrm{PGL}(2,\mathbb{F}_q)| = q(q-1)(q+1),$$

e $|\mathrm{PSL}(2,\mathbb{F}_q)|$ è uguale a $|\mathrm{SL}(2,\mathbb{F}_q)|$ o alla sua metà, a seconda che q sia pari (e quindi potenza di 2) o dispari. (Se q è una potenza di 2 abbiamo $\mathrm{SL}(2,\mathbb{F}_q) \cong \mathrm{PGL}(2,\mathbb{F}_q) \cong \mathrm{PSL}(2,\mathbb{F}_q)$.) Ad esempio,

$$\begin{array}{llll}
|\mathrm{GL}(2,\mathbb{F}_2)| = 6, & & & \\
|\mathrm{GL}(2,\mathbb{F}_3)| = 48, & |\mathrm{SL}(2,\mathbb{F}_3)| = |\mathrm{PGL}(2,\mathbb{F}_3)| = 24, & |\mathrm{PSL}(2,\mathbb{F}_3)| = 12, & \\
|\mathrm{GL}(2,\mathbb{F}_4)| = 180, & |\mathrm{SL}(2,\mathbb{F}_4)| = 60, & & \\
|\mathrm{GL}(2,\mathbb{F}_5)| = 480, & |\mathrm{SL}(2,\mathbb{F}_5)| = |\mathrm{PGL}(2,\mathbb{F}_5)| = 120, & |\mathrm{PSL}(2,\mathbb{F}_5)| = 60, & \\
|\mathrm{GL}(2,\mathbb{F}_7)| = 2016, & |\mathrm{SL}(2,\mathbb{F}_7)| = |\mathrm{PGL}(2,\mathbb{F}_7)| = 336, & |\mathrm{PSL}(2,\mathbb{F}_7)| = 168, & \\
|\mathrm{GL}(2,\mathbb{F}_9)| = 5760, & |\mathrm{SL}(2,\mathbb{F}_9)| = |\mathrm{PGL}(2,\mathbb{F}_9)| = 720, & |\mathrm{PSL}(2,\mathbb{F}_9)| = 360, &
\end{array}$$

ma anche $|\mathrm{GL}(3,\mathbb{F}_2)| = 168 = 2^3 \cdot 3 \cdot 7$. Abbiamo già incontrato gruppi di alcuni di questi ordini, ed infatti

$$\begin{array}{ll}
\mathrm{GL}(2,\mathbb{F}_2) \cong S_3, & \\
\mathrm{PGL}(2,\mathbb{F}_3) \cong S_4 & (\text{ma} \ncong \mathrm{SL}(2,\mathbb{F}_3), \text{ che invece ha centro non banale}), \\
\mathrm{PSL}(2,\mathbb{F}_3) \cong A_4, & \\
\mathrm{PGL}(2,\mathbb{F}_5) \cong S_5 & (\text{ma} \ncong \mathrm{SL}(2,\mathbb{F}_5), \text{come sopra}), \text{ e} \\
\mathrm{SL}(2,\mathbb{F}_4) \cong \mathrm{PSL}(2,\mathbb{F}_5) \cong A_5. &
\end{array}$$

[3]Gli ordini di questi tre tipi di gruppi lineari sono polinomi in q. I gradi di questi polinomi, cioè n^2, n^2-1 e n^2-1, sono le dimensioni, reali o complesse, dei corrispondenti gruppi di Lie reali o complessi, $\mathrm{GL}(n,F)$, $\mathrm{SL}(n,F)$, e $\mathrm{PGL}(n,F)$, per $\mathbb{F} = \mathbb{R}$ o $\mathbb{C}$. Anche $\mathrm{PSL}(n,F)$ ha dimensione n^2-1, la stessa del gruppo $\mathrm{SL}(n,F)$ di cui è quoziente, perché il quoziente è fatto rispetto al sottogruppo discreto $Z \cap \mathrm{SL}(n,F)$.

Quest'ultimo è il piú piccolo gruppo semplice non abeliano. Il successivo gruppo semplice non abeliano, andando in ordine crescente, è $\mathrm{PSL}(2,\mathbb{F}_7) \cong \mathrm{GL}(3,\mathbb{F}_2)$. Il successivo ancora è $\mathrm{PSL}(2,\mathbb{F}_9) \cong A_6$, di ordine $6!/2 = 360 = 2^3 \cdot 3^2 \cdot 5$. (I successivi sono, nell'ordine, $\mathrm{SL}(2,\mathbb{F}_8)$ di ordine $504 = 2^3 \cdot 3^2 \cdot 7$, $\mathrm{PSL}(2,\mathbb{F}_{11})$ di ordine $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$, $\mathrm{PSL}(2,\mathbb{F}_{13})$ di ordine $1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$, $\mathrm{PSL}(2,\mathbb{F}_{17})$ di ordine $2448 = 2^4 \cdot 3^2 \cdot 17$, ed A_7 di ordine $7!/2 = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.)

Si dimostra che $\mathrm{PSL}(n,\mathbb{F}_q)$ è un gruppo semplice se $n \geq 2$, con le sole eccezioni viste dei casi $(n,q) = (2,2)$ e $(2,3)$.

3.5. Applicazioni delle azioni

Costruzione di isomorfismi.

Esempio. Il gruppo $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2)$ agisce transitivamente sull'insieme dei tre vettori non nulli di $(\mathbb{F}_2)^2 \setminus \{0\}$, cioè $(1,0)$, $(0,1)$ e $(1,1)$, e si vede subito che l'azione è fedele. Ne otteniamo un isomorfismo $\mathrm{GL}(2,\mathbb{F}_2) \to S_3$.

Esempio. Il gruppo $\mathrm{SL}(2,\mathbb{F}_4)$ agisce transitivamente sull'insieme dei 15 vettori non nulli di $(\mathbb{F}_4)^2 \setminus \{0\}$. Ma naturalmente manda vettori proporzionali in vettori proporzionali, e quindi agisce, sempre transitivamente, sull'insieme delle 5 rette per l'origine in $(\mathbb{F}_4)^2$, cioè sulla retta proiettiva $P^1(\mathbb{F}_4) = \mathbb{F}_4 \cup \{\infty\}$. Si vede facilmente che l'azione è fedele. (In generale, il nucleo dell'azione di $\mathrm{SL}(2,\mathbb{F}_q)$ o $\mathrm{GL}(2,\mathbb{F}_q)$ sulla retta proiettiva $P^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ consiste delle matrici scalari, e quindi si ha un'azione fedele del corrispondente gruppo proiettivo; nel presente caso però l'unica matrice scalare è l'identità.) Ne otteniamo un isomorfismo $\mathrm{SL}(2,\mathbb{F}_4) \to S_5$. La sua immagine ha ordine 60, e quindi deve coincidere con l'unico sottogruppo di S_5 di indice 2, che è A_5.

L'isomorfismo $\mathrm{PGL}(2,\mathbb{F}_5) \cong S_5$, da cui segue subito che $\mathrm{PSL}(2,\mathbb{F}_5) \cong A_5$, è piú difficile da costruire (mentre è invece facile da costruire un omomorfismo iniettivo di $\mathrm{PGL}(2,\mathbb{F}_5)$ in S_6).

Il carattere associato a un'azione. Il carattere associato ad un'azione di G su un insieme finito Ω è la funzione definita per $g \in G$ da

$$\sharp\{x \in \Omega : \omega g = \omega\},$$

cioè $\chi(g)$ indica il numero di punti fissi di (cioè fissati da) g nell'azione.

Il carattere χ assume lo stesso valore su elementi coniugati di G, cioè $\chi(g^h) = \chi(g)$ se $g, h \in G$, quindi è sufficiente calcolarlo su un elemento di ciascuna classe di coniugio. Inoltre $\chi(g^m) \geq \chi(g)$ per ogni intero m, da cui segue che $\chi(g^m) = \chi(g)$ se m è primo con l'ordine $|g|$ di g.

Il lemma di Cauchy-Frobenius. Se G e Ω sono finiti, il numero di orbite di G su Ω è uguale a $\frac{1}{|G|}\sum_{g \in G} \chi(g)$, cioè al numero medio di punti fissi di g al variare di $g \in G$.

DIMOSTRAZIONE. Abbiamo

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}\chi(g) &= \frac{1}{|G|}\sum_{g\in G}\sharp\{x\in\Omega : \omega g=\omega\}\\ &= \frac{1}{|G|}\,\sharp\{(g,\omega)\in G\times\Omega : \omega g=\omega\}\\ &= \frac{1}{|G|}\sum_{\omega\in\Omega}\sharp\{g\in G : \omega g=\omega\}\\ &= \sum_{\omega\in\Omega}\frac{|G_\omega|}{|G|} = \sum_{\omega\in\Omega}\frac{1}{|\omega G|}.\end{aligned}$$

Raggruppando gli addendi corrispondenti ad una stessa orbita, stiamo sommando $|\omega G|\cdot(1/|\omega G|)=1$ per ciascun'orbita, ottenendo cosí come somma il numero di orbite. □

Applicazione a problemi di conteggio. Esempio: collane di perline [vedi lezioni]. Esempio: grafi [vedi lezioni o [**CUD02**]]

CAPITOLO 4

I teoremi di Sylow

4.1. Enunciati e dimostrazioni

[Vedi lezioni e documento separato.]

4.2. Applicazione ai gruppi semplici

[Vedi lezioni e documento separato. Qui solo una traccia.]

Teorema. Se un gruppo semplice non abeliano G soddisfa $|G| \leq 100$, allora $|G| = 60$.

DIMOSTRAZIONE. La dimostrazione utilizza diversi lemmi, ciascuno dei quali esclude certi possibili valori per $|G|$. Nelle ipotesi assunte, per p, q, r primi distinti abbiamo:

(1) $|G| \neq p^a$ per ogni a (tali gruppi hanno centro non banale);
(2) $|G| \neq pq$ (tali gruppi, già studiati in precedenza, hanno un p-sottogruppo di Sylow normale o un q-sottogruppo di Sylow normale);
(3) $|G| \neq p^2q$ (anche questi hanno un p-sottogruppo di Sylow normale o un q-sottogruppo di Sylow normale); [1]
(4) $|G| \neq pqr$;
(5) $|G| \neq 2p^a, 3p^a, 4p^a$, per $p \neq 2, 3, 2$ risp.; infatti in questi casi un p-sottogruppo di Sylow ha indice minore di 5, ma un gruppo semplice non abeliano G non può avere un sottogruppo proprio di indice minore di 5, in quanto l'azione per moltiplicazione sull'insieme dei suoi laterali sinistri darebbe un omomorfismo iniettivo di G nel gruppo S_n, che è risolubile per $n < 5$;
(6) $|G|$ non è il doppio di un numero dispari. [2]

Tenendo conto di tutte queste condizioni, per $|G| \leq 100$ rimangono le seguenti possibilità:

$$40 = 2^3 \cdot 5, \qquad 56 = 2^3 \cdot 7, \qquad 60 = 2^2 \cdot 3 \cdot 5, \qquad 72 = 2^3 \cdot 3^2,$$
$$80 = 2^4 \cdot 5, \qquad 84 = 2^2 \cdot 3 \cdot 7, \qquad 88 = 2^3 \cdot 11.$$

I casi 40, 84, 88 sono facili da escludere in quanto un arbitrario gruppo di uno di tali ordini deve avere $n_p = 1$ per un certo p. Nei casi 56 e 80 tale conclusione

[1] Un teorema di Burnside, che si dimostra mediante la teoria della rappresentazione, afferma che i gruppi di ordine $p^a q^b$ sono risolubili, e quindi non possono essere semplici non abeliani.

[2] Questo è un caso speciale del fatto, di ragioni piú profonde, che i 2-sottogruppi di Sylow di un gruppo semplice non abeliano non possono essere ciclici.

non è cosí immediata, ma anch'essi si possono escludere facilmente contando gli elementi di un certo ordine, come nella dimostrazione del punto (3).

Concludiamo che $|G| = 60$. □

Teorema. Se G è un gruppo semplice di ordine 60, allora $G \cong A_5$.

Dimostrazione. Con i soliti ragionamenti si scopre che $n_5 = 6$, $n_3 = 10$, e $n_2 = 5$ o 15. Nel primo caso otteniamo un omomorfismo di G in S_5, anzi in A_5 ed iniettivo, essendo G semplice, che quindi è l'isomorfismo cercato. Nel secondo caso (da escludere), contando gli elementi di ordine 2, 3 e 5 si trova che i 2-sottogruppi di Sylow non possono essere tutti disgiunti, e quindi ve n'è almeno due con intersezione non banale, diciamoli P_1 e P_2. Notando che essi sono entrambi abeliani in quanto hanno ordine $4 = 2^2$, se $1 \neq y \in P_1 \cap P_2$ allora $\mathbf{C}_G(y)$ li contiene entrambi e quindi ha ordine maggiore di 4 (e multiplo di 4). Pertanto il suo indice è un divisore proprio di 15, e naturalmente maggiore di 1 altrimenti y sarebbe centrale in G. Il valore 3 non è possibile per quanto visto in precedenza, mentre il valore 5 di nuovo fornisce un isomorfismo di G con A_5. (In realtà il caso $n_2 = 15$ non può avvenire, come si vede a posteriori, perché cosí non accade in A_5.) □

4.3. Altri esempi di applicazione

Esempio. Un gruppo di ordine $255 = 3 \cdot 5 \cdot 17$ è necessariamente ciclico. Infatti dai teoremi di Sylow otteniamo che $n_7 = 1$, mentre $n_5 = 1$ o 51, e $n_3 = 1$ o 85. Se fosse $n_5 = 51$ allora G avrebbe $4 \cdot 51 = 204$ elementi di ordine 5, mentre se fosse $n_3 = 85$ allora G avrebbe $2 \cdot 85 = 170$ elementi di ordine 3. Chiaramente queste possibilità non possono valere entrambe, e quindi G ha o un 5-sottogruppo di Sylow normale, o un 3-sottogruppo di Sylow normale. Contando semplicemente gli elementi di ordine p, q e r piú di questo non si può ottenere. Ma c'è un altro ragionamento possibile, anche avendo solo notato che G ha un p-sottogruppo di Sylow normale, diciamolo P. Se Q e R sono un q-sottogruppo di Sylow e un r-sottogruppo di Sylow, allora PQ e PR sono sottogruppi di G, e quindi hanno ordini $3 \cdot 5$ e $3 \cdot 17$. I teoremi di Sylow applicati a PQ e PR mostrano che Q e R sono loro sottogruppi normali, rispettivamente (infatti abbiamo già mostrato che gruppi di tali ordini sono ciclici). Ma allora $PQ \leq N_G(p)$, da cui $n_q \leq 5$ e perciò $n_q = 1$. Analogamente, $n_r = 1$. Quindi G è il prodotto diretto (interno) di PQ e R, diciamo, e pertanto è ciclico.

Esercizio. Se esiste un gruppo semplice G di ordine $168 = 2^3 \cdot 3 \cdot 7$, allora esso ha esattamente 48 elementi di ordine 7.

CAPITOLO 5

Cenni di teoria della rappresentazione

5.1. Rappresentazioni e moduli.

Moduli irriducibili e completamente riducibili. Teorema di Maschke. Lemma di Schur. Si veda [**CUD02**, Chapter 4].

5.2. Tabelle dei caratteri.

Caratteri. Si veda [**CUD02**, Section 5.1].

Relazioni di ortogonalità. Ricordo i fatti fondamentali, di cui posponiamo o omettiamo le dimostrazioni (si veda [**CUD02**, Section 5.2]).

I caratteri formano una base ortonormale per lo spazio delle funzioni di classe su G (cioè le funzioni $G \to \mathbb{C}$ che sono costanti sulle classi di coniugio), rispetto al prodotto Hermitiano

$$(\chi|\psi) = \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)}.$$

L'ortonormalità dei caratteri è anche detta la *prima relazione di ortogonalità* per la tabella dei caratteri di G, nel senso che rappresenta l'ortogonalità delle righe della tabella (con le entrate pesate in modo opportuno). In particolare, rappresentazioni irriducibili non equivalenti hanno caratteri distinti, e ne segue che due rappresentazioni (eventualmente riducibili) sono equivalenti se e solo se esse hanno lo stesso carattere. Un'altra conseguenza è che il numero di caratteri irriducibili (cioè di rappresentazioni irriducibili) di G è uguale al numero di classi di coniugio di G (cioè la tabella dei caratteri è quadrata).

Si vede facilmente che la prima relazione di ortogonalità, insieme al fatto che i caratteri formano una base per lo spazio delle funzioni di classe, è equivalente ad una opportuna ortogonalità delle colonne della tabella, detta la *seconda relazione di ortogonalità*

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(g)\overline{\chi(h)} = \begin{cases}|\mathbf{C}_G(g)| & \text{se } g \text{ e } h \text{ sono coniugati in } G,\\ 0 & \text{altrimenti.}\end{cases}$$

Il caso particolare $h = 1$ esprime il fatto importante che $\rho = \sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\chi$, dove ρ è la rappresentazione regolare di G (cioè quella che si ottiene dall'azione regolare di G, l'azione di G su se stesso per moltiplicazione, e quindi $\rho(1) = |G|$ e $\rho(g) = 0$ per $g \neq 1$). Dunque il modulo regolare contiene tutti i moduli irriducibili per G come sottomoduli, ciascuno con molteplicità pari alla sua dimensione (o *grado*).

CAPITOLO 6

Cenni sui gruppi di Lie

In questo capitolo assumiamo che il campo F sia $\mathbb{R}$ o $\mathbb{C}$. Per il poco tempo a disposizione sorvoleremo sugli aspetti analitici dei gruppi di Lie. Inoltre, ometteremo quasi tutte le dimostrazioni.

6.1. Gruppi di Lie, sottogruppi, omomorfismi

Un *gruppo di Lie* (*reale* o *complesso* a seconda che $F = \mathbb{R}$ o $\mathbb{C}$) è un gruppo G che sia allo stesso tempo una varietà differenziabile (diciamo C^∞) e tale che la mappa *moltiplicazione* $G \times G \to G, \quad (g, h) \mapsto gh$ sia differenziabile. In altre parole, le coordinate (locali) di gh devono essere funzioni differenziabili delle coordinate di g e quelle di h. Da questo segue facilmente (ad esempio, [**FS97**, Exercise 9.1]) che anche la mappa *inverso* $G \to G, \quad g \mapsto g^{-1}$ è differenziabile. Notate che ogni gruppo di Lie complesso è automaticamente un gruppo di Lie reale di dimensione doppia (ma non viceversa).

Esempio. Esempi di gruppi di Lie su K sono: F, F^n, F^*, $\mathrm{GL}(n, F)$ (cioè le trasformazioni lineari invertibili di uno spazio vettoriale di dimensione n), $\mathrm{AGL}(n, F)$ (cioè le trasformazioni affini invertibili di uno spazio affine di dimensione n), i vari altri gruppi lineari o lineari proiettivi che abbiamo introdotto, quali ortogonali, ecc.

Ad esempio, nel caso di $\mathrm{GL}(n, F)$ esiste un sistema di coordinate globali date dalle n^2 componenti di una matrice $g \in \mathrm{GL}(n, F)$; i coefficienti di un prodotto gh sono dati da $\sum_j g_{ij} h_{jk}$, quindi funzioni polinomiali, e perciò differenziabili, delle componenti di g e di h; analogamente, la componente generica di g^{-1} è un polinomio nelle componenti di g diviso per $\det(g)$, che è anch'esso funzione polinomiale dei g_{ij}, quindi le coordinate di g^{-1} sono funzioni differenziabili di quelle di g.

Un sottogruppo H di un gruppo di Lie G è detto un *sottogruppo di Lie* se è anche una sottovarietà di G. Essenzialmente ciò significa (se G ha dimensione n e H ha dimensione m) che in un intorno in G di ciascun elemento di H, il sottogruppo H è definito dall'annullarsi di $n - m$ di funzioni differenziabili, e la matrice Jacobiana di queste funzioni rispetto alle n coordinate locali di G ha rango massimo (cioè $n - m$) nell'intorno considerato. (Per il Fatto Importante notato piú sotto, basta verificarlo in un intorno di 1.)

Esempio. Il gruppo speciale lineare $\mathrm{SL}(n, F)$ è un sottogruppo di Lie di $\mathrm{GL}(n, F)$, di codimensione 1 in quanto definito (globalmente in quanto $\mathrm{GL}(n, F)$ ha coordinate globali) dalla singola equazione $\det(g) = 1$. Quindi $\mathrm{SL}(n, F)$ ha dimensione $n^2 - 1$.

Il gruppo ortogonale $\mathrm{O}(n, F)$ è il sottogruppo di $\mathrm{GL}(n, F)$ definito dalla condizione $gg^\intercal = 1$. Scritta in coordinate questa condizione si esprime con le equazioni $\sum_j g_{ij}\, g_{kj} = \delta_{ik}$. Assumendo $i \le k$ per simmetria, queste equazioni sono in numero di $n(n+1)/2$, e si verifica che sono "indipendenti" nel senso che la corrispondente matrice Jacobiana non si annulla mai. Quindi $\mathrm{O}(n, F)$ ha codimensione $n(n+1)/2$ in $\mathrm{GL}(n, F)$, e perciò è un gruppo di Lie di dimensione $n(n-1)/2$.

Il gruppo unitario $\mathrm{U}(n)$ è un sottogruppo di $\mathrm{GL}(n, \mathbb{C})$ definito dalla condizione $g\bar{g}^\intercal = 1$ (cioè $gg^* = 1$). Scritta in coordinate questa condizione si esprime con le equazioni $\sum_j g_{ij}\, \bar{g}_{kj} = \delta_{ik}$. Per ciascuna coppia di indici (i, k) con $i < k$ abbiamo un'equazione (di funzioni complesse, differenziabili in senso reale ma non in senso complesso), che diventa due equazioni separando parti reale e parte immaginaria. Per $i = k$ abbiamo la singola equazione $\sum_j |g_{ij}|^2 = 1$. Dunque abbiamo in totale n^2 equazioni reali, che si possono verificare "indipendenti" studiando la matrice Jacobiana. Poichè $\mathrm{GL}(n, \mathbb{C})$, visto come gruppo di Lie reale, ha dimensione $2n^2$, concludiamo che $\mathrm{U}(n)$ è un sottogruppo di Lie reale di $\mathrm{GL}(n, \mathbb{C})$, di dimensione n^2.

Una mappa fra gruppi di Lie G ed H è un *omomorfismo* (di gruppi di Lie) se è un omomorfismo di gruppi astratti, ed è anche una mappa differenziabile.

Fatto importante. Segue dalla definizione di gruppo di Lie che la mappa *traslazione a sinistra* $L_g : x \mapsto gx$ (cosí come la *traslazione a destra* $R_g : x \mapsto xg$) è differenziabile, e naturalmente cosí è la sua inversa $L_{g^{-1}}$. Dunque ogni intorno di un generico elemento g di G è diffeomorfo ad un intorno dell'origine, tramite $L_{g^{-1}}$ (o $R_{g^{-1}}$, se preferiamo). Ne segue che proprietà *locali* di G si possono studiare in un intorno dell'elemento neutro 1 (piuttosto che in un intorno di un punto generico). In particolare, per verificare che un sottogruppo H di un gruppo di Lie G è un sottogruppo di Lie basta verificarlo in un intorno dell'elemento neutro di G. Analogamente, se G e H sono gruppi di Lie, per verificare che un omomorfismo di gruppi astratti $G \to H$ è un omomorfismo di gruppi di Lie basta verificare che è differenziabile in un intorno dell'elemento neutro di G. Un'altra conseguenza importante di questo fatto è che ogni gruppo di Lie (reale) G è una varietà orientabile (si legga ad esempio [**FS97**, 9.1]).

6.2. Azione di un gruppo di Lie su una varietà

Un'azione [1] di un gruppo di Lie G su una varietà differenziabile X è un omomorfismo α di G in $\mathrm{Diff}(X)$, il gruppo dei diffeomorfismi di X, tale che la mappa $G \times X \to X$, $(g, x) \mapsto gx$ sia differenziabile. (In pratica è un'azione come gruppo astratto, con la richiesta aggiuntiva che tutte le mappe in gioco siano differenziabili.)

Orbite e stabilizzatori sono definiti come per le azioni di gruppi astratti, e godono delle seguenti proprietà.

[1] Nell'area dei gruppi di Lie è piú comune scrivere le mappe a sinistra, e ci adeguiamo, malgrado la differente notazione usata nei capitoli precedenti.

TEOREMA (orbita-stabilizzatore). *Per ogni punto $x \in X$, la mappa $\alpha_x : G \to X$, $g \mapsto \alpha(g)x$ (che ha per immagine l'orbita di x) ha rango costante, diciamo k (cioè la matrice Jacobiana ha rango costante k). Inoltre:*

1. *lo stabilizzatore G_x è un sottogruppo di Lie di G, di codimensione k;*
2. *per qualche intorno U dell'elemento neutro in G, l'insieme $\alpha(U)x$ è una sottovarietà di X di dimensione k;*
3. *se l'orbita $\alpha(G)x$ è una sottovarietà di X allora essa ha dimensione k.*

L'orbita $\alpha(G)x$ *non è* sempre una sottovarietà di X, ma se lo è (1) e (3) insieme danno l'analogo per i gruppi di Lie della formula $|G| = |G \cdot \omega| \cdot |G_\omega|$ per le azioni dei gruppi astratti. Questo può essere utile per calcolare la dimensione di gruppi di Lie che sono stabilizzatori in opportune azioni.

ESEMPIO. Sia V uno spazio vettoriale di dimensione n su F, e sia $b(\cdot,\cdot)$ una forma bilineare simmetrica (o prodotto scalare) non degenere su V. (Ricordo che b è non degenere (o non singolare) se il *radicale* $V^\perp := \{v \in V : b(v,w) = 0 \text{ per ogni } w \in V\}$ della forma è il sottospazio nullo, cioè se $b(v,w) = 0$ per ogni $w \in V$ implica che $v = 0$.) Possiamo definire $\mathrm{O}(V,b)$ come l'insieme delle mappe lineari invertibili $g \in \mathrm{GL}(V)$ che rispettano il prodotto scalare b, nel senso che $b(gv,gw) = b(v,w)$ per ogni $v,w \in V$. Prendendo $V = F^n$ con il prodotto scalare standard $b(x,y) := \sum_i x_i y_i$ (rappresentato dalla matrice identità I_n) si ottiene $\mathrm{O}(n,F)$.

Il gruppo $\mathrm{GL}(n,F)$ agisce sullo spazio $B_+(V)$ delle forme bilineari simmetriche su V, ponendo $(g\cdot b)(v,w) = b(g^{-1}v, g^{-1}w)$. Il gruppo ortogonale $\mathrm{O}(V,b)$ è proprio lo stabilizzatore della forma b in questa azione. Se la forma b è non degenere, allora la sua orbita è aperta in $B_+(V)$ (perché essere non degenere equivale al fatto che la matrice della forma rispetto ad una qualsiasi base abbia determinante non nullo, e il determinante è una funzione continua). Quindi l'orbita è una sottovarietà di $B_+(V)$, di dimensione $\dim B_+(V) = n(n+1)/2$, e il teorema ci permette di concludere che

$$\dim \mathrm{O}(V,b) = \dim \mathrm{GL}(V) - \dim B_+(V) = n(n-1)/2.$$

Forme nella stessa orbita si dicono *equivalenti*. (Se preferiamo, le matrici rispetto di forme equivalenti rispetto ad una stessa base si possono anche pensare come matrici della stessa forma rispetto a basi diverse.) Sappiamo che stabilizzatori di forme equivalenti sono coniugati in $\mathrm{GL}(V)$, e sono perciò isomorfi. Se $F = \mathbb{C}$ allora c'è un'unica orbita di forme non degeneri (cioè tutti i prodotti scalari non degeneri su $\mathbb{C}$ sono equivalenti), e quindi c'è un unico gruppo ortogonale, $\mathrm{O}(n,\mathbb{C})$. Invece, se $F = \mathbb{R}$ le orbite di forme non degeneri sono descritte dalla *segnatura* (teorema di Sylvester): ci sono dunque $n+1$ orbite, rappresentate dalle forme $\sum_{i=1}^r x_i y_i - \sum_{i=r+1}^n x_i y_i$, per $r = 0, \ldots, n$. (La prima consiste delle forme definite positive, e l'ultima di quelle definite negative.) I corrispondenti stabilizzatori sono, per definizione, i gruppi $\mathrm{O}(r, n-r)$. Ma dato che scambiare i ruoli di r e $n-r$ è, a meno di equivalenza, come cambiar segno alla forma, i corrispondenti gruppi ortogonali sono isomorfi. Pertanto possiamo limitarci a considerare i gruppi ortogonali $\mathrm{O}(r, n-r)$ con $r \geq n-r$. Si verifica che questi sono tutti non

isomorfi, e quindi su $\mathbb{R}$ abbiamo $\lfloor n/2 \rfloor$ gruppi ortogonali diversi. (Incidentalmente, su un campo finito ce ne sono due non isomorfi, per $n \geq 2$.) Come visto sopra, tutti hanno la stessa dimensione $n(n-1)/2$, ottenuta senza far calcoli dal teorema orbita-stabilizzatore.

Un modo equivalente di svolgere la precedente discussione è fissare una base $v_1, \ldots, v_n$ dello spazio V, e invece di lavorare con le forme b lavorare con le corrispondenti matrici rispetto alla base fissata: la matrice della forma b è la matrice $B = (b_{ij})$, dove $b_{ij} = b(v_i, v_j)$. [...]

Esempio. Naturalmente il gruppo $\mathrm{GL}(n, F)$ agisce anche sullo spazio $B_-(V)$ delle forme bilineari alternanti (cioè antisimmetriche) su V. Lo stabilizzatore della forma b in questa azione è il *gruppo simplettico* $\mathrm{Sp}(V, b)$. Se la forma b è non degenere, allora la sua orbita è aperta in $B_-(V)$, e grazie al teorema orbita-stabilizzatore concludiamo che

$$\dim \mathrm{Sp}(V, b) = \dim \mathrm{GL}(V) - \dim B_-(V) = n(n+1)/2.$$

Le forme bilineari alternanti sono molto diverse, e molto piú semplici, di quelle simmetriche. Infatti, qualunque sia il campo F, se esiste una forma alternante non degenere su V allora $n = \dim V$ è pari, e tutte le forme alternanti non degeneri su V sono equivalenti (cioè formano una sola orbita sotto l'azione di $\mathrm{GL}(V)$). Prendendo $V = F^n$ e scrivendo $n = 2r$, un rappresentante è la forma $\sum_{i=1}^{r} x_i y_{r+i} - \sum_{i=r+1}^{n} x_{r+i} y_i$, che ha matrice $\left[\begin{smallmatrix} 0 & I_r \\ -I_r & 0 \end{smallmatrix}\right]$. (Volendo potremmo anche prendere la forma equivalente $\sum_{i=1}^{r} x_i y_{n-i} - \sum_{i=r+1}^{n} x_{n-i} y_i$.) Il suo stabilizzatore è il gruppo simplettico $\mathrm{Sp}(n, F)$.

Esempio. Il gruppo $\mathrm{GL}(n, \mathbb{C})$ agisce sullo spazio $H(V)$ delle forme bilineari hermitiane su $V = \mathbb{C}^n$, cioè tali che $b(w, v) = \overline{b(w, v)}$. Benché $\mathrm{GL}(n, \mathbb{C})$ sia un gruppo di Lie complesso, esso va qui considerato come gruppo di Lie reale (di dimensione $2n^2$), in quanto $H(V)$ è solo uno spazio vettoriale su $\mathbb{R}$ (di dimensione n^2), e l'azione è un'azione di $\mathrm{GL}(n, \mathbb{C})$ come gruppo di Lie reale. Analogamente agli esempi precedenti, le forme hermitiane non-degeneri formano orbite aperte, quindi di dimensione n^2. Grazie al teorema-orbita-stabilizzatore, i corrispondenti stabilizzatori, che sono i gruppi unitari $\mathrm{U}(r, n-r)$, diciamo con $r \geq n - r$, hanno tutti dimensione $2n^2 - n^2 = n^2$.

6.3. Nucleo e immagine di un omomorfismo, quoziente

Se $f : G \to H$ è un omomorfismo di gruppi di Lie, possiamo definire un'azione di G sulla varietà H ponendo $\alpha(g)h = f(g)h$. Quindi definiamo la mappa $\alpha : G \to \mathrm{Diff}(H)$ come $g \mapsto (h \mapsto f(g)h)$, la composizione dell'omomorfismo f con l'azione di H su se stesso per traslazione a sinistra. Allora l'orbita dell'elemento neutro 1 di H, ed il corrispondente stabilizzatore in G, sono l'immagine $f(G)$ ed il nucleo $\ker(f)$ dell'omomorfismo f. Applicando il teorema-orbita-stabilizzatore a questa situazione otteniamo il seguente teorema.

Teorema. *Sia $f : G \to H$ un omomorfismo di gruppi di Lie. Allora f (che coincide con la mappa α_1 ha rango costante, diciamo k, ed inoltre*

(1) $\ker(f)$ *è un sottogruppo di Lie di* G*, di codimensione* k*;*
(2) *per qualche intorno* U *dell'elemento neutro in* G*, l'insieme* $f(U)$ *è una sottovarietà di* H *di dimensione* k*;*
(3) *se* $f(G)$ *è un sottogruppo di Lie di* H*, allora esso ha dimensione* k*.*

Mostriamo con un esempio che l'immagine di un omomorfismo non è sempre un sottogruppo di Lie. Quindi, piú in generale, le orbite di un'azione di gruppi di Lie non sono sempre sottovarietà.

Esempio. Consideriamo il gruppo $\mathbb{T} = \mathrm{U}(1) = \{z \in \mathbb{C} : |z| = 1\} \cong \mathbb{R}/\mathbb{Z}$, cioè il *toro* unidimensionale. Allora $\mathbb{T}^2 := \mathbb{T} \times \mathbb{T}$ è un gruppo di Lie reale di dimensione due. Se $\alpha \in \mathbb{R}$ è un numero irrazionale, l'immagine dell'omomorfismo iniettivo di gruppi di Lie $f : \mathbb{R} \to \mathbb{T}^2$ dato da $f(x) = (e^{ix}, e^{i\alpha x})$ è denso in $\mathbb{T}^2$, e dunque non è una sottovarietà di $\mathbb{T}^2$ (e quindi è un sottogruppo astratto ma non di Lie).

Se G è compatto questo problema non si può presentare: si dimostra che le orbite di un'azione di un gruppo di Lie compatto sono sottovarietà. In particolare, l'immagine di un gruppo di Lie compatto sotto un omomorfismo di gruppi di Lie è sempre un sottogruppo di Lie.

Se H è un sottogruppo di Lie del gruppo di Lie G, tutti i suoi laterali sinistri gH (o destri Hg) sono sottovarietà differenziabili di G, tutte diffeomeorfe fra loro (infatti gH è l'immagine di H sotto la traslazione a sinistra L_g, che è un diffeomorfismo di G).

È piú complicato mostrare che, se H è un sottogruppo di Lie del gruppo di Lie G, allora l'insieme G/H di laterali sinistri di H in G è ammette una naturale struttura di varietà differenziabile. Se poi H è un sottogruppo normale (di Lie di G), allora con tale struttura differenziabile G/H è un gruppo di Lie.

Data un'azione transitiva $\alpha : g \mapsto (x \mapsto g \cdot x)$ del gruppo di Lie G sulla varietà differenziabile X, sappiamo dal caso dei gruppi astratti che per ogni $x \in X$ la mappa $G/G_x \to X, \quad gG_x \mapsto g \cdot x$, è una biiezione, e commuta con l'azione di G (cioè è G-*equivariante*, cioè è un'equivalenza di azioni, dove l'azione di G su G/G_x è quella per traslazione a sinistra); nel caso dei gruppi di Lie si dimostra che questa biiezione è un diffeomorfismo. Ciò estende ai gruppi di Lie l'osservazione fatta per i gruppi astratti, che le azioni transitive di un gruppo (astratto o di Lie) si possono già trovare "internamente" al gruppo, come azioni su G/H per opportuni sottogruppi H.

Bibliografia

[CUD02] Arjeh Cohen, Rosane Ushirobira, and Jan Draisma, *Group theory for Maths, Physics and Chemistry*, note di un corso tenuto presso la Eindhoven University of Technology, 2007.

[FS97] J. Fuchs and C. Schweigert, *Symmetries, Lie Algebras and Representations (A graduate course for physicists)*, Cambridge University Press, 1997.

[FH91] W. Fulton and J. Harris, *Representation Theory – A first course*, Springer, 1991.

[Her64] I. N. Herstein *Topics in Algebra*, Blaisdell Publishing, 1964.

[SW86] D. H. Sattinger and O. L. Weaver, *Lie Groups and Algebras with Applications to Physics, Geometry and Mechanics*, Springer, 1986.