

Teoria dei Gruppi.

Note di Sandro Mattarei

Queste Note raccolgono scarni appunti su alcuni argomenti per il corso di Teoria dei gruppi dell'anno 2007/08, leggermente ampliate durante l'anno 2008/09. Questa è la versione di fine corso (8 maggio 2009).

Indice

Capitolo 1. Gruppi astratti. Azioni	5
1.1. Nozioni fondamentali sui gruppi; il gruppo simmetrico S_n	5
1.2. Azione di un gruppo su un insieme	8
1.3. Vari esempi di gruppi	12
1.4. Applicazioni delle azioni	16
1.5. I teoremi di Sylow	17
Capitolo 2. Teoria della rappresentazione	21
2.1. Rappresentazioni e moduli.	21
2.2. Tabelle dei caratteri.	21
Capitolo 3. Cenni sui gruppi di Lie	23
3.1. Gruppi di Lie, sottogruppi, omomorfismi	23
3.2. Azione di un gruppo di Lie su una varietà	24
3.3. Nucleo e immagine di un omomorfismo, quoziente	26
Bibliografia	29

Gruppi astratti. Azioni

1.1. Nozioni fondamentali sui gruppi; il gruppo simmetrico S_n

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

Omomorfismi. Omomorfismi, nucleo, gruppo quoziente. [Vedi lezioni.]

Ci sono tre teoremi importanti sugli omomorfismi, detti spesso *i teoremi di isomorfismo*. Il primo ed il secondo (anche se talvolta il secondo ed il terzo si scambiano di ordine) sono i seguenti.

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

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 $HN/N \cong H/(H \cap N)$.*

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 $(h_1, k_1) \cdot (h_2, k_2) := (h_1 h_2, k_1 k_2)$. 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.]

Permutazioni. I vari modi di rappresentare una permutazione, in particolare la scrittura come prodotto di cicli disgiunti. *Notazione: in questo corso componiamo le mappe da destra a sinistra.* 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:

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

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 (incluso 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 $\text{sgn}(g) := (-1)^{n-r}$, 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 k è pari o dispari a seconda che g sia pari o dispari (che sembrerebbe la definizione più naturale, ma è più problematica).

DIMOSTRAZIONE. Il punto cruciale è mostrare che se g è una permutazione e t è una trasposizione allora $\text{sgn}(tg) = -\text{sgn}(g)$; 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. Rinominando eventualmente i vari simboli, possiamo sempre supporre che il prodotto tg inizi, nei due casi, nei modi seguenti:

$$(1, 2)(1, \dots, i, 2, \dots, j) = (1, \dots, i)(2, \dots, j),$$

$$(1, 2)(1, \dots, i)(2, \dots, j) = (1, \dots, i, 2, \dots, j);$$

ciascuna segue dall'altra componendola a sinistra con la trasposizione $(1, 2)$. Le due formule mostrano che tg , scritta come prodotto di cicli disgiunti, ha un ciclo in più o in meno di g , rispettivamente, e quindi $\text{sgn}(tg) = -\text{sgn}(g)$ vale in entrambi i casi. \square

A questo punto segue che vale $\text{sgn}(gh) = \text{sgn}(g)\text{sgn}(h)$ per due permutazioni qualsiasi g, h , cioè che la mappa $\text{sgn} : S_n \rightarrow \{\pm 1\}$ 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

$$\prod_{1 \leq i < j \leq n} (g(j) - g(i)) = \text{sgn}(g) \prod_{1 \leq i < j \leq n} (j - i).$$

(Notate che è sufficiente verificare la formula nel caso in cui g è una trasposizione; determinate allora quali differenze $g(j) - g(i)$ sono negative, e verificate che esse sono in numero dispari.) Questo suggerisce un altro modo di definire il segno di una permutazione, come $\text{sgn}(g) = \prod_{1 \leq i < j \leq n} (g(j) - g(i)) / (j - i)$ (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], più 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. Per ottenere un gruppo dobbiamo pensare a trasformazioni più generali, costituite da successioni di mosse elementari, legalmente applicabili ad una configurazione con la casella 16 vuota, e che la lasciano di nuovo vuota dopo la loro applicazione. Tali trasformazioni si possono comporre arbitrariamente, e quindi formano un sottogruppo di S_{16} . Ma poiché la casella vuota parte da e ritorna alla posizione 16, ogni tale trasformazione deve essere prodotto di un numero *pari* di mosse elementari (cioè trasposizioni), e quindi appartiene ad A_{16} . Ne segue che, rimuovendo dal puzzle due quadratini e rimettendoli nelle posizioni scambiate (e quindi applicando, in modo illegale, una trasposizione), lo si porta in una posizione da cui non si può legalmente raggiungere la posizione standard.

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

Notate che ${}^h g = g$ se e solo se $gh = hg$.

Per $x, y, h \in G$ vale anche ${}^h(xy) = {}^h x {}^h y$. Essa esprime il fatto che la mappa $x \mapsto {}^h x$ 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 più in generale se $n \in \mathbb{Z}$, vale $({}^h g)^n = {}^h(g^n)$, in particolare, elementi coniugati hanno lo stesso ordine.

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 ${}^\alpha \beta$ 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

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

per dimostrarla basta verificare che i due membri danno lo stesso risultato se applicati a αi_j , 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 biettivamente alle *partizioni* del numero naturale n (cioè ai modi di scrivere n come somma di naturali non crescenti e non nulli). 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 $3^2 2 1$.

1.2. Azione di un gruppo su un insieme

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

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

Ad un'azione corrisponde in modo naturale un omomorfismo di gruppi $G \rightarrow \text{Sym}(\Omega)$, $g \mapsto (\omega \mapsto g \cdot \omega)$. Il nucleo di tale omomorfismo è detto il *nucleo* dell'azione: $\{g \in G : g \cdot \omega = \omega \text{ per ogni } \omega \in \Omega\}$. Per ogni $\omega \in \Omega$ definiamo lo *stabilizzatore* di ω come $G_\omega = \text{Stab}_G(\omega) := \{g \in G : g \cdot \omega = \omega\}$. 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 $\varphi : G \rightarrow \text{Sym}(\Omega)$, vi è associata in modo naturale un'azione di G su Ω ponendo $g \cdot \omega := \varphi(g)(\omega)$. Perciò, azioni di G su Ω e omomorfismi $G \rightarrow \text{Sym}(\Omega)$ sono concetti equivalenti.

Data un'azione di G su Ω , l'*orbita* di un elemento $\omega \in \Omega$ è $G \cdot \omega := \{g \cdot \omega : g \in G\}$. L'azione è *transitiva* (o si dice talvolta che Ω è uno *spazio omogeneo per G*) se $G \cdot \omega = \Omega$ 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 .

ESEMPIO. L'azione naturale di S_n . [Vedi lezioni.]

ESEMPIO. Esempio: $G = \text{SO}(2)$, il gruppo delle rotazioni del piano che fissano un punto O , agisce sui punti del piano in modo naturale. Le orbite sono le circonferenze di centro O .

ESERCIZIO. 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, $G_{g \cdot \omega} = g(G_\omega)g^{-1}$.

ESEMPIO. Nell'azione *naturale* di S_n su $\{1, \dots, n\}$ lo stabilizzatore G_i della cifra i è costituito dalle permutazioni che fissano i ; se j è un'altra cifra avremo, ad esempio, $(ij)G_i(ij)^{-1} = (ij)G_i(ij) = G_j$.

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

$$G/G_\omega \rightarrow G \cdot \omega \subseteq \Omega, \quad gG_\omega \mapsto g \cdot \omega$$

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

DIMOSTRAZIONE. Abbiamo

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

Quindi la mappa è ben definita e biiettiva. \square

OSSERVAZIONI. Per i gruppi di Lie, sotto opportune condizioni vale un teorema analogo, con $|G| = |G \cdot \omega| \cdot |G_\omega|$ rimpiazzata da $\dim(G) = \dim(G \cdot \omega) + \dim(G_\omega)$.

Azione per coniugio. Un gruppo G agisce su se stesso per coniugio, ponendo $g \cdot \omega := g\omega g^{-1}$. 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 ${}^G h$ è data da $|{}^G h| = |G : \mathbf{C}_G(h)|$ e, in particolare, divide $|G|$. Il nucleo dell'azione è il centro $\mathbf{Z}(G)$.

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, \dots, g_r sono rappresentanti per le classi di coniugio di G .

Applicazione: ogni p -gruppo (cioè gruppo di ordine una potenza di un primo p) non banale 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.

ESEMPIO. Classi di coniugio dei gruppi diedrali. [Vedi lezioni.]

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 $G \rightarrow \text{Sym}(G)$ ha in realtà immagine contenuta in $\text{Aut}(G)$. L'immagine di questa mappa è un sottogruppo normale di $\text{Aut}(G)$, indicato con $\text{Inn}(G)$, il *gruppo degli automorfismi interni* di G , cioè quelli della forma $\gamma_g : x \mapsto gxg^{-1}$ per qualche $g \in G$. Grazie al teorema fondamentale sugli omomorfismi, $\text{Inn}(G)$ è isomorfo al gruppo quoziente $G/\mathbf{Z}(G)$.

Azione per coniugio e sottogruppi normali. Se N è un sottogruppo normale di G , allora l'azione di G per coniugio manda elementi di N in elementi di N . Dunque ogni classe di coniugio di G è interamente contenuta in N o nel suo complemento in G . Detto in altro modo, N è unione di (alcune delle) classi di coniugio di G . Perciò G agisce per coniugio su N .

In questa azione, elementi di N che sono coniugati in N vengono mandati in elementi di N che sono coniugati in N : due generici elementi coniugati di N sono x e xyx^{-1} , con $x, y \in N$; se li coniughiamo entrambi sotto un elemento g di G otteniamo

$$gxg^{-1} \quad \text{e} \quad gyxy^{-1}g^{-1} = (gyg^{-1})(gxg^{-1})(gyg^{-1})^{-1},$$

che sono coniugati in N , essendo $gyg^{-1} \in N$. Quindi se Ω è l'insieme delle classi di coniugio di N , l'azione per coniugio di G induce un'azione di G su Ω . Ma N agisce banalmente in questa azione, cioè è contenuto nel nucleo. Ne concludiamo che G/N agisce su Ω .

Un'orbita di questa azione consiste di un'insieme di classi di coniugio di N , la cui unione forma una classe di coniugio di G . Dato che queste classi di coniugio di N permutate da G devono chiaramente essere lunghe uguali, ne traiamo la conclusione seguente: ogni classe di coniugio di G contenuta nel sottogruppo normale N è unione di classi di coniugio di N , tutte della stessa lunghezza, e il cui numero divide $|G/N|$. In particolare, se $|G/N| = 2$ (ad esempio se $G = S_n$ e $N = A_n$) una classe di coniugio di G contenuta in N , o è una classe di coniugio di N , o

è l'unione di due classi di coniugio di N aventi la stessa lunghezza. La classe di coniugio di un elemento g di G si spezza in $|C_G(g) : C_N(g)|$ classi di N di uguale lunghezza.

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 .

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

Notando che $(n_1 h_1)(n_2 h_2) = (n_1 (h_1 n_2 h_1^{-1})) (h_1 h_2)$, dove $h_1 n_2 h_1^{-1} \in N$, e che la mappa $h \mapsto (n \mapsto h n h^{-1})$ è omomorfismo di H in $\text{Aut}(N)$, siamo portati a dare la seguente definizione. Dati due gruppi N e H , ed un omomorfismo $\alpha : H \rightarrow \text{Aut}(N)$, che possiamo indicare $\alpha : h \mapsto \alpha_h$, il *prodotto semidiretto (esterno)* di N e H rispetto all'omomorfismo α , indicato con $N \rtimes_\alpha H$ (o semplicemente $N \rtimes H$, purché sia chiaro quale sia α) è l'insieme prodotto cartesiano $N \times H$ con l'operazione

$$(n_1, h_1)(n_2, h_2) = (n_1 \alpha_{h_1}(n_2), h_1 h_2).$$

Si verifica (esercizio) che $N \rtimes_\alpha H$ è un gruppo, e che è il prodotto semidiretto interno di $\bar{N} = \{(n, 1) : n \in N\}$ e $\bar{H} = \{(1, h) : h \in H\}$.

Azioni per moltiplicazione. G agisce su $\Omega = G$ per *moltiplicazione (a sinistra)*, detta anche *traslazione (a sinistra)*, ponendo $g \cdot \omega := g\omega$ per $g, \omega \in G$. L'azione è transitiva, e fedele, cioè il nucleo è 1 . Anzi, lo stabilizzatore di un punto (e quindi tutti gli stabilizzatori) è 1 (un'azione transitiva con questa proprietà si dice *regolare*).

Vi è associato un omomorfismo iniettivo $G \rightarrow \text{Sym}(G)$. 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.

Se $H \leq G$, ponendo $g \cdot xH := gxH$ per $g, x \in G$ otteniamo un'azione, anch'essa detta per *traslazione (a sinistra)*, di G sull'insieme G/H (che non è un gruppo se H non è normale!) dei laterali sinistri di H . Qui gli stabilizzatori sono i coniugati di H . Il nucleo, cioè la loro intersezione, è $H_G = \bigcap_{x \in G} xHx^{-1}$, detto il *cuore* di H in G , che è il piú grande sottogruppo normale di G contenuto in H . Notate che $H_G = H$ se e solo se H è normale in G .

Ad esempio, se $|G : H| = n$ ne otteniamo un omomorfismo $G \rightarrow S_n$, con nucleo $H_G = \bigcap_{x \in G} xHx^{-1}$, e quindi un omomorfismo iniettivo $G/H_G \rightarrow S_n$. Ne segue che se G ha un sottogruppo H 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 $H \triangleleft G$. 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 $H = H_G \triangleleft G$.

Esempio. Sia G un gruppo di ordine pq , dove p e q sono primi distinti, diciamo con $p < q$. Mostriamo che allora G è prodotto semidiretto di un sottogruppo normale di ordine q e un sottogruppo di ordine p . Notate che grazie a Lagrange i possibili ordini di elementi di G sono 1, p , q e pq . Iniziamo mostrando che G ha necessariamente un elemento di ordine p ed uno di ordine q .¹

Il caso in cui G è abeliano è facile. Se G ha un elemento di ordine pq allora G è ciclico. D'altra parte G non può avere solo elementi di ordine 1 e p (o analogamente 1 e q), perché allora sarebbe un gruppo abeliano finito di esponente p , e quindi (vedendolo come spazio vettoriale sul campo con p elementi) dovrebbe avere ordine una potenza di p , il che non è. Quindi G deve avere un elemento di ordine p ed uno di ordine q . In tal caso G è il prodotto diretto dei sottogruppi da essi generati, e quindi, nuovamente, G è ciclico. Pertanto, d'ora in poi possiamo assumere che G non sia abeliano.

Per l'equazione delle classi G ha almeno un elemento $g \neq 1$ la cui classe ha lunghezza non divisibile per p . Perciò $\mathbf{C}_G(g)$ ha ordine multiplo di p , quindi pq o p . Nel primo caso avremmo che g è un elemento centrale, quindi il sottogruppo $\langle g \rangle$ è contenuto nel centro di G e $G/\langle g \rangle$ è ciclico per questione di ordine. Per un esercizio fatto seguirebbe che G è abeliano, ma stiamo supponendo che cosí non sia. Nel secondo caso il sottogruppo non banale $\langle g \rangle$ di $\mathbf{C}_G(g)$. Quindi g è un elemento di ordine p , come si voleva. In modo analogo, G ha anche un elemento di ordine q .

Se P e Q sono i sottogruppi generati da un elemento di ordine p ed uno di ordine q , avremo che Q è normale avendo indice p . Chiaramente $P \cap Q = 1$, e ne segue che $G = Q \rtimes P$, 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

¹Questo è un caso speciale del seguente lemma di Cauchy: se un primo p divide l'ordine di un gruppo finito, allora il gruppo ha almeno un elemento di ordine p .

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.

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_5 e S_5 , ed usando l'azione di G per traslazione sinistra su G/H , dimostrate che $|G : H| \geq n$. (In altre parole, S_n non ha sottogruppi "più grandi" di S_{n-1} , a parte se stesso e A_n .)

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

1.3. Vari esempi di gruppi

I gruppi diedrali. Il gruppo D_n (talvolta indicato D_{2n}) 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

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

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

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

In effetti $a^j b$ 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 dà luogo ad un omomorfismo iniettivo $D_n \rightarrow S_n$.

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 $BAB^{-1} = A^{-1}$ (ovvero $BAB = A^{-1}$ visto che $B^1 = 1$), che si scrive anche $BA = A^{-1}B$, o ancora $BABA = 1$. 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 $a^j b$, ed esprimendo il risultato finale nuovamente nella forma a^j o $a^j b$). In modo piú formale,

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

è una *presentazione* di D_n [si veda piú sotto].

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 bene comunque verificare queste affermazioni in modo indipendente dalla geometria, ad esempio notando che $a(a^j b)a^{-1} = a^{j+1}ba^{-1} = a^{j+2}b$, ecc.

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 $X \rightarrow G$ estende in modo unico ad un omomorfismo $F \rightarrow G$. (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). Più 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 $\text{GL}(2, \mathbb{Q})$ generato dalle matrici $A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ 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 $F \rightarrow G$, dove F è un gruppo libero: avremo allora $G \cong F/R$, dove R è il nucleo dell'omomorfismo. Più utilmente, 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 più 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 $X \cup X^{-1}$. Più 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 $w_1w_2^{-1}$ (cioè è equivalente all'uguaglianza $w_1w_2^{-1} = 1$). Ancora più 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. $G = \langle x, a \mid x^2 = a^n = 1, xax^{-1} = a^{-1} \rangle$ 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 $a = xy$ nella prima, e l'equivalente $y = ax^{-1}$ nella seconda. Le presentazioni $G = \langle x, a \mid x^2 = 1, xax^{-1} = a^{-1} \rangle = \langle x, y \mid x^2 = y^2 = 1 \rangle$, definiscono invece il *gruppo diedrale infinito* D_∞ . Ogni gruppo diedrale D_n è isomorfo ad un quoziente di D_∞ .

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

$$1 = x_i^2 = (x_jx_{j+1})^3 = (x_kx_\ell)^2,$$

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 .

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

Alcuni gruppi lineari. Il *gruppo lineare generale* $GL(n, F)$ è il gruppo delle matrici $n \times n$ invertibili a coefficienti nel campo F , ed il *gruppo lineare speciale* $SL(n, F)$ è il sottogruppo normale costituito da quelle di determinante 1 (cioè il nucleo dell'omomorfismo $\det : GL(n, F) \rightarrow F^*$). L'azione naturale di $GL(n, F)$ sullo spazio (dei vettori colonna) 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 $GL(n, F)$ è uguale al numero di basi di \mathbb{F}_q^n , perciò

$$|GL(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Grazie al teorema fondamentale sugli omomorfismi abbiamo poi

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

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

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

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

(Attenzione però: $SL(n, \mathbb{F}_q)$ e $PGL(n, \mathbb{F}_q)$ hanno lo stesso ordine, ma in generale non sono isomorfi.)² Come abbiamo visto, il centro di $SL(n, F)$ consiste delle matrici scalari di determinante 1, cioè è $Z \cap SL(n, F)$, dove come sopra Z indica il centro di $GL(n, F)$. Il gruppo quoziente $PSL(n, F) := SL(n, F) / (Z \cap SL(n, F))$ è il *gruppo lineare speciale proiettivo*. Le matrici scalari $\text{diag}(\alpha, \dots, \alpha)$ di determinante 1 sono tante quante le soluzioni di $\alpha^n = 1$ in F , e quindi al massimo n . Se F è il campo finito \mathbb{F}_q , il loro numero è il massimo comun divisore $(n, q - 1)$ (poiché \mathbb{F}_q è ciclico di ordine $q - 1$). Avremo quindi

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

In particolare, per $n = 2$ abbiamo

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

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

²Gli 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, $GL(n, F)$, $SL(n, F)$, e $PGL(n, F)$, per $\mathbb{F} = \mathbb{R}$ o \mathbb{C} . Anche $PSL(n, F)$ ha dimensione $n^2 - 1$, la stessa del gruppo $SL(n, F)$ di cui è quoziente, perché il quoziente è fatto rispetto al sottogruppo discreto $Z \cap SL(n, F)$.

$\mathrm{PGL}(2, \mathbb{F}_q) \cong \mathrm{PSL}(2, \mathbb{F}_q)$.) Ad esempio,

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

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

$$\begin{aligned} \mathrm{GL}(2, \mathbb{F}_2) &\cong S_3, \\ \mathrm{PGL}(2, \mathbb{F}_3) &\cong S_4 \text{ (ma } \not\cong \mathrm{SL}(2, \mathbb{F}_3)\text{, in quanto questo ha centro non banale),} \\ \mathrm{PSL}(2, \mathbb{F}_3) &\cong A_4, \\ \mathrm{PGL}(2, \mathbb{F}_5) &\cong S_5 \text{ (ma } \not\cong \mathrm{SL}(2, \mathbb{F}_5)\text{, come sopra), e} \\ \mathrm{SL}(2, \mathbb{F}_4) &\cong \mathrm{PSL}(2, \mathbb{F}_5) \cong A_5, \end{aligned}$$

che è il più piccolo gruppo semplice non abeliano. Il successivo gruppo semplice non abeliano, andando per ordine crescente, è $\mathrm{PSL}(2, \mathbb{F}_7) \cong \mathrm{GL}(3, \mathbb{F}_2)$. Il successivo ancora è $\mathrm{PSL}(2, \mathbb{F}_7) \cong A_6$. 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 $(2, 3)$.

1.4. 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 $(1, 0)^\top$, $(0, 1)^\top$ e $(1, 1)^\top$, e si vede subito che l'azione è fedele. Ne otteniamo un isomorfismo $\mathrm{GL}(2, \mathbb{F}_2) \rightarrow S_3$.

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 $\mathrm{SL}(2, \mathbb{F}_4) \rightarrow S_5$. La sua immagine ha ordine 60, e quindi deve coincidere con l'unico sottogruppo di S_5 di indice 2, che è A_5 .

ESERCIZIO. (1) Sia $G = \mathrm{GL}(2, \mathbb{F}_3)$ il gruppo delle matrici invertibili 2×2 a coefficienti nel campo con tre elementi $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. (Per semplicità indichiamo gli elementi di \mathbb{F}_3 con $0, 1, -1$, piuttosto che $\bar{0} = 0 + 3\mathbb{Z}$, ecc.) Considerate l'azione naturale di G sull'insieme $\Omega = \mathbb{F}_3^2 \setminus \{(0, 0)^\top\}$ dei vettori colonna non nulli, a coefficienti in \mathbb{F}_3 . Considerate l'azione *naturale* di G su Ω , cioè quella dove vg è definito come il prodotto del vettore riga $v \in \Omega$ per la matrice $g \in G$. Mostrate

che tale azione è transitiva e fedele, ottenendone quindi un omomorfismo iniettivo $\mathrm{GL}(2, \mathbb{F}_3) \rightarrow S_8$.

(2) Ora sia $P^1\mathbb{F}_3$ lo spazio proiettivo associato allo spazio vettoriale \mathbb{F}_3^2 (cioè la *retta proiettiva* su \mathbb{F}_3). Dunque i suoi elementi sono le rette per l'origine in \mathbb{F}_3^2 , ovvero (togliendo loro l'origine, che è comune a tutte) le coppie di elementi opposti di Ω . Mostrate che l'azione di G su Ω induce un'azione di G su $P^1\mathbb{F}_3$. (Bisogna mostrare che l'azione di G manda elementi di $P^1\mathbb{F}_3$ in elementi di $P^1\mathbb{F}_3$). Mostrate che il nucleo di questa seconda azione è il centro Z di G (cioè l'insieme delle matrici scalari di G). Deducetene che il gruppo lineare proiettivo $\mathrm{PGL}(2, \mathbb{F}_3) = \mathrm{GL}(2, \mathbb{F}_3)/Z$ è isomorfo al gruppo simmetrico S_4 .

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 più difficile da costruire.

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

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

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

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

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

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

1.5. I teoremi di Sylow

1.5.1. Enunciati e dimostrazioni. [Vedi lezioni e documento separato.]

1.5.2. 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);³
- (4) $|G| \neq pqr$;
- (5) $|G| \neq 2p^a, 3p^a, 4p^a$, per $p \neq 2, 3, 2$ risp. (perchè un p -sottogruppo di Sylow avrebbe indice minore di 5, e 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.⁴

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

$$\begin{array}{llll} 40 = 2^3 \cdot 5, & 56 = 2^3 \cdot 7, & 60 = 2^2 \cdot 3 \cdot 5, & 72 = 2^3 \cdot 3^2, \\ 80 = 2^4 \cdot 5, & 84 = 2^2 \cdot 3 \cdot 7, & 88 = 2^3 \cdot 11, & 99 = 3^2 \cdot 11. \end{array}$$

Lo stesso ragionamento del punto (4) mostra che se fosse $|G| = 5p^a$ (con $p \neq 5$) allora G sarebbe isomorfo ad un sottogruppo di S_5 , anzi di A_5 (altrimenti $G \cap A_5$ sarebbe un sottogruppo normale proprio di G), e quindi $|G|$ dividerebbe $|A_5| = 60$; ciò esclude le possibilità 40 e 80.

Di nuovo lo stesso ragionamento mostra che se $|G| = p^m r$, con $m \geq 1, r > 1$ e $p \nmid r$, allora $p^m \mid (r-1)!$ (infatti se H è un p -sottogruppo di Sylow, l'azione di G per moltiplicazione sui laterali sinistri di H dà un omomorfismo iniettivo di G in S_r e quindi $|G|$ divide $r!$); ciò esclude le possibilità 88 e 99.

Un ragionamento ancora analogo mostra che, per ogni divisore primo p di $|G|$, il numero n_p di p -sottogruppi di Sylow supera 4 (perchè n_p è anche l'indice del normalizzante di uno di essi). Ciò permette di escludere 72, in quanto $n_3 \mid 8$ e $n_3 \equiv 1 \pmod{3}$ sono incompatibili con $n_3 > 4$.

Piú in generale, se $|G| = 2^3 q^m$, con q primo e $m > 1$, da $n_q \mid 8, n_q \equiv 1 \pmod{q}$ e $n_q > 4$ segue che $n_q = 8$ e quindi $q = 7$. Questo sarebbe un modo

³Un 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.

⁴Questo è un caso speciale del fatto, piú profondo, che i 2-sottogruppi di Sylow di un gruppo semplice non abeliano non possono essere ciclici.

alternativo di escludere 40 o 88. Da solo esso non permette di escludere 56. **Esercizio:** completatelo con altri argomenti in modo da escludere 56.

Anche l'esclusione di 84 è un facile esercizio, e quindi concludiamo che $|G| = 60$, come volevamo. \square

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 $C_G(y)$ 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, 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 così non è in A_5 .) \square

1.5.3. 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 più 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.

CAPITOLO 2

Teoria della rappresentazione

2.1. Rappresentazioni e moduli.

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

2.2. 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 $G \rightarrow \mathbb{C}$ 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*

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

Il caso particolare $h = 1$ esprime il fatto importante che $\rho = \sum_{\chi \in \text{Irr}(G)} \chi(1)\chi$, 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 traslazione, 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*).

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.

3.1. 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* $G \times G \rightarrow G$, $(g, h) \mapsto gh$ 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* $G \rightarrow G$, $g \mapsto g^{-1}$ 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 più 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 $O(n, F)$ è il sottogruppo di $GL(n, F)$ definito dalla condizione $gg^T = 1$. Scritta in coordinate questa condizione si esprime con le equazioni $\sum_j g_{ij} g_{kj} = \delta_{ik}$. Assumendo $i \leq k$ 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 $O(n, F)$ ha codimensione $n(n+1)/2$ in $GL(n, F)$, e perciò è un gruppo di Lie di dimensione $n(n-1)/2$.

Il gruppo unitario $U(n)$ è un sottogruppo di $GL(n, \mathbb{C})$ definito dalla condizione $g\bar{g}^T = 1$ (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 $GL(n, \mathbb{C})$, visto come gruppo di Lie reale, ha dimensione $2n^2$, concludiamo che $U(n)$ è un sottogruppo di Lie reale di $GL(n, \mathbb{C})$, 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* $L_g : x \mapsto gx$ (così come la *traslazione a destra* $R_g : x \mapsto xg$) è differenziabile, e naturalmente così 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 $G \rightarrow H$ 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]).

3.2. Azione di un gruppo di Lie su una varietà

Un’azione di un gruppo di Lie G su una varietà differenziabile X è un omomorfismo α di G in $\text{Diff}(X)$, il gruppo dei diffeomorfismi di X , tale che la mappa $G \times X \rightarrow X$, $(g, x) \mapsto gx$ 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.

TEOREMA (orbita-stabilizzatore). *Per ogni punto $x \in X$, la mappa $\alpha_x : G \rightarrow X$, $g \mapsto \alpha(g)x$ (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 degenera su V . (Ricordo che b è non degenera (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 $O(V, b)$ come l'insieme delle mappe lineari invertibili $g \in GL(V)$ 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 $O(n, F)$.

Il gruppo $GL(n, F)$ 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 $O(V, b)$ è proprio lo stabilizzatore della forma b in questa azione. Se la forma b è non degenera, allora la sua orbita è aperta in $B_+(V)$ (perché essere non degenera 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

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

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 $GL(V)$, 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, $O(n, \mathbb{C})$. 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 $r = 0, \dots, n$. (La prima consiste delle forme definite positive, e l'ultima di quelle definite negative.) I corrispondenti stabilizzatori sono, per definizione, i gruppi $O(r, n-r)$. 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 $O(r, n-r)$ 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, \dots, 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 $GL(n, F)$ 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* $Sp(V, b)$. Se la forma b è non degenere, allora la sua orbita è aperta in $B_-(V)$, e grazie al teorema orbita-stabilizzatore concludiamo che

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

Le forme bilineari alternanti sono molto diverse, e molto più 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 $GL(V)$). 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 $\begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix}$. (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 $Sp(n, F)$.

ESEMPIO. Il gruppo $GL(n, \mathbb{C})$ agisce sullo spazio $H(V)$ delle forme bilineari hermitiane su $V = \mathbb{C}^n$, cioè tali che $b(w, v) = \overline{b(v, w)}$. Benché $GL(n, \mathbb{C})$ 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 $GL(n, \mathbb{C})$ 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 $U(r, n-r)$, diciamo con $r \geq n-r$, hanno tutti dimensione $2n^2 - n^2 = n^2$.

3.3. Nucleo e immagine di un omomorfismo, quoziente

Se $f : G \rightarrow H$ 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 $\alpha : G \rightarrow \text{Diff}(H)$ 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 $f : G \rightarrow H$ 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 $\mathbb{T} = U(1) = \{z \in \mathbb{C} : |z| = 1\} \cong \mathbb{R}/\mathbb{Z}$, 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 $f : \mathbb{R} \rightarrow \mathbb{T}^2$ 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 diffeomorfe 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 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 $G/G_x \rightarrow X$, $gG_x \mapsto g \cdot x$, 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.
- [SW86] D. H. Sattinger and O. L. Weaver, *Lie Groups and Algebras with Applications to Physics, Geometry and Mechanics*, Springer, 1986.