Lezioni di
Teoria dei Gruppi

Andrea Mori
Dipartimento di Matematica
Università di Torino

Maggio 2005

Questo lavoro è dedicato alla memoria di

Lia Venanzangeli (1959–2004)

amica e compagna.

Gigni de nihilo nihilum,
in nihilum nil posse reverti.
PERSIO, *Satira III, 83–84.*

Prefazione

TESTO PREFAZIONE

Andrea Mori

Torino, Febbraio 2004

Indice

Introduzione

La matematica è una gigantesca costruzione intellettuale, molto difficile, se non impossibile, di essere compresa nella sua interezza. Mi piace a volte pensarla come ad un iceberg, con una sua piccola parte visibile ed una grande, invisibile. Per parte visibile intendo quella utile al mondo, per la tecnologia, la fisica, le scienze naturali, eccetera, di cui è innegabile l'importanza e la ragione sociale. [...] D'altra parte nel suo sviluppo la matematica ha acquisito una sua vita propria, ed i matematici si sono vieppiù interessati a problemi puramente matematici [...]. Questo forma la parte invisibile dell'iceberg. [...] Ciò non significa che queste ricerche mai troveranno applicazione, che la parte invisibile diventi visibile. L'esperienza mostra il contrario. [...] Ma questo non ha importanza per il matematico, che lavora in un mondo di forme intellettuali dotato di leggi e motivazioni proprie e che è spesso guidato da considerazioni estetiche.
Armand BOREL, *dal discorso di accettazione del Premio Balzan,* (1962)[1]

TESTO INTRODUZIONE

[1] T.d.A.

Lezione 1

Prime definizioni e proprietà

Le strutture sono le armi del matematico.
BOURBAKI
Pluralitas non est ponenda sine necessitate.
GUGLIELMO di OCKHAM (1285?–1349?).

1.1 Definizione di gruppo.

Sia G un insieme non vuoto. Un'*operazione binaria* definita su G è una funzione

$$\cdot : G \times G \longrightarrow G \tag{1.1}$$

che per comodità denoteremo $\cdot(a, b) = a \cdot b = ab$ per ogni a, $b \in G$ e chiameremo *prodotto* di a e b. L'operazione (1.1) è detta soddisfare la

- *proprietà associativa*, se per ogni a, b, $c \in G$ vale l'identità $(ab)c = a(bc)$;
- *proprietà commutativa*, se per ogni a, $b \in G$ vale l'identità $ab = ba$.

Se la proprietà associativa è soddisfatta è possibile definire ricorsivamente in modo non ambiguo il prodotto di tre o più elementi:

$$abc = (ab)c, \qquad abcd = (abc)d, \qquad \text{eccetera.}$$

In particolare, per $n = 1, 2, 3, \ldots$ e $a \in G$ poniamo

$$a^n = a \cdots a, \qquad n \text{ fattori.}$$

Un elemento $u \in G$ è detto essere un *elemento neutro* per l'operazione (1.1) se per ogni $a \in G$ valgono le identità

$$au = ua = a.$$

Se l'elemento neutro esiste ed è unico viene solitamente denotato 1 od 1_G se l'insieme G non è ben precisato dal contesto.

Nota Bene. Un'operazione che soddisfa la proprietà commutativa è sovente denotata col simbolo $+$ e l'elemento $+(a, b) = a+b$ è detto somma di a e b. Se l'elemento neutro dell'operazione $+$ è unico, esso è solitamente denotato 0 o 0_G.

Possiamo dare ora la definizione di gruppo.

Definizione 1.1.1. *Un gruppo G è un insieme non vuoto dotato di un'operazione binaria tale che:*

1. *è soddisfatta la proprietà associativa;*
2. *esiste un elemento neutro $u \in G$;*
3. *per ogni elemento $x \in G$ esiste un elemento $y \in G$ tale che $xy = yx = u$.*

Si noti che non si richiede che la proprietà commutativa sia soddisfatta. Un gruppo in cui la proprietà commutativa risulti soddisfatta si dice *gruppo abeliano*.

Una conseguenza immediata della definizione è che in un gruppo G vale la *regola di cancellazione*:

Teorema 1.1.2. *Per ogni a, b, $c \in G$,*

$$ac = bc \Rightarrow a = b \qquad e \qquad ca = cb \Rightarrow a = b.$$

Dimostrazione. Se $y \in G$ è tale che $cy = u$ si ha

$$ac = bc \Rightarrow acy = bcy \Rightarrow au = bu \Rightarrow a = b$$

e analogamente per la cancellazione a sinistra. ■

Dalla regola di cancellazione segue immediatamente che in un gruppo

- esiste un unico elemento neutro u;
- per ogni elemento x esiste un unico elemento y tale che $xy = yx = u$.

È dunque lecito parlare de *l'elemento inverso* di un elemento $x \in G$. Esso viene denotato x^{-1}. Se il gruppo è abeliano e l'operazione denotata $+$, l'inverso di un elemento x è detto anche *opposto* e denotato $-x$. Vale la formula

$$(xy)^{-1} = y^{-1}x^{-1} \qquad \text{(notare lo scambio di ordine!)}.$$

Infatti si ha $(xy)y^{-1}x^{-1} = x(yy^{-1})x^{-1} = xx^{-1} = 1$.

Diamo ora alcuni esempi fondamentali di gruppi.

Esempi 1.1.3.

1. Gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ dei numeri interi, razionali, reali e complessi rispettivamente sono gruppi abeliani rispetto alla consueta operazione di somma. L'elemento neutro è, in ciascun caso, il numero 0.

   Gli stessi insiemi non sono gruppi rispetto alla consueta operazione di prodotto perchè 0 non ammette inverso.

   L'insieme $\mathbb{N} = \{0, 1, 2, \ldots\}$ dei numeri naturali non è un gruppo rispetto alla somma perchè gli elementi non nulli sono privi di opposto in $\mathbb{N}$.

2. Sia $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ od un campo qualunque e poniamo $G = K^\times = K - \{0\}$. Allora G è un gruppo abeliano rispetto alla consueta operazione di somma. In ciascuno caso l'elemento neutro è il numero 1, e l'inverso del numero x è il numero $1/x$.

   L'insieme $\mathbb{Z} - \{0\}$ non è un gruppo rispetto alla consueta operazione di prodotto in quanto l'inverso dei numeri interi $x \neq \pm 1$ non è un numero intero.

3. L'insieme $\mathbb{Z}/n\mathbb{Z}$ delle classi resto modulo n è un gruppo abeliano rispetto all'operazione di somma $\overline{x} + \overline{y} = \overline{x+y}$ con elemento neutro $\overline{0}$ e $-\overline{x} = \overline{-x}$ per ogni $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$.

   La classe $\overline{1}$ è l'elemento neutro dell'operazione di prodotto $\overline{xy} = \overline{xy}$. D'altra parte, per l'identità di Bezout, esiste una classe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tale che $\overline{xy} = \overline{1}$ se e soltanto se $\mathrm{MCD}(x, n) = 1$. Quindi $\mathbb{Z}/n\mathbb{Z}$ non è un gruppo rispetto al prodotto, ma

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \text{ tale che } \mathrm{MCD}(x, n) = 1\}$$

   lo è.

4. Sia X un insieme qualunque. Una *permutazione* su X è una funzione biettiva $f : X \to X$. Poniamo

$$\mathfrak{S}_X = \{\text{permutazioni su } X\}.$$

   L'insieme $\mathfrak{S}_X$ è un gruppo rispetto all'operazione di composizione di funzioni $f \circ g(x) = f(g(x))$ per ogni $x \in X$. L'elemento neutro è la mappa identità $i_X : X \to X$, $i_X(x) = x$ per ogni $x \in X$, e l'inverso di una permutazione f è la funzione inversa f^{-1}.

   Quando X è un insieme finito con n elementi, ad esempio $X = \{1, \dots, n\}$, il gruppo $\mathfrak{S}_X$ si denota solitamente $\mathfrak{S}_n$ e si dice *gruppo delle permutazioni su n elementi* (questa notazione verrà giustificata nell'esempio 2.1.7(2)). Il gruppo $\mathfrak{S}_n$ conta $n!$ elementi ed è non abeliano se $n \geq 3$. Infatti siano a, b e c tre elementi distinti di X ed f e $g \in \mathfrak{S}_n$ tali che $f(a) = a$, $f(b) = c$, $f(c) = b$ e $g(a) = b$, $g(b) = c$, $g(c) = a$. Allora $f \circ g(a) = c$ e $g \circ f(a)b$ e quindi $f \circ g \neq g \circ f$.

   Ricordiamo qui alcuni fatti riguardanti le permutazioni in $\mathfrak{S}_n$ che ci saranno utili in seguito. Una permutazione $f \in \mathfrak{S}_n$ si denota solitamente

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

   La permutazione f è detta ciclica, o ciclo, se esiste un sottoinsieme $X' = \{x_1, x_2, \dots, x_l\} \subseteq \{1, 2, \dots, n\}$ tale che

$$f(x_1) = x_2, f(x_2) = x_3, \dots, f(x_l) = f(x_1), \qquad \text{e} \qquad f(x) = x \quad \text{per ogni } x \notin X'.$$

   Denoteremo tale ciclo

$$f = (x_1\ x_2\ \dots\ x_\ell)$$

   e chiamiamo lunghezza del ciclo f l'intero $\ell(f) = l$. Due cicli $f = (x_1\ x_2\ \dots\ x_r)$ e $g = (y_1, y_2, \dots, y_s)$ si dicono disgiunti se

$$\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots, y_s\} = \emptyset.$$

   Allora:

   (a) se $f \in \mathfrak{S}_n$ è un ciclo, la sua lunghezza $\ell(f)$ è il più piccolo intero positivo r tale che $f^r = 1$;

   (b) cicli disgiunti commutano in $\mathfrak{S}_n$;

   (c) ogni permutazione $f \in \mathfrak{S}_n$ si decompone come prodotto di cicli disgiunti e tale decomposizione è unica.

Il primo punto discende dall'osservazione che l'effetto della permutazione f^r sugli elementi di X' è $f(x_k) = x_{k+r}$ per ogni $k = 1, \ldots, l$ e dove l'indice $k+r$ deve essere preso modulo l. Il secondo punto segue subito calcolando l'effetto delle composizioni dei cicli sul generico elemento $k \in \{1, \ldots, n\}$. La decomposizione del terzo punto si ottiene induttivamente come segue. Poniamo $Y = \emptyset$ e scegliamo $k \in \{1, \ldots, n\} - Y$. Sia r il più piccolo intero positivo tale che $f^r(k) = k$ e poniamo

$$c_1 = (k \ f(k) \ \ldots \ f^{r-1}(k)).$$

Se $\{k, f(k), \ldots, f^{r-1}(k)\} = \{1, 2, \ldots, n\}$ si ha $f = c_1$ e l'affermazione è vera. Altrimenti si ripeta la procedura con Y sostituito da $Y \cup \{k, f(k), \ldots, f^{r-1}(k)\}$ per ottenere un nuovo ciclo c_2 disgiunto dal preceente e così via. Siccome ad ogni passaggio l'insieme Y diventa strettamente più grande, ad un certo punto si ottiene $Y = \{1, 2, \ldots, n\}$ e se $c_1, \ldots, c_t$ sono i cicli disgiunti sin lì prodotti risulta

$$f = c_1 \cdots c_t.$$

Lasciamo per esercizio (vedi problema 1.2) il compito di dimostare che tale decomposizione è unica.

Nota Bene : coerentemente con l'interpretazione delle permutazioni come funzioni, adotteremo la convenzione secondo cui le permutazioni si compongono da destra verso sinistra. Ad esempio (1 3 2)(2 4 1) = (2 4 3), eccetera.

5. Sia V uno spazio vettoriale su un campo K e sia $\mathrm{Aut}(V)$ l'insieme di tutti gli automorfismi lineari $T : V \to V$. La composizione di automorfismi definisce una struttura di gruppo su $\mathrm{Aut}(V)$. L'elemento neutro è la mappa identità i_V e l'inverso di un automorfismo lineare T è la funzione inversa T^{-1}.

6. Sia R un anello e sia $\mathrm{M}_n(R)$ l'insieme delle matrici $n \times n$ ad elementi in R. Il prodotto righe per colonne di due matrici $A = (a_{ij})$ e $B = (b_{ij})$, definito come

$$(a_{ij})(b_{ij}) = (c_{ij}) \qquad \text{dove } c_{ij} = \textstyle\sum_{k=1}^{n} a_{ik} b_{kj} \text{ per ogni } 1 \leq i, j \leq n$$

ha la proprietà che $\det(AB) = \det(A)\det(B)$ (Teorema di Binet) ed ammette come elemento neutro la matrice identità $I_n = (\delta_{ij})$. Una matrice A ammette inverso esattamente quando l'elemento $\det(A) \in R$ possiede inverso in R. In tal caso si ha $A^{-1} = \frac{1}{\det(A)}((-1)^{i+j} A_{ij})^t$ dove A_{ij} è il determinante della matrice di ordine $n-1$ ottenuta da A cancellando la riga i-esima e la colonna j-esima e $(\ )^t$ indica la trasposizione. Dunque il sottoinsieme

$$\mathrm{GL}_n(R) = \{A \in \mathrm{M}_n(R) \text{ tale che } \det(A) \text{ è invertibile in } R\}$$

è un gruppo detto *gruppo lineare generale di rango n a coefficienti in R.*

1.2 Sottogruppi

Un gruppo può contenere al suo interno dei gruppi più piccoli.

Definizione 1.2.1. *Un sottoinsieme non vuoto H di un gruppo G ne è un sottogruppo se è un gruppo rispetto all'operazione di G ristretta alle coppie in $H \times H$.*

Si noti che per la proprietà di cancellazione (che vale in G) un elemento neutro per l'operazione di G ristretta ad H deve essere neutro anche per G. Pertanto un sottoinsieme H di G è un sottogruppo se

1. per ogni a, $b \in H$ risulta $ab \in H$;
2. $1 \in H$;
3. per ogni $a \in H$ risulta $a^{-1} \in H$.

Per le applicazioni il criterio seguente torna spesso utile.

Proposizione 1.2.2. *Un sottoinsieme H di un gruppo G è un sottogruppo se e soltanto se per ogni a, $b \in H$ risulta $ab^{-1} \in H$.*

Dimostrazione. La condizione è ovviamente necessaria. Per la sufficienza ponendo $a = b \in H$ si ha innanzitutto $1 \in H$. Posto poi $a = 1$ si ha che se $b \in H$, allora $b^{-1} \in H$. Infine, prendendo a e b^{-1} si ottiene $ab \in H$. ■

Il simbolo $H < G$ significa che H è un sottogruppo di G.

Esempi 1.2.3.

1. Qualunque sia G, il sottoinsieme $\{1\}$ costituito dal solo elemento neutro è un sottogruppo. Anche G stesso è un sottogruppo di G. Tali sottogruppi sono detti *banali*.
2. Chiaramente $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ e $\mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$.
3. Dato $m \in \mathbb{Z}$ consideriamo il sottoinsieme di $\mathbb{Z}$ costituito dai multipli di m, cioè
$$\mathbb{Z}m = \{km \,|\, k \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$
Esso è un sottogruppo di $\mathbb{Z}$ in quanto per ogni h, $k \in \mathbb{Z}$ si ha $hm - km = (h-k)m \in \mathbb{Z}m$. Se $m \neq 0, \pm 1$ il sottogruppo $\mathbb{Z}m$ non è banale. Viceversa, sia $H < \mathbb{Z}$ un sottogruppo non banale. Si vede subito che l'insieme $\{h \in H \,|\, h > 0\}$ è un sottoinsieme non vuoto di $\mathbb{N} - \{0\}$ e quindi ammette un elemento minimo m. Per ogni $h \in H$ l'algoritmo di divisione euclidea permette di scrivere $h = mq + r$ con $0 \leq r < m$. Riscrivere tale relazione come $r = h - mq$ rende evidente il fatto che $r \in H$ e quindi, per minimalità di m, deve essere $r = 0$. Dunque h è un multiplo di m, cioè $H = \mathbb{Z}m$.
4. Se $Y \subset X$, possiamo considerare il sottoinsieme
$$\mathfrak{S}_{X,Y} = \{f \in \mathfrak{S}_X \text{ tale che } f(y) = y \text{ per ogni } y \in Y\}$$
delle permutazioni che "lasciano fisso" Y. Per ogni f, $g \in \mathfrak{S}_{X,Y}$ risulta $f \circ g^{-1}(y) = f(g^{-1}(y)) = f(y) = y$ per ogni $y \in Y$ e quindi $\mathfrak{S}_{X,Y}$ è un sottogruppo di $\mathfrak{S}_X$.
5. Sia R un anello. Poniamo
$$\mathrm{SL}_n(R) = \{A \in \mathrm{GL}_n(R) \text{ tale che } \det(A) = 1\}.$$
Chiaramente $I_n \in \mathrm{SL}_n(R)$ e dal Teorema di Binet segue che se $\det(A) = \det(B) = 1$ allora $\det(AB) = \det(A^{-1}) = 1$. Pertanto $\mathrm{SL}_n(R)$ è un sottogruppo di $\mathrm{GL}_n(R)$, detto *gruppo lineare speciale di rango n a coefficienti in R*.

6. Sia G un gruppo qualunque. Il *centro* di G è il sottogruppo

$$Z(G) = \{x \in G \text{ tali che } xg = gx \text{ per ogni } g \in G\}.$$

Il centro $Z(G)$ è abeliano e $Z(G) = G$ se e soltanto se G è abeliano. Per verificare che $Z(G)$ è un sottogruppo si osservi che dalla relazione $xg = gx$ segue, moltiplicando a destra e a sinistra per x^{-1} che $gx^{-1} = x^{-1}g$. Dunque da $x, y \in Z(G)$ segue $gxy^{-1} = xgy^{-1} = xy^{-1}g$, cioè $xy^{-1} \in Z(G)$.

Come esempio concreto osserviamo che

$$Z(\mathfrak{S}_n) = \{1\}, \qquad \text{se } n \geq 3.$$

Infatti se $1 \neq f \in \mathfrak{S}_n$ esiste x tale che $f(x) = y \neq x$. Siccome $n \geq 3$ esiste $z \in \{1, \ldots, n\} - \{x, y\}$. Allora si vede subito che $f \circ (y\ z) \neq (y\ z) \circ f$ e quindi $f \notin Z(\mathfrak{S}_n)$.

7. Sia $n \geq 3$ e sia P_n il poligono regolare con n lati che possiamo pensare centrato nell'origine delle coordinate del piano $\mathbb{R}^2$. Sia D_n l'insieme delle isometrie f di $\mathbb{R}^2$ che lasciano invariato P_n, cioè tali che $f(P_n) = P_n$. È chiaro che D_n è un gruppo, detto *gruppo diedrale di ordine* n, perchè la composizione di isometrie è un'isometria così come l'inversa di un'isometria è un'isometria e la richiesta $f(P_n) = P_n$ resta soddisfatta sia per composizione che per passaggio all'inversa. Si vede subito che:

   - ogni elemento di D_n fissa il centro di P_n e quindi D_n può rivedersi come sottogruppo del gruppo $\mathcal{I}_0$ studiato nel problema 1.2;
   - ogni elemento di D_n permuta i vertici di P_n in quanto i vertici possono essere caratterizzati come i punti del poligono a distanza massima dal centro. Pertanto, assegnata una numerazione dei vertici, il gruppo D_n può rivedersi come un sottogruppo del gruppo $\mathfrak{S}_n$.

   Per la seconda osservazione sopra, possiamo subito concludere che D_n è un gruppo finito. Le seguenti trasformazioni sono visibilmente elementi di D_n:

   - le n potenze
   $$r^0 = \mathrm{id}, r, r^2, \ldots, r^{n-1}$$
   della rotazione oraria r di $2\pi/n$ radianti. Esse costituiscono un sottogruppo in D_n.
   - le simmetrie assiali, per cui dobbiamo distinguere due casi secondo la parità di n. Se n è dispari ci sono n simmetrie per gli n assi che congiungono un vertice al centro e bisecano il lato opposto. Se n è dispari ci sono $n/2$ simmetrie per gli assi che congiungono coppie di vertici opposti e $n/2$ simmetrie che bisecano coppie di lati opposti.

   In ogni caso si hanno n simmetrie assiali e siccome evidentemente nessuna simmetria è una rotazione, abbiamo così almeno 2n elementi in D_n. Il nostro obiettivo ora è di dimostrare che quelli costruiti sono tutti gli elementi di D_n e di determinarne la struttura di gruppo.

   Consideriamo un lato di P_n e ne siano P e Q i vertici ordinati nel senso di rotazione oraria. Siccome P e Q costituiscono, pensati come definenti vettori nel piano, una base di $\mathbb{R}^2$, un elemento $f \in D_n$ resta completamente determinato da $f(P)$ e $f(Q)$. Se $f(P)$ precede $f(Q)$ nel verso orario, f risulta essere una rotazione (infatti se P' è il vertice che precede P, allora $f(P')$ deve essere il vertice che precede $f(P)$ e così via a ritroso). Se invece $f(Q)$ precede $f(P)$ e se r^k è la rotazione che sposta P in $f(P)$, allora l'elemento $r^{-k}f \in D_n$ non

è l'identità e fissa P e deve dunque essere la simmetria $s = s_P$ rispetto all'asse passante per P. Dunque gli elementi di D_n sono tutti e soli quelli della forma

$$r^k s^\epsilon \qquad k \in \{0, 1, \ldots, n-1\} \quad \epsilon \in \{0, 1\}.$$

Inoltre, un'analisi del comportamento delle isometrie sui vertici (vedi problema 1.2) permette di ottenere la relazione

$$sr^k = r^{-k}s \qquad k \in \{0, 1, \ldots, n-1\} \tag{1.2}$$

che insieme all'ovvia $s^2 = 1$ determina completamente la tavola di moltiplicazione (e quindi la struttura) di D_n.

L'insieme dei sottogruppi di un gruppo G è ordinato naturalmente dall'inclusione (insiemistica). Si osservi che dal criterio 1.2.2 segue immediatamente che:

1. se $K < H$ e se $H < G$ allora $K < G$;
2. se $\{H_i\}_{i\in I}$ è una famiglia arbitraria di sottogruppi di G allora $\bigcap_{i\in I} H_i$ è un sottogruppo di G.

Invece l'unione insiemistica di due (o più) sottogruppi non è, in generale, un sottogruppo. Ad esempio, in $\mathbb{Z}$ l'unione $H = \mathbb{Z}2 \cup \mathbb{Z}3$ non è un sottogruppo in quanto $1 = 3 - 2 \notin H$. Se $\{H_i\}_{i\in I}$ è una famiglia arbitraria di sottogruppi di G chiamiamo *sottogruppo generato dagli* H_i il più piccolo sottogruppo di G contenente $H = \bigcup_{i\in I} H_i$. Lo denotiamo $\langle H\rangle$.

Esempio 1.2.4. Siano $a, b \in \mathbb{Z}$ con $d = \mathrm{MCD}(a, b)$ e $m = \mathrm{mcm}(a, b)$. Allora $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ e $\langle \mathbb{Z}a \cup \mathbb{Z}b\rangle = \mathbb{Z}d$. Infatti $\mathbb{Z}a \cap \mathbb{Z}b$ è costituito interamente da interi multipli simultaneamente di a e di b (ed m è il più piccolo tale intero) e

$$\langle \mathbb{Z}a \cup \mathbb{Z}b\rangle = \{xa + yb \,|\, x, y \in \mathbb{Z}\} = \mathbb{Z}d$$

per l'identità di Bezout.

Più in generale, se $H \subset G$ è un qualunque sottoinsieme di G chiamiamo *sottogruppo generato da* H, denotato $\langle H\rangle$, il più piccolo sottogruppo di G contenente H. Se risulta $G = \langle H\rangle$ diciamo che G *è generato da* H. In particolare, se $g \in G$ risulta

$$\langle g\rangle = g^{\mathbb{Z}} = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\} \subseteq G$$

in quanto $g^m(g^n)^{-1} = g^{m-n} \in \langle g\rangle$, vedi problema 1.2, e quindi il sottoinsieme di tutte le potenze di g è il più piccolo sottogruppo di G che contiene l'elemento g (si noti l'analogia con i sottogruppi $\mathbb{Z}m$ di $\mathbb{Z}$). Il sottogruppo $\langle g\rangle$ è detto *sottogruppo ciclico generato da* g e se $H < G$ è della forma $H = \langle g\rangle$ diremo che g è un generatore di H. Infine, G stesso è un *gruppo ciclico generato da* g se $G = \langle g\rangle$.

Esempi 1.2.5.

1. Gli esempi standard di gruppi ciclici sono $\mathbb{Z} = \langle 1\rangle$ e $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1}\rangle$.
2. Il sottogruppo delle rotazioni in un gruppo diedrale è ciclico.
3. Il gruppo $\mathbb{Q}$ non è ciclico. Infatti se $q = \frac{m}{n} \in \mathbb{Q}$ i denominatori dei numeri razionali in $\langle q\rangle = \{0, \pm q, \pm 2q, \ldots\}$ sono dei divisori di n. Quindi, ad esempio, $\frac{1}{2}q \in \mathbb{Q} - \langle q\rangle$.

4. In $\mathfrak{S}_n$ una trasposizione è un ciclo di lunghezza 2. Ogni ciclo è prodotto di trasposizioni, in quanto
$$(x_1\ x_2\ \dots\ x_l) = (x_1\ x_2)(x_1\ x_3)\cdots(x_1\ x_l).$$
Siccome ogni permutazione è prodotto di cicli, vedi esempio 1.1.3(4), ogni permutazione può scriversi come prodotto di trasposizioni, cioè
$$\mathfrak{S}_n = \langle T\rangle, \qquad \text{dove } T = \{\text{trasposizioni}\}.$$
Contrariamente alla decomposizione di una permutazione in cicli disgiunti, la scrittura di una permutazione come prodotto di trasposizioni non è unica, ad esempio
$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 4)(1\ 3)(4\ 3)(1\ 2).$$
È però vero che la parità del numero delle trasposizioni che occorrono per ottenere una data permutazione è ben determinata, ovvero
$$t_1\cdots t_r = \tau_1\cdots\tau_s \quad \text{con } t_i \text{ e } \tau_j \text{ trasposizioni} \quad \Longrightarrow \quad r \equiv s \bmod 2$$
Infatti se la permutazione f si potesse scrivere come prodotto di un numero pari e anche come prodotto di un numero dispari di trasposizioni, il prodotto $1 = ff^{-1}$ ci permetterebbe di scrivere la permutazione identica come prodotto di un numero dispari di trasposizioni. Sia k il più piccolo numero intero tale che 1 ammette una scrittura come prodotto di $2k+1$ trasposizioni:
$$1 = t_1 t_2 \cdots t_{2k+1}. \tag{1.3}$$
Sia x un elemento che compare in una delle trasposizioni t_i. Ogni segmento della forma $(x\ y)(z\ z')$ con $\{x,y\}\cap\{z,z'\} = \emptyset$ può riscriversi $(z\ z')(x\ y)$ ed ogni segmento della forma $(x\ y)(y\ z)$ può riscriversi $(y\ z)(x\ z)$ senza modificare il numero delle trasposizioni. Quindi possiamo assumere che x non compare nelle prime $r < 2k+1$ trasposizioni e che sia
$$t_{r+1}\cdots t_{2k+1} = (x\ y_{r+1})\cdots(x\ y_{2k+1}).$$
Se gli y_i sono tutti distinti quello appena scritto è il ciclo $(x\ y_{2k+1}\ \dots\ y_{r+1})$, cosa impossibile perchè la permutazione a destra in (1.3) non lascerebbe fisso x. Deve allora essere $y_u = y_v$ con $u \neq v$. Utilizzando ora l'identità $(x\ z)(x\ y) = (x\ y)(y\ z)$ possiamo avvicinare le due trasposizioni $(x\ y)$ fino a renderle adiacenti. A questo punto possono essere eliminate dalla scrittura (1.3), ottenendo una nuova scrittura con $2k-1 = 2(k-1)+1$ trasposizioni. Questo contraddice la minimalità di k.

Possiamo allora definire
$$A_n = \{f \in \mathfrak{S}_n \text{ tali che } f \text{ è prodotto di un numero pari di trasposizioni}\}$$
e risulta chiaro che si tratta di un sottogruppo di $\mathfrak{S}_n$ che contiene $\frac{1}{2}n!$ elementi. Esso prende il nome di *gruppo alterno su n elementi*. Ad esempio A_3 è il sottogruppo ciclico di $\mathfrak{S}_3$ generato dal ciclo (1 2 3).

Vale la pena notare che il sottogruppo $\langle g\rangle$ non è necessariamente costituito da infiniti elementi potendosi avere delle ripetizioni; ad esempio in $G = \mathbb{Z}/12\mathbb{Z}$ si ha $\langle\overline{4}\rangle = \{\overline{0},\overline{4},\overline{8}\}$. Si hanno 2 possibilità.

1. Non esistono ripetizioni fra i g^n. In tal caso $\langle g\rangle$ contiene infiniti elementi. Diciamo che g ha ordine infinito, $\mathrm{ord}(g) = \infty$.

2. Esistono a, $b \in \mathbb{Z}$ con $a \neq b$ tali che $g^a = g^b$. Allora $g^{a-b} = 1$ e pertanto l'insieme $\{t > 0 \,|\, g^t = 1\}$ è non vuoto. Sia m il minimo di tale insieme. Per ogni $n \in \mathbb{Z}$, scritto $n = mq + r$ con $0 \leq r < m$, si ha

$$g^n = g^{mq+r} = (g^m)^q g^r = 1^q g^r = g^r.$$

D'altra parte $g^a = g^b$ con $0 \leq b < a < m$ contraddice la minimalità di m e quindi

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$$

consiste di esattamente m elementi. Diciamo che g ha ordine m, $\mathrm{ord}(g) = m$.

Lo stesso (sotto)gruppo ciclico ammette più di in generatore. Nel primo caso, in cui $\mathrm{ord}(g) = \infty$, si ha $\langle g \rangle = \langle g^{-1} \rangle$ e per ogni $n \neq 0, \pm 1$ l'elemento $h = g^n$ non genera $\langle g \rangle$ in quanto le potenze di h sono solo le potenze di g con esponente multiplo di n. La situazione è più complessa nel secondo caso.

Proposizione 1.2.6. *Se* $\mathrm{ord}(g) = m$ *allora* $\langle g \rangle = \langle g^n \rangle$ *se e soltanto se* $\mathrm{MCD}(m, n) = 1$

Dimostrazione. Risulta $\langle g \rangle = \langle g^n \rangle$ se e soltanto se $g = (g^n)^t$ per un opportuno t. Siccome $g^s = 1$ se e soltanto se $s \equiv 1 \bmod m$, la condizione è equivalente a quella di poter trovare t e t' tali che $tn - t'm = 1$. Questo è possibile se e soltanto se $\mathrm{MCD}(m, n) = 1$.■

Questo risultato permette di reintrepretare la funzione ϕ di Eulero,

$$\phi(n) = |\{x \in \mathbb{N} \text{ tali che } 1 \leq x \leq n \text{ e } \mathrm{MCD}(x, n) = 1\}|$$

come

$$\phi(n) = \text{numero dei generatori di un gruppo ciclico con } n \text{ elementi}$$

(dall'esempio 1.1.3(3) si ha anche $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$).

Nel caso dei gruppi ciclici possiamo determinare esplicitamente tutti i sottogruppi.

Teorema 1.2.7. *Sia* $G = \langle g \rangle$ *un gruppo ciclico. Allora:*

1. *se* G *è infinito, i sottogruppi di* G *sono tutti e soli quelli della forma* $\langle g^n \rangle$ *con* $n \in \mathbb{Z}$. *Inoltre* $\langle g^m \rangle < \langle g^n \rangle$ *se e soltanto se* $m|n$;
2. *se* $\mathrm{ord}(g) = n$, G *possiede uno ed uno solo sottogruppo con* m *elementi per ogni divisore* m *di* n. *Tale sottogruppo è ciclico e generato da* $g^{n/m}$.

Dimostrazione. Nel primo caso l'unica cosa non ovvia è che ogni sottogruppo non banale è della forma $\langle g^n \rangle$ per un opportuno $n \neq 0, \pm 1$. Sia $H < G$. Ogni elemento di G è della forma g^t con $t \in \mathbb{Z}$. Siccome H non è banale, esiste un $n > 0$ minimale rispetto alla condizione $g^n \in H$. A questo punto si procede come nell'esempio 1.2.3(2).

Nel secondo caso la dimostrazione è analoga. Se $H < G$, $H \neq \{1\}$, ragionando come sopra si ottiene $H = \langle g^d \rangle$ per un d opportuno (minimo tale che $g^d \in H$). A questo punto si scriva $n = dq + r$ con $0 \leq r < d$: allora $1 = g^n = (g^d)^q g^r$ e quindi $g^r = (g^d)^{-q} \in H$. Per minimalità di d risulta $r = 0$, cioè $d|n$. Siccome gli elementi $1, g^d, g^{2d}, \ldots, g^{(\frac{n}{d}-1)d}$ sono tutti distinti, H è un sottogruppo con $m = n/d$ elementi ed è chiaramente l'unico con tale proprietà.■

In particolare, il teorema appena dimostrato implica che in un gruppo ciclico $G = \langle g \rangle$ con n elementi per ogni divisore $d|n$ ci sono esattamente d elementi tali che $x^d = 1$, precisamente quelli del sottogruppo $\langle g^{n/d} \rangle$. Vediamo ora che questa proprietà caratterizza i gruppi ciclici.

Teorema 1.2.8. *Sia G un gruppo finito con n elementi tale che per ogni divisore $d|n$ l'insieme degli $x \in G$ tali che $x^d = 1$ ha al più d elementi. Allora G è ciclico.*

Dimostrazione. Iniziamo col dimostrare che se $n \geq 1$ è un intero, allora

$$n = \sum_{d|n} \phi(d). \tag{1.4}$$

Infatti c'è una partizione $\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} \Phi_d$ dove Φ_d è l'insieme dei generatori del sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ con d elementi. Allora $n = |\mathbb{Z}/n\mathbb{Z}| = \sum_d |\Phi_d| = \sum_d \phi(d)$ è la (1.4).

Sia $d|n$ e supponiamo esista $x \in G$ tale che $\mathrm{ord}(x) = d$. Per ogni elemento $y \in \langle x \rangle$ vale $y^d = 1$ e quindi, per ipotesi, ogni altro elemento di G di ordine d appartiene a $\langle x \rangle$. Dunque di elementi di ordine d ce ne è o $\phi(d)$ o nessuno. Dovendosi avere

$$G = \bigcup_{d|n} \{\text{elementi di ordine } d\}$$

dovrà essere $n = \sum_d |\{\text{elementi di ordine } d\}| \leq \sum_d \phi(d) = n$ per la (1.4). Quindi l'insieme degli elementi di ordine d è non vuoto per ogni d ed in particolare devono esistere elementi di ordine n. ■

Questo risultato ha la seguente notevole applicazione.

Corollario 1.2.9. *Sia K un campo e sia G un sottogruppo finito del gruppo moltiplicativo $K^\times$. Allora G è ciclico.*

Dimostrazione. In un campo l'equazione $x^d = 1$ ammette al più d soluzioni qualunque sia d. ■

Esempio 1.2.10. Un caso importante del corollario precedente è quello del gruppo

$$\mu_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$$

detto *gruppo delle radici n-esime dell'unità*. Tale gruppo ha n elementi perchè i suoi elementi sono le radici complesse del polinomio $X^n - 1$ che è privo di radici multiple. Per il corollario, μ_n è ciclico. Un generatore di μ_n è chiamato *radice n-esima primitiva dell'unità*.

Particolarizzando il corollario al caso dei campi finiti si ottiene il

Teorema 1.2.11. *Il gruppo moltiplicativo di un campo finito è ciclico.*

Si noti che la dimostrazione di tale risultato non offre alcun indizio per la determinazione, in concreto, di un generatore di $\mathbb{F}_{p^\times}$. Citiamo, a tale proposito, la celebre congettura seguente che resta tuttora indimostrata per ogni valore di n.

Congettura 1.2.12 (Artin)**.** *Sia $n \in \mathbb{N}$ un numero intero non quadrato. Allora la classe $\bar{n}$ modulo p genera $\mathbb{F}_{p^\times}$ per infiniti primi p.*

PROBLEMI

Il simbolo G denota sempre un gruppo.

1.1. Dimostrare l'unicità dell'elemento neutro e dell'inverso di un elmento in un gruppo.

1.2. Sia $a \in G$. Dimostrare dapprima che per ogni $n = 1, 2, 3, \ldots$ si ha $a^{n-1} = (a^{-1})^n$. Poi, posto $a^{-n} = (a^n)^{-1}$, mostrare che per ogni m, $n \in \mathbb{Z}$ si ha $a^{m+n} = a^m a^n$.

1.3. Dimostrare che in G le equazioni $ax = b$ e $xa = b$ ammettono sempre una soluzione e che essa è unica.

1.4. Dimostrare che G è abeliano se e soltanto se $(xy)^2 = x^2y^2$ per ogni x, $y \in G$.

1.5. Sia $f = (x_1\ x_2\ \ldots\ x_r)$ un ciclo in $\mathfrak{S}_n$. Dimostrare che $f^{-1} = (x_r\ x_{r-1}\ \ldots\ x_1)$.

1.6. Decomporre in prodotto di cicli disgiunti le permutazioni

$$\begin{pmatrix} 1&2&3&4&5&6\\ 4&6&5&1&2&3 \end{pmatrix}, \qquad \begin{pmatrix} 1&2&3&4&5&6&7&8&9\\ 8&6&1&5&9&2&4&3&7 \end{pmatrix} \qquad \begin{pmatrix} 1&2&3&4&5&6&7&8&9&10&11\\ 8&7&3&2&11&5&4&10&6&1&9 \end{pmatrix}$$

e riscrivere come prodotto di cicli disgiunti i seguenti prodotti di cicli

$$(1\ 4\ 7)(4\ 5\ 2), \qquad (2\ 3)(3\ 5)(5\ 2), \qquad (3\ 1\ 5\ 6)(4\ 1\ 2\ 6).$$

1.7. Dimostrare l'unicità della decomposizione di una permutazione in cicli disgiunti.

1.8. Dimostrare che se G è finito con un numero pari di elementi esiste $g \in G$, $g \neq 1$, tale che $g = g^{-1}$. Dedurre quindi che G possiede un sottogruppo con 2 elementi.

1.9. Nello spazio vettoriale reale $\mathbb{R}^n$ consideriamo la metrica euclidea standard $d(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}$. Sia $\mathcal{I}_0$ l'insieme delle isometrie di $\mathbb{R}^n$ che lasciano fisso il punto O, cioè

$$\mathcal{I}_0 = \{f : \mathbb{R}^n \to \mathbb{R}^n \text{ tali che } f(0) = 0 \text{ e } d(x, y) = d(f(x), f(y)) \text{ per ogni } x, y \in \mathbb{R}^n\}.$$

Si dimostri che:

1. ogni $f \in \mathcal{I}_0$ è completamente individuata dai valori $f(x_1), \ldots, f(x_n)$ dove $\{x_1, \ldots, x_n\}$ è una base di $\mathbb{R}^n$;
2. ogni $f \in \mathcal{I}_0$ è lineare;
3. $\mathcal{I}_0$ è un sottogruppo del gruppo $\mathrm{Aut}(\mathbb{R}^n)$ dell'esempio 1.1.3(5).

1.10. Dimostrare dettagliatamente la formula (1.2) per il gruppo diedrale D_n

1.11. Sia $H \subset G$ un sottoinsieme e sia $\mathcal{H}$ l'insieme dei sottogruppi $K < G$ tale che $H \subset K$. Dimostrare che $\langle H \rangle = \bigcap_{K \in \mathcal{H}} K$.

1.12. Determinare un generatore del gruppo moltiplicativo del campo con p elementi, p primo, per $p \leq 19$.

Lezione 2

Omomorfismi

The Theory of Groups is a branch of mathematics in which one does something to something and then compares the result with the result obtained from doing the same thing to something else, or something else to the same thing.
James R. NEWMAN, *The World of Mathematics (1956)*

2.1 Definizione ed esempi

Siamo ora interessati a studiare le funzioni tra gruppi. Tra tutte le funzioni isoliamo quelle che sono compatibili, nel senso preciso della definizione seguente, con le operazioni.

Definizione 2.1.1. *Siano G e H due gruppi. Una funzione $f\colon G \to H$ è detta un omomorfismo se vale l'uguaglianza*

$$f(xy) = f(x)f(y) \quad \text{per ogni } x,\, y \in G. \tag{2.1}$$

La relazione (2.1) ha due implicazioni immediate per un omomorfismo f:

1. $f(1) = 1$, ottenibile applicando la legge di cancellazione a $f(x) = f(x1) = f(x)f(1)$;
2. per ogni $x \in G$, deve aversi
$$f(x^{-1}) = f(x)^{-1}. \tag{2.2}$$
Infatti dal punto precedente si ha $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$.

Denotiamo $\mathrm{Hom}(G, H)$ l'insieme degli omomorfismi $G \to H$.

Osservazioni 2.1.2.
1. Se $G = \langle g \rangle$ è ciclico, ogni elemento $f \in \mathrm{Hom}(G, H)$ (qualunque sia H) è completamente determinato da $f(g)$. Infatti una semplice induzione su n mostra che $f(g^n) = f(g)^n$ se $n > 0$, e poi la relazione si estende ad ogni $n \in \mathbb{Z}$ prendendo in considerazione (2.2).
2. La funzione costante $e_0 : G \to H$ che assegna ad ogni $g \in G$ l'elemento neutro di H, cioè $e_0(g) = 1$, è un omomorfismo per cui si ha sempre $\mathrm{Hom}(G, H) \neq \emptyset$. D'altra parte è possibile che e_0 sia l'unico elemento in $\mathrm{Hom}(G, H)$. Ad esempio, ogni $f \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ è determinata da $f(\overline{1})$ w dovendosi avere, in $\mathbb{Z}$, l'uguaglianza $nf(\overline{1}) = f(n\overline{1}) = f(\overline{n}) = f(\overline{0}) = 0$ si ha l'unica possibilità $f(\overline{1}) = 0$ e quindi $f = e_0$.

Diamo ora degli esempi di omomorfismi.

Esempi 2.1.3. 1. Per ogni gruppo G la funzione identità $\mathrm{id}\colon G \to G$ definita come $\mathrm{id}(g) = g$.

2. La funzione esponenziale
$$\exp : \mathbb{R} \longrightarrow \mathbb{R}^\times, \qquad t \mapsto e^t.$$

3. La funzione
$$E : \mathbb{R} \longrightarrow \mathbb{C}^\times, \qquad t \mapsto e^{2\pi i t} = \cos(2\pi t) + i\mathrm{sen}(2\pi t).$$

4. La funzione f che ad ogni intero $n \in \mathbb{Z}$ associa la classe resto $\overline{n} \in \mathbb{Z}/N\mathbb{Z}$.

5. La funzione $\det\colon \mathrm{GL}_n(K) \to K^\times$ che associa ad ogni matrice $n \times n$ il suo determinante.

6. La funzione
$$\varphi_N\colon \mathbb{Z}/N\mathbb{Z} \longrightarrow \mu_N, \qquad \overline{n} \mapsto \zeta^n$$
dove ζ è una radice primitiva n-esima dell'unità.

Ad un omomorfismo $f\colon G \to H$ è associato il suo *nucleo*

$$\ker(f) = \{g \in G \mid f(g) = 1\}$$

Il nucleo $\ker(f)$ è un sottogruppo di G in quanto $f(1) = 1$, $f(x^{-1}) = f(x)^{-1} = 1$ se $x \in \ker(f)$ e $f(xy) = f(x)f(y) = 1$ se x, $y \in \ker(f)$. Il prossimo risultato rende esplicita la relazione tra il nucleo di un omomorfismo e le proprietà generali di quest'ultimo.

Proposizione 2.1.4. *Un omomorfismo f è iniettivo se e soltanto se* $\ker(f) = \{1\}$.

Dimostrazione. Se f non è iniettivo, esistono $x \neq y$ in G tale che $f(x) = f(y)$. Allora $f(xy^{-1}) = 1$ e dunque $1 \neq xy^{-1} \in \ker(f)$.

Viceversa se esiste $1 \neq x \in \ker(f)$, si ha $f(x) = f(1) = 1$ e dunque f non è iniettiva. ■

Esempi 2.1.5. Con riferimento alla lista di esempi 2.1.3 e mantenendo la stessa numerazione:

1. chiaramente $\ker(\mathrm{id}) = \{1\}$;

2. si ha $e^t = 1$ solo per $t = 0$, dunque $\ker(\exp) = \{0\}$;

3. si ha simultaneamente $\cos(x) = 1$ e $\mathrm{sen}(x) = 0$ se e soltanto se x è un multiplo intero di 2π, cioè $\ker(E) = \mathbb{Z}$;

4. $\overline{n} = \overline{0}$ in $\mathbb{Z}/N\mathbb{Z}$ se e soltanto se n è un multiplo di N, cioè $\ker(f) = \mathbb{Z}N$;

5. $\ker(\det) = \mathrm{SL}_n(K)$ (vedi esempio 1.2.3.(5));

6. $\zeta^n = 1$ se e soltanto se n è un multiplo di N. D'altra parte i multipli di N, cioè $\mathbb{Z}N$, sono esattamente gli interi che hanno classe resto nulla modulo N. Pertanto $\ker(\varphi_N) = \{\overline{0}\}$.

L'immagine $f(G)$ dell'omomorfismo f è un sottogruppo di H: se $f(x) = a$ e $f(y) = b$ si ha $f(xy^{-1}) = f(x)f(y)^{-1} = ab^{-1} \in f(G)$.

Definizione 2.1.6. *Un omomorfismo $f\colon G \to H$ è un isomorfismo se è biettivo.*

Diremo che due gruppi G e H sono *isomorfi*, in simboli $G \simeq H$, se esiste un isomorfismo $f\colon G \to H$. Naturalmente un omomorfismo tra gruppi isomorfi non è necessariamente un isomorfismo, ad esempio la funzione $x \mapsto 2x$ definisce un omomorfismo $\mathbb{Z} \to \mathbb{Z}$ che non è suriettivo.

Se f è un isomorfismo, esiste la funzione inversa f^{-1} che è anch'essa un isomorfismo. Infatti se $x, y \in H$ e se $f(a) = x$, $f(b) = y$ si ha $f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$. Insieme col fatto che la mappa id è un isomorfismo e che la composizione di isomorfismi è un isomorfismo (vedi Problema 2.2), questo mostra che la relazione di isomorfismo tra gruppi è una relazione di equivalenza.

Esempi 2.1.7.

1. La funzione esponenziale ha come immagine il sottogruppo $\mathbb{R}^{>0}$ del gruppo moltiplicativo $\mathbb{R}^\times$ costituito dai numeri positivi. Dunque la funzione esponenziale definisce un isomorfismo $\mathbb{R} \xrightarrow{\sim} \mathbb{R}^{>0}$ il cui inverso è la funzione logaritmo.

2. Sia $\psi : X \to Y$ una biezione tra insiemi. Allora l'associazione $f \mapsto \psi^{-1} \circ f \circ \psi$ definisce un isomorfismo $\mathfrak{S}_Y \xrightarrow{\sim} \mathfrak{S}_X$ che ha come inverso la mappa $h \mapsto \psi \circ h \circ \psi^{-1}$. Dunque la classe di isomorfismo di $\mathfrak{S}_X$ dipende solo dalla classe di equipollenza di X, giustificando la notazione $\mathfrak{S}_n$ se $|X| = n$ (vedi Esempio 1.1.3(4)).

3. Siano $G = \langle g \rangle$ e $H = \langle h \rangle$ due gruppi ciclici tali che $\mathrm{ord}(g) = \mathrm{ord}(h) \in \mathbb{N} \cup \{\infty\}$. Allora la funzione $f : G \to H$ tale che $f(g) = h$ è un isomorfismo. Quindi ogni gruppo ciclico è isomorfo o a $\mathbb{Z}$, se infinito, o a $\mathbb{Z}/m\mathbb{Z}$, se costituito da m elementi.

   In particolare $\mathbb{Z}/n\mathbb{Z} \simeq \mu_n$ e l'isomorfismo può realizzarsi come $\overline{n} \mapsto \zeta^n$ (vedi esempio 2.1.3.(6)) per una scelta di radice primitiva n-esima ζ. In tal senso l'isomorfismo $\mathbb{Z}/n\mathbb{Z} \simeq \mu_n$ non è canonico[1].

4. Sia K un campo qualunque, V un K-spazio vettoriale di dimensione n. Fissata una base $\{e_1, \ldots, e_n\}$ di V, ad ogni trasformazione K-lineare $T : V \to V$ resta associata la matrice $M(T) = (m_{ij}) \in \mathrm{M}_n(K)$ secondo la regola

$$T(e_j) = \sum_{i=1}^{n} m_{ij} e_i. \tag{2.3}$$

   Si verifica che $M(T \circ T') = M(T)M(T')$ (prodotto righe per colonne) e che l'associazione $T \mapsto M(T)$ è una biezione. Per quest'ultima, si noti che la 2.3 dice che T è completamente determinata da $M(T)$ e, letta da destra verso sinistra, che ogni matrice $M = (m_{ij})$ definisce una trasformazione lineare T tale che $M = M(T)$. Restringendo la definizione a $T \in \mathrm{Aut}(V)$, resta così definito un isomorfismo $M : \mathrm{Aut}(V) \xrightarrow{\sim} \mathrm{GL}_n(K)$, anch'esso non canonico.

Una proprietà importante degli omomorfismi è quella di conservare i sottogruppi, nel senso della

Proposizione 2.1.8. *Sia $f\colon G \to G'$ un omomorfismo di gruppi e siano H e H' sottogruppi di G e G' rispettivamente. Allora*

1. *$f(H)$ è un sottogruppo di G',*
2. *$f^{-1}(H')$ è un sottogruppo di G.*

[1] Diciamo che un isomorfismo $f : G \xrightarrow{\sim} H$ è *canonico* se per ogni $g \in G$ la definizione di $f(g)$ non dipende da scelte arbitrarie. Per un esempio di isomorfismo canonico vedi il Teorema 3.4.1.

Dimostrazione. Se $x = f(a)$ e $y = f(b)$ sono elementi di $f(H)$ si ha $xy^{-1} = f(ab^{-1}) \in f(H)$. Se, invece, a e $b \in G$ sono tali che $f(a), f(b) \in H'$, allora risulta $f(ab^{-1}) = f(a)f(b)^{-1} \in H'$, cioè $ab^{-1} \in f^{-1}(H')$. ■

In particolare, l'immagine $\mathrm{im}(f) = f(G)$ di un omomorfismo $f : G \to H$ è un sottogruppo di H.

2.2 Automorfismi, coniugio.

Un *automorfismo* di un gruppo G è un isomorfismo $G \xrightarrow{\sim} G$. L'identità è un automorfismo così come l'inverso di un automorfismo e il composto di due automorfismi è un automorfismo. Quindi l'insieme

$$\mathrm{Aut}(G) = \{\text{automorfismi di } G\} \subseteq \mathrm{Hom}(G, G),$$

è un gruppo rispetto all'operazione di composizione di funzioni.

Esempio 2.2.1. Sia $G = \langle g \rangle$ un gruppo ciclico. Sappiamo che un omomorfismo $\phi \in \mathrm{Hom}(G, G)$ è completamente determinato da $\phi(g)$. L'omomorfismo ϕ è un automorfismo se e soltanto se $\phi(g)$ è anch'esso un generatore di G.

- Nel caso $G \simeq \mathbb{Z}$ ci sono 2 generatori e quindi 2 automorfismi: l'identità e l'automorfismo tale che $\phi(g) = g^{-1}$. Siccome $\phi \circ \phi = \mathrm{id}$, risulta che $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.
- Nel caso $G \simeq \mathbb{Z}/n\mathbb{Z}$ i generatori sono in corrispondenza biunivoca con le classi resto invertibili modulo n. Osserviamo che la funzione

  $$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \qquad \overline{m} \mapsto \phi_{\overline{m}} \quad \text{dove } \phi_{\overline{m}}(\overline{a}) = \overline{am}$$

  è un isomorfismo perchè $\phi_{\overline{mm'}} = \phi_{\overline{m}} \circ \phi_{\overline{m'}}$ (hanno lo stesso effetto sul generatore $\overline{1}$).

Una classe importante di automorfismi di un gruppo G è quella degli *automorfismi interni*. L'automorfismo interno associato all'elemento $g \in G$ è la funzione

$$\phi_g : G \longrightarrow G, \qquad \phi_g(x) = gxg^{-1} \text{ per ogni } x \in G;$$

essa è un automorfismo in quanto:

- $\phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y)$;
- $\ker \phi_g = \{1\}$ perchè se $\phi_g(x) = gxg^{-1} = 1$, moltiplicando a sinistra per g^{-1} e a destra per g si ottiene $x = 1$;
- per ogni $y \in G$ si ha $y = \phi_g(g^{-1}yg)$.

L'insieme degli automorfismi interni di G, denotato $\mathrm{Int}(G)$ è un sottogruppo di $\mathrm{Aut}(G)$. Infatti si ha $\phi_1 = \mathrm{id}$, ${\phi_g}^{-1} = \phi_{g^{-1}}$ e $\phi_g \circ \phi_h = \phi_{gh}$ per ogni g, $h \in G$. L'ultima uguaglianza si ottiene osservando che $\phi_g \circ \phi_h(x) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = \phi_{gh}(x)$ per ogni $x \in G$, e la precedente ponendo $h = g^{-1}$ in questa.

Definizione 2.2.2. *Due elementi x, $y \in G$ si dicono coniugati se esiste $g \in G$ tale che $y = gxg^{-1}$.*

Il coniugio è una relazione di equivalenza (vedi problema 2.2) e la classe di coniugio dell'elemento g è denotata $[g]$. Vale la caratterizzazione

$$Z(G) = \{g \in G \,|\, [g] = \{g\}\}.$$

Il fatto seguente mette in maggior risalto la correlazione tra commutatività e coniugio.

Proposizione 2.2.3. *In un gruppo G due elementi x e y sono coniugati se e soltanto se esistono a e $b \in G$ tali che $x = ab$ e $y = ba$.*

Dimostrazione. In un verso, basta osservare che $ab = a(ba)a^{-1}$. Nell'altra direzione, se $y = gxg^{-1}$ si ponga $a = g$ e $b = xg^{-1}$.■

Nel gruppo $\mathfrak{S}_n$ il calcolo dell'effetto di un automorfismo interno si riduce al calcolo dell'automorfismo su un generico ciclo.

Proposizione 2.2.4. *Sia $x = (x_1\ x_2\ \dots x_l)$ un ciclo in $\mathfrak{S}_n$ e sia $f \in \mathfrak{S}_n$ una permutazione qualunque. Allora*

$$fxf^{-1} = (f(x_1)\ f(x_2)\ \dots f(x_l)).$$

Dimostrazione. Posto $y = (f(x_1)\ f(x_2)\ \dots f(x_l))$ bisogna controllare che y e fxf^{-1} hanno lo stesso effetto su ciascun $t \in \{1, \dots, n\}$. Se $t = f(x_i)$ per qualche $i = 1, \dots, l$, allora $fxf^{-1}(t) = fx(x_i) = f(x_{i+1}) = y(t)$.

Se, invece, $t \neq f(x_i)$ per ogni $i = 1, \dots, l$, allora $fxf^{-1}(t) = ff^{-1}(t) = t$ e $y(t) = t$. ■

In particolare, coniugando i cicli non si cambia la loro lunghezza. Viceversa, cicli che hanno la stessa lunghezza sono coniugati: se $x = (x_1\ x_2\ \dots x_l)$ e $y = (y_1\ y_2\ \dots y_l)$ sono due cicli di lunghezza l una qualunque permutazione $f \in \mathfrak{S}_n$ tale che $f(x_i) = y_i$ per ogni $i = 1, \dots, n$ soddisfa la relazione $y = fxf^{-1}$, come si verifica facilmente.

Diciamo che due permutazioni $x, y \in \mathfrak{S}_n$ hanno la stessa struttura ciclica se si decompongono nello stesso numero di cicli disgiunti di pari lunghezza. Siccome i cicli della decomposizione di x e di y sono disgiunti, la permutazione f sopra può essere costruita in modo da coniugare ciascun ciclo di x in un ciclo di y di medesima lunghezza. Pertanto risulta $y = fxf^{-1}$.

Assegnare una particolare struttura ciclica in $\mathfrak{S}_n$ vuol dire assegnare numeri interi positivi $l_1 \leq l_2 \leq \dots \leq l_k$ tali che

$$n = l_1 + l_2 + \dots + l_k. \tag{2.4}$$

Una tale scrittura è detta *partizione di n*. Viceversa assegnata una partizione di n come in (2.4) è possibile trovare una permutazione $f \in \mathfrak{S}_n$ con corrispondente struttura ciclica, ad esempio

$$f = (1\ \dots\ l_1)(l_1 + 1\ \dots\ l_1 + l_2) \cdots (n - l_k + 1\ \cdots\ n).$$

Possiamo riassumere la discussione sin qui condotta nel seguente enunciato.

Teorema 2.2.5. *Nel gruppo $\mathfrak{S}_n$ due permutazioni sono coniugate se e soltanto se hanno la stessa struttura ciclica. Inoltre, le classi di coniugio sono in numero uguale a quello delle partizioni di n.*

La determinazione del numero $p(n)$ delle partizioni di n, per cui non esitono formule esatte, è un problema difficile su cui esiste una vasta letteratura. In queste note ricordiamo solo (senza dimostrazione) due risultati classici. Nel primo si ottiene una forma chiusa per la funzione generatrice della successione $p(n)$.

Teorema 2.2.6 (Eulero)**.** *C'è un identità*

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1 - q^n}.$$

Il secondo risultato fornisce l'andamento asintotico per la successione $p(n)$ per $n \to \infty$.

Teorema 2.2.7 (Hardy-Ramanujan, 1917)**.** *Per $n \to \infty$ si ha*

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

PROBLEMI

2.1. Siano $f : G \to H$ e $g : H \to K$ due omomorfismi. Mostrare che la composizione $g \circ f : G \to K$ è un omomorfismo e, in particolare, che se f e g sono isomorfismi anche $g \circ f$ lo è.

2.2. Sia $f : G \to H$ un omomorfismo e $K < H$. Mostrare che $f^{-1}(K) < G$.

2.3. Siano G e H due gruppi e supponiamo $G \simeq H$. Dimostrare che $\mathrm{Aut}(G) \simeq \mathrm{Aut}(H)$.

2.4. Verificare che la relazione di coniugio fra gli elementi di un gruppo G è un'equivalenza.

2.5. Mostrare che per ogni $h \in G$ si ha $\mathrm{ord}(h) = \mathrm{ord}(ghg^{-1})$.

2.6. Mostrare che se $H < G$, allora $gHg^{-1} < G$ per ogni $g \in G$.

Lezione 3

Gruppi quozienti

3.1 Classi laterali

Sia G un gruppo ed H un suo sottogruppo. Consideriamo la relazione

$$x \varrho y \quad \Longleftrightarrow \quad xy^{-1} \in H.$$

Si verifica facilmente che la relazione ϱ è una relazione di equivalenza. Infatti:

- $xx^{-1} = 1 \in H$ qualunque sia x (riflessività);
- se $x \varrho y$, allora $xy^{-1} \in H$ e $(xy^{-1})^{-1} = yx^{-1} \in H$, cioè $y \varrho x$ (simmetria);
- se $x \varrho y$ e $y \varrho x$, allora $(xy^{-1})(yz^{-1}) = xz^{-1} \in H$ come prodotto di elementi in H, cioè $x \varrho z$ (transitività).

In modo del tutto analogo si dimostra che la relazione

$$x \sigma y \quad \Longleftrightarrow \quad x^{-1}y \in H$$

è un'equivalenza. Le due relazioni ϱ e σ coincidono se il gruppo G è abeliano, ma non coincidono in generale: se $G = \mathfrak{S}_3$ e $H =< (1\ 2) >$, posto $x = (1\ 2\ 3)$ e $y = (2\ 3)$ si ha $xy^{-1} = (1\ 2) \in H$ e $x^{-1}y = (1\ 3) \notin H$. La classe di equivalenza di un elemento $x \in G$ secondo la ϱ è costituita dagli elementi y tali che $xy^{-1} \in H$, cioè dagli elementi $y \in G$ scrivibili nella forma hx con $h \in H$. Pertanto essa è l'insieme

$$Hx := \{hx \in G \text{ tale che } h \in H\},$$

detto il *laterale destro* di H definito da x. Analogamente, la classe di equivalenza di $x \in G$ secondo la σ è il *laterale sinistro* di H definito da x, cioè l'insieme

$$xH := \{xh \in G \text{ tale che } h \in H\}.$$

Proposizione 3.1.1. *I laterali destri (oppure sinistri) di un sottogruppo $H < G$ costituiscono una partizione di G. Inoltre, ciascuno di essi è in biezione con H.*

Dimostrazione. Che i laterali formino una partizione è immediato dal fatto che sono delle classi di equivalenza. Inoltre, per ogni $x \in G$ la funzione che ad $h \in H$ associa l'elemento hx è una biezione $H \xrightarrow{\sim} Hx$ in quanto è ovviamente suriettiva e dall'uguaglianza $h_1x = h_2x$ segue $h_1 = h_2$ per la proprietà di cancellazione. ■

Siccome ϱ e σ sono equivalenze, possiamo considerare gli insiemi quozienti G/ϱ e G/σ.

Proposizione 3.1.2. *C'è una biezione $G/\varrho \leftrightarrow G/\sigma$.*

Dimostrazione. Consideriamo la funzione che associa al laterale destro Hx il laterale sinistro $x^{-1}H$. Si ha

$$Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow y^{-1} \in x^{-1}H \Leftrightarrow x^{-1}H = y^{-1}H$$

e dunque l'associazione è biettiva. ■

Definizione 3.1.3. *Sia $H < G$, Chiamiamo indice di H in G la cardinalità dell'insieme quoziente G/ϱ. In simboli,*

$$[G : H] := |G/\varrho| = |G/\sigma|\,.$$

Si noti che si può senz'altro avere $[G : H] = \infty$, ad esempio nel caso $G = \mathbb{Z}$ e $H = \{0\}$, ma anche $|G| = \infty$ e $[G : H]$ finito, come nel caso $G = \mathbb{Z}$ e $H = n\mathbb{Z}$ $(n \neq 0)$ dove $[G : H] = n$.

Teorema 3.1.4 (Lagrange)**.** *Sia G un gruppo finito e $H < G$. Allora $|H|$ divide $|G|$ e*

$$[G : H] = \frac{|G|}{|H|}.$$

Dimostrazione. Dalla partizione in laterali $G = \bigcup Hx$ si ottiene $|G| = \sum |Hx|$. Siccome $|H| = |Hx|$ per ogni x e siccome il numero degli addendi è $[G : H]$, la formula enunciata si ottiene subito. ■

Corollario 3.1.5. *Sia G un gruppo finito.*

1. *Per ogni $g \in G$, $\mathrm{ord}(g)$ divide $|G|$. In particolare $g^{|G|} = 1$.*
2. *Se $|G| = p$ è primo, allora G è ciclico e $G \simeq \mathbb{Z}/\mathbb{Z}p$.*

Dimostrazione. Il primo punto segue subito dal teorema di Lagrange applicato al sottogruppo $H = \langle g \rangle$.

Per il secondo punto, si scelga $g \neq 1$. Per il primo punto deve essere $\mathrm{ord}(g) = p$ e dunque $G = \langle g \rangle$. Allora c'è un isomorfismo

$$G \xrightarrow{\sim} \mathbb{Z}/\mathbb{Z}p, \qquad g^n \mapsto \bar{n} = n\bar{1}.$$

■

La teoria fin qui svolta ci permette di dimostrare molto rapidamente il seguente risultato celebre.

Teorema 3.1.6 (Eulero)**.** *Sia $n > 1$ un intero e sia a tale che* $\mathrm{MCD}(a, n) = 1$. *Allora*

$$a^{\phi(n)} \equiv 1 \bmod n$$

Dimostrazione. La condizione su a, n equivale a dire che $\bar{a}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$. Siccome $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ la congruenza enunciata è una conseguenza immediata del punto 1 del Corollario precedente. ■

3.2 Sottogruppi normali

Abbiamo visto sopra con un esempio concreto come, in generale, $Hg \neq gH$ per un sottogruppo $H < G$ ed un elemento $g \in G$. Chiedere che risulti $gH = Hg$ equivale evidentemente a chiedere che $H = gHg^{-1}$. Possiamo riprafasare questa equivalenza nel modo seguente.

Osservazione 3.2.1. Sia $H < G$ e $g \in G$. C'è una coincidenza di laterali destri e sinistri $Hg = gH$ se e soltanto se $\phi_g(H) = H$ dove ϕ_g è l'automorfismo interno definito da g.

Definizione 3.2.2. *Un sottogruppo $H < G$ si dice normale se soddisfa le seguenti condizioni fra loro equivalenti:*

- *i laterali destri di H coincidono con i laterali sinistri;*
- *H è trasformato in sè da ogni automorfismo interno.*

Esempi 3.2.3. 1. I sottogruppi banali sono normali.

2. Se G è abeliano, ogni sottogruppo di G è normale.
3. Il centro $Z(G)$ è sempre normale in G. Infatti se $z \in Z(G)$ e $g \in G$ si ha $gzg^{-1} = g^{-1}gz = z$.
4. Se $f : G \to G'$ è un omomorfismo, il nucleo $\ker(f)$ è normale in G. Infatti, per ogni $k \in \ker(f)$ e per ogni $g \in G$ si ha $f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g)f(g)^{-1} = 1$, cioè $gkg^{-1} \in \ker(f)$.

   Ad esempio il gruppo lineare speciale SL_n è normale nel gruppo lineare GL_n in quanto è il nucleo del determinante.
5. Se $[G : H] = 2$ le partizioni di G nei laterali destri e sinistri devono essere $G = H \cup Hg$ e $G = H \cup gH$ dove $g \notin H$. Pertanto si ha $Hg = gH$ e H risulta normale.

   Come caso speciale di questa situazione il gruppo alterno A_n è un sottogruppo normale di $\mathfrak{S}_n$.
6. Il sottogruppo $\mathrm{Int}(G)$ degli automorfismi interni di un gruppo G è un sottogruppo normale del gruppo $\mathrm{Aut}(G)$. Infatti se $g \in G$ e $f \in \mathrm{Aut}(G)$ si ha

   $$f\phi_g f^{-1}(x) = f(gf(x)g^{-1}) = f(g)xf(g)^{-1} \qquad \text{per ogni } x \in G$$

   e dunque $f\phi_g f^{-1} = \phi_{f(g)} \in \mathrm{Int}(G)$.

Una conseguenza immediata della definizione è che un sottogruppo è normale se e soltanto se è unione di classi di coniugio. Usiamo questo fatto per determinare i sottogruppi normali di $\mathfrak{S}_n$ per $n = 3$ e 4. Sappiamo che le classi di coniugio in $\mathfrak{S}_n$ corrispondono alle partizioni di n ed assegnata una partizione π indichiamo con C_π la classe di coniugio corrispondente e $c_\pi = |C_\pi|$. Si determinano le tabelle seguenti (vedi problema 3.4): per $\mathfrak{S}_3$ si ha

$$c_{1+1+1} = 1, \qquad c_{1+2} = 3, \qquad c_3 = 2 \tag{3.1}$$

e per $\mathfrak{S}_4$ si ha

$$c_{1+1+1+1} = 1, \qquad c_{1+1+2} = 6, \qquad c_{1+3} = 8, \qquad c_{2+2} = 3, \qquad c_4 = 6. \tag{3.2}$$

La compatibilità col Teorema di Lagrange restringe i possibili sottogruppi normali di $\mathfrak{S}_3$ a

$$H = C_{1+1+1} \cup C_3,$$

che è effettivamente un sottogruppo, e i possibili sottogruppi normali di $\mathfrak{S}_4$ a

$$H_1 = C_{1+1+1+1} \cup C_{2+2}, \qquad H_2 = C_{1+1+1+1} \cup C_{1+3} \cup C_{2+2}.$$

Essi sono entrambi sottogruppi: H_2 è il gruppo alterno A_4 e H_1 è un sottogruppo perchè ogni elemento di struttura ciclica $2+2$ coincide col suo inverso e il prodotto di due tali elementi distinti è ancora dello stesso tipo. Si noti che $H_1 < H_2$.

Definizione 3.2.4. *Un gruppo G si dice semplice se gli unici sottogruppi normali di G sono i sottogruppi abeliani.*

Proposizione 3.2.5. *I soli gruppi abeliani semplici sono i gruppi ciclici di ordine primo.*

Dimostrazione. Un gruppo ciclico di ordine primo non possiede sottogruppi non banali e quindi è semplice.

Se G è abeliano con n elementi ed n non è primo, basta controllare che G possiede un sottogruppo non banale. Si scelga una decomposizione $n = rs$ in fattori $1 < r, s < n$ e sia $g \in G$, $g \neq 1$. Se $\mathrm{ord}(g) < n$, $\langle g \rangle$ è un sottogruppo proprio non banale. Se, invece $G = \langle g \rangle$ allora il sottogruppo ciclico $\langle g^r \rangle$ è un sottogruppo proprio non banale. ■

L'esempio successivo riveste una certa importanza.

Teorema 3.2.6. *Il gruppo alterno A_n è semplice se $n \geq 5$.*

Dimostrazione. Sia $N \neq \{1\}$ un sottogruppo normale di A_n e scegliamo un elemento $x \in N$, $x \neq 1$, tale da minimizzare il numero degli elementi j tali che $x(j) \neq j$. Supponiamo che la decomposizione di x in cicli disgiunti contenga un ciclo di lunghezza ≥ 4. A meno di coniugio possiamo scrivere

$$x = (1\ 2\ 3\ 4\ \ldots)(\ldots)\ldots(\ldots).$$

Poniamo $y = (1\ 2\ 3)x(1\ 2\ 3)^{-1} = (2\ 3\ 1\ 4\ \ldots)(\ldots)\ldots(\ldots)$. Allora $xy^{-1} \in N$ perchè N è normale. Però $y^{-1}x = (1\ 2\ 3\ 4\ \ldots)(4\ 1\ 3\ 2\ \ldots)\ldots = (2)(3\ 1\ \ldots)\ldots$ sposta meno elementi di quanti ne sposta x. Pertanto nella decomposizione di x possono comparire solo cicli di lunghezza ≤ 3.

Supponiamo che x si decomponga come un ciclo di lunghezza 3 ed altri cicli non banali. A meno di coniugio possiamo supporre che

$$x = (1\ 2\ 3)\ldots, \qquad \text{e } x(4) \neq 4.$$

Poniamo $z = (4\ 1\ 2)x(4\ 1\ 2)^{-1} = (2\ 4\ 3)(1\ \ldots)\ldots$. Allora $zx \in N$ perchè N è normale. Però $zx = (2\ 4\ 3\ \ldots)(1\ \ldots)(1\ 2\ 3\ \ldots)(4\ \ldots)\ldots = (2)(1\ 4\ \ldots)\ldots$ sposta meno elementi di quanti ne sposta x.

Se nella decomosizione di x compaiono due trasposizioni, poniamo $x = (1\ 2)(3\ 4)\ldots$ e coniugando con il 3-ciclo $(1\ 2\ 5)$, cosa possibile perchè $n \geq 5$, otteniamo $w = (1\ 2\ 5)x(1\ 2\ 5)^{-1} = (2\ 5)(3\ 4)\ldots$ e $wx = (2\ 5)(3\ 4)\ldots(1\ 2)(3\ 4)\ldots = (1\ 2)(2\ 5)\ldots$ è un elemento di N che sposta meno elementi di x.

In definitiva x è un ciclo di lunghezza ≤ 3.

Ma x non può essere una trasposizione, perchè le trasposizioni non stanno in A_n e se $x = (1\ 2\ 3)$ allora coniugando con $(1\ 2)(3\ k)$ si ha che ogni 3-ciclo della forma $(2\ 1\ k)$ con $k = 4, \ldots, n$ è in N.

Ogni elemento $g \in A_n$ si scrive come prodotto di un numero pari di trasposizioni della forma $(2\ h)$. Raggruppando tali trasposizioni a due a due si ottiene una scrittura di g come prodotto di di cicli $(2\ k)(2\ h) = (2\ h\ k)$. Inoltre $(2\ h\ k) = (2\ 1\ k)(2\ 1\ h)(2\ 1\ h)$ e quindi g ammette una scrittura come prodotto di cicli della forma $(2\ 1\ k)$ con $k = 4, \ldots, n$. Questo vuol dire che l'insieme di tali cicli genera A_n, cioè $N = A_n$. ■

Teorema 3.2.7. *Ad eccezione del caso $n = 4$, il gruppo alterno A_n è l'unico sottogruppo normale non banale di $\mathfrak{S}_n$.*

Dimostrazione. I casi $n \leq 4$ o sono ovvi o sono stati discussi precedentemente. Se $n \geq 5$ la dimostrazione procede come per il teorema precedente con l'ulteriore possibilità che l'elemento x possa una trasposizione. Ma contenendo una trasposizione un sottogruppo normale dovrà contenerle tutte e le trasposizioni generano $\mathfrak{S}_n$.■

3.3 Costruzione del gruppo quoziente

Sia N un sottogruppo normale nel gruppo G e consideriamo l'insieme dei laterali $G/\varrho = G/\sigma$ che per comodità penseremo come laterali destri. Osserviamo che vale un'identità

$$NxNy = \{nxn'y \in G \,|\, n, n' \in N\} = Nxy.$$

di sottoinsiemi di G. Infatti, se $n \in N$ risulta $nxy = (nx)(1y) \in NxNy$, e se $n' \in N$ esiste (vedi Problema 3.4) $m \in N$ tale che $xn' = mx$ e quindi $nxn'y = nmxy \in Nxy$. Definiamo allora un'operazione in G/ϱ ponendo

$$(Nx) \cdot (Ny) = Nxy. \tag{3.3}$$

Osservazione 3.3.1. *Nel caso in cui N non è normale, la* (3.3) *non è ben definita (vedi Problema 3.4) e quindi non definisce un'operazione nell'insieme quoziente.*

Verifichiamo ora che l'insieme quoziente con l'operazione (3.3) soddisfa gli assiomi di gruppo della Definizione 1.1.1. Infatti l'operazione

- è associativa, in quanto $(Nx) \cdot ((Ny) \cdot (Nz)) = (Nx) \cdot (Nyz) = Nx(yz) = N(xy)z = (Nxy) \cdot (Nz) = ((Nx) \cdot (Ny)) \cdot (Nz)$ per ogni $x, y, z \in G$.
- possiede un elemento neutro $N = N1$, in quanto $(N) \cdot (Nx) = (Nx) \cdot N = Nx$ per ogni $x \in G$
- possiede l'elemento inverso di ogni elemento Nx, in quanto $(Nx)(Nx^{-1}) = Nxx^{-1} = N$.

Definizione 3.3.2. *L'insieme dei laterali di un sottogruppo normale N di G con l'operazione* (3.3) *si chiama gruppo quoziente di G rispetto ad N e si denota G/N.*

Si noti come tale definizione generalizza in modo diretto la costruzione elementare delle classi resto $\mathbb{Z}/N\mathbb{Z}$ modulo un numero intero N. Diremo che G/N è un quoziente non banale di G se N non è un sottogruppo banale.

Si osservi che se G è abeliano, ogni suo quoziente è abeliano. D'altra parte, un gruppo non abeliano può possedere quozienti abeliani non banali, ad esempio il quoziente $\mathfrak{S}_3/\langle(1\ 2\ 3)\rangle$ ha 2 elementi e pertanto è abeliano a fortiori.

L'associazione

$$\pi \colon G \longrightarrow G/N, \qquad \pi(g) = Ng$$

è, in conseguenza diretta della definizione (3.3) un omomorfismo suriettivo (detto *omomorfismo quoziente canonico*) il cui nucleo è evidentemente

$$\ker(\pi) = \{g \in G \,|\, \pi(g) = 1_{G/N}\} = \{g \in G \,|\, Ng = N\} = N.$$

Ricordando l'esempio 3.2.3(4), otteniamo la caratterizzazione dei sottogruppi normali di un gruppo G come i nuclei degli omomorfismi con dominio G.

Nota Bene. Per semplificare la notazione, nel seguito indicheremo talvolta G/H l'insieme dei laterali sinistri di H in G anche quando H non è necessariamente normale. Analogamente denoteremo $H\backslash G$ l'insieme dei laterali destri.

3.4 I teoremi d'omomorfismo

La costruzione del gruppo quoziente G/H ha lo svantaggio di essere astratta: anche in casi concreti, lo studio del quoziente G/H non è sempre agevole. Torna utile, a volte, identificare il quoziente con un gruppo più concreto. I teoremi di isomorfismo offrono uno strumento tecnico per la realizzazione di questo obiettivo.

Teorema 3.4.1 (Primo Teorema d'Isomorfismo)**.** *Sia $f : G \to H$ un omomorfismo di gruppi. Allora $G/\ker(f) \simeq \mathrm{im}(f)$.*

Dimostrazione. Consideriamo la funzione $\bar{f} : G/\ker(f) \to \mathrm{im}(f)$ tale che $\bar{f}(\bar{x}) = f(x)$ dove, per brevità, abbiamo posto $\bar{x} = \ker(f)x$. La funzione $\bar{f}$ è ben definita perchè se $\bar{x} = \bar{y}$ allora esiste $g \in \ker(f)$ tale che $y = gx$ e allora $f(y) = f(gx) = f(g)f(x) = f(x)$.

Osserviamo che $\bar{f}$ è un omomorfismo in quanto $\bar{f}(\bar{x}\bar{y}) = f(xy) = f(x)f(y) = \bar{f}(\bar{x})\bar{f}(\bar{y})$ ed è iniettivo perchè se $\bar{f}(\bar{x}) = f(x) = 1$ allora $x \in \ker(f)$, ovvero $\bar{x} = 1$, cioè $\ker(\bar{f}) = \{1\}$. Siccome $\bar{f}$ è ovviamente suriettivo, $\bar{f}$ realizza l'isomorfismo dell'enunciato. ■

Il Primo Teorema d'Isomorfismo viene talvolta rappresentato per mezzo del diagramma commutativo

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow \\ G/\ker(f) & \xrightarrow{\bar{f}} & \mathrm{im}(f) \end{array}$$

dove π è l'omomorfismo quoziente canonico e la mappa verticale destra l'inclusione.

Esempi 3.4.2.

1. La mappa esponenziale $E : \mathbb{R} \to \mathbb{C}^\times$, $E(t) = e^{2\pi it}$ dell'esempio 2.1.3(3) ha nucleo $\mathbb{Z}$ (vedi esempio 2.1.5(3) e immagine il sottogruppo S^1 dei numeri complessi di norma 1. Pertanto dal Teorema 3.4.1 risulta un isomorfismo
$$\mathbb{R}/\mathbb{Z} \simeq S^1.$$

2. Ogni numero complesso non nullo z si può scrivere in modo unico non ambiguo nella forma $z = re^{2\pi it}$ con $r \in \mathbb{R}^\times$. La mappa
$$f\colon \mathbb{C}^\times \longrightarrow \mathbb{R}^\times, \qquad f(z) = r$$
ha $\ker(f) = S^1$ e $\mathrm{im}(f) = \mathbb{R}^{>0}$. Pertanto si ha un isomorfismo
$$\mathbb{C}^\times/S^1 \simeq \mathbb{R}^{>0}.$$

3. L'applicazione $z \mapsto z^2$ definisce un omomorfismo $S^1 \to S^1$. Esso è suriettivo (di ogni numero complesso si può estrarre una radice quadrata) e ha come nucleo il sottogruppo $\{\pm 1\}$. Dunque si ha un isomorfismo
$$S^1/\{\pm 1\} \simeq S^1.$$
Tale esempio mostra come un gruppo infinito possa essere isomorfo ad un suo quoziente non banale.

4. La mappa
$$\Phi : G \longrightarrow \mathrm{Aut}(G), \qquad \Phi(g) = \phi_{g^{-1}}$$

che associa ad un elemento g l'automorfismo interno $x \mapsto gxg^{-1}$ è un omomorfismo in quanto $\Phi(gh)(x) = \phi_{gh}(x) = ghxh^{-1}g^{-1} = \phi_g(\phi_h(x)) = (\Phi(g) \circ \Phi(h))(x)$ per ogni $x \in G$. L'omomorfismo Φ ha nucleo $\ker(\Phi) = \{g \in G \,|\, gxg^{-1} = x \text{ per ogni } x \in G\} = Z(G)$ e quindi

$$G/Z(G) \simeq \mathrm{im}(\Phi) = \mathrm{Int}(G).$$

Siano H e K sottogruppi di G e poniamo

$$HK = \{g \in G \,|\, g = hk \text{ per opportuni } h \in H \text{ e } k \in K\}.$$

In generale $HK \neq KH$ e nessuno dei due è un sottogruppo di G. Se però K è normale, si ha $HK = \cup_{h\in H} hK = \cup_{h\in H} Kh = KH$ e HK risulta essere un sottogruppo di G (vedi Problema 3.4) e precisamente il sottogruppo generato da $H \cup K$.

Possiamo ora enunciare gli altri due teoremi d'isomorfismo.

Teorema 3.4.3 (Secondo Teorema d'Isomorfismo)**.** *Siano H e K sottogruppi di un gruppo G e supponiamo H normale nel sottogruppo generato da $H \cup K$. Allora*

1. *$H \cap K$ è normale in K, e*
2. *$\langle H \cup K\rangle / H \xrightarrow{\sim} K/(H \cap K)$.*

Dimostrazione. Siccome H è normale in $\langle H \cup K\rangle$ risulta, come nella discussione precedente, $\langle H \cup K\rangle = HK = KH$. Consideriamo l'omomorfismo quoziente canonico composto con l'inclusione di K in HK,

$$K \longrightarrow HK \xrightarrow{\pi} HK/H.$$

Tale composizione è evidentemente suriettiva in quanto gli elementi del quoziente HK/H sono i laterali Hk con $k \in K$. Il nucleo della composizione è costituito dagli elementi $k \in K$ tali che $Hk = H$ come laterali in HK e questo succede esattamente quando $k \in H \cap K$. Ciò dimostra il punto 1 in quanto $H \cap K$ si è dimostrato essere nucleo di un certo omomorfismo, ed anche il punto 2 come diretta applicazione del Teorema 3.4.1. ■

Teorema 3.4.4 (Terzo Teorema d'Isomorfismo)**.** *Siano $K < H$ sottogruppi normali di un gruppo G. Allora*

1. *H/K è normale in G/K, e*
2. *$\frac{G/K}{H/K} \simeq G/H$.*

Dimostrazione. Definiamo una funzione $f : G/K \to G/H$ ponendo $f(Kg) = Hg$ per ogni $g \in G$. La funzione f è ben definita perchè se $Kg = Kg'$ allora esiste $k \in K \subset H$ tale che $kg = g'$ e dunque $Hg = Hg'$. La funzione f è evidentemente suriettiva ed è un omomorfismo, perchè $f(Kx \cdot Ky) = f(Kxy) = Hxy = Hx \cdot Hy = f(Kx)f(Ky)$.

Il nucleo di f è costituito dai laterali Kg tali che $Hg = H$ e questo si ha se e soltanto se $g \in H$. Pertanto $\ker(f) = H/K$ e questo prova il punto 1 immediatamente, ed il punto 2 come applicazione del Teorema 3.4.1. ■

Esempi 3.4.5. 1. Consideriamo i sottogruppi S^1 e $\mathbb{R}^\times$ di $\mathbb{C}^\times$. Essi sono entrambi normali e $S^1\mathbb{R}^\times = \mathbb{C}^\times$ cosicchè il Secondo Teorema di Isomorfismo fornisce isomorfismi

$$\frac{\mathbb{C}^\times}{\mathbb{R}^\times} \simeq \frac{S^1}{\{\pm 1\}} \simeq S^1.$$

e

$$\frac{\mathbb{C}^\times}{\mathbb{R}^\times} \simeq \frac{\mathbb{R}^\times}{\{\pm 1\}} \simeq \mathbb{R}^{>0}.$$

L'ultimo isomorfismo si ottiene applicando il Primo Teorema d'Isomorfismo all'omomorfismo $|\cdot| : \mathbb{R}^\times \to \mathbb{R}^{>0}$.

2. Se d è un divisore di N, c'è un inclusione $N\mathbb{Z} \leq d\mathbb{Z}$ di sottogruppi di $\mathbb{Z}$. Allora per il Terzo Teorema d'Isomorfismo
$$\frac{\mathbb{Z}/N\mathbb{Z}}{d\mathbb{Z}/N\mathbb{Z}} \simeq \mathbb{Z}/d\mathbb{Z}.$$

Concludiamo questa sezione mostrando come la struttura dei sottogruppi di un gruppo quoziente G/N sia ottenibile da quella di G. Precisamente, vale il risultato seguente.

Teorema 3.4.6. *Sia N un sottogruppo normale in G. L'omomorfismo quoziente canonico π definisce una corrispondenza biunivoca*

$$\{ \begin{smallmatrix} \textit{sottogruppi di } G \\ \textit{contenenti } N \end{smallmatrix} \} \longleftrightarrow \{\textit{sottogruppi di } G/N\}$$

che conserva indici e normalità.

Dimostrazione. Al sottogruppo $N < H < G$ associamo il sottogruppo $\pi(H) = H/N$ di G/N. È chiaro che tale associazione è iniettiva: se $\pi(H) = H/N = K/N = \pi(K)$ si ottiene $H = K$ dall'unione dei vari laterali. Viceversa, se $H < G/N$ allora $\pi^{-1}(H)$ è un sottogruppo di G che contiene $N = \pi^{-1}(1)$.

Se $N < K$ è un sottogruppo normale di G, allora $Kg = gK$ per ogni $g \in G$ e quindi $\pi(K)\pi(g) = \pi(g)\pi(K)$. Siccome π è suriettiva, questo mostra che tutti i laterali destri di $\pi(K)$ coincidono con i sinistri e quindi $\pi(K)$ è normale.

Se $K < G/N$ è normale, scrivendo $K = H/N = \pi(H)$ con $N < H < G$ si vede che H è il nucleo della composizione $G \to G/N \to \frac{G/N}{K}$. Pertanto $H = \pi^{-1}(K)$ è normale in G.

Infine per qualunque sottogruppo $N < H < G$, l'associazione $Hh \mapsto (H/N)Nh$ tra i laterali di H in G e quelli di H/N in G/N è evidentemenete suriettiva, ed è anche iniettiva perchè se $g, g' \in G$ sono tali che $(H/N)\pi(g) = (H/N)\pi(g')$ allora esistono $n, n' \in N$ e $h \in H$ tali che $g = nhn'g'$ e siccome $N < H$ questo mostra che $Hg = Hg'$. Resta dunque provata l'uguaglianza $[G : H] = [G/N : \pi(H)]$. ∎

PROBLEMI

3.1. Spiegare perchè l'associazione $Hx \mapsto xH$ non definisce, in generale, una biezione tra laterali destri e sinistri di un sottogruppo $H < G$.

3.2. Sia $H =< (1\ 2\ 3\ 4) >$ in $\mathfrak{S}_4$. Calcolare $[\mathfrak{S}_4 : H]$ e determinare un sistema completo di rappresentanti per i laterali destri e per i laterali sinistri.

3.3. Sia $N < G$. Si dimostri che N è normale se e soltanto se vale la condizione seguente: per ogni $g \in G$ e per ogni $n \in N$ esiste un $n' \in N$ tale che $ng = gn'$.

3.4. Sia $K < H < G$ una catena di sottogruppi in G. Si dimostri che se K è normale in G allora K è normale in H. Mostrare invece con un controesempio che se H è normale in G allora non necessariamente K è normale in G.

3.5. Ricostruire le tabelle (3.1) e (3.2).

3.6. Trovare un esempio esplicito di sottogruppo non normale $H < G$ ed elementi $x, x', y, y' \in G$ tali che $Hx = Hx'$, $Hy = Hy'$ ma $Hxy \neq Hx'y'$.

3.7. Si spieghi perchè un gruppo finito G non può avere quozienti non banali isomorfi a G stesso.

3.8. Generalizzare l'esempio 3.4.2(3) ottenendo un isomorfismo $S^1/\mu_n \simeq S^1$ per ogni $n \geq 1$.

3.9. Dimostrare che se H e K sono sottogruppi di G tali che $HK = KH$, allora HK è un sottogruppo di G e difatti $HK = \langle H \cup K \rangle$.

Lezione 4

Altre costruzioni

In questa lezione studieremo due altre tecniche, in aggiunta alla costruzione dei ruppi quozienti, che permettono di ottenere nuovi gruppi a partire da altri già disponibili.

4.1 Prodotti

Siano G_1 e G_2 due gruppi. Consideriamo l'insieme prodotto cartesiano

$$G = G_1 \times G_2 = \{(g_1, g_2) \,|\, g_1 \in G_1, g_2 \in G_2\}$$

e su esso definiamo l'operazione di *prodotto componente per componente*

$$(g_1, g_2)(g'_1, g'_2) = (g_1 g'_1, g_2 g'_2). \tag{4.1}$$

È facile vedere che l'operazione 4.1 definisce su G una struttura di gruppo. Infatti:

- l'associatività dell'operazione 4.1 segue immediatamente dall'associatività in ciascuna componente;
- se u_i è l'elemento neutro in G_i $(i = 1, 2)$ l'elemento (u_1, u_2) è neutro in G;
- l'elemento $(g_1, g_2) \in G$ ha inverso (g_1^{-1}, g_2^{-1}).

Definizione 4.1.1. *Il gruppo $G = G_1 \times G_2$ è detto prodotto diretto (esterno) dei gruppi G_1 e G_2.*

Esempi 4.1.2. 1. Siano m, n due interi tali che $\mathrm{MCD}(m, n) = 1$. Allora

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}.$$

Infatti, $d = \mathrm{ord}(\bar{1}, \bar{1})$ è il più piccolo intero positivo per cui $d(\bar{1}, \bar{1}) = (\bar{d}, \bar{d}) = (\bar{0}, \bar{0})$, e quindi $d = \mathrm{mcm}(m, n) = \frac{mn}{\mathrm{MCD}(m,n)} = mn$. Dunque $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è ciclico.

2. Il gruppo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ consiste dei 4 elementi

$$u = (\bar{0}, \bar{0}), e_1 = (\bar{1}, \bar{0}), e_2 = (\bar{0}, \bar{1}), e_3 = (\bar{1}, \bar{1})$$

che soddisfano le relazioni

$$e_1^2 = e_2^2 = e_3^2 = u, \qquad e_i e_j = e_k$$

ogniqualvolta $\{i, j, k\} = \{1, 2, 3\}$. In particolare G non è ciclico.

Sul gruppo prodotto $G = G_1 \times G_2$ sono definiti due omomomorfismi suriettivi

$$\mathrm{pr}_i : G \longrightarrow G_i, \quad \mathrm{pr}_i(g_1, g_2) = g_i \qquad i = 1, 2$$

detti, rispettivamente, la prima e la seconda proiezione. Il risultato seguente mostra come i gruppi G_1 e G_2 possano essere ricostruiti a partire dal prodotto.

Proposizione 4.1.3. *Sia $G = G_1 \times G_2$ il prodotto dei gruppi G_1 e G_2. Allora esistono sottogruppi H_i in G, $i = 1, 2$, tali che*

1. *$H_i \simeq G_i$,*
2. *H_i è normale in G,*
3. *$G = H_1 H_2$,*
4. *$H_1 \cap H_2 = \{1_G\}$.*

Dimostrazione. Poniamo $H_1 = \{(g_1, 1)\} = \ker(\mathrm{pr}_2)$ e $H_2 = \{(1, g_2)\} = \ker(\mathrm{pr}_1)$. I punti 1, 2 e 4 sono evidenti. Per il punto 3 basta osservare che $(g_1, g_2) = (g_1, 1)(1, g_2)$. ■

Definizione 4.1.4. *Se G è un gruppo che possiede due sottogruppi H_1 e H_2 che soddisfano le proprietà 1–4 della Proposizione 4.1.3 diciamo che G è prodotto diretto (interno) di H_1 e H_2.*

Il nostro obiettivo è ora di mostrare che non c'è sostanziale differenza tra prodotto diretto esterno ed interno. È necessario dimostrare due Lemmi preliminari.

Lemma 4.1.5. *Siano H e K due sottogruppi normali in un gruppo G tali che $H \cap K = \{1_G\}$. Allora $hk = kh$ per ogni $h \in H$, $k \in K$.*

Dimostrazione. Consideriamo l'elemento $x = hkh^{-1}k^{-1} \in G$. Associando $(hkh^{-1})k^{-1}$, per normalità di K si ha $x \in K$ ed Associando $h(kh^{-1}k^{-1})$, per normalità di H si ha $x \in H$. In definitiva $x = 1$, cioè $hk = kh$. ■

Lemma 4.1.6. *Siano H e K due sottogruppi normali in un gruppo G tali che $G = HK$ e $H \cap K = \{1_G\}$. Allora ogni $g \in G$ ammette un'unica scrittura $g = hk$ con $h \in H$ e $k \in K$.*

Dimostrazione. Una scrittura $g = hk$ esiste per ipotesi. Posto $g = hk = h'k'$, si ha $kk'^{-1} = h^{-1}h' \in H \cap K$, da cui $h = h'$ e $k = k'$. ■

Possiamo ora dimostrare quanto promesso in precedenza.

Teorema 4.1.7. *Sia G un gruppo prodotto diretto interno di due suoi sottogruppi G_1 e G_2. Allora $G \simeq G_1 \times G_2$.*

Dimostrazione. Consideriamo la funzione

$$G_1 \times G_2 \longrightarrow G, \qquad (g_1, g_2) \mapsto g_1 g_2.$$

Essa è un omomorfismo per il Lemma 4.1.5 e per il Lemma 4.1.6 è iniettivo. ■

Esempi 4.1.8. 1. $\mathbb{Z}$ non è isomorfo al prodotto di due suoi sottogruppi perchè due sottogruppi non banali di $\mathbb{Z}$ hanno intersezione non banale.

2. $\mathfrak{S}_n$ non è isomorfo al prodotto di due suoi sottogruppi perchè possiede, se $n \neq 4$, un solo sottogruppo normale e due soli sottogruppi normali ad intersezione non banale se $n = 4$.

3. Se m ed n sono interi con $\mathrm{MCD}(m, n) = 1$ allora

$$\mathbb{Z}/mn\mathbb{Z} \simeq m\mathbb{Z}/mn\mathbb{Z} \times n\mathbb{Z}/mn\mathbb{Z}$$

(vedi Esempio 4.1.2(1)).

Finora ci siamo limitati. per semplicità al caso del prodotto di due gruppi. In realtà il prodotto diretto può essere definito per una famiglia arbitraria $\{G_i\}_{i\in\mathcal{I}}$ di gruppi. Se la famiglia $\mathcal{I}$ è finita, la generalizzazione è immediata: assegnati gruppi $G_1, G_2, \ldots, G_n$ il loro prodotto diretto è l'insieme $G = \prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$ con operazione

$$(g_1, g_2, \ldots, g_n)(g'_1, g'_2, \ldots, g'_n) = (g_1 g'_1, g_2 g'_2, \ldots, g_n g'_n).$$

Tutti i risultati enunciati e dimostrati sopra per il caso del prodotto di 2 gruppi continuano a valere in questa situazione più generale.

Se la famiglia $\mathcal{I}$ ù infinita la definizione corretta è la seguente.

Definizione 4.1.9. *Sia $\{G_i\}_{i\in\mathcal{I}}$ una famiglia arbitraria di gruppi. Si dice prodotto diretto della famiglia il gruppo*

$$\mathcal{G} = \prod_{i\in\mathcal{I}} G_i = \left\{\textit{funzioni } f : \mathcal{I} \to \textstyle\bigcup_{i\in\mathcal{I}} G_i \textit{ tali che } f(i) \in G_i \textit{ per ogni } i \in \mathcal{I}\right\}$$

con l'operazione

$$(f \cdot f')(i) = f(i)f'(i). \tag{4.2}$$

È facile controllare che l'operazione 4.2 definisce effettivamente un gruppo e che:

1. le proiezioni $\mathrm{pr}_i : \mathcal{G} \to G_i$ sono omomorfismi suriettivi,

2. il sottogruppo H_i di $\mathcal{G}$ costituito dalle $f \in \mathcal{G}$ tali che $f(j) = 1$ per ogni $j \neq i$ è normale ed isomorfo a G_i,

3. i vari sottogruppi H_i commutano fra di loro elemento per elemento.

È però falso che i sottogruppi H_i generano $\mathcal{G}$: se $f \in \mathcal{G}$ è tale che $f(i) \neq 1$ per un insieme infinito di indici i, non c'è modo di scrivere f come prodotto di elementi ciascuno dei quali preso in un H_i. Pertanto, un gruppo non può essere prodotto diretto di una sua famiglia di sottogruppi se tale famiglia è infinita.

Il prodotto diretto $\mathcal{G}$ possiede il seguente sottogruppo notevole.

Definizione 4.1.10. *Sia $\{G_i\}_{i\in\mathcal{I}}$ una famiglia arbitraria di gruppi. Si dice somma diretta della famiglia il gruppo*

$$G = \bigoplus_{i\in\mathcal{I}} G_i = \{f \in \mathcal{G} \textit{ tali che } f(i) = 1 \textit{ eccetto che per un numero finito di } i \in \mathcal{I}\}$$

Vale la seguente caratterizzazione.

Proposizione 4.1.11. *Sia $\{G_i\}_{i\in\mathcal{I}}$ una famiglia arbitraria di gruppi. La somma diretta G della famiglia è il sottogruppo del prodotto diretto $\mathcal{G}$ generato dai sottogruppi H_i.*

Dimostrazione. Se $f_1 \in H_{i_1}, \ldots, f_n \in H_{i_n}$ il prodotto $g = f_1 \cdots f_n$ è in G perchè $g(j) = 1$ se $j \notin \{i_1 \ldots i_n\}$.

Viceversa, se $g \in G$ e se $g(j) = 1$ per ogni $j \notin \{i_1 \ldots i_n\}$, allora $g = f_1 \cdots f_n$ dove

$$f_k(i) = \begin{cases} g(i) & \text{se } i = i_k, \\ 1 & \text{altrimenti.} \end{cases}$$

■

4.2 Limiti

Una *famiglia induttiva* (G_n, ϕ_n) di gruppi è il dato per ogni $n \in \mathbb{Z}$ di un gruppo abeliano G_n e di un omomorfismo $\phi_n : G_n \to G_{n+1}$. Una famiglia induttiva può dunque rappresentarsi come un diagramma

$$\ldots \longrightarrow G_{n-1} \xrightarrow{\phi_{n-1}} G_n \xrightarrow{\phi_n} G_{n+1} \longrightarrow \ldots.$$

Il caso significativo più semplice di famiglia induttiva è quello in cui ogni gruppo G_n è sottogruppo di un gruppo H e ogni ϕ_n è un'inclusione. In tal caso l'unione insiemistica $G = \bigcup_{n\in\mathbb{Z}} G_n$ è un sottogruppo di H in quanto se $x, y \in G$ esiste un indice $N \in \mathbb{Z}$ tale che $x, y \in G_N$ e dunque $xy^{-1} \in G_N \subset G$. Come esempio concreto si consideri il seguente.

Esempio 4.2.1. Fissato un numero primo p poniamo $G_n = \{1\}$ se $n \leq 0$ e $G_n = \mu_{p^n} < \mathbb{C}^\times$ se $n > 0$. Come ϕ_n prendiamo l'inclusione $\mu_{p^n} \hookrightarrow \mu_{p^{n+1}}$ e poniamo

$$\mu_{p^\infty} := \bigcup_{i\in\mathbb{Z}} \mu_{p^n} = \{z \in \mathbb{C} \text{ tali che } z^{p^n} = 1 \text{ per un } n \text{ opportuno}\}.$$

Si noti che μ_{p^∞} è un gruppo infinito in cui ogni elemento ha ordine finito.

Per una famiglia induttiva qualunque non ha senso procedere direttamente con un unione dei G_n perchè le mappe ϕ_n non sono necessariamente iniettive. Nel caso in cui i gruppi G_n sono abeliani procediamo come segue.

1. Sia $G = \bigoplus_{n\in\mathbb{Z}} G_n$ la somma diretta dei gruppi G_n. Per ogni n, sia $f_n : G_n \to G$ l'inclusione dell'addendo n-esimo nella somma diretta.

2. Sia H il sottogruppo di G generato da tutti gli elementi della forma

   $$f_n(g) - f_{n+1}(\phi_n(g))$$

   per ogni $n \in \mathbb{Z}$ e per ogni $g \in G_n$.

Definizione 4.2.2. *Si dice gruppo limite diretto della famiglia induttiva (G_n, ϕ_n) di gruppi abeliani, denotato*

$$\varinjlim_n (G_n, \phi_n) = \varinjlim_n (G_n),$$

il gruppo quoziente $\left(\bigoplus_{n\in\mathbb{Z}} G_n\right)/H$

Componendo le mappe f_n con l'omomorfismo quoziente $\pi : \bigoplus_{n\in\mathbb{Z}} G_n \to \varinjlim (G_n)$ si ottengono mappe $\bar{f}_n : G_n \to \varinjlim (G_n)$ che soddisfano la compatibilità

$$\bar{f}_n = \bar{f}_{n+1} \circ \phi_n$$

per ogni $n \in \mathbb{Z}$, in quanto $\bar{f}_n(g) = f_n(g)+H = f_{n+1}(\phi_n(g))+H = \bar{f}_{n+1}(\phi_n(g))$ per ogni $g \in G_n$.

Nel caso in cui i G_n non sono abeliani consideriamo l'unione disgiunta $A = \bigcup_{n\in\mathbb{Z}} G_n$ che, naturalmente, non è un gruppo. Diciamo che $h \in G_{n+k}$ è un iterato di $g \in G_n$ se $k = 0$ e $g = h$, oppure se

$$h = \phi_{n+k-1} \circ \cdots \circ \phi_n(g).$$

In A introduciamo la relazione di equivalenza

$$x \equiv y \qquad \Leftrightarrow \qquad \text{esiste } z \in A \text{ tale che } z \text{ è iterato sia di } x \text{ che di } y \tag{4.3}$$

e indicata $[x]$ la classe di equivalenza di $x \in A$ definiamo un operazione di prodotto nell'insieme quoziente ponendo

$$[x][y] = [x'y'] \tag{4.4}$$

dove $x', y' \in G_N$ sono iterati rispettivamente di x ed y per un opportuno $N \gg 0$. L'operazione è ben definita:

- se $x'', y'' \in G_{N'}$ sono altri iterati di x e y ed assumendo $N' > N$ è chiaro che x'' e y'' sono iterati di x' e y' rispettivamente cosicchè $[x'y'] = [x''y'']$;
- se $x \sim g$ e $y \sim h$ possiamo scegliere come x' e y' iterati comuni a x e g ed a y e h rispettivamente.

L'operazione appena definita soddisfa le richieste per la struttura di gruppo: l'associatività segue immediatamente dall'associatività dell'operazione nei singoli G_n e chiaramente [1] è un elemento neutro e $[x]^{-1} = [x^{-1}]$.

Definizione 4.2.3. *Si dice gruppo limite diretto della famiglia induttiva (G_n, ϕ_n), denotato*

$$\varinjlim_n (G_n, \phi_n) = \varinjlim_n (G_n),$$

il gruppo definito sull'insieme $A/\sim$ dall'operazione (4.4).

Esempi 4.2.4. 1. Sia K un campo e consideriamo la famiglia induttiva

$$\ldots \longrightarrow 1 \longrightarrow 1 \longrightarrow \mathrm{GL}_1 \xrightarrow{\phi_1} \mathrm{GL}_2(K) \xrightarrow{\phi_2} \mathrm{GL}_3(K) \longrightarrow \ldots$$

dove $\phi_n(M) = \begin{pmatrix} M & \\ & 1 \end{pmatrix}$. Allora gli iterati di una matrice M si ottengono prolungando la diagonale principale col valore 1 ripetuto e riempiendo gli altri posti con degli zeri. Questo permette di moltiplicare fra loro, nel limite

$$\mathrm{GL}_\infty(K) = \varinjlim_n \mathrm{GL}_n(K),$$

matrici di dimensioni diverse ottenendo un gruppo che le include tutte.

2. Sia H_n una arbitaria successione di gruppi, $n = 1, 2, \ldots$. Per ogni $n > 0$ poniamo $G_n = H_1 \times \cdots H_n$. Ci sono inclusioni ovvie $G_n \hookrightarrow G_{n+1}$ che fanno dei G_n una famiglia induttiva. Nel limite $\varinjlim G_n$ ogni elemento $g \in G_n$ è identificato con quelli ottenuti da $g = (g_1, \ldots, g_n)$ riempiendo con 1 le coordinate successive alla n-esima. Risulta allora chiaro che

$$\varinjlim_n H_1 \times \cdots H_n = \bigoplus_{n\geq 0} H_n$$

Una *famiglia proiettiva* (G_n, ψ_n) di gruppi è il dato per ogni $n \in \mathbb{Z}$ di un gruppo abeliano G_n e di un omomorfismo $\phi_n : G_{n+1} \to G_n$. Una famiglia induttiva può dunque rappresentarsi come un diagramma

$$\ldots \longrightarrow G_{n+1} \xrightarrow{\psi_n} G_n \xrightarrow{\psi_{n-1}} G_{n-1} \longrightarrow \ldots.$$

Si noti che, da un punto di vista grafico, una famiglia proiettiva si ottiene da una induttiva (e viceversa) semplicemente scambiando il verso delle frecce.

Sia (G_n, ψ_n) una famiglia proiettiva. Un elemento $(g_n) \in \prod_{n\in\mathbb{Z}} G_n$ si dice essere coerente per la famiglia se

$$\psi_n(g_{n+1}) = g_n \qquad \text{per ogni } n \in \mathbb{Z}.$$

L'insieme degli elementi coerenti forma un sottogruppo del prodotto $\prod_{n\in\mathbb{Z}} G_n$ in quanto se (g_n) e (h_n) sono coerenti, allora $\psi_n(g_{n+1}h_{n+1}^{-1}) = \psi_n(g_{n+1})\psi_n(h_{n+1}^{-1}) = g_n h_n^{-1}$.

Definizione 4.2.5. *Si dice limite inverso della famiglia proiettiva (G_n, ψ_n), denotato*

$$\varprojlim_n (G_n, \psi_n) = \varprojlim_n G_n,$$

il sottogruppo di $\prod_{n\in\mathbb{Z}} G_n$ degli elementi coerenti.

Si noti che per ogni $k \in \mathbb{Z}$ la k-esima proiezione $\mathrm{pr}_k : \prod_{n\in\mathbb{Z}} G_n \to G_k$ definisce, per restrizione, un omomorfismo

$$\pi_k : \varprojlim_n G_n \longrightarrow G_k.$$

Inoltre, valgono evidentemente le compatibilità

$$\pi_k = \psi_k \circ \pi_{k+1}.$$

Esempi 4.2.6.

1. Poniamo $G_n = \mathbb{Z}$ e $\psi_n(x) = 2x$ per ogni $n \in \mathbb{Z}$. Sia $(a_n) \in \varprojlim_n \mathbb{Z}$: risulta $a_n = 2^{-n}a_0 \in \mathbb{Z}$ per ogni $n \gg 0$ e questo è possibile se e solo se $a_0 = 0$, nel qual caso deve essere $a_n = 0$ per ogni $n \in \mathbb{Z}$. Quindi

   $$\varprojlim_n \mathbb{Z} = (0).$$

   In particolare, questo esempio mostra come gli omomorfismi π_k non siano necessariamente suriettivi.

2. Se nell'esempio precedente sostituiamo $\mathbb{Z}$ con $\mathbb{Q}$, allora riusciamo a costruire degli elementi coerenti non banali. Ad esempio, per ogni $q \in \mathbb{Q}$ l'elemento (a_n) con $a_n = 2^{-n}q$ è coerente. D'altra parte, è chiaro che ogni elemento coerente deve avere questa forma con $q = a_0$ e quindi

   $$\varprojlim_n \mathbb{Q} = \mathbb{Q}.$$

   Si noti che ogni $\pi_k : \varprojlim_n \mathbb{Q} \to \mathbb{Q}$ realizza l'isomorfismo.

3. Fissato un numero primo p, si consideri la famiglia proiettiva

   $$\ldots \longrightarrow \mathbb{Z}/p^3\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots$$

   dove $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ è la mappa quoziente canonica. Il limite inverso

   $$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

è detto gruppo dei *numeri interi p-adici*. Ogni numero intero p-adico è una successione $a_1, a_2, \ldots$ di numeri interi tali che

$$a_{n+1} - a_n \equiv 0 \bmod p^n$$

e due tali successioni $a_1, a_2, \ldots$ e $b_1, b_2, \ldots$ rappresentano lo stesso numero p-adico se e soltanto se $p^n | (a_n - b_n)$ per ogni n. La somma in $\mathbb{Z}_p$ corrisponde alla somma di successioni componente per componente. In particolare le successioni costanti $a_n = k$ con $k \in \mathbb{Z}$ sono numeri interi p-adici, cioè c'è un'inclusione

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p.$$

D'altra parte è chiaro che $\mathbb{Z}$ è un sottogruppo proprio di $\mathbb{Z}_p$, ad esempio la successione $1, 4, 13, 40, 121, \ldots$ definita ricorsivamente dalla regola $a_{n+1} - a_n = 3^n$ rappresenta un elemento in $\mathbb{Z}_3$ non in $\mathbb{Z}$.

In questo caso, le mappe $\pi_k : \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ sono suriettive, perchè lo sono già ristrette a $\mathbb{Z}$. In termini di successioni

$$\ker(\pi_k) = \{a_1, a_2, \ldots \text{ tali che } a_1 = \ldots = a_k = 0\}$$

ed allora per ogni $y \in \ker(\pi_k)$ esiste $x \in \mathbb{Z}_p$ tale che $y = p^k x$. D'altra parte, l'inclusione $p^k\mathbb{Z}_p \subseteq \ker(\pi_k)$ è ovvia. Dunque

$$\ker(\pi_k) = p^k\mathbb{Z}_p$$

e per il Primo Teorema d'Isomorfismo

$$\frac{\mathbb{Z}_p}{p^k\mathbb{Z}_p} \xrightarrow{\sim} \mathbb{Z}/p^k\mathbb{Z}.$$

L'esempio dei numeri interi p-adici ammette la seguente generalizzazione. Sia G un gruppo qualunque e sia assegnata una successione decrescente $G = G_0 > G_1 > G_2 > \ldots$ di sottogruppi normali. Allora ci sono mappe quoziente canoniche

$$G/G_{n+1} \longrightarrow G/G_n, \qquad G_{n+1}g \mapsto G_n g$$

e possiamo considerare la famiglia proiettiva

$$\ldots \longrightarrow G/G_3 \longrightarrow G/G_2 \longrightarrow G/G_1 \longrightarrow \{1\} \longrightarrow \{1\} \longrightarrow \ldots$$

ed il limite

$$\widehat{G} := \varprojlim_n (G/G_n)$$

detto anche il completamento di G rispetto alla famiglia $\{G_n\}$. Come nel caso dei numeri p-adici, che si riottiene ponendo $G = \mathbb{Z}$ e $G_n = p^n\mathbb{Z}$, abbiamo un omomorfismo

$$G \longrightarrow \widehat{G}, \qquad g \mapsto (G_n g).$$

Teorema 4.2.7. *L'omomorfismo $G \to \widehat{G}$ è iniettiva se e soltanto se $\bigcap_{n\geq 0} G_n = \{1\}$.*

Dimostrazione. Un elemento $g \in G$ diventa l'elemento neutro in $\widehat{G}$ se e soltanto se $G_n g = G_n$ per ogni n, cioè quando $g \in G_n$ per ogni n. Questo rende evidente che il nucleo della mappa $G \to \widehat{G}$ è $\bigcap_{n\geq 0} G_n = \{1\}$. ∎

Esempio 4.2.8. Sia $G = \mathbb{C}[X]$, il gruppo additivo dei polinomi in una variabile a coefficienti complessi, e poniamo $G_n = X^n\mathbb{C}[X]$, il sottogruppo dei polinomi che hanno 0 come radice di molteplicità $\geq n$. Siccome ogni laterale in G/G_n ammette un ed un solo rappresentante di grado $\leq n-1$, un elemento $P \in \widehat{G}$ può essere pensato come una successione $(p_n(X))$ dove $p_n(X)$ è un polinomio di grado $\leq n-1$ e $p_{n+1}(X) - p_n(X) = c_nX^n$ per un opportuno $c_n \in \mathbb{C}$. Partendo da $p_0 = c_0$ e sostituendo ricorsivamente, a P resta identificata la serie formale $P(X) = c_0 + c_1X + c_2X^2 + \ldots$.

D'altra parte, ragionando al contrario, ad ogni serie formale $P(X) = c_0 + c_1X + c_2X^2 + \ldots$ resta canonicamente associato un elemento in $\widehat{G}$. Dunque

$$\widehat{\mathbb{C}[X]} = \mathbb{C}[[X]].$$

PROBLEMI

4.1. Dimostrare che $\mathbb{Z} \times \mathbb{Z}$ non è ciclico.

4.2. Dimostrare che $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ non è ciclico per ogni $n \geq 2$.

4.3. Verificare che $Z(G \times H) = Z(G) \times Z(H)$.

4.4. Dimostrare che $\mathrm{Int}(G \times G) = \mathrm{Int}(G) \times \mathrm{Int}(G)$ ma che $\mathrm{Aut}(G) \times \mathrm{Aut}(G)$ è un sottogruppo proprio non banale di $\mathrm{Aut}(G \times G)$

4.5. Enunciare correttamente e dimostrare le generalizzazioni della Proposizione 4.1.3 e del Teorema 4.1.7 nel caso di un prodotto finito di gruppi.

4.6. Per ogni $i = 1, 2, \ldots$ sia $G_i = \mathbb{Z}$ una copia del gruppo dei numeri interi. Sia $G = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}$ e $\mathcal{G} = \prod_{i\in\mathbb{N}} \mathbb{Z}$. Dimostrare che

$$\mathcal{G} \simeq \mathrm{Hom}(G, \mathbb{Z}).$$

4.7. Verificare che la relazione (4.3) è un'equivalenza.

4.8. Verificare che nel caso dei gruppi abeliani le definizioni 4.2.2 e 4.2.3 sono equivalenti.

Lezione 5

Azioni

5.1 Azione di un gruppo su un insieme

Sia G un gruppo e sia X un insieme.

Definizione 5.1.1. *Un'azione sinistra di G su X è una mappa*

$$G \times X \longrightarrow X, \qquad (g, x) \mapsto g \cdot x$$

tale che

1. *per ogni $g, h \in G$ e per ogni $x \in X$ si ha $g \cdot (h \cdot x) = (gh) \cdot x$,*
2. *per ogni $x \in X$ si ha $1 \cdot x = x$*

Si noti che la seconda richiesta non è un caso particolare della prima. Se è data un'azione sinistra di G su X diremo che G agisce a sinistra su X.

Simmetricamente si definisce azione destra di G su X il dato di una mappa

$$X \times G \longrightarrow X, \qquad (x, g) \mapsto x \cdot g$$

tale che

1. per ogni $g, h \in G$ e per ogni $x \in X$ si ha $(x \cdot g) \cdot h = x \cdot (gh)$,
2. per ogni $x \in X$ si ha $x \cdot 1 = x$

Diremo che G agisce a destra su X se è assegnata un'azione destra di G su X.

Esempi 5.1.2. 1. Si consideri il caso in cui $X = G$. Allora la mappa di prodotto in G può essere vista alternativamente come il dato di un'azione a sinistra o a destra di G su se stesso. Nel primo caso si ha $g \cdot x = gx$ e nel secondo caso $x \cdot g = xg$.

   Vale la pena osservare che la moltiplicazione a destra non è un'azione sinistra! Infatti, posto $g \cdot x = xg$, si ha in generale

   $$g \cdot (h \cdot x) = g \cdot (xh) = xhg = (hg) \cdot x \neq (gh) \cdot x$$

   perchè il gruppo G non è commutativo.

2. Sia X l'insieme delle funzioni definite su G a valori complessi e pensiamo G dotato dell'azione destra su se stesso data dalla moltiplicazione a destra come nell'esempio precedente. Allora G agisce a sinistra su X come

$$(g \cdot \phi)(x) = \phi(xg) \qquad \text{per ogni } \phi \in X \text{ e per ogni } g, x \in G$$

in quanto $(g \cdot (h \cdot \phi))(x) = (h \cdot \phi))(xg) = \phi(xgh) = (gh) \cdot \phi(x)$ e, ovviamente, $1 \cdot \phi = \phi$.

Osserviamo che $(\phi \cdot g)(x) = \phi(xg)$ non definisce un'azione destra su X in quanto $((\phi \cdot g) \cdot h)(x) = (\phi \cdot g)(xh) = \phi(xhg) = (\phi \cdot (hg))(x) \neq (\phi \cdot (gh))(x)$ in generale.

Risultati perfettamente simmetrici si ottengono a partire dall'azione sinistra di G su se stesso data dalla moltiplicazione.

3. Il coniugio $g \cdot x = gxg^{-1}$ definisce un'azione sinistra di G su se stesso in quanto

$$g \cdot (h \cdot x) = gh \cdot xg^{-1}ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x$$

e ovviamente $1 \cdot x = x$.

Supponiamo assegnata un'azione (sinistra) del gruppo G sull'insieme X. Lasciamo al lettore il compito di rileggere le definizioni e i risultati seguenti nel caso delle azioni destre.

Definizione 5.1.3. Sia $x \in X$.

1. Si dice *stabilizzatore* di x il sottoinsieme

$$G_x = \{g \in G \text{ tali che } g \cdot x = x\} \subset G.$$

2. Si dice *orbita* di x il sottoinsieme

$$\mathrm{Orb}(x) = \{y = g \cdot x \in X \text{ tali che } g \in G\} \subset X.$$

3. Si dice *nucleo dell'azione* di x il sottogruppo

$$\{g \in G \text{ tali che } g \cdot x = x \text{ per ogni } x \in X\} = \bigcap_{x \in X} G_x.$$

Riassumiamo nell'unico enunciato seguente le proprietà fondamentali di un'azione.

Teorema 5.1.4. *Sia data un'azione del gruppo G sull'insieme X. Allora:*

1. *Per ogni $g \in G$, la funzione $\Phi_g : X \to X$, $\Phi_g(x) = g \cdot x$ è una biezione.*
2. *Per ogni $x \in X$ lo stabilizzatore G_x è un sottogruppo di G.*
3. *Per ogni $x \in X$ c'è una biezione di insiemi $G/G_x \xrightarrow{\sim} \mathrm{Orb}(x)$.*
4. *L'insieme delle orbite costituisce una partizione di X.*
5. *Se due elementi $x, y \in X$ appartengono alla stessa orbita allora gli stabilizzatori G_x e G_y sono coniugati.*
6. *Il nucleso dell'azione è un sottogruppo normale di G*

Dimostrazione. Per le regole che definiscono un'azione le mappe Φ_g e $\Phi_{g^{-1}}$ sono inverse una dell'altra. Questo prova il punto 1.

Per il punto 2 si osserva direttamente che $1 \cdot x$ e $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ se $g, h \in G_x$. Inoltre, se $g \in G_x$ si ha

$$x = 1 \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x,$$

cioè $g^{-1} \in G_x$.

Per il punto 3, la mappa

$$G/G_x \longrightarrow X, \qquad gG_x \mapsto g \cdot x$$

è ben definita ed iniettiva. Ben definita perchè se $\gamma \in G_x$ si ha $g\gamma \cdot x = g \cdot (\gamma \cdot x) = g \cdot x$ ed iniettiva perchè se se $g \cdot x = h \cdot x$ allora $gh^{-1} \cdot x = x$ e dunque $gh^{-1} \in G_x$. Allora la mappa definisce una biezione di G/G_x con la sua immagine in X, che è evidentemente $\mathrm{Orb}(x)$.

Per il punto successivo, si osservi innanzitutto che essendo $x \in \mathrm{Orb}(x)$ si ha sicuramente $X = \cup_{x \in X} \mathrm{Orb}(x)$. Per dimostrare che l'unione è disgiunta si osservi che se $y = h \cdot x \in \mathrm{Orb}(x)$ allora ogni elemento in $\mathrm{Orb}(y)$ è della forma $g \cdot (h \cdot x) = gh \cdot x$ e dunque $\mathrm{Orb}(y) \subseteq \mathrm{Orb}(x)$. Siccome però $x = h^{-1} \cdot y \in \mathrm{Orb}(y)$ vale anche l'inclusione simmetrica e pertanto $\mathrm{Orb}(x) = \mathrm{Orb}(y)$.

Inoltre, se $y = g \cdot x \in \mathrm{Orb}(x)$ si verifica immediatamente che

$$G_y = gG_xg^{-1}.$$

Infine, il nucleo dell'azione è il nucleo dell'omomorfismo $G \to \mathfrak{S}_X$ che ad ogni $g \in G$ assegna la permutazione Φ_g. ■

Definizione 5.1.5. Un'azione del gruppo G sull'insieme X si dice

1. *transitiva* se $X = \mathrm{Orb}(x)$ per un elemento $x \in X$ (e quindi per tutti),
2. *fedele* se ha nucleo banale.

Esempi 5.1.6.

1. L'azione di G su se stesso per moltiplicazione sinistra è sicuramente transitiva e fedele, $G = \mathrm{Orb}(1)$, e per ogni $g \in G$ lo stabilizzatore G_g consiste del solo elemento neutro.

2. Nell'azione di G su se stesso data dal coniugio le orbite coincidono con le classi di coniugio e quindi. in generale, l'azione non è transitiva. Per ogni $x \in G$ lo stabilizzatore

   $$G_x = \{g \in G \text{ tali che } gx = xg\}$$

   è anche detto *centralizzante* di x in G, denotato $C_G(x)$, e può essere caratterizzato come il più grande sottogruppo di G commutante con x. Se G è finito, per il Teorema 5.1.4(3) risulta

   $$\frac{|G|}{|C_G(x)|} = |[x]|\,.$$

   L'azione non è neanche fedele perchè il suo nucleo coincide col centro $Z(G)$.

3. Fissato un sottogruppo $H < G$, il gruppo G agisce sui laterali G/H per moltiplicazione sinistra, $g \cdot (xH) = gxH$. L'azione è transitiva perchè per ogni $g \in G$, $gH = g \cdot H$ e risulta chiaramente

   $$G_{gH} = gHg^{-1}.$$

4. Sia *calH* l'insieme dei sottogruppi di G. Allora G agisce su $\mathcal{H}$ per coniugio. L'orbita $\mathrm{Orb}(H)$ è costituita da tutti i sottogruppi coniugati di H e lo stabilizzatore

$$G_H = \{g \in G \text{ tali che } gHg^{-1} = H\},$$

detto anche *normalizzante* di H in G e denotato $N_G(H)$, può essere caratterizzato come il più grande sottogruppo di G contenente H in cui H è normale.

5. Il gruppo S^1 (Esempio 3.4.2(1)) agisce su $\mathbb{C}$ per moltiplicazione. Se per $w, z \in \mathbb{C}$ risulta $\|w\| = \|z\| \neq 0$, allora $\zeta = w/z \in S^1$ e $\zeta z = w$. Questo dimostra che per ogni $z \in \mathbb{C}$

$$\mathrm{Orb}(z) = \{w \in \mathbb{C} \text{ tali che } \|w\| = \|z\|\}$$

e la decomposizione in orbite di $\mathbb{C}$ è la decomposizione di un piano in circonferenze concentriche. Per quanto riguarda gli stabilizzatori, si ha

$$S^1_z = \begin{cases} \{1\} & \text{se } z \neq 0 \\ S^1 & \text{se } z = 0 \end{cases}$$

5.2 La formula di Burnside

Sia G un gruppo finito che agisce su un insieme finito X. Un problema generale è la determinazione del numero C delle orbite.

Consideriamo la funzione

$$\chi : G \longrightarrow \mathbb{N}$$

dove $\chi(g)$ è definito essere il numero degli elementi fissati da g, cioè il numero degli $x \in X$ tali che $g \cdot x = x$, Vale allora il risultato seguente.

Teorema 5.2.1 (Formula di Burnside)**.**

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

Dimostrazione. Considerimao la somma $\sum_{g \in G} \chi(g)$. un elemento $x \in X$ è fissato da g se e soltanto se $g \in G_x$. Dunque, il contributo di x alla somma è $|G_x|$. Siccome stabilizzatori di elementi nella stessa orbita sono coniugati e sottogruppi coniugati contengono lo stesso numero di elementi, gli elementi di $\mathrm{Orb}(x)$ danno complessivamente un contributo alla somma pari a

$$|\mathrm{Orb}(x)|\,|G_x| = [G : G_x]\,|G_x| = |G|\,.$$

Il contributo di ogni orbita è dunque lo stesso ed allora $\sum_{g \in G} \chi(g) = C\,|G|$. La formula segue immediatamente. ■

Esempio 5.2.2. *Nell'azione di G su se stesso per coniugio, gli elementi fissati da g sono gli elementi del centralizzante $C_G(g)$, Pertanto, per la Formula di Burnside ci sono*

$$c(G) = \frac{1}{|G|} \sum_{g \in G} |C_G|\,(g)$$

classi di coniugio in G.

La funzione χ gode di alcune proprietà che ne semplificano il calcolo.

Proposizione 5.2.3. *1. Se $g, h \in G$ sono coniugati, allora $\chi(g) = \chi(h)$.*

2. Se $\langle g \rangle = \langle h \rangle$ allora $\chi(g) = \chi(h)$.

Dimostrazione. Scritto $h = \gamma g \gamma^{-1}$ si osservi che g fissa x se e soltanto se h fissa $\gamma \cdot x$. Questo definisce una biezione tra l'insieme degli elementi fissati da g e l'insieme degli elementi fissati da h e prova il punto 1.

Per il punto 2 si osservi che una potenza di g fissa tutti gli elementi fissati da g. Questo basta, perchè g e h sono uno potenza dell'altro. ■

In particolare, se $G = \langle g \rangle$ è ciclico di ordine n, la Formula di Burnside diventa

$$C = \frac{1}{n} \sum_{d|n} \chi(g^d)\phi(n/d). \tag{5.1}$$

Infatti per la Proposizione precedente la funzione χ assume lo stesso valore sui $\phi(n/d)$ generatori dell'unico sottogruppo di G di ordine n/d, e g^d è uno di questi.

Esempio 5.2.4. Ad una tavola circolare siedono n persone ciascuna dei quali indossa un cappello di uno tra k colori possibili. Il numero totale delle configurazioni di colori è k^n ma due configurazioni definiscono la stessa disposizione se una si ottiene dall'altra per una rotazione. Dunque il numero delle disposizioni è uguale al numero C delle orbite dell'azione del gruppo ciclico delle rotazioni sull'insieme delle configurazioni. tale gruppo ciclico è generato da g, rotazione antioraria di $2\pi/n$. Per la formula semplificata di Burnside (5.1),

$$C = \frac{1}{n} \sum_{d|n} k^{n/d}\phi(n/d) = \sum_{d|n} k^d \phi(d)$$

in quanto le configurazioni fissate da g^d sono esattamente quelle che ripetono ciclicamente le prime n/d posizioni (che sono arbitrarie). Ad esempio, se $n = 10$ e $k = 3$, $C = \frac{1}{10}(3 + 3^2 + 3^5 \cdot 4 + 3^{10} \cdot 4) = 23718$.

Faremo ora vedere come dalla Formula di Burnside si possa far discendere un classico risultato di Jordan che a sua volta ha alcune interessanti conseguenze apparentemente non legate alla teoria dei gruppi. Premettiamo il seguente risultato tecnico sulla funzione χ.

Lemma 5.2.5. $\frac{1}{|G|} \sum_{g \in G} \chi^2(g) \geq 2$

Dimostrazione. Consideriamo l'azione di G su $X \times X$ data da $g \cdot (x, x') = (gx, gx')$ (azione componente per componente). Una coppia (x, x') è fissata da g se e soltanto se x e x' sono fissati da g. Dunque $\chi^2(g)$ è il numero degli elementi fissati da G in $X \times X$ e per la Formula di Burnside $\frac{1}{|G|} \sum_{g \in G} \chi^2(g)$ conta le orbite in cui è ripartito $X \times X$. D'altra parte, l'azione componente per componente muta la diagonale

$$\Delta = \{(x, x) \text{ tale che } x \in X\} \subseteq X \times X$$

in sè, e quindi devono esserci almeno due orbite distinte. ■

Possiamo ora enunciare il risultato seguente.

Teorema 5.2.6 (Jordan)**.** *Sia G un gruppo che agisce transitivamente su un insieme finito X tale che $|X| \geq 2$. Allora esiste un elemento $g \in G$ che agisce su X senza fissare punti.*

Dimostrazione. Sia K il nucleo dell'azione. Allora, per il Primo Teorema d'Omomorfismo, il gruppo quoziente G/K è isomorfo ad un sottogruppo di $\mathfrak{S}_X$ ed in particolare è finito. Possiamo allora assumere che G è finito.

Poniamo $n = |X|$ e denotiamo G_o il sottoinsieme di G degli elementi che agiscono senza fissare punti, cioè il sottopinsieme degli elementi di G per cui $\chi(g) = 0$. Per ogni $g \in G - G_o$ si ha $1 \leq \chi(g) \leq n$ e quindi

$$(\chi(g) - 1)(\chi(g) - n) \leq 0.$$

Siccome si ha $\frac{1}{|G|} \sum_{g \in G - G_o} (\chi(g) - 1)(\chi(g) - n) \leq 0$ vale la stima

$$\frac{1}{|G|} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n) \leq \frac{1}{|G|} \sum_{g \in G_o} (\chi(g) - 1)(\chi(g) - n) = \frac{1}{|G|} |G_o| \, n.$$

La parte sinistra di questa disuguaglianza si scrive anche $\frac{1}{|G|} \sum_{g \in G} (\chi^2 - (n+1)\chi(g) + n)$. Siccome l'azione di G è transitiva si ha $\frac{1}{|G|} \sum_{g \in G} \chi(g) = 1$ per la Formula di Burnside e usando anche il Lemma precedente si ottiene una seconda stima

$$1 = 2 - (n+1) + n \leq \frac{1}{|G|} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n).$$

Combinando le due stime si ottiene

$$|G_o| \, \frac{n}{|G|} \geq 1$$

e quindi, in particolare, $|G_o| > 0$. ■

Osservazione 5.2.7. La dimostrazione presentata qui del Teorema di Jordan, dovuta a P. J. Cameron e A. M. Cohen [1] permette di ottenere la stima più precisa

$$\frac{|G_o|}{|G|} > \frac{1}{n}.$$

Una discussione sia pure sommaria di alcune conseguenze del Teorema di Jordan risulterebbe troppo lunga per queste note. Il lettore interessato è invitato a consultare [2] dove vengono discusse le applicazioni seguenti

Teorema 5.2.8. *Sia S^1 il cerchio unitario e sia $f : T \to S$ un ricoprimento finito di grado ≥ 2 di uno spazio topologico S con T connesso per archi. Allora esiste una mappa continua $\varphi : S^1 \to S$ che non può essere sollevata al ricoprimento T.*

Teorema 5.2.9. *Sia $f \in \mathbb{Z}[X]$ un polinomio irriducibile di grado $n \geq 2$ e per ogni primo p sia $N_p(f)$ il numero degli zeri di f modulo p. Allora l'insieme dei primi tali che $N_p(f) = 0$ ha densità $\geq \frac{1}{n}$*

Con riferimento a quest'ultimo teorema si ricorda che la densità di un insieme di numeri primi $\mathcal{P}$ è δ se

$$\delta = \lim_{x \to \infty} \frac{\{p \in \mathcal{P} \text{ tali che } p \leq x\}}{\pi(x)}$$

dove $\pi(x)$ denota il numero dei primi $\leq x$. Quindi, in particolare, un insieme $\mathcal{P}$ di primi di densità > 0 contiene infiniti primi.

PROBLEMI

5.1. Sia G un gruppo. Verificare che le posizioni

$$g \cdot x = xg^{-1}, \qquad x \cdot g = g^{-1}x$$

definiscono rispettivamente un'azione sinistra ed un'azione destra di G su se stesso.

5.2. Dimostrare direttamente usando la definizione di sottogruppo normale che il nucleo di una azione è normale.

5.3. Dimostrare le caratterizzazioni del centralizzante C_g e del normalizzante $N_G(H)$ menzionante negli esempi 5.1.6(2) e (4) rispettivamente.

5.4. Supponiamo che un gruppo G agisca transitivamente su un insieme X. Dimostrare che allora X è necessariamente finito e che $|X|$ divide $|G|$.

5.5. Determinare il numero di anagrammi di una parola assegnata di n lettere non necessariamente distinte.

5.6. Il gruppo $\mathrm{GL}_n(\mathbb{R})$ ha un'azione naturale su $\mathbb{R}^n$: una matrice A agisce su un vettore colonna X per moltiplicazione AX. Descrivere orbite e stabilizzatori.

Lezione 6

Gruppi finiti

In questa lezione raccogliamo alcuni risultati sui gruppi finiti che possono essere dimostrati facendo ricorso ad una particolare azione del gruppo stesso o di qualche suo sottogruppo notevole. La teoria dei gruppi finiti per sua stessa natura si presta ad argomentazioni di tipo aritmetico-combinatorico che proveremo anche ad illustrare con qualche esempio concreto

6.1 Gruppi finiti e permutazioni

Il primo risultato che vogliamo dimostrare è il seguente.

Teorema 6.1.1 (Cayley)**.** *Sia G un gruppo finito di ordine n. Allora G è isomorfo ad un sottogruppo del gruppo $\mathfrak{S}_n$.*

Dimostrazione. Consideramio l'azione (sinistra) di G su se stesso data dalla moltiplicazione a sinistra. Come abbiamo osservato nell'esempio 5.1.6(1) tale azione è fedele.

Dunque assegnare ad ogni $g \in G$ la permutazione $x \mapsto gx$ di G definisce un omomorfismo iniettivo $G \to \mathfrak{S}_G$. Siccome $|G| = n$ risulta $\mathfrak{S}_G \simeq \mathfrak{S}_n$ e G rimane identificto ad un sottogruoppo di $\mathfrak{S}_n$. ■

Un modo concettuale per esprimere tale risultato è che la collezione dei gruppi $\mathfrak{S}_n$, $n = 2, 3, \ldots$, con i loro sottogruppi esaurisce la teoria dei gruppi finiti. In realtà questo punto di vista può risultare illusorio nel senso che la teoria dei gruppi finiti risulta affatto semplificata da questa osservazione.

Possiamo porci il problema di determinare un immersione minimale di un gruppo G in un gruppo di permutazioni: assegnato un gruppo finito G, qual è il valore minimo di n per cui G è isomorfo ad un sottogruppo di $\mathfrak{S}_n$? Per il Teorema di Cayley sappiamo che risulta $n \leq |G|$ e per la dimostrazione che ne abbiamo dato è evidente che il problema è equivalente a quello della determinazione del più piccolo insieme X (dove la grandezza è misurata dalla cardinalità $|X|$) su cui G agisce fedelmente. Ci limitiamo qui a qualche osservazione.

Osservazioni 6.1.2.

1. Condizione necessaria per avere $G < \mathfrak{S}_n$ è che $|G|$ divida $n!$. Già questo basta a concludere che se G è ciclico di ordine primo l'immersione data dal Teorema di Cayley è minimale.

2. Supponiamo G ciclico di ordine n e sia

$$n = p_1 \cdots p_r$$

la decomposizione primaria di n dove i primi p_i non sono necessariamente distinti e poniamo $N = \sum_{i=1}^{r} p_i$. Allora il prodotto di cicli disgiunti

$$(1 \ \dots \ p_1)(p_1+1 \ \dots \ p_1+2)\cdots(N-p_r+1 \ \dots N) \in \mathfrak{S}_N$$

ha ordine esattamente N e quindi $G < \mathfrak{S}_N$.

3. Fissato n, la determinazione delle partizioni di n permette di specificare le strutture cicliche e quindi gli ordini degli elementi di $\mathfrak{S}_n$, vedi Teorema 2.2.5. Questo permette di stabilire quali gruppi ciclici sono immergibili in $\mathfrak{S}_n$. Ad esempio

$n =$	2	ordini	$\{1,2\}$
	3		$\{1,2,3\}$
	4		$\{1,2,3,4\}$
	5		$\{1,2,3,4,5,6\}$
	6		$\{1,2,3,4,5,6,8,9\}$

6.2 Invertire Lagrange?

Sia G un gruppo finito con $|G| = n$. Il Teorema di Lagrange 3.1.4 esprime una condizione necessaria per l'esistenza di un sottogruppo $H < G$ con $|H| = d$: precisamente deve aversi che d divide n.

Possiamo chiederci se la condizione "d divide n" è anche sufficiente per l'esistenza di un sottogruppo H con d elementi oppure, in caso negativo, isolare delle classi di gruppi per cui questo accade e per cui possiamo dire, con un certo abuso di linguaggio che "il Teorema di Lagrange si inverte". Ad esempio, sappiamo dal Teorema 1.2.7 che i gruppi ciclici possiedono un sottogruppo per ogni divisore dell'ordine.

Iniziamo dimostrando il risultato classico seguente.

Teorema 6.2.1 (Cauchy)**.** *Sia G un gruppo finito e sia p un numero primo che divide $|G|$. Allora esiste in G un sottogruppo con p elementi.*

Dimostrazione. È chiaro che basta trovare un elemento $1 \neq g \in G$ tale che $g^p = 1$. Consideriamo l'insieme

$$X = \{(g_1, \dots, g_p) \in G^p \text{ tali che } g_1 \cdots g_p = 1\}.$$

Sull'insieme X agisce il gruppo $\mathbb{Z}/p\mathbb{Z}$ per permutazioni cicliche: se $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ si ha

$$\bar{k} \cdot (g_1, \dots, g_p) = (g_{k+1}, \dots, g_p, g_1, \dots, g_k) \in X$$

in quanto posto $a = g_1 \cdots g_k$ e $b = g_{k+1} \cdot g_p$ la relazione $g_1 \cdots g_p = ab = 1$ implica $ba = g_{k+1} \cdot g_p g_1 \cdots g_k = 1$. Ci sono due tipi di orbite per questa azione:

1. le orbite costituite da un unico elemento, e
2. le orbite costituite da p elementi.

Se supponiamo ci siano r orbite di tipo 1 e s orbite di tipo 2 risulta $|X| = r + ps$.

D'altra parte ogni scelta arbitraria di $p-1$ elementi $g_1, \dots, g_{p-1}$ in G può essere completata in modo unico ad un elemento di X ponendo $g_p = (g_1 \cdots g_{p-1})^{-1}$ Dunque risulta anche $|X| = |G|^{p-1}$. Confrontando le due valutazioni di $|X|$ si ottiene

$$|G|^{p-1} = r + ps$$

da cui $p|r$. Siccome $r \geq 1$ in quanto $(1, \ldots, 1) \in X$ deve essere $r \geq p \geq 2$ e quindi esiste $1 \neq g \in G$ tale che $(g, \ldots, g) \in X$, cioè $g_p = 1$. ■

Vediamo ora come il Teorema di Cauchy permetta di costruire sottogruppi di ordine arbitrario per G appartenente a due classi notevoli di gruppi finiti.

Teorema 6.2.2. *Sia G un gruppo abeliano finito con $|G| = n$. Allora G possiede almeno un sottogruppo di ordine d per ogni divisore d di n.*

Dimostrazione. Sia $n = p_1 \cdots p_r$ la decomposizione primaria di n dove non si richiede che i primi siano distinti. Procediamo per induzione su r. Nel caso in cui $r = 1$ l'enunciato è ovviamente soddisfatto.

Possiamo quindi assumere il Teorema vero per ordini decomponibili come prodotto di $\leq r-1$ primi. Sia d un divisore di n. Se $d = 1$ l'asserto è ovviamente vero per d. Se $d > 1$ scegliamo un primo $p|d$ e sia C un sottogruppo di ordine p di G, la cui esistenza è garantita dal Teorema di Cauchy. Per l'abelianità di G, il sottogruppo C è normale e possiamo considerare il sottogruppo quoziente G/C. A meno di riordinare i primi nella decomposizione di n possiamo assumere $p = p_r$ e allora

$$|G/C| = \frac{n}{p_r} = p_1 \cdots p_{r-1}.$$

Per ipotesi induttiva G/C possiede un sottogruppo $\bar{H}$ di ordine d/p_r. Allora il sottogruppo H controimmagine in G di $\bar{H}$ secondo la mappa quoziente possiede d elementi. ■

Definiamo ora la seconda classe di gruppi finiti per cui riusciremo ad invertire il Teorema di Lagrange.

Definizione 6.2.3. *Sia p un numero primo. Un gruppo finito G è detto un p-gruppo se $|G| = p^n$, $n \in \mathbb{N}$.*

Al risultato vero e proprio è necessario anteporre il lemma seguente.

Lemma 6.2.4. *Sia G un p-gruppo. Allora $Z(G) \neq \{1\}$.*

Dimostrazione. Consideriamo le orbite dell'azione di G su se stesso per coniugio, cioè le classi di coniugio in G. Ogni classe di coniugio è costituita o da un unico elemento, oppure da un numero di elementi multiplo di p (perchè è identificabile ad un certo insieme completo di laterali di G). Inoltre $Z(G)$ è l'unione delle classi di coniugio costituite da un unico elemento ed allora la partizione

$$G = Z(G) \bigcup \bigcup_{[x] \neq \{x\}} [x]$$

fornisce, passando alle cardinalità, un'identità $p^n = |Z(G)| + \sum_{[x] \neq \{x\}} |[x]| = |Z(G)| + pM$, da cui $p \,|Z(G)|$. Siccome $Z(G)$ contiene sicuramente un elemento (l'elemento neutro) ne deve contenere almeno $p \geq 2$. ■

Possiamo ora enunciare il risultato sui p-gruppi.

Teorema 6.2.5. *Sia G un p-gruppo con $|G| = p^n$. Allora G possiede un sottogruppo con p^t elementi per ogni $1 \leq t \leq n$.*

Dimostrazione. Procediamo per induzione su n, il caso $n = 1$ essendo ovvio.

Sia dunque G un p-gruppo con p^n elementi. Per il Lemma precedente il centro $Z(G)$ di G non è banale. Applicando il Teorema di Cauchy a $Z(G)$, deduciamo l'esistenza di un sottogruppo C con p elementi tale che $C < Z(G)$. siccome ogni elemento di C commuta con tutto G, il

sottogruppo C è normale in G e possiamo considerare il gruppo quoziente G/C che ha p^{n-1} elementi.

Possiamo allora produrre un sottogruppo $H < G$ con p^t elementi come controimmagine di un sottogruppo $\bar{H} < G/C$ con p^{t-1} elementi. Quest'ultimo esiste per ipotesi induttiva. ■

Però è possibile trovare esempi di gruppi che non possiedono sottogruppi di un dato divisore del loro ordine.

Esempio 6.2.6. Con l'Esempio 3.2.3(3) si è visto che un sottogruppo di indice 2 è forzatamente normale. se $n \geq 5$ il gruppo alterno A_n ha ordine pari in quanto $2|(n!/2)$. Per quanto appena ricordato, se A_n possedesse un sottogruppo di ordine $n!/4$, questo sarebbe normale, contraddicendo il fatto che A_n è semplice (Teorema 3.2.6). Pertanto A_n non possiede sottogruppi di ordine $n!/4$.

Il risultato seguente non è direttamente legato alla costruzione di sottogruppi di un determinato ordine, ma è una generalizzazione della proprietà dei sottogruppi di indice 2 utilizzata nell'esempiuo appena discusso.

Teorema 6.2.7. *sia G un gruppo finito e sia p il più piccolo divisore primo di $|G|$. Allora ogni sottogruppo $H < G$ tale che $[G : H] = p$ è normale.*

Dimostrazione. Se $H < G$ ha indice p, l'azione di G sui p laterali sinistri di H per moltiplicazione sinistra definisce un'applicazione

$$f : G \longrightarrow \mathfrak{S}_p$$

che si riconosce subito essere un omomorfismo. Posto $K = \ker(f)$, il Primo Teorema d'Isomorfismo permette di rivedere il gruppo quoziente G/K come un sottogruppo di $\mathfrak{S}_p$.

Sia q un fattore primo di $|G/K|$.

- Siccome $|G/K|$ divide $|\mathfrak{S}_p| = p!$ deve essere $q \leq p$, e
- siccome q divide $|G|$ deve essere anche, per ipotesi$q \geq p$.

Quindi $q = p$, cioè G/K è un p-gruppo. Però p^2 non divide $|\mathfrak{S}_p|$ e dunque $|G/K| = p$. Si noti che per definizione $KH \subset H$, e quindi $K \subset H$. Siccome $[G : K] = [G : H]$ deve essere $H = K$ e quindi H è normale in qunto nucleo di un omomorfismo. ■

6.3 Il Teorema di Sylow

Vogliamo ora dimostrare i risultati classici ottenuti da Sylow che restano una delle chiavi fondamentali per comprendere la struttura dei gruppi finiti. Premettiamo una definizione.

Definizione 6.3.1. *Sia G un gruppo finito e sia p un numero primo con $|G| = p^t m$ e $(p, m) = 1$. Si dice p-sottogruppo di Sylow di G (o più semplicemente p-Sylow) un sottogruppo $H < G$ tale che $|H| = p^t$.*

In altri termini, un p-Sylow in G è un p-sottogruppo del più alto ordine possibile. Indicheremo $\mathrm{Syl}_p(G)$ l'insieme dei p-Sylow di G. A priori, potrebbe risultare $\mathrm{Syl}_p(G) = \emptyset$ ed il primo dei risultati di Sylow nega proprio questa possibilità. Si noti che sia la definizione che il risultato seguente restano sensate per p che non divide $|G|$ o per G stesso un p-gruppo, ma in tal caso l'unico p-Sylow esistente è banale.

Teorema 6.3.2. *Sia G un gruppo finito con $p^t m$ elementi dove p è primo e $(p, m) = 1$. Allora:*

1. $\mathrm{Syl}_p(G)$ *contiene almeno un elemento;*
2. *se* P *è un* p*-sottogruppo di* G *e se* $S \in \mathrm{Syl}_p(G)$*, esiste* $g \in G$ *tale che* $gPg^{-1} < S$*;*
3. *posto* $n_p = \left|\mathrm{Syl}_p(G)\right|$ *si ha*
   - $n_p \equiv 1 \bmod p$*, e*
   - $n_p | m$*.*

Dimostrazione.

1. Consideriamo l'insieme
$$\mathcal{P} = \{A \subset G \text{ tali che } |A| = p^t\}$$
che evidentemenete ha cardinalità $|\mathcal{P}| = \binom{p^t m}{p^t}$. Osserviamo che risulta
$$|\mathcal{P}| \equiv m \bmod p$$
ed in particolare $|\mathcal{P}|$ non è un multiplo di p. Infatti nell'anello $\mathbb{Z}/p\mathbb{Z}[X,Y]$ vale l'identità $(X+Y)^{p^t} = X^{p^t} + Y^{p^t}$ e, pertanto, confrontando i coefficienti di $X^{p^t} Y^{p^t(m-1)}$ nell'identità
$$\sum_{k=0}^{p^t m} \binom{p^t m}{k} X^k Y^{p^t m - k} = (X+Y)^{p^t m} = (X^{p^t} + Y^{p^t})^m = \sum_{j=0}^{m} X^{p^t j} Y^{p^t (m-j)}$$
si ottiene $\binom{p^t m}{p^t} = m$ in $\mathbb{Z}/p\mathbb{Z}$. L'insieme $\mathcal{P}$ è ripartito nelle orbite dell'azione di G data da moltiplicazione sinistra, $g \cdot A = gA$. Per quanto appena osservato deve esistere almeno un'orbita $\mathcal{O} \subset \mathcal{P}$ tale che $|\mathcal{O}|$ non è un multiplo di p. Scegliamo un elemento $A \in \mathcal{O}$ e sia G_A il suo stabilizzatore. Allora:
   - dall'identificazione $G/G_A \simeq \mathcal{O}$ risulta $p^t m = |G| = |G_A|\,|\mathcal{O}|$, e quindi p^t divide $|G_A|$ per quanto detto sopra;
   - per ogni $a \in A$, deve aversi $G_A a \subseteq A$ e quindi $|G_A| \leq |A| = p^t$.

   Mettendo insieme le due cose, concludiamo che $|G_A| = p^t$ e quindi G_A è un p-Sylow.

2. Consideriamo l'insieme $S\backslash G$ degli m laterali destri di S su cui facciamo agire P per moltiplicazione destra. Le orbite dell'azione di un p-gruppo o sono banali (ridotte cioè ad un unico elemento) oppure contengono un numero di elementi multiplo di p. Siccome p non divide m, l'insieme $S\backslash G$ deve contenere almeno un'orbita banale, esiste cioè un laterale Sg tale che $Sgh = Sg$ per ogni $h \in P$. Dunque $ghg^{-1} \in S$ per ogni $h \in P$, ovvero $gPg^{-1} \subset S$.

3. Sia $\mathrm{Syl}_p(G) = \{S_0, S_1, \ldots, S_r\}$, cosicchè $n_p = 1 + r$. Se $r = 0$ le affermazioni sono vere, dunque possiamo supporre $r > 0$.

   Il coniugato di un p-Sylow è un p-Sylow, e se $g \in S_0$, il coniugato gS_ig^{-1} non è S_0 se $i \neq 0$ (altrimenti si otterrebbe subito $S_i = S_0$). Dunque S_0 agisce per coniugio sull'insieme $\mathcal{S} = \{S_1, \ldots, S_r\}$. Supponiamo esista un indice $i > 0$ per cui
$$gS_ig^{-1} = S_i \qquad \text{per ogni } g \in S_0.$$
   Allora S_0 e S_i sono due p-Sylow nel normalizzante $N_G(S_i)$ e per il punto precedente (applicato al gruppo $N_G(S_i)$) S_0 e S_i dovrebbero essere coniugati e questo non è possibile perchè S_i è normale in $N_G(S_i)$.

Dunque $\mathcal{S}$ è ripartito in orbite, ciascuna delle quali ha un numero di elementi multiplo di p. Allora anche $r = |\mathcal{S}|$ è un multiplo di p. Questo dimostra che $n_p \equiv 1 \bmod p$.

Infine, osserviamo che per il punto precedente G agisce transitivamente su $\mathrm{Syl}_p(G) = \{S_0, S_1, \ldots, S_r\}$ per coniugio e $S_0 < G_{S_0} = N_G(S_0)$. Dunque

$$n_p = \left|\mathrm{Syl}_p(G)\right| = [G : N_G(S_0)] = \frac{|G|}{|N_G(S_0)|}$$

e siccome $p^t \,|\, |N_G(S_0)|$ risulta $n_p | m$.

La dimostrazione del Teorema di Sylow è così completa.

Vediamo alcuni esempi concreti di come il Teorema di Sylow permetta di ottenere informazioni sulla struttura di alcuni gruppi.

Esempi 6.3.3. 1. Sia G un gruppo finito con $|G| = pq$ dove $p < q$ sono due primi distinti tali che p non divide $q - 1$. Allora G è ciclico.

Infatti per il Teorema 6.2.7 un q-Sylow è normale perchè ha indice p. Sia ora S un p-Sylow ed $N = N_{G(S)}$ il suo normalizzante. Siccome $S < N$ ci sono due sole possibilità: o $vassN = p$ (cioè $N = S$), o $|N| = pq$ (cioè $N = G$). Se $|N| = p$, allora $[G : N] = q$ e siccome l'indice del normalizzante di un sottogruppo è il numero dei coniugati di quel sottogruppo, risulta $n_p = q$. Questo però contraddice il Teorema di Sylow ($n_p \equiv 1 \bmod p$) in quanto per ipotesi $q - 1$ non è un multiplo di p. Deve dunque aversi $N = G$, cioè $n_p = 1$ ed S è normale. In definitiva, il p-Sylow ed il q-Sylow sono ciclici entrambi normali e quindi commutano elemento per elemento. Il prodotto di un generatore di uno per un generatore dell'altro ha ordine pq e quindi G è ciclico.

In virtù di questo esempio tra i gruppi di ordine ≤ 100 sono ciclici quelli di ordine

$$15, \quad 33, \quad 35, \quad 51, \quad 65, \quad 69, \quad 77, \quad 85, \quad 87, \quad 91, \quad 95.$$

2. Sia G un gruppo finito con $|G| = 2p$ dove p è un primo (si noti che questo caso non rientra tra quelli dell'esempio precedente). Allora G possiede un p-Sylow normale S e le possibilità per n_2 sono due: o $n_2 = 1$ o $n_2 = p$.

Nel primo caso, l'unico 2-Sylow è normale e ragionando come nell'esempio precedente si vede che G è ciclico. Nel secondo caso, i p 2-Sylow forniscono p elementi distinti di ordine 2. Fissiamo un elemento y di ordine 2, siccome $y \notin S$ deve risultare

$$G = S \cup Sy = \{s^k y^\epsilon \,|\, k = 0, 1, \ldots, p-1, \epsilon = 0, 1\}$$

dove abbiamo scelto $S =< s >$. Se z un altro elemento di ordine 2 deve aversi $z = s^t y$ per un qualche $t \neq 0$ e allora $1 = z^2 = s^t y s^t y$, da cui $y s^t y = s^{-t}$. Se k è un inverso moltiplicativo di t modulo p,prendendo k-esime potenze otteniamo $(y s^t y)^k = s^{-tk} = s^{-1}$ da cui

$$sy = y s^{-1}.$$

La struttura di G è così completamente determinata.

3. Sia G un gruppo finito con 30 elementi. Allora G possiede un sottogruppo normale non banale.

Infatti possiamo dimostrare che almeno uno dei numeri n_2, n_3, n_5 è uguale ad 1. Se così non fosse, il Teorema di Sylow permette le sole altre possibilità

$$n_2 = 3, 5, 15 \qquad n_3 = 10 \qquad n_5 = 6.$$

Consideriamo due qualunque sottogruppi di Sylow distinti S e S' in G. Siccome il loro ordine è 2 o 3 o 5, devono essere ciclici e privi di sottogruppi propri, cosicchè $S \cap S' = \{1\}$. Anche nel caso in cui si avessero solo 3 2-Sylow. i sottogruppi di Sylow necessiterebbero un totale di $3 + 10 \times 2 + 6 \times 4 = 47$ elementi oltre l'elemento neutro, contraddicendo l'ipotesi $|G| = 30$.

PROBLEMI

6.1. Fissato $r > 0$, sia $G = (\mathbb{Z}/2\mathbb{Z})^r$. Qual è il più piccolo valore di n tale che $G < \mathfrak{S}_n$? Tale minimo valore n è anche il più piccolo intero per cui $|G| = 2^r$ divide $n!$?

6.2. Estendere a piacere la tabella dell'osservazione 6.1.2(3).

6.3. Dimostrare che un gruppo finito G con $|G| = 2m$ dove $m > 1$ è dispari, possiede sempre un sottogruppo normale non banale (Suggerimento: considerare nell'azione di G su se stesso per moltiplicazione destra la permutazione indotta da un elemento di ordine 2).

6.4. Dimostrare che l'intersezione di tutti i p-Sylow di un gruppo finito G è un sottogruppo normale di G.

6.5. Sia H un sottogruppo normale di un gruppo finito G. Si dimostri che se S è un p-Sylow in G, allora $H \cup S$ è un p-sylow in H. Inoltre, si dimoostri che se p non divide $[G : H]$ allora H contiene tutti i p-Sylow di G.

6.6. Si dimostri che G è un gruppo finito G con $|G| \in \{20, 36, 48, 200\}$ possiede almeno un sottogruppo normale non banale.

clearpage

Lezione 7

Generatori (e relazioni)

7.1 Gruppi liberi

Se $\mathcal{X}$ è un insieme non vuoto e $x \in \mathcal{X}$ possiamo costruire un gruppo $\langle x \rangle$ prendendo come insieme l'insieme $\{x\} \times \mathbb{Z}$ con l'operazione $(x, m) + (x, n) = (x, m + n)$. Si tratta chiaramente di un gruppo ciclico infinito, quindi isomorfo a $\mathbb{Z}$ stesso. Risulterà conveniente denotare l'elemento $(x, n) \in X$ o come nx (se si vuole usare una notazione additiva) o come x^n (se si vuole usare una notazione moltiplicativa).

Definizione 7.1.1. *Sia $\mathcal{X}$ un insieme. Si dice gruppo abeliano libero su $\mathcal{X}$ il gruppo*

$$L = L_{\mathcal{X}} = \bigoplus_{x \in \mathcal{X}} \langle x \rangle.$$

La cardinalità di $\mathcal{X}$ si dice rango di L, in simboli $\mathrm{rg}(L) = |\mathcal{X}|$.

Per definizione, il tipico elemento di L è un'espressione

$$n_1 x_1 + n_2 x_2 + \ldots n_r x_r$$

dove $x_1, x_2, \ldots, x_r$ sono arbitrari elementi di $\mathcal{X}$ e $n_1, n_2, \ldots, n_r$ sono numeri interi arbitrari (la scrittura additiva è puramente convenzionale). Si può osservare sin da ora una certa analogia formale tra un gruppo abeliano libero ed uno spazio vettoriale: la differenza sostanziale è che nell'espressione di un vettore arbitrario come combinazione lineare dei vettori di una base i coefficienti sono liberi di variare in un campo, mentre nel caso di un gruppo abeliano libero i coefficienti non nulli non risultano in generale invertibili. Nella sua essenzialità, questo fatto rende impossibile applicare *tout court* le tecniche dell'algebra lineare ai gruppi abeliani finitamente generati ed alcuni fatti veri per gli spazi vettoriali risulatno falsi per i gruppi abeliani liberi. Vediamo alcuni esempi.

Esempi 7.1.2. 1. Sia L un gruppo abeliano libero su $\mathcal{X}$. Un sottoinsieme $\mathcal{Y} \subset L$ è detto un sistema di generatori per L se ogni elemento $x \in L$ può scriversi nella forma $x = n_1 y_1 + \ldots n_r y_r$ con $y_1, \ldots, y_r \in \mathcal{Y}$ e $n_1, \ldots, n_r \in \mathbb{Z}$.

Supponiamo che $\mathcal{Y}$ sia un sistema di generatori per L tale che $|\mathcal{Y}| > \mathrm{rg}(L)$ (disuguaglianza stretta). Allora, in generale NON è possibile trovare un sistema di generatori $\mathcal{Y}' \subset \mathcal{Y}$ tale che $|\mathcal{Y}'| = \mathrm{rg}(L)$. Ad esempio $\{2, 3\}$ è un sistema di generatori di $\mathbb{Z}$, ma nè 2, nè 3 singolarmente generano $\mathbb{Z}$.

Diremo che un sistema di generatori $\mathcal{Y}$ è *minimale* se:

(a) $|\mathcal{Y}| = \mathrm{rg}(L)$,

(b) ogni sottoinsieme proprio $\mathcal{Y}' \subset \mathcal{Y}$ non è un sistema di generatori per L.

2. Un gruppo abeliano libero L può avere sottogruppi liberi di pari rango. Ad esempio l'inclusione $\mathbb{Z} \supset 2\mathbb{Z}$ è un inclusione di moduli liberi di rango 1.

3. Sia L un gruppo abeliano libero su $\mathcal{X}$ di rango n e supponiamo assegnato un sistema minimale di generatori $\{y_1, \ldots, y_n\}$. Allora le espressioni

$$y_i = \sum_{j=1}^{n} \alpha_{i,j} x_j, \qquad x_i = \sum_{j=1}^{n} \beta_{i,j} y_j$$

per $i = 1, \ldots, n$ definiscono matrici $A = (\alpha_{i,j})$ e $B = (\beta_{i,j})$ per cui vale la relazione $AB = I_n$, come si riconosce subito sostituendo un'espressione nell'altra. Essendo le matrici a coefficienti in $\mathbb{Z}$ deve risultare $\det A = \pm 1$. Pertanto, si vede che i sistemi di generatori con n elementi sono in corrispondenza biunivoca con le matrici a coefficienti in $\mathbb{Z}$ di determinante ± 1.

Siano $\mathcal{X}$ e $\mathcal{Y}$ due insiemi e supponiamo che esista una biezione $f : \mathcal{X} \xrightarrow{\sim} \mathcal{Y}$. Allora l'applicazione

$$L_{\mathcal{X}} \longrightarrow L_{\mathcal{Y}}, \qquad \sum_{x \in \mathcal{X}} n_x x \mapsto \sum_{x \in \mathcal{X}} n_x f(x)$$

è un isomorfismo. Dunque, gruppi abeliani liberi dello stesso rango sono isomorfi. Il prossimo risultato mostra che il rango individua esattamente la classe d'isomorfismo di gruppi abeliani liberi.

Teorema 7.1.3. *Siano L e L' due gruppi abeliani liberi isomorfi. Allora* $\mathrm{rg}(L) = \mathrm{rg}(L')$.

Dimostrazione. Sia $\Phi : L \to L'$ un isomorfismo di L con L'. Scegliamo un numero primo p e sia pL il sottogruppo di L e costituito dagli elementi dell forma $px = x + \ldots + x$ (p volte) con $x \in L$. Sia pL' l'analogo sottogruppo di L'. La composizione

$$L \xrightarrow{\Phi} L' \xrightarrow{\pi} L'/pL'$$

è ovviamente suriettiva e ha come nucleo il sottogruppo

$$K = \{x \in L \text{ tali che } \Phi(x) \in pL'\} = \{x \in L \text{ tali che esiste } y \in L' \text{ con } py = \Phi(x)\}.$$

Se vale $py = \Phi(x)$ in L', risulta $x = px'$ dove $x' \in L$ è l'unico elemento tale che $\Phi(x') = y$. Pertanto $K = pL$ e, per il Primo Teorema d'Isomorfismo, esiste un isomorfismo di gruppi abeliani

$$\bar{\Phi} : L/pL \xrightarrow{\sim} L'/pL'.$$

Si noti che per la classe resto $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$, la moltiplicazione $\bar{k}\bar{x} = k\bar{x} = \overline{kx}$ è ben definita e definisce una struttura di $\mathbb{Z}/p\mathbb{Z}$-spazio vettoriale su L/pL e L'/pL' e che l'isomorfismo è allora un isomorfismo di spazi vettoriali. Allora si ha

$$\mathrm{rg}(L) = \dim_{\mathbb{Z}/p\mathbb{Z}}(L/pL) = \dim_{\mathbb{Z}/p\mathbb{Z}}(L'/pL') = \mathrm{rg}(L'). \quad \blacksquare$$

I gruppi abeliani liberi ammettono, fra tutti i gruppi, una importante caratterizzazione, per la quale è necessario premettere una definizione.

Definizione 7.1.4. *Sia $\mathcal{X}$ un insieme non vuoto e sia $\mathcal{A}_\mathcal{X}$ l'insieme delle coppie (A, ϕ) con*

- *A gruppo abeliano,*
- *$\phi : \mathcal{X} \to A$ una funzione.*

Un elemento (A_u, ϕ_u) si dice universale per $\mathcal{A}_\mathcal{X}$ se per ogni $(A, \phi) \in \mathcal{A}_\mathcal{X}$ esiste un unico omomorfismo $f : A_u \to A$ tale che la composizione

$$\mathcal{X} \xrightarrow{\phi_u} A_u \xrightarrow{f} A$$

è uguale a ϕ.

Teorema 7.1.5. *Sia $\mathcal{X}$ un insieme non vuoto.*

1. *Se (A_u, ϕ_u) e $(B_u, \psi_u) \in \mathcal{A}_\mathcal{X}$ sono entrambi universali per $\mathcal{A}_\mathcal{X}$, allora esiste un unico isomorfismo $\alpha : A_u \to B_u$ tale che $\alpha \circ \phi_u = \psi_u$.*
2. *$(L_\mathcal{X}, \mathcal{X} \subset L_\mathcal{X})$ è universale per $\mathcal{A}_\mathcal{X}$.*

Dimostrazione. Per universalità di (A_u, ϕ_u) deve esistere un unico omomorfismo $\alpha : A_u \to B_u$ tale che $\alpha \circ \phi_u = \psi_u$. Simmetricamente, per universalità di (B_u, ψ_u) deve esistere un unico omomorfismo $\beta : B_u \to A_u$ tale che $\beta \circ \psi_u = \phi_u$. Componendo α con β si hanno omomomorfismi

$$\beta \circ \alpha : A_u \longrightarrow A_u, \qquad \alpha \circ \beta : B_u \longrightarrow B_u$$

tali che $\beta \circ \alpha \circ \phi_u = \phi_u$ e $\alpha \circ \beta \circ \psi_u = \psi_u$. Applicando ancora la definizione di universalità, si ottiene $\beta \circ \alpha = \mathrm{id}_{A_u}$ e $\alpha \circ \beta = \mathrm{id}_{B_u}$. Dunque α è un'isomorfismo. Questo dimostra il punto 1.

Per il punto 2 basta osservare che per ogni $(A, \phi) \in \mathcal{A}_\mathcal{X}$ l'omomorfismo $f : L_\mathcal{X} \to A$ tale che

$$f(n_1 x_1 + \ldots + n_r x_r) = n_1 \phi(x_1) + \ldots + n_r \phi(x_r)$$

estende l'applicazione $\phi : \mathcal{X} \to A$ ed è l'unico ad avere tale proprietà. ■

Una applicazione di una certa importanza teorica di questa proprietà universale dei gruppi abeliani liberi è la seguente. Supponiamo assegnato un omomorfismo di gruppi

$$f : G \longrightarrow H.$$

Per ogni gruppo Γ la composizione con f definisce un'applicazione

$$f_* : \mathrm{Hom}(\Gamma, G) \longrightarrow \mathrm{Hom}(\Gamma, H), \qquad f_*(\phi) = \alpha \circ \phi.$$

Possiamo chiederci se delle proprietà di f si riflettono in proprietà di f_*, in generale o anche sotto certe condizioni da imporre al gruppo Γ.

Proposizione 7.1.6. *Sia L un gruppo abeliano libero e sia $f : G \to H$ un omomorfismo suriettivo di gruppi abeliani. Allora per ogni omomorfismo $\alpha \in \mathrm{Hom}(L, H)$ esiste un omomorfismo $\beta \in \mathrm{Hom}(L, G)$ tale che $f_*(\beta) = f \circ \beta = \alpha$.*

Dimostrazione. Sia $\mathcal{X}$ un insieme minimale di generatori per L e per ogni $x \in \mathcal{X}$ si usi la suriettività di f per scegliere un elemento $g_x \in G$ tale che $f(g_x) = \alpha(x)$.

Per la proprietà universale di L, esiste un unico omomorfismo $\beta : L \to G$ che estende la funzione $x \mapsto g_x$. Si controlla subito che β ha la proprietà voluta. ■

Possiamo prendere spunto dalla caratterizzazione del Teorema 7.1.5 dei gruppi abeliani liberi come gruppi abeliani soddisfacenti una certa proprietà universale per definire i gruppi liberi nel caso generale (non abeliano). La definizione seguente è un'immediata generalizzazione della Definizione 7.1.4.

Definizione 7.1.7. *Sia $\mathcal{X}$ un insieme non vuoto e sia $\mathcal{G}_\mathcal{X}$ l'insieme delle coppie (G, ϕ) con*

- *G un gruppo,*
- *$\phi : \mathcal{X} \to A$ una funzione.*

Un elemento (G_u, ϕ_u) si dice universale per $\mathcal{G}_\mathcal{X}$ se per ogni $(G, \phi) \in \mathcal{G}_\mathcal{X}$ esiste un unico omomorfismo $f : G_u \to G$ tale che la composizione

$$\mathcal{X} \xrightarrow{\phi_u} G_u \xrightarrow{f} G$$

è uguale a ϕ.

La dimostrazione del punto 1 del Teorema 7.1.5 si adatta facilmente per ottenere una dimostrazione del risultato seguente.

Teorema 7.1.8. *Se (G_u, ϕ_u) e $(H_u, \psi_u) \in \mathcal{G}_\mathcal{X}$ sono entrambi universali per $\mathcal{G}_\mathcal{X}$, allora esiste un unico isomorfismo $\alpha : G_u \to H_u$ tale che $\alpha \circ \phi_u = \psi_u$.*

Definizione 7.1.9. *Sia $\mathcal{X}$ un insieme non vuoto. Un gruppo F si dice gruppo libero su $\mathcal{X}$ se esiste un'applicazione $\phi : \mathcal{X} \to F$ tale che (F, ϕ) è universale per $\mathcal{G}_\mathcal{X}$.*

Naturalmente il problema che ci si pone ora è quello di decidere se un elemento universale per $\mathcal{G}_\mathcal{X}$ esiste o meno. Risolveremo questo problema costruendo, per un assegnato insieme non vuoto $\mathcal{X}$ un gruppo $F_\mathcal{X}$ con un'immersione $\mathcal{X} \hookrightarrow F_\mathcal{X}$ che risulterà essere universale per $\mathcal{G}_\mathcal{X}$.

Per questa costruzione, l'insieme $\mathcal{X}$ prende tradizionalmente il nome di *alfabeto* e i suoi elementi quello di *lettere*. Una *parola* è una scrittura arbitraria

$$x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_r^{\epsilon_r} \tag{7.1}$$

dove x_i è una lettera (le ripetizioni sono ammesse) e $\epsilon_i = \pm 1$ per ogni $i = 1, \dots, r$ (se $\epsilon_i = 1$ l'esponente viene generalmente omesso dalla scrittura della parola). Tra le parole includiamo la parola vuota. Data la parola 7.1, le sue sottoparole sono le parole della forma $x_i^{\epsilon_i} \dots x_j^{\epsilon_j}$ con $1 \le i \le j \le r$. Una parola è detta *ridotta* se non contiene sottoparole della forma xx^{-1} o $x^{-1}x$. Sono esempi di parole ridotte sull'alfabeto $\mathcal{X} = \{a, b, c\}$ le parole

$$ab^{-1}, \qquad c^{-1}aab, \qquad a^{-1}, c^{-1}bb^{-1}ca^{-1}ab^{-1}$$

l'ultima delle quali è non ridotta. Da una parola se ne ottiene sempre una ridotta cancellando le sottoparole della forma $x^\epsilon x^{-\epsilon}$: dall'esempio sopra in cui

$$c^{-1}bb^{-1}ca^{-1}ab^{-1} \quad \to \quad c^{-1}cb^{-1} \quad \to \quad b^{-1}$$

si vede che l'operazione di riduzione può richiedere più di un passaggio. È comunque chiaro che la procedura di riduzione produce una ben definita parola ridotta. Poniamo

$$F_\mathcal{X} = \{\text{parole ridotte nell'alfabeto } \mathcal{X}\}$$

dove l'operazione tra parole è la *giustapposizione* seguita, se necessario, da una riduzione:

$$(x_1^{\epsilon_1} \cdots x_r^{\epsilon_r})(y_1^{\varepsilon_1} \cdots y_s^{\varepsilon_s}) = x_1^{\epsilon_1} \cdots x_r^{\epsilon_r} y_1^{\varepsilon_1} \cdots y_s^{\varepsilon_s}.$$

Con tale operazione $F_\mathcal{X}$ è un gruppo in quanto:

1. la giustapposizione di parole è sicuramente associativa,

2. la parola vuota è un elemento neutro per la giustapposizione,
3. la parola $x_1^{\epsilon_1}x_2^{\epsilon_2}\dots x_r^{\epsilon_r}$ ammette come inversa la parola $x_r^{-\epsilon_1}\dots x_2^{-\epsilon_2}x_1^{-\epsilon_1}$.

Esempi 7.1.10. 1. Se $\mathcal{X}=\{x\}$ è costituito da un'unica lettera, ogni parola ridotta è di uno dei due tipi seguenti
$$x^n := \underbrace{x\dots x}_{n}, \qquad x^{-m} := \underbrace{x^{-1}\dots x^{-1}}_{m}.$$
Si vede subito che $x^n x^{-m} = x^{n-m}$ e quindi che $F_{\{x\}} \simeq L_{\{x\}} \simeq \mathbb{Z}$.

2. Se $|\mathcal{X}| \geq 2$ il gruppo $F_{\mathcal{X}}$ non è commutativo: $(a)(b) = ab \neq ba = (b)(a)$.

Ogni lettera $x \in \mathcal{X}$ può essere rivista come parola costituita da quell'unica lettera. Quindi $F_{\mathcal{X}}$ è naturalmente equipaggiato con un'applicazione (di fatto un'immersione) $\phi_{\mathcal{X}} : \mathcal{X} \to F_{\mathcal{X}}$.

Teorema 7.1.11. *Sia $\mathcal{X}$ un insieme non vuoto. Allora $(F_{\mathcal{X}}, \phi_{\mathcal{X}})$ è universale per $\mathcal{G}_{\mathcal{X}}$.*

Dimostrazione. Sia $(G,\phi) \in \mathcal{G}_{\mathcal{X}}$. Per ogni parola $x_1^{\epsilon_1}\dots x_r^{\epsilon_r} \in F_{\mathcal{X}}$ poniamo
$$f(x_1^{\epsilon_1}\dots x_r^{\epsilon_r}) = \phi(x_1)^{\epsilon_1}\cdots\phi(x_r)^{\epsilon_r} \in G.$$
Evidentemente

1. $f : F_{\mathcal{X}} \to G$ è un omomorfismo,
2. per ogni lettera $x \in \mathcal{X}$, $f(x) = f \circ \phi_{\mathcal{X}}(x) = \phi(x)$.

D'altra parte la richiesta che un omomorfismo $f' : F_{\mathcal{X}} \to G$ soddisfi la relazione $f \circ \phi_{\mathcal{X}} = \phi$ lo fa coincidere con f su qualunque parola, e quindi $f' = f$. ■

7.2 Presentazioni

Una delle ragioni per introdurre la classe dei gruppi liberi (abeliani o no) è che essi permettono, nel senso reso preciso dal prossimo risultato, di ricostruire qualsiasi gruppo.

Teorema 7.2.1. *Sia G un gruppo. Allora G è isomorfo al quoziente di un gruppo libero.*

Dimostrazione. Scegliamo un insieme $\mathcal{X}$ di generatori di G. L'inclusione naturale di $\mathcal{X}$ in G definisce un elemento $(G,\mathcal{X}) \in \mathcal{G}_{\mathcal{X}}$. per il Teorema 7.1.11 esiste (ed è unico) un omomorfismo $f : F_{\mathcal{X}} \to G$ tale che, con un piccolo abuso di notazione. $f(x) = x$.

Siccome $\mathcal{X}$ genera G l'omomorfismo f è suriettivo e dunque $G \simeq F_{\mathcal{X}}/\ker(f)$ per il Primo Teorema d'Isomorfismo. ■

Se il gruppo G è abeliano, $(G,\mathcal{X}) \in \mathcal{A}_{\mathcal{X}}$ e allora, con identica dimostrazione, otteniamo il risultato particolare seguente.

Teorema 7.2.2. *Sia G un gruppo abeliano. Allora G è isomorfo al quoziente di un gruppo abeliano libero.*

Esempi 7.2.3. 1. Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n. Allora G è quoziente del gruppo abeliano libero $L_{\{g\}} \simeq \mathbb{Z}$. Questo è consistente col fatto che $G \simeq \mathbb{Z}/n\mathbb{Z}$.

2. Il gruppo $\mathfrak{S}_n$ è generato dalle trasposizioni. Risulta però $(1\ x)(1\ y)(1\ x) = (x\ y)$ e quindi le $n-1$ trasposizioni $(1\ 2),\dots,(1\ n-1)$ bastano a generare $\mathfrak{S}_n$. Allora $\mathfrak{S}_n$ è quoziente del gruppo libero su $n-1$ lettere.

Sia G un gruppo e supponiamo di ave espresso G come quoziente F/K con $F = F_{\mathcal{X}}$ gruppo libero. Il Teorema 7.2.2 ci assicura che questo è sempre possibile. Si vede facilmente (Problema 7.2) che le classi degli elementi di $\mathcal{X}$ generano G. Un sottoinsieme $\mathcal{K} \subset F$ è detto costituire un *sistema completo di relazioni* per G se K è il più piccolo sottogruppo normale di F contenente $\mathcal{K}$.

Definizione 7.2.4. *Una presentazione di un gruppo G è il dato di un alfabeto $\mathcal{X}$ e di un sottoinsieme di parole $\mathcal{K} \subset F_{\mathcal{X}}$, in simboli*

$$G = \langle \mathcal{X} | \mathcal{K} \rangle,$$

tali che $G = F_{\mathcal{X}}/K$ e $\mathcal{K}$ è un sistema completo di relazioni per G.

Esempi 7.2.5.

1. Il gruppo ciclico di ordine n ammette la presentazione
$$\langle \{x\} | \{x^n\} \rangle.$$
2. Il gruppo $\mathfrak{S}_3$ è generato dalle trasposizioni (1 2) e (1 3) e quindi ammette la presentazione
$$\langle \{x, y\} | \{x^2, y^2, (xy)^3\} \rangle.$$
3. Il gruppo abeliano libero su due generatori $\mathbb{Z} \times \mathbb{Z}$ può rivedersi come quoziente del gruppo libero su 2 generatori. Le relazioni sono quelle che rendono il gruppo abeliano e pertanto una sua presentazione è
$$\langle \{x, y\} | \{xyx^{-1}y^{-1}\} \rangle.$$

Se ogni gruppo G ammette una presentazione perchè, come abbiamo visto, è quoziente di un gruppo libero, bisogna però insistere sul punto che lo stesso gruppo ammette diverse presentazioni. Una ragione per questo fatto è che non esite un insieme di generatori canonico. Ad esempio, il gruppo $\mathfrak{S}_3$ ammette come generatori anche le permutazioni (1 2) e (1 2 3) e pertanto può essere presentato anche come

$$\langle \{x, y\} | \{x^2, y^3, (xy)^2, (xy^2)^2\} \rangle.$$

Sorge quindi il problema di trovare criteri per decidere quando due presentazioni $\langle \mathcal{X} | \mathcal{K} \rangle$ e $\langle \mathcal{X}' | \mathcal{K}' \rangle$ definiscono gruppi isomorfi. Sfortunatamente questo problema è sostanzialmente impossibile da risolvere persino in casi concreti non troppo semplici.

PROBLEMI

7.1. Sia L il gruppo abeliano libero su $\mathcal{X} = \{x_1, x_2, \ldots\}$. Verificare che $\{x_1, x_2 - x_1, x_3 - x_2, \ldots\}$ è un sistema minimale di generatori per L.

7.2. Completare i dettagli della dimostrazione del Teorema 7.1.3 dimostrando in particolare che

1. L/pL e L'/pL' sono $\mathbb{Z}/p\mathbb{Z}$-spazi vettoriali,
2. se $\mathcal{X}$ è un sistema minimale di generatori per L, allora le classi degli elementi di $\mathcal{X}$ costituiscono una base di L/pL.

7.3. Supponiamo $|\mathcal{X}| \geq 2$. Dimostrare che $Z(F_{\mathcal{X}}) = \{1\}$.

7.4. Sia $G = F/K$ con $F = F_{\mathcal{X}}$ gruppo libero. Si dimostri che le classi laterali definite dagli elementi di $\mathcal{X}$ generano G.

Lezione 8

Gruppi abeliani finitamente generati

8.1 Torsione

Sia G un gruppo abeliano che denoteremo additivamente. In questa lezione l'ipotesi fondamentale che faremo su G è quella che G sia *finitamente generato*, cioè che ammetta un insieme finito di generatori o, equivalentemente, che sia quoziente di un gruppo abeliano libero di rango finito.

Se $g_1, g_2 \in G$ sono due elementi tali che $\mathrm{ord}(g_1) = n_1$, $\mathrm{ord}(g_2) = n_2$ e $\langle g_1\rangle \cap \langle g_2\rangle = \{0\}$ risulta

$$\mathrm{ord}(g_1 g_2) = n \qquad \text{dove } n = \mathrm{mcm}(n_1, n_2).$$

Infatti, per ogni $k \in \mathbb{Z}$ si ha $k(g_1 + g_2) = kg_1 + kg_2$ e non potendo mai essere $kg_1 = -kg_2$ a meno che $kg_1 = kg_2 = 0$, il più piccolo valore positivo di k per cui $k(g_1 + g_2) = 0$ è il minimo comune multiplo degli ordini di g_1 e g_2.

Esempi 8.1.1. 1. Se G non è abeliano, il prodotto di due elementi di ordine finito non ha necessariamente ordine finito. Ad esempio le matrici

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} \cos\theta & \mathrm{sen}\theta \\ \mathrm{sen}\theta & -\cos\theta \end{pmatrix}$$

hanno entrambe ordine 2 (sono delle riflessioni), ma il loro prodotto

$$BA = \begin{pmatrix} \cos\theta & -\mathrm{sen}\theta \\ \mathrm{sen}\theta & \cos\theta \end{pmatrix}$$

è una rotazione che ha ordine infinito se $\theta \notin 2\pi\mathbb{Q}$.

2. Se $\langle g_1\rangle \cap \langle g_2\rangle \neq \{0\}$ l'ordine esatto di $g_1 + g_2$ può essere minore del minimo comune multiplo degli ordini di g_1 e g_2, ma ne è comunque un divisore.

Dal fatto che il prodotto di elementi di ordine finito ha ordine finito segue che il sottoinsieme

$$G_{\mathrm{tor}} = \{g \in G \text{ tali che } \mathrm{ord}(g) \text{ è finito}\}$$

è un sottogruppo, detto *sottogruppo di torsione* di G.

Esempi 8.1.2. 1. Si ha certamente $\mathbb{Z}_{\mathrm{tor}} = \{0\}$ e, più in generale $L_{\mathrm{tor}} = \{0\}$ per ogni gruppo abeliano libero L.

2. Se G è un gruppo (abeliano) finito, si ha $G_{\text{tor}} = G$.

3. D'altra parte, se $G = G_{\text{tor}}$ non necessariamente il gruppo G è finito. Il gruppo μ_{p^∞} dell'esempio 4.2.1 è un gruppo infinito che coincide col suo sottogruppo di torsione.

Si hanno due casi estremi:

- $G_{\text{tor}} = \{0\}$, nel qual caso G è detto *privo di torsione*;
- $G_{\text{tor}} = G$, nel qual caso G è detto *gruppo di torsione*.

Il prossimo risultato deve essere interpretato alla luce degli esempi precedenti.

Proposizione 8.1.3. *Un gruppo abeliano finitamente generato e di torsione è finito.*

Dimostrazione. Sia $\{g_1, \dots, g_t\}$ un insieme di generatori di G e sia $n_i = \text{ord}(g_i)$ per $i = 1, \dots, t$. Allora ogni elemento $g \in G$ ammette un'espressione

$$g = r_1 g_1 + \cdots + r_t g_t$$

con $0 \leq r_i < n_i$ per ogni $i = 1, \dots, t$. Allora G ha al più $\prod_{i=1}^{t} n_i < \infty$ elementi. ■

Il prossimo risultato mostra come la torsione possa essere eliminata mediante un semplice passaggio al quoziente.

Proposizione 8.1.4. *Sia G un gruppo abeliano. Allora il gruppo G/G_{tor} è privo di torsione.*

Dimostrazione. Indichiamo per semplicità $\bar{g}$ il laterale $G_{\text{tor}} + g$ per $g \in G$. Se $\text{ord}(\bar{g}) = n < \infty$ in G/G_{tor} risulta $n\bar{g} = G_{\text{tor}}$, cioè $ng \in G_{\text{tor}}$. Ciò implica che esiste un $m > 0$ tale che $m(ng) = (mn)g = 0$ in G. Ma allora $g \in G_{\text{tor}}$, ovvero $\bar{g} = 0$. ■

Per poter dimostrare il risultato fondamentale di questa sezione abbiamo bisogno di un lemma tecnico preliminare.

Lemma 8.1.5. *Sia G un gruppo abeliano finitamente generato. Se esistono un insieme di generatori minimale $\{g_1, \dots, g_r\}$ per G e interi non tutti nulli $m_1, \dots, m_r$ tali che*

$$m_1 g_1 + \cdots + m_r g_r = 0,$$

allora $G_{\text{tor}} \neq \{0\}$.

Dimostrazione. Sia $\mathcal{E}$ l'insieme dei numeri interi che compaiono come coefficienti di qualche identità $m_1 x_1 + \cdots + m_s x_s = 0$ per un qualunque insieme di generatori minimale in G. Per ipotesi $\mathcal{E} \neq \{0\}$ e siccome $\mathcal{E}$ contiene l'opposto di ogni suo elemento, $\mathcal{E}$ possiede un minimo positivo che denotiamo e. Sia

$$ey_1 + e_2 y_2 + \cdots + e_t y_t$$

un identità in cui compare e. Si ha $|e_i| \geq e$ per ogni $i = 2, \dots, r$ e l'algoritmo di divisione euclidea permette di scrivere la relazione precedente come

$$e(y_1 + q_2 y_2 + \cdots + q_t y_t) + r_2 y_2 + \cdots r_t y_t$$

con $e_i = q_i e + r_i$ e $0 \leq r_i < e$ per ogni $i = 2, \dots, t$. Posto $z_1 = y_1 + q_2 y_2 + \cdots q_t y_t$, l'insieme $\{z_1, y_2, \dots, y_t\}$ è un nuovo sistema minimale di generatori in quanto

- $y_1 = z_1 - q_2 y_2 - \cdots - q_t y_t$, e

- eliminando qualunque elemento non si riottiene più y_1.

In particolare, $z_1 \neq 0$. Allora, per minimalità di e, deve essere $r_2 = \ldots = r_t = 0$ e $z_1 \in G_{\text{tor}}$. ■

vale allora il risultato seguente, che caratterizza i gruppi abeliani liberi in termini della loro torsione.

Teorema 8.1.6. *Un gruppo abeliano finitamente generato e privo di torsione è libero.*

Dimostrazione. Scegliamo un sistema minimale di generatori $\{g_1, \ldots, g_r\}$ del gruppo abeliano finitamente generato G e sia $H_i = \langle g_i \rangle$ per $i = 1, \ldots, r$. Siccome G è privo di torsione, ogni H_i è ciclico infinito, cioè isomorfo a $\mathbb{Z}$. Per costruzione, ogni $g \in G$ si esprime nella forma $g = m_1 g_1 + \cdots m_r g_r$ per un'opportuna scelta di interi $m_1, \ldots, m_r$ e quindi

$$G = H_1 + \cdots + H_r. \tag{8.1}$$

Sia $\widehat{H_i}$ il sottogruppo di G generato dagli elementi $g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_r$. Se l'intersezione $H_i \cap \widehat{H_i}$ fosse non banale, si avrebbe un elemento $y \neq 0$ che ammette la doppia espressione $y = m_i g_i = m_1 g_1 + \cdots + \ldots + m_{i-1} g_{i-1} + m_{i+1} g_{i+1} + \cdots + m_r g_r$ e quindi un'identità

$$m_1 g_1 + \cdots + \ldots + m_{i-1} g_{i-1} - m_i g_i + m_{i+1} g_{i+1} + \cdots + m_r g_r = 0$$

dove i coefficienti a sinistra non sono tutti nulli. Per il lemma precedente il gruppo G dovrebbe avere torsione, ma siccome così non è, deve essere

$$H_i \cap \widehat{H_i} = \{0\}. \tag{8.2}$$

Per la generalizzazione del Teorema 4.1.7 al caso di un mumero arbitrario ma finito di sottogruppi, le 8.1 e 8.2 implicano subito che $G \simeq H_1 \times \cdots H_r$. ■

8.2 Teoremi di struttura

Il nostro obiettivo è ora quello di determinare la struttura di un gruppo abeliano finitamente generato. Al risultato finale si arriverà per gradi. Iniziamo con lo studiare i sottogruppi di un gruppo abeliano libero finitamente generato.

Teorema 8.2.1. *Sia G un gruppo abeliano libero finitamente generato di rango n e sia $H < G$. Allora H è libero di rango $m \leq n$.*

Dimostrazione. Procediamo per induzione su n. Se $n = 1$ è $G \simeq \mathbb{Z}$ e dall'analisi dei sottogruppi di $\mathbb{Z}$ fatta nell'esempio 1.2.3(3) sappiamo che o $H = \{0\}$, o H è un sottogruppo ciclico (infinito) generato da un elemento di G. In ogni caso l'asserto del Teorema è verificato.

Supponiamo dunque $n > 1$ e fissiamo un sistema minimale di generatori $\{g_1, \ldots, g_n\}$ di G. Se risulta $H < G' = \{g_1, \ldots, g_{n-1}\}$, H è un sottogruppo di un gruppo libero di rango $n-1$ e possiamo applicare direttamente l'ipotesi induttiva. Eliminato questo caso, possiamo allora assumere che esiste un elemento $h \in H$ della forma

$$h = m_1 g_1 + \ldots + m_n g_n, \qquad m_n \neq 0.$$

Stiamo dunque assumendo che l'insieme $\mathcal{E}$ dei numeri interi che compaiono come coefficiente di g_n nelle espressioni degli elementi di H non è banale. Siccome H contiene gli opposti dei suoi

elementi, la medesima cosa succede per $\mathcal{E}$ e quindi resta individuato il minimo postivo s di $\mathcal{E}$. Fissiamo

$$\ell = m_1 g_1 + \ldots + m_{n-1} g_{n-1} + s g_n \in H.$$

Per ogni $h = m_1 g_1 + \ldots + m_n g_n \in H$, posto $m_n = qs + r$ con $0 \leq r < s$ si ha $h - q\ell = \ldots + r g_n \in H$ e quindi, per la minimalità di r, $h - q\ell \in H' < G'$ dove abbiamo posto $H' = H \cap G'$.

Consideriamo ora il gruppo $H' + \langle \ell \rangle$. Evidentemente $H' + \langle \ell \rangle < H$, e siccome ogni $h \in H$ può scriversi come $h = (h - q\ell) + q\ell$ vale anche l'inclusione opposta e in definitiva $H = H' + \langle \ell \rangle$. Per ipotesi induttiva, H' è libero di rango $m - 1 \leq \mathrm{rg}(G') = n - 1$ e scegliamone un sistema minimale di generatori $\{\ell_1, \ldots, \ell_{m-1}\}$. Allora H è generato da $\{\ell_1, \ldots, \ell_{m-1}, \ell\}$. Una relazione $a_1 \ell_1 + \ldots + a_{m-1} \ell_{m-1} + a\ell = 0$ riscritta in termini dei generatori $g_1, \ldots, g_n$ diventa

$$b_1 g_1 + \ldots + b_{n-1} g_{n-1} + a g_n = 0$$

perchè g_n non interviene nei ℓ_i e quindi dapprima $a = 0$ e poi allora anche $a_1 = \ldots = a_{m-1} = 0$. Pertanto H è libero di rango m. ■

Corollario 8.2.2. *Sia G un gruppo abeliano finitamente generato e sia $H < G$. Allora H è finitamente generato.*

Dimostrazione. siccome G è finitamente generato, G è quoziente di un gruppo abeliano libero L di rango finito. Denotiamo $\pi : L \to G$ la mappa quoziente. Allora $\pi^{-1}(H)$ è un sottogruppo di L che per il teorema precedente deve essere libero di rango finito. Se $h_1, \ldots, h_t$ sono generatori di $\pi^{-1}(H)$ gli elementi $\pi(h_1), \ldots, \pi(h_t)$ sono ovviamente dei generatori di H. ■

Nell'altra situazione estrema, in cui il gruppo abeliano in questione è finito, si ha il teorema di struttura seguente.

Teorema 8.2.3. *Sia G un gruppo abeliano finito con n elementi. Allora G è isomorfo ad un prodotto $C_1 \times \ldots \times C_t$ dove ciascun C_i è un sottogruppo ciclico di G e se indichiamo e_i l'ordine di C_i si ha*

1. *$e_{i+1} | e_i$ per ogni $i = 1, 2, \ldots, t-1$;*
2. *$\prod_{i=1}^{t} e_i = n$;*
3. *gli e_i sono univocamente determinati dalle due condizioni precedenti.*

Dimostrazione. Iniziamo la dimostrazione osservando che se $x \in G$ è un elemento di ordine massimo, allora l'ordine di ogni altro elemento $y \in G$ divide l'ordine di x. Infatti, se così non fosse, per un qualche primo p risulterebbe $\mathrm{ord}(y) = p^h r$ e $\mathrm{ord}(x) = p^k s$ con $h > k$ e $(p, rs) = 1$. Allora $\mathrm{ord}(p^k x) = s$ e $\mathrm{ord}(ry) = p^h$ sono coprimi e pertanto $\mathrm{ord}(p^k x + ry) = p^h s > \mathrm{ord}(x)$ contraddicendo la massimalità di $\mathrm{ord}(x)$.

Se poi $H = \langle x \rangle$ è il sottogruppo ciclico generato da un elemento di ordine massimo, ogni laterale $H + y$, $y \in G$, contiene un elemento di ordine uguale all'ordine di $H + x$ in G/H. Infatti, se $m = \mathrm{ord}(H + y)$ deve essere $my \in H$ e quindi $my = tx$ per un certo t. Allora $\mathrm{ord}(my) = h/d$ dove $h = \mathrm{ord}(x)$ e $d = (h, t)$. Se $\mathrm{ord}(y) = s$ si ha da una parte $s = mq$ e dall'altra $s | m(h/d)$. Ma siccome h/d divide q (perchè $q(my) = 1$) si ha anche $m(h/d) | s$ e quindi in definitiva $s = m(h/d)$. Per quanto detto prima $s | h$, cioè $m(h/d) | h$ e quindi $m = dk$. Posto $u = t/d$ si ha dunque $my = (mku)x$ e posto $z = y - (ku)x$ risulta $z \in H + y$ e $mz = 1$. Infine non può essere $\mathrm{ord}(z) < m$ altrimenti si avrebbe anche $\mathrm{ord}(H + y) < m$.

Possiamo ora procedere per induzione su n, il caso $n = 1$ essendo ovvio.

Assumiamo allora $n > 1$ e scegliamo in G un elemento g_1 di ordine massimo $e_1 > 1$ e poniamo $C_1 = \langle g_1 \rangle$. Il gruppo quoziente G/C_1 ha $n/e_1 < n$ elementi e quindi, per ipotesi induttiva, si decompone come

$$G/C_1 \simeq \langle C_1 + g_2 \rangle \times \ldots \times \langle C_1 + g_t \rangle$$

dove gli ordini dei sottogruppi soddisfano le proprietà di divisibilità enunciate dal teorema. Per quanto detto precedentemente, possiamo assumere $\mathrm{ord}(g_i) = e_i$ per $i = 2, \ldots, t$ e $e_2 = \mathrm{ord}(g_2)|e_1$. Per ogni $g \in G$ si ha una decomposizione di laterali

$$C_1 g = h_2(C_1 g_2) + \cdots + h_t(C_1 g_t) = C_1 + (h_2 g_2 + \cdots + h_t g_t),$$

quindi $g = h_1 g_1 + h_2 g_2 + \cdots + h_t g_t$. Ciò implica che $G = C_1 + \langle g_2 \rangle + \cdots + \langle g_t \rangle$ e siccome $|G| = |C_1|\,|\langle g_2 \rangle| \cdots |\langle g_t \rangle|$ deve risultare $G = C_1 \times C_2 \times \cdots \times C_t$ dove $C_t = \langle g_t \rangle$. Questo dimostra i punti 1 e 2 del teorema.

Per dimostrare che i valori e_i sono univocamente determinati supponiamo di avere due decomposizioni

$$G \simeq C_1 \times \cdots \times C_t \simeq D_1 \times \cdots \times D_s \tag{8.3}$$

dove $D_i = \langle h_i \rangle$ è ciclico di ordine f_i e tali valori soddisfano anch'essi i punti 1 e 2 del teorema. Si osservi che $f_1 = e_1$ perchè è, in ogni caso, il massimo ordine degli elementi di G. Per assurdo supponiamo $\{e_1, \ldots, e_t\} \neq \{f_1, \ldots, f_s\}$ e sia k il minimo indice tale che $e_k \neq f_k$. Senza perdere in generalità, possiamo assumere $e_k > f_k$.

Consideriamo allora $f_k G$, il sottogruppo di G costituito dagli elementi che sono multipli f_k-esimi in G. Dalla prima decomposizione in (8.3) si ha

$$f_k G = \langle f_k g_1 \rangle \times \cdots \times \langle f_k g_k \rangle \times \cdots \times \langle f_k g_\ell \rangle,$$

dove $e_\ell > f_k \geq e_{\ell+1}$, e dalla seconda decomposizione in (8.3) si ha

$$f_k G = \langle f_k h_1 \rangle \times \cdots \times \langle f_k h_{k-1} \rangle.$$

Siccome per $j < k$ si ha $\mathrm{ord}(f_k h_j) = f_j/f_k$, quest'ultima scrittura per $f_k G$ permette di valutare

$$|f_k G| = \frac{f_1}{f_k} \cdots \frac{f_{k-1}}{f_k} = \frac{e_1 \cdots e_{k-1}}{f_k^{k-1}}$$

mentre dalla precedente si ottiene

$$|f_k G| \geq \frac{e_1 \cdots e_{k-1}}{f_k^{k-1}} \frac{e_k}{(e_k, f_k)} > \frac{e_1 \cdots e_{k-1}}{f_k^{k-1}}$$

che è un'evidente contraddizione. Questo completa la dimostrazione del teorema. ■

Nel caso generale, otteniamo il seguente teorema di struttura.

Teorema 8.2.4. *Sia G un gruppo abeliano finitamente generato. Allora G è isomorfo ad un prodotto $F \times T$ dove F è un gruppo abeliano libero di rango finito e T è un gruppo abeliano finito.*

Dimostrazione. Poniamo $T = G_{\mathrm{tor}}$. Dal Corollario 8.2.2 sappiamo che T è finitamente generato, e quindi finito per la Proposizione 8.1.3.

Consideriamo il quoziente G/T ed osserviamo che $(G/T)_{\mathrm{tor}} = \{1\}$ in quanto se esistesse $g \in G$ col laterale $T + g$ elemento di ordine finito in G/T, per la commutatività di G si avrebbe $m(Tg) = T + mg = T$ per un opportuno $m > 0$. Ma allora $mg \in T$ e quindi $g \in T$, cioè $T + g = T$.

Per il Teorema 8.1.6 il quoziente G/T è libero e possiamo trovare elementi $g_1, \ldots, g_s \in G$ (s minimo) tali che

$$G/T = \langle T + g_1 \rangle + \cdots + \langle T + g_s \rangle.$$

Sia $F = \langle g_1, \ldots, g_s \rangle < G$. Il sottogruppo F è privo di torsione, in quanto se risultasse $t = m_1 g_1 + \cdots + m_s g_s \in T$ per qualche scelta non banale di coefficienti $m_1, \ldots, m_s$, allora risulterebbe $m_1(T + g_1) + \cdots + m_s(T + g_s) = T$ in G/T e per il Lemma 8.1.5 il quoziente G/T non potrebbe essere privo di torsione.

Per ogni $g \in G$, per le posizioni fatte, si ha una scrittura $T + g = m_1(T + g_1) + \cdots + m_s(T + g_s) = T + (m_1 g_1 + \cdots + m_s g_s)$ in G/T che riletta in G fornisce una decomposizione $G = T + F$.

Abbiamo così controllato che i sottogruppi T ed F soddisfano le condizioni affinchè G risulti il loro prodotto diretto (vedi il Teorema 4.1.7 e la discussione che lo precede). ∎

Concludiamo questa sezione mostrando come combinando i risultati sin qui ottenuti possiamo migliorare il risultato iniziale sui sottogruppi di un gruppo libero. Il risultato che otterremo ora deve essere visto come una generalizzazione nell'ambito dei gruppi abeliani liberi della ben nota proprietà degli spazi vettoriali per cui una base di uno sottospazio può essere completata ad una base dello spazio.

Teorema 8.2.5 (dei divisori principali)**.** *Sia F un gruppo abeliano libero di rango n e sia H un sottogruppo di F. Allora esistono un insieme minimali di generatori $\{u_1, \ldots, u_n\}$ di F e numeri interi $e_1, \ldots . e_m$, $m \leq n$ tali che*

1. *e_{i+1} divide e_i per ogni $i = 1, 2, \ldots, m-1$;*
2. *$\{e_1 u_1, \ldots, e_m u_m\}$ è un sistema minimale di generatori di H.*

Dimostrazione. Dal teorema 8.2.1 sappiamo che H è libero e dal teorema 8.2.4 sappiamo che il quoziente F/H, che è sicuramente abeliano e finitamente generato è isomorfo ad un prodotto $L \times T$ dove L è abeliano libero e T è finito. Di fatto $T = (F/H)_{\mathrm{tor}}$.

Denotando ancora una volta $\bar{f}$ il laterale $H + f$ di un elemento $f \in F$, possiamo trovare elementi $\ell_1, \ldots, \ell_r, t_1, \ldots, t_s$ di F tali che

$$L = \bigoplus_{i=1}^{r} \mathbb{Z}\bar{\ell}_i, \qquad T = \langle \bar{t}_1 \rangle \times \cdots \times \langle \bar{t}_s \rangle$$

dove i periodi $e_i = \mathrm{ord}(\bar{t}_i)$ soddisfano le proprietà enunciate nel teorema 8.2.3. Poniamo

$$L' = \langle \ell_1, \ldots, \ell_r \rangle, \qquad T' = \langle t_1, \ldots, t_s \rangle$$

(sottogruppi di F). Si noti in particolare che L' e T' sono liberi. Se $\pi : F \to F/H$ è la mappa quoziente si ha una decomposizione

$$F = L' \times \pi^{-1}(T).$$

Infatti la condizione $L' \cap \pi^{-1}(T)$ è palesemente soddisfatta, mentre per ogni $f \in F$ l'esistenza di una scrittura $\bar{f} = m_1 \bar{\ell}_1 + \ldots + m_r \bar{\ell}_r + \bar{t}$ con $\bar{t} \in T$ implica che $f - (m_1 \ell_1 + \ldots + m_r \ell_r) \in \pi^{-1}(T)$, quindi provando che $F = L' + \pi^{-1}(T)$.

Per la proposizione 7.1.6 esiste un omomorfismo $\phi : \pi^{-1}(T) \to T'$ tale che la composizione

$$\pi^{-1}(T) \xrightarrow{\phi} T' \xrightarrow{\pi_{|T'}} T$$

è la mappa quoziente canonica. Poniamo $K = \ker(\phi)$. Si noti che $K \subseteq H$. Risulta $K \cap T' = \{0\}$ per ragioni ovvie e, con ragionamento simile a quello fatto più sopra, $\pi^{-1}(T) = K + T'$. Dunque

$\pi^{-1}(T) = K \times T'$ ed in particolare $H = (H \cap K) \times T'$. Siccome $K/H \cap K$ è libero (in quanto privo di torsione) possiamo scegliere un sistema minimo di generatori $\{k_1, \ldots, k_t\}$ del gruppo abeliano libero K in modo che $H \cap K = \langle k_1, \ldots, k_h \rangle$ con $0 \leq h \leq t$. In definitiva, otteniamo una scrittura

$$F = \mathbb{Z}\ell_1 \times \cdots \times \mathbb{Z}\ell_r \times \mathbb{Z}k_1 \times \cdots \times \mathbb{Z}k_t \times \mathbb{Z}t_1 \times \cdots \times \mathbb{Z}t_s$$

tale che

$$H = \mathbb{Z}k_1 \times \cdots \times \mathbb{Z}k_h \times \mathbb{Z}e_1t_1 \times \cdots \times \mathbb{Z}e_st_s.$$

Il teorema è dunque dimostrato. ■

8.3 Reticoli

Studieremo ora una classe notevole di gruppi abeliani che risulteranno finitamente generati (e, di fatto, liberi). Iniziamo osservando che la struttura di gruppo dello spazio euclieo $\mathbb{R}^n$ è compatibile con la struttura metrica nel senso che le funzioni addizione e passaggio all'opposto

$$x + y \mapsto x + y, \qquad x \mapsto -x$$

sono continue. Ne segue che per ogni $x \in \mathbb{R}^n$ le traslazioni $\Phi_x : \mathbb{R}^n \to \mathbb{R}^n$, $\Phi_x(y) = x + y$ sono omeomorfismi in quanto funzioni continue, perchè restrizioni di una funzione continua, con inversa continua.

Un sottogruppo $\Lambda < \mathbb{R}^n$ si dice *discreto* se è discreto come sottospazio dello spazio metrico $\mathbb{R}^n$, cioè se per ogni $\lambda \in \Lambda$ è possibile trovare $\epsilon > 0$ tale che λ è l'unico elemnto di Λ nella sfera aperta $S(\lambda, \epsilon)$ di centro λ e raggio ϵ. Vale la caratterizzazione seguente.

Lemma 8.3.1. *Sia $\Lambda < \mathbb{R}^n$ un sottogruppo. Le seguenti affermazioni sono equivalenti.*

1. *Λ è discreto.*
2. *Per ogni sottoinsieme compatto $K \subset \mathbb{R}^n$ l'intersezione $\Lambda \cap K$ consiste di un numero finito di elementi.*
3. *Esiste un $\epsilon > 0$ tale che $S(0, \epsilon) \cap \Lambda = \{0\}$.*

Dimostrazione. L'equivalenza tra i primi due punti è una ben nota caratterizzazione dei sottospazi discreti di $\mathbb{R}^n$.

L'implicazione $1 \Rightarrow 3$ è parte della definizione, e quindi resta da far vedere solo l'implicazione inversa. Sia dunque $\lambda \in \Lambda$ e sia $S(0, \epsilon) \cap \Lambda = \{0\}$. Allora $\Phi_\lambda(S(0, \epsilon)) = S(\lambda, \epsilon)$ e chiaramente $S(0, \epsilon) \cap \Lambda = \{\lambda\}$. ■

Esempi 8.3.2.

1. Il prototipo dei sottogruppi discreti di $\mathbb{R}^n$ è il gruppo $\mathbb{Z}^n$ dei vettori che hanno componenti intere rispetto alla base canonica di $\mathbb{R}^n$. Si noti che $\mathbb{Z}^n$ è libero.
2. Supponiamo $n = 1$ e sia $\Lambda < \mathbb{R}$ un sottogruppo discreto non nullo. Siccome Λ contiene gli opposti dei suoi elementi ed è discreto, deve esistere in Λ un minimo positivo λ_0. Siccome $\mathbb{R}$ è privo di torsione, $\mathbb{Z}\lambda_0 < \Lambda$. Supponiamo esista $x \in \Lambda - \mathbb{Z}\lambda_0$. A meno di sostituire x con il suo opposto e per la minimalità di λ_0 deve esistere un intero n tale che $n\lambda_0 < x < (n+1)\lambda_0$. Ma allora $0 < x - n\lambda_0 < \lambda_0$ contraddice la minimalità di λ_0. Si vede così che Λ è libero di rango 1.

L'obiettivo principale di questa sezione è quello di mostrare come, in un certo senso, la situazione generale non sia dissimile da quella dell'esempio appena fatto.

Teorema 8.3.3. *Sia Λ un sottogruppo discreto di $\mathbb{R}^n$. Allora esistono $r \leq n$ vettori linearmente indipendenti $x_1, \ldots, x_r$ tali che*

$$\Lambda = \bigoplus_{i=1}^{r} \mathbb{Z} x_i.$$

Dimostrazione. Sia $\{y_1, \ldots, y_r\}$ un insieme massimale di vettori $\mathbb{R}$-linearmente indipendenti in Λ e consideriamo il sottoinsieme $\mathcal{P}$ dei vettori $x \in \mathbb{R}^n$ che ammettono una scrittura

$$x = \alpha_1 y_1 + \ldots + \alpha_r y_r$$

con $0 \leq \alpha_i \leq 1$ per ogni $i = 1, \ldots, r$. L'insieme $\mathcal{P}$ è chiuso e limitato e dunque è compatto. Pertanto $\mathcal{P} \cap \Lambda$ è finito.

Per la massimalità di $\{y_1, \ldots, y_r\}$, ogni elemento $\lambda \in \Lambda$ può scriversi come combinazione lineare $\lambda = a_1 y_1 + \cdots + a_r y_r$ a coefficienti $a_i \in \mathbb{R}$. Fissato un tale elemento λ consideriamo la successione $\{\lambda_n\}$ definita da

$$\lambda_n = n\lambda - \sum_{i=1}^{r} [na_i] y_i = \sum_{i=1}^{r} (na_i - [na_i]) y_i.$$

Siccome $0 \leq na_i - [na_i] \leq 1$, la successione è in $\mathcal{P} \cap \Lambda$. Per la finitezza di $\mathcal{P} \cap \Lambda$ otteniamo allora che:

1. Λ è finitamente generato, in quanto potendo scrivere $\lambda = \lambda_1 + \sum_{i=1}^{r} [a_i] y_i$ si vede che ogni elemento è combinazione lineare a coefficienti interi degli y_i e di $\mathcal{P} \cap \Lambda$;
2. devono esistere interi $m \neq n$ tali che $\lambda_m = \lambda_n$. In particolare otteniamo l'uguaglianza $(m-n)a_i = [ma_i] - [na_i]$ per ogni coefficiente a_i e quindi $a_i \in \mathbb{Q}$.

Dunque Λ è un gruppo abeliano libero generato da un numero finito di vettori che sono combinazioni lineari degli y_i a coefficienti razionali. Sia M un multiplo comune dei denominatori che compaiono tra i coefficienti dei generatori di Λ. Posto $\Lambda' = M\Lambda$ risulta

$$\Lambda' < \bigoplus_{i=1}^{r} \mathbb{Z} y_i \tag{8.4}$$

e quindi Λ' è un gruppo abeliano libero di rango $\leq r$ per il teorema 8.2.1. D'altra parte la moltiplicazione per M definisce un isomorfismo $\Lambda \xrightarrow{\sim} \Lambda'$ e quindi $\mathrm{rg}(\Lambda') = \mathrm{rg}(\Lambda) \geq r$ dove l'ultima disuguaglianza segue dall'inclusione $\bigoplus_{i=1}^{r} \mathbb{Z} y_i < \Lambda$. Dal confronto delle disuguaglianze segue che $\mathrm{rg}(\Lambda) = r$. Dunque, ritornando alla (8.4) e applicando il Teorema dei divisori principali 8.2.5 si vede che esiste un sistema di generatori $\{y'_1, \ldots, y'_r\}$ e numeri interi $e_1, \ldots, e_r$ (le cui proprietà di divisibilità sono qui irrilevanti) tali che i vettori $x_i = \frac{e_i}{M} y'_i$ formano un insieme minimale di generatori per Λ. Siccome i vettori y_i sono linearmente indipendenti su $\mathbb{R}$, anche gli x_i devono esserlo. ■

Definizione 8.3.4. *Un reticolo è un sottogruppo discreto $\Lambda < \mathbb{R}^n$ tale che* $\mathrm{rg}(\Lambda) = n$.

Risulta chiaro dal teorema 8.3.3 che i reticoli in $\mathbb{R}^n$ sono esattamente i gruppi abeliani liberi generati dalle basi di $\mathbb{R}^n$. D'altra parte, assegnate due basi $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_n\}$ di $\mathbb{R}^n$ i corrispondenti reticoli concidono se e soltanto se esiste una matrice $M \in \mathrm{SL}_n(\mathbb{Z})$ che trasforma una base nell'altra. Questo segue subito dall'osservazione che si ha coincidenza dei reticoli esattamente quando ogni elemento di una base si può scrivere come combinazione lineare a coefficienti in $\mathbb{Z}$ dell'altra.

La proposizione seguente generalizza l'esempio 3.4.2

Proposizione 8.3.5. *Sia $\Lambda < \mathbb{R}^n$ un reticolo. Allora*

$$\frac{\mathbb{R}}{\Lambda} \simeq \underbrace{S^1 \times \cdots \times S^1}_{n \text{ copie}}.$$

Dimostrazione. Sia $\{x_1, \ldots, x_n\}$ una base di $\mathbb{R}_n$ tale che $\Lambda = \bigoplus_{i=1}^n \mathbb{Z}x_i$. Siccome è anche $\mathbb{R}^n = \bigoplus_{i=1}^n \mathbb{R}x_i$ risulta subito $\mathbb{R}^n/\Lambda = \bigoplus_{i=1}^n (\mathbb{R}x_i/\mathbb{Z}x_i) \simeq \bigoplus_{i=1}^n (\mathbb{R}/\mathbb{Z})$. ■

Ricordando che si ha un'identificazione $\mathbb{C}^n \simeq \mathbb{R}^{2n}$, un reticolo in C^n è il gruppo abeliano libero generato da una $2n$-pla di vettori linearmente $\mathbb{R}$-indipendenti di $\mathbb{C}^n$. La presenza di una struttura complessa ha delle implicazioni notevolissime per la geometria del quoziente $\mathbb{C}^n/\Lambda$ la cui analisi va ben oltre gli scopi ed i limiti di queste lezioni. Per una discussione dettagliata dell'esempio seguente si veda [**?**]

Esempio 8.3.6 (Weierstrass)**.** Sia $\Lambda < \mathbb{C}$ un reticolo e consideriamo la funzione di variabile complessa

$$\wp(z) = \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right),$$

detta funzione $\wp$ di Weierstrass. La funzione $\wp(z)$ converge ad una funzione meromorfa su $\mathbb{C}$ con poli di ordine 2 e residuo nullo nei punti di Λ e soddisfa la relazione funzionale

$$\wp(z+\lambda) = \wp(z) \qquad \text{per ogni } \lambda \in \Lambda.$$

Insieme alla sua derivata $\wp'(z)$ la funzione $\wp$ di Weierstrass soddisfa l'identità

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

dove $g_2 = g_{2,\Lambda} = 60G_{4,\Lambda}$, $g_3 = g_{3,\Lambda} = 140G_{6,\Lambda}$ e $G_{2k,\Lambda} = \sum_{\lambda \in \Lambda - \{0\}} \lambda^{-2k}$ è la cosiddetta serie di Eisenstein di peso $2k$. Dunque, la funzione $z \mapsto [\wp(z) : \wp'(z) : 1]$ identifica il quoziente $\mathbb{C}/\Lambda$ con la cubica proiettiva piana E_Λ di equazione

$$y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3 \tag{8.5}$$

Si osserva che:

1. la cubica E_Λ è priva di punti singolari in quanto il suo discriminante $g_2^3 - 27g_3^2$ risulta essere sempre non nullo. Inoltre ogni cubica non singolare E può essere trasformata mediante un opportuno cambiamento di coordinate proiettive in una cubica di equazione (8.5). In altre parole, al variare di Λ tra i reticoli di $\mathbb{C}$ le cubiche E_Λ esauriscono le classi di isomorfismo di cubiche proiettive piane.

2. L'identificazione $\mathbb{C}/\Lambda \simeq E_\Lambda$ permette di trasportare la struttura di gruppo da $\mathbb{C}/\Lambda$ alla cubica. Tale struttura di gruppo sulla cubica è caratterizzata dal fatto che tre punti $P, Q, R \in E_\Lambda$ sono allineati se e soltanto se $P + Q + R = 0$.

PROBLEMI

8.1. Si dimostri l'affermazione fatta nell'esempio 8.1.1(2).

8.2. Sia $f : G \to H$ un omomorfismo di gruppi. Dimostrare che f definisce, per restrizione un omomorfismo $f_{\text{tor}} : G_{\text{tor}} \to H_{\text{tor}}$ e dire se le seguenti affermazioni sono vere o false.

1. f iniettiva $\Rightarrow f_{\mathrm{tor}}$ iniettiva;
2. f suriettiva $\Rightarrow f_{\mathrm{tor}}$ suriettiva;

8.3. Sia $G = L \times H$ dove L è un gruppo abeliano libero e H è un gruppo abeliano tale che $H_{\mathrm{tor}} = H$. Dimostrare che $G_{\mathrm{tor}} = H$ e che $G/G_{\mathrm{tor}} \simeq L$.

8.4. Sia G un gruppo non abeliano e supponiamo che l'insieme G_{tor} degli elementi di ordine finito sia un sottogruppo. Allora si dimostri che G_{tor} è un sottogruppo normale e che il quoziente G/G_{tor} è privo di torsione.

8.5. Siano p e q due primi distinti. Spiegare perchè l'identità $p\frac{1}{p} - q\frac{1}{q} = 0$ mostra che il gruppo additivo $\mathbb{Q}$ non è libero. Far discendere da questo fatto che $\mathbb{Q}$ non è finitamente generato.

Lezione 9

Estensioni, I

9.1 Prodotto semidiretto

Riconsideriamo il gruppo diedrale D_n introdotto nell'Esempio 1.2.3.7. Il sottogruppo C_n delle rotazioni è ciclico di ordine n generato dalla rotazione r di $2\pi/n$ radianti e quindi normale. Se S è il sottogruppo di D_n di ordine 2 generato dalla simmetria s risulta

$$D_n = C_n S, \qquad C_n \cap S = \{1\}$$

e anche $D_n/C_n \simeq S$, ma D_n non è isomorfo al prodotto $C_n \times S$ (ad esempio perché quest'ultimo è abeliano mentre D_n non lo è). Questo esempio mostra che è possibile avere due gruppi non isomorfi G e G' con sottogruppi normali $K < G$, $K' < G'$ in modo che risulti

$$K \simeq K', \qquad G/K \simeq G'/K'.$$

Sorge quindi spontaneo il problema di classificare i gruppi G che possiedono un sottogruppo normale isomorfo al gruppo K con quoziente G/K isomorfo al gruppo H, per H e K gruppi assegnati.

Definizione 9.1.1. *Il gruppo G è detto* prodotto semidiretto del sottogruppo K mediante il sottogruppo H *se*

1. $G = KH$;
2. K *è normale in* G;
3. $K \cap H = \{1\}$.

Esempi 9.1.2.

1. Per quanto detto sopra, il gruppo diedrale D_n è prodotto semidiretto del gruppo delle rotazioni mediante il sottogruppo S generato da una simmetria.
2. Sia $\tau \in \mathfrak{S}_n$ una trasposizione qualunque e sia $T < \mathfrak{S}_n$ il sottogruppo di ordine 2 da essa generato. Dalla decomposizione in laterali $\mathfrak{S}_n = A_n \cup A_n\tau$ segue che $\mathfrak{S}_n = A_nT$ e $\mathfrak{S}_n$ è prodotto semidiretto di A_n mediante T.
3. Sia $\mathrm{GL}_2(\mathbb{R})^+$ il sottogruppo delle matrici in $\mathrm{GL}_2(\mathbb{R})$ a determinante positivo e sia $U < \mathrm{GL}_2(\mathbb{R})$ il sottogruppo di ordine 2 generato dalla matrice $u = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Poiché
$$\mathrm{GL}_2(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})^+ \cup \mathrm{GL}_2(\mathbb{R})^+ \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$$
risulta $\mathrm{GL}_2(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})^+U$ e $\mathrm{GL}_2(\mathbb{R})$ è prodotto semidiretto di $\mathrm{GL}_2(\mathbb{R})^+$ mediante U.

Se G è prodotto semidiretto di K mediante H, l'applicazione $Kh \mapsto h$ definisce un omomorfismo $G/K \to H$ in quanto, per normalità di K, $(Kh)(Kh') = Khh'$. Tale omomorfismo è evidentemenete suriettivo ed è anche iniettivo perché ha nucleo banale. Quindi

$$G/K \simeq H.$$

Si osservi che in $G = KH$ si ha anche

$$(kh)(k'h') = k(hkh^{-1})hh',$$

cioè, la moltiplicazione in G è completamente determinata dalla decomposizione $G = KH$ e dall'azione di coniugio di H su K, che possiamo rivedere come un particolare omomorfismo

$$\varphi\colon H \longrightarrow \mathrm{Aut}(K),$$

detto *omomorfismo strutturale* del prodotto semidiretto.

Esempi 9.1.3. 1. Nel caso del gruppo diedrale D_n, l'omomorfismo strutturale $\varphi\colon S \to \mathrm{Aut}(C_n)$ è quello per cui $\varphi(s)(r) = r^{-1}$.

2. Nel caso del gruppo $\mathrm{GL}_2(\mathbb{R})$ dell'esempio 3 sopra, l'omomorfismo strutturale $\varphi\colon U \to \mathrm{Aut}(\mathrm{GL}_2(\mathbb{R})^+)$ è
$$\varphi\left(\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)\right) = \left(\left(\begin{smallmatrix} a & -c \\ -b & d \end{smallmatrix}\right)\right).$$

Viceversa, supponiamo assegnati gruppi H e K ed un omomorfismo $\varphi\colon H \to \mathrm{Aut}(K)$. Nell'insieme prodotto $K \times H$ consideriamo l'operazione

$$(k, h) \cdot (k', h') = (k\varphi(h)(k'), hh'). \tag{9.1}$$

Osserviamo che:

1. L'operazione è associativa, infatti

   $$((k, h) \cdot (k', h')) \cdot (k'', h'') = (k\varphi(h)(k'), hh') \cdot (k'', h'') = (k\varphi(h)(k')\varphi(hh')(k''), hh'h'')$$

   e

   $$(k, h) \cdot ((k', h') \cdot (k'', h'')) = (k, h) \cdot (k'\varphi(h')(k''), h'h'') = (k\varphi(h)(k'\varphi(h')(k'')), hh'h'')$$

   ed è chiaro che le due espressioni finali coincidono;

2. l'elemento $(1, 1)$ è neutro per l'operazione 9.1, come si verifica subito;

3. per ogni $(k, h) \in K \times H$ si ha

   $$(k, h) \cdot (\varphi(h^{-1})(k^{-1}), h^{-1}) = (\varphi(h^{-1})(k^{-1}), h^{-1}) \cdot (k, h) = (1, 1).$$

Pertanto l'operazione (9.1) definisce sull'insieme $K \times H$ una struttura di gruppo che denotiamo

$$K \times_\varphi H.$$

Osservazione 9.1.4. Come gruppo $K \times_\varphi H$ non è, in generale, isomorfo al prodotto diretto $K \times H$ (ad esempio, anche se K ed H sono abeliani non è detto che $K \times_\varphi H$ lo sia). Il prodotto diretto $K \times H$ si riottiene come caso particolare di questa costruzione per φ omomorfismo costante, cioè $\varphi(h) = \mathrm{id}_K$ per ogni $h \in H$.

Il risultato seguente può essere visto, anche alla luce dell'osservazione precedente, come un analogo della coincidenza tra prodotto diretto esterno ed interno (teorema 4.1.7).

Teorema 9.1.5. *Siano H e K gruppi e sia assegnato un omomorfismo $\varphi\colon H \to \mathrm{Aut}(K)$. Allora esistono*

1. *un sottogruppo normale K^* in $K \times_\varphi H$ con un isomorfismo $\alpha : K \to K^*$,*
2. *un sottogruppo H^* in $K \times_\varphi H$ con un isomorfismo $\beta : H \to H^*$,*

tali che $K \times_\varphi H$ è prodotto semidiretto di K^* mediante H^* con l'omomorfismo strutturale $\varphi^* : H^* \to \mathrm{Aut}(K^*)$ tale che

$$\varphi(h^*) = \alpha \circ \varphi(\beta^{-1}(h^*)) \circ \alpha^{-1}, \qquad \text{per ogni } h^* \in H^*.$$

Dimostrazione. Poniamo $K^* = \{(k,1) \,|\, k \in K\}$ e $H^* = \{(1,h) \,|\, h \in H\}$. Dal calcolo degli inversi fatto sopra risulta $(k,1)^{-1} = (k^{-1},1)$ e $(1,h)^{-1} = (1,h^{-1})$, quindi

$$(k,1)(k',1)^{-1} = (k(k')^{-1},1) \qquad \text{e} \qquad (1,h)(1,h')^{-1} = (1,h(h')^{-1})$$

da cui risulta subito che K^* e H^* sono sottogruppi di $K \times_\varphi H$ e che le applicazioni $\alpha(k) = (k,1)$ e $\beta(h) = (1,h)$ sono isomorfismi di K in K^* e di H in H^* rispettivamente. Inoltre K^* è normale perché è il nucleo dell'omomorfismo suriettivo

$$K \times_\varphi H \longrightarrow H, \qquad (k,h) \mapsto h$$

Osserviamo anche che l'identità $(k,h) = (k,1)\cdot(1,h)$ comporta che $K \times_\varphi H = K^*H^*$ e ovviamente $K^* \cap H^* = \{(1,1)\}$. Dunque $K \times_\varphi H$ è prodotto semidiretto di K^* mediante H^*.

Resta solo da determinare l'omomorfismo strutturale. Ricordando che l'omomorfismo strutturale si ottiene dall'azione per coniugio di H^* su K^*, per concludere basta osservare che

$$(1,h)\cdot(k,1)\cdot(1,h^{-1}) = (\varphi(h)(k),1)$$

ed applicare le identificazioni α e β definite sopra. ■

Se il teorema rende evidente ul fatto che un elemento g del prodotto semidiretto $G = KH$ si decompone in modo unico come $g = kh$ con $k \in K$ e $h \in H$ e altresì chiaro che la scelta del sottogruppo H per scrivere la decomposizione non è unica.

Definizione 9.1.6. Un complemento di K in $K \times_\varphi H$ è un sottogruppo H' di $K \times_\varphi H$ tale che $K \times_\varphi H$ è prodotto semidiretto di K mediante H', cioè

1. $K \times_\varphi H = KH'$,
2. $K \cap H' = \{1\}$.

Esempio 9.1.7. La realizzazione del gruppo diedrale D_n come prodotto semidiretto si ottiene fissando una scelta di simmetria assiale s. Un'altra scelta s', e le simmetrie assiali sono in tutto n, definisce un nuovo sottogruppo $S' = \langle s' \rangle$ ed una nuova decomposizione $D_n = C_n S'$. Ciascun S' èun complemento di C_n in D_n.

Osservazione 9.1.8. Un modo naturale per ottenere complementi di K nel prodotto semidiretto $K \times_\varphi H$ èquello di considerare i coniugati di H. Si noti che se $H' = gHg^{-1}$, decomposto $g = kh$ con $k \in K$ e $h \in H$, si ha $H^prime = kHk^{-1}$. Cioèbasta coniugare H per elementi in K.

È possibile che omomorfismi $\varphi, \psi\colon H \to \mathrm{Aut}(K)$ diversi producano gruppi $K \times_\varphi H$ e $K \times_\psi H$ isomorfi tra di loro. Il risultato seguente fornisce un criterio di isomorfismo.

Proposizione 9.1.9. *Siano H e K gruppi e siano $\varphi, \psi\colon H \to \mathrm{Aut}(K)$ omomorfismi assegnati. Se esitono automorfismi $\alpha\colon K \to K$ e $\beta\colon H \to H$ tali che*

$$\psi(\beta(h)) \circ \alpha = \alpha \circ \varphi(h) \qquad \text{per ogni } h \in H$$

allora $K \times_\varphi H$ e $K \times_\psi H$ sono isomorfi.

Dimostrazione. Si verifica facilmente che la condizione enunciata è esattamente quella che rende la biezione $(k, h) \mapsto (\alpha(k), \beta(h))$ un omomorfismo.■

L'esempio seguente mostra come la tecnica di costruzione dei prodotti semidiretti fornita dal teorema 9.1.5 possa servire, congiuntamente con la proposizione 9.1.9 per risolvere dei problemi di classificazione.

Esempio 9.1.10. Sia G un gruppo finito con 12 elementi. Il numero dei 3-Sylow in G è $n_3 = 1$ oppure $n_3 = 4$ (vedi teorema 6.3.2). Siccome un 3-Sylow è ciclico di ordine 3, nel caso in cui $n_3 = 4$ gli elementi di ordine 3 sono 8 lasciando spazio per un solo 2-Sylow (che ha ordine 4). Dunque, G possiede sempre un sottogruppo di Sylow normale. Poiché Sylow relativi a divisori primi distinti hanno intersezione banale e 12 possiede solo 2 fattori primi distinti, G è sempre prodotto semidiretto di un p-Sylow S_p mediante un q-Sylow S_q, $\{p, q\} = \{2, 3\}$. A meno di isomorfismi,

$$S_3 = \mathbb{Z}/3\mathbb{Z} \qquad \text{e} \qquad S_2 = \mathbb{Z}/4\mathbb{Z}, \text{ oppure } (\mathbb{Z}/2\mathbb{Z})^2.$$

Abbiamo quindi le seguenti possibilità:

1. $S_2 = (\mathbb{Z}/2\mathbb{Z})^2$ è normale in G. Gli automorfismi di S_2 si ottengono permutando in modo arbitrario gli elementi non nulli di S_2, cioè $\mathrm{Aut}(S_2) = \mathfrak{S}_3$. Per un omomorfismo strutturale

   $$\varphi\colon \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathfrak{S}_3$$

   abbiamo dunque 3 scelte,

   $$\varphi_1(\overline{1}) = 1, \qquad \varphi_2(\overline{1}) = (1\ 2\ 3), \qquad \varphi_3(\overline{1}) = (1\ 3\ 2).$$

   Per l'osservazione 9.1.4 $(\mathbb{Z}/2\mathbb{Z})^2 \times_{\varphi_1} \mathbb{Z}/3\mathbb{Z}$ è il prodotto diretto $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Invece, la proposizione 9.1.9 per $\alpha = 1$ e $\beta(x) = x^2$ implica che

   $$(\mathbb{Z}/2\mathbb{Z})^2 \times_{\varphi_2} \mathbb{Z}/3\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times_{\varphi_3} \mathbb{Z}/3\mathbb{Z}.$$

   Il prodotto semidiretto $(\mathbb{Z}/2\mathbb{Z})^2 \times_{\varphi_2} \mathbb{Z}/3\mathbb{Z}$ ha una partizione in 4 laterali $S_3 \cup aS_3 \cup bS_3 \cup cS_4$ con $a^2 = b^2 = c^2 = 1$. L'omomorfismo strutturale φ_2 è tale che l'azione di G su se stesso per moltiplicazione sinistra permuta tali laterali, definendo un'inclusione $G \hookrightarrow \mathfrak{S}_4$. Allora deve essere $G = A_4$, unico sottogruppo di $\mathfrak{S}_4$ con 12 elementi.

2. $S_2 = \mathbb{Z}/4\mathbb{Z}$ è normale in G. Il gruppo degli automorfismi di S_2 è $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) = (\mathbb{Z}/4\mathbb{Z})^\times$, un gruppo di ordine 2. Pertanto l'unico omomorfismo

   $$\varphi\colon \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(S_2)$$

   è l'omomorfismo costante e $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$.

3. $S_3 = \mathbb{Z}/3\mathbb{Z}$ è normale in G e $\mathrm{Aut}(S_3) \simeq \mathbb{Z}/2\mathbb{Z}$. Gli omomorfismi strutturali costanti $S_2 \to \mathrm{Aut}(S_3)$ danno luogo a gruppi prodotto già considerati sopra. Se $S_2 = (\mathbb{Z}/2\mathbb{Z})^2$ ci sono 3 omomorfismi non costanti

$$\varphi_{1,2,3} \colon S_2 \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

che corrispondono ai tre sottogruppi di indice 2 in $(\mathbb{Z}/2\mathbb{Z})^2$. Siccome gli automorfismi di $(\mathbb{Z}/2\mathbb{Z})^2$ permutano fra loro questi sottogruppi, per la proposizione 9.1.9 i vari prodotti semidiretti $\mathbb{Z}/3\mathbb{Z} \times_{\varphi_i} (\mathbb{Z}/2\mathbb{Z})^2$, $i = 1, 2, 3$, sono tutti isomorfi fra di loro ed isomorfi al gruppo diedrale D_6. Per quest'ultimo fatto, basta osservare che l'elemento non banale $x \in \ker(\varphi)$, inducendo l'azione identica su S_3, commuta con S_3 e quindi è nel centro di G. Pertanto il sottogruppo $H = \langle x \rangle$ è l'intersezione dei 2-Sylow in G e l'automorfismo non banale indotto dall'omomorfismo strutturale manda un generatore del gruppo ciclico con 6 elementi $\mathbb{Z}/3\mathbb{Z} \times H$ nel suo inverso. Questa è la caratterizzazione strutturale del gruppo diedrale.

Se, invece, $S_2 \simeq \mathbb{Z}/4\mathbb{Z}$ otteniamo il gruppo $\Gamma = S_3 \times_\varphi S_2$ caratterizzato dalla relazione

$$yxy^{-1} = x^{-1} \qquad \text{per } S_2 = \langle y \rangle \text{ e } S_3 = \langle x \rangle.$$

Quindi, in definitiva, esistono esattamente 5 gruppi di ordine 12:

$$\mathbb{Z}/12\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \qquad A_4, \qquad D_6, \qquad \Gamma.$$

Tra questi, solo i primi 2 sono quelli abeliani, come confermato dal teorema di struttura per i gruppi abeliani finiti (teorema 8.2.3).

9.2 Il primo gruppo di coomologia

Iniziamo con le definizioni seguenti.

Definizione 9.2.1. Una successione di gruppi ed omomorfismi

$$\ldots \longrightarrow G_{n-1} \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \longrightarrow \ldots$$

si dice *esatta* se $\mathrm{im}(f_{n-1}) = \ker(f_n)$ per ogni $n \in \mathbb{Z}$.

Resta implicitamente inteso che l'insieme degli indici $n \in \mathbb{Z}$ per cui esiste un gruppo G_n può essere limitato inferiormente e/o superiormente, ottenendo delle successioni esatte "tronche". In particolare abbiamo la nozione seguente.

Definizione 9.2.2. Una *successione esatta corta* è una successione esatta

$$1 \longrightarrow K \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1. \tag{9.2}$$

Risulta chiaro come una successione esatta corta possa estendersi ad una successione esatta nel senso della definizione 9.2.1 aggiungendo a sinistra ed a destra una successione di gruppi banali $\{1\}$. L'uso della notazione $\{1\}$ per il gruppo banale presuppone l'uso della notazione moltiplicativa: può essere anche denotato $\{0\}$ laddove sia richiesto dal contesto. Nel caso di una successione esatta corta (9.2), l'esattezza si traduce in quanto segue:

- α è iniettiva, in quanto $\ker(\alpha) = \mathrm{im}(\{1\} \to K) = \{1\}$;

- β è suriettiva, in quanto $\mathrm{im}(\beta) = \ker(H \to \{1\}) = H$;
- $K = \mathrm{im}(\alpha) = \ker(\beta)$, e dunque K è normale in G e

$$\frac{G}{K} \simeq \frac{G}{\mathrm{im}(\alpha)} \simeq \frac{G}{\ker(\beta)} \simeq \mathrm{im}(\beta) = H$$

per il primo teorema d'isomorfismo 3.4.1.

Quindi, in particolare, per ogni scelta di gruppi K ed H e di omomorfismo $\varphi : H \to \mathrm{Aut}(K)$ c'è una successione esatta corta

$$1 \longrightarrow K \longrightarrow K \times_\varphi H \longrightarrow H \longrightarrow 1.$$

Siano Γ e G due gruppi arbitrari. Il dato di un omomorfismo

$$\varphi : \Gamma \longrightarrow \mathrm{Aut}(G)$$

definisce un'azione sinistra di Γ su G che denotiamo

$$^\gamma g = \varphi(\gamma)(g), \qquad \text{per ogni } \gamma \in \Gamma \text{ e } g \in G.$$

Infatti $^1 g = \varphi(1)(g) = \mathrm{id}(g) = g$ e $^{\gamma\gamma'} g = \varphi(\gamma\gamma')(g) = \varphi(\gamma)(\varphi(\gamma')(g)) = {}^\gamma({}^{\gamma'} g)$. Poniamo allora definire il *sottogruppo dei Γ-invarianti*

$$G^\Gamma = \{g \in G \mid {}^\gamma g = g \text{ per ogni } \gamma \in \Gamma\}.$$

Si tratta effettivamente di un sottogruppo di G in quanto per ogni $\gamma \in \Gamma$:

1. $^\gamma 1 = \varphi(\gamma)(1) = 1$;
2. $^\gamma(gg') = \varphi(\gamma)(gg') = \varphi(\gamma)(g)\varphi(\gamma)(g') = {}^\gamma g\, {}^\gamma g' = gg'$ per ogni g, $g' \in G^\Gamma$;
3. $({}^\gamma g)^{-1} = {}^\gamma(g^{-1})$ per ogni $g \in G$ perché $^\gamma g\, ^\gamma(g^{-1}) = \varphi(\gamma)(gg^{-1}) = 1$ ed in particolare $^\gamma(g^{-1}) = g^{-1}$ per ogni $g \in G^\Gamma$.

Supponiamo assegnato un sottogruppo $K < G$ con la proprietà che $^\gamma K \subseteq K$ per ogni $ga \in \Gamma$. Allora l'azione di Γ sui laterali sinistri data da

$$^\gamma Kg = K\, {}^\gamma g$$

è ben definita in quanto se $Kg = Kg'$ si ha $g' = kg$ per un opportuno $k \in K$ e quindi $^\gamma g' = {}^\gamma k\, {}^\gamma g \in K\, {}^\gamma g$, cioè $K\, {}^\gamma g = K\, {}^\gamma g'$. In particolare, se K è anche normale l'azione di Γ su G discende ad un'azione di Γ sul gruppo quoziente G/K e possiamo certamente considerare il sottogruppo dei Γ-invarianti di quest'ultimo, $(G/K)^\Gamma$. Il rapporto generale tra K^Γ, G^Γ e $(G/K)^\Gamma$ è espresso, nel linguaggio della successione esatta (**??**) dalla proposizione seguente.

Proposizione 9.2.3. *La restrizione delle mappe α e β ai rispettivi gruppi di Γ-invarianti definisce una successione esatta*

$$\{1\} \longrightarrow K^\Gamma \xrightarrow{\alpha^\Gamma} G^\Gamma \xrightarrow{\beta^\Gamma} H^\Gamma.$$

Dimostrazione. Infatti risulta che:

1. α^Γ è iniettiva perché K^Γ è un sottogruppo di G^Γ;

2. se $k \in K^\Gamma$ allora $\beta^\Gamma(k) = \beta(k) = 0$;

3. se $\beta^\Gamma(x) = 0$, allora $x \in K \cap G^\Gamma = K^\Gamma$. ■

In generale, però, la successione esatta non si completa ad una successione esatta corta, ovvero l'omomorfismo β^Γ non è necessariamente suriettivo.

Esempi 9.2.4. 1. Siano $G = (\mathbb{Z}/2\mathbb{Z})^2 = \{0, a, b, c\}$, $K = \{0, c\}$ e $\Gamma = \{1, \gamma\}$ dove $\gamma \in \mathrm{Aut}(G) \simeq \mathfrak{S}_3$ è tale che ${}^\gamma a = b$, ${}^\gamma b = a$ e ${}^\gamma c = c$. Allora

$$G^\Gamma = \{0, c\} = K, \qquad (G/K)^\Gamma = \{K, K + a\}$$

e $\beta^\Gamma(c) = K + c = K$, cioè β^Γ è la mappa costante nulla (quindi non suriettiva).

2. Siano $G = \mathbb{Z}$, $K = 2\mathbb{Z}$ e $\Gamma = \{1, \gamma\}$ con ${}^\gamma n = -n$ per ogni $n \in \mathbb{Z}$. In questo caso β^Γ non può essere suriettiva in quanto $\mathbb{Z}^\Gamma = \{0\}$, ma $(\mathbb{Z}/2\mathbb{Z})^\Gamma \neq (0)$ perché ${}^\gamma 1 = -1 \equiv 1 \bmod 2$.

Ci poniamo dunque il problema di determinare delle condizioni necessarie e sufficienti affinchè la mappa β^Γ ri sulti suriettiva o, equivalentemente, affinchè risulti $G^\Gamma/K^\Gamma \simeq (G/K)^\Gamma$. Per semplificare l'esposizione e rendere più intelligibili i risultati, da ora in poi supporremo verificata la seguente

Ipotesi: K è abeliano

Compatibilmente con l'ipotesi di abelianità useremo la notazione additiva per la struttura di gruppo di K. Però quando K sarà pensato come sottogruppo di G manterremo la notazione moltiplicativa.

Premettiamo una definizione ed alcuni risultati di carattere generale.

Definizione 9.2.5. Sia A un gruppo abeliano e sia Γ un gruppo qualsiasi con assegnata azione $\varphi : \Gamma \to \mathrm{Aut}(A)$ di Γ su A. Un *omomorfismo crociato* di Γ a valori in A è una funzione $f : \Gamma \to A$ tale che

$$f(\gamma\gamma') = f(\gamma) + {}^\gamma f(\gamma') \qquad \text{per ogni } \gamma, \gamma' \in \Gamma.$$

Denotiamo $Z^1(\Gamma, A)$ l'insieme degli omomorfismi crociati di Γ a valori in A. Come si verifica immediatamente, l'operazione naturale di somma fra funzionI, $(f + f')(\gamma) = f(\gamma) + f'(\gamma)$ rende $Z^1(\Gamma, A)$ un gruppo abeliano.

Osservazioni 9.2.6. In generale gli omomorfismi crociati non sono omomorfismi ma:

1. un omomorfsmo crociato è un'isomorfismo esattamente quando l'azione di Γ è banale;

2. se f è un omomorfismo crociato, si ha $f(1) = f(1 \cdot 1) = f(1) + {}^1 f(1) = f(1) + f(1)$ e dunque $f(1) = 0$.

Nella nozione di omomorfismo crociato è codificata la struttura del gruppo semidiretto $A \times_\varphi \Gamma$, come precisato dal risultato seguente.

Teorema 9.2.7. *Sia A un gruppo abeliano e sia Γ un gruppo qualsiasi con assegnata azione $\varphi : \Gamma \to \mathrm{Aut}(A)$ di Γ su A. Allora c'è una corrispondenza biunivoca*

$$Z^1(\Gamma, A) \longleftrightarrow \{\textit{complementi di } A \textit{ in } A \times_\varphi \Gamma\}$$

Dimostrazione. Iniziamo con $f \in \mathbb{Z}^1(\Gamma, A)$ e consideriamo il sottoinsieme $\Gamma_f$di $A \times_\varphi \Gamma$ definito da

$$\Gamma_f = \{(f(\gamma), \gamma) \mid \gamma \in \Gamma\}$$

(cioè il grafico di f). Vogliamo dimostrare che Γ_f è un complemento di A. Prima di tutto verifichiamo che è un sottogruppo di $A \times_\varphi \Gamma$.

1. Per ogni γ, $\gamma' \in \Gamma$ si ha $(f(\gamma), \gamma)(f(\gamma'), \gamma') = (f(\gamma) + {}^{\gamma}f(\gamma'), \gamma\gamma') = (f(\gamma\gamma'), \gamma\gamma') \in \Gamma_f$;
2. $(0, 1) \in \Gamma_f$ per l'osservazione 9.2.6;
3. per ogni $\gamma \in \Gamma$, $(f(\gamma), \gamma)^{-1} = {}^{(\gamma^{-1})}(f(\gamma)^{-1}) = (f(\gamma^{-1}), \gamma^{-1}) \in \Gamma_f$.

A questo punto occorre controllare che le condizione della definizione 9.1.6 sono soddisfatte.

1. Ogni $x = (a, \gamma) \in A \times_\varphi \Gamma$ si può scrivere nella forma $x = (a - f(\gamma), 1)(f(\gamma), \gamma)$. Questo dimostra che $A \times_\varphi \Gamma = A\Gamma_f$;
2. per l'unicit della scrittura secondo la decomposizione $A \times_\varphi \Gamma = A\Gamma$, l'unico elemento in A della forma $(f(\gamma), \gamma)$ è $(0, 1)$.

Nell'altra direzione, iniziamo con un complemento Γ' di A in $A \times_\varphi \Gamma$. La scrittura di $(0, \gamma) \in \Gamma$ secondo la decomposizione $A \times_\varphi \Gamma = A\Gamma'$ definisce un elemento $a_\gamma \in A$ tale che $(a_\gamma, \gamma) \in \Gamma'$. D'altra parte, se (a, γ), (a', γ') sono entrambi in Γ' risulta

$$(a, \gamma)(a', \gamma')^{-1} = (a, \gamma)({}^{(\gamma^{-1})}(-a'), \gamma^{-1}) = (a - a', 1) \in A \cap \Gamma' = \{1\},$$

cioè $a = a'$. Pertanto, per ogni $\gamma \in \Gamma$ l'elemento a_γ è l'unico tale che $(a_\gamma, \gamma) \in \Gamma'$ e dovendo essere a fortiori $(a_\gamma, \gamma)(a_{\gamma'}, \gamma') = (a_{\gamma\gamma'}, \gamma\gamma')$ si verifica facilmente che la funzione $f_{\Gamma'} : \Gamma \to A$, $f_{\Gamma'}(\gamma) = a_\gamma$ è un omomorfismo crociato.

La caratterizzazione di Γ_f come grafico di f e di $f_{\Gamma'}$ come la funzione di cui Γ' è il grafico endono evidente che le costruzioni sono l'una l'inversa dell'altra. Pertanto la corrispondenza è certamente biunivoca. ■

Fissato un elemento $a \in A$, consideriamo la funzione $f : \Gamma \to A$ definita da

$$f(\gamma) = {}^{\gamma}a - a. \tag{9.3}$$

Essa è un elemento di $Z^1(\Gamma, A)$ in quanto per ogni γ, $\gamma' \in \Gamma$ vale $f(\gamma\gamma') = {}^{\gamma\gamma'}a - a = {}^{\gamma}({}^{\gamma'}a - a) + ({}^{\gamma}a - a) = {}^{\gamma}f(\gamma') + f(\gamma)$. Un omomorfismo crociato della forma (9.3) si dice *principale*. Siccome

$$({}^{\gamma}a - a) - ({}^{\gamma}b - b) = {}^{\gamma}(a - b) - (a - b) \qquad \text{per ogni } a, b \in A$$

l'insieme $B^{\mathrm{l}}(\Gamma, A)$ degli omomorfismi crociati principali è un sottogruppo di $Z^1(\Gamma, A)$.

Definizione 9.2.8. *Il* primo gruppo di coomologia *di* Γ *a coeffcienti in* A *è il gruppo quoziente*

$$H^1(\Gamma, A) = \frac{Z^1(\Gamma, A)}{B^1(\Gamma, A)}.$$

Esempio 9.2.9. Nel caso in cui Γ agisce su A in modo banale sappiamo dall'osservazione 9.2.6.1 che $Z^1(\Gamma, A) = \hom(\Gamma, A)$. Inoltre non ci sono omomorfismi crociati principali non nulli perchè per ogni $a \in A$ e per ogni $\gamma \in \Gamma$ si ha ${}^{\gamma}a - a = a - a = 0$, ovvero $B^1(\Gamma, A) = \{0\}$. In definitiva

$$H^1(\Gamma, A) = \frac{\hom(\Gamma, A)}{\{0\}} = \hom(\Gamma, A).$$

Il prossimo risultato spiega il significato del primo gruppo di coomologia dal punto di vista della biezione del teorema 9.2.7.

Teorema 9.2.10. *Sia A un gruppo abeliano e sia Γ un gruppo qualsiasi con assegnata azione $\varphi : \Gamma \to \mathrm{Aut}(A)$ di Γ su A. Allora c'è una corrispondenza biunivoca canonica*

$$H^1(\Gamma, A) \longleftrightarrow \{\textit{classi di coniugio di complementi di } A \textit{ in } A \times_\varphi \Gamma\}.$$

In essa, la classe degli omomorfismi crociati principali corrisponde alla classe di coniugio di Γ.

Dimostrazione. In virtù della già acquisita corrispondenza biunivoca del teorema 9.2.7, è sufficiente dimostrare che se Γ_1 e Γ_2 sono complementi di A in $A \times_\varphi \Gamma$ con corrispondenti omomorfismi crociati f_1 e f_2, allora Γ_1 e Γ_2 sono coniugati se e soltanto se $f_1 - f_2 \in B^1(\Gamma, A)$.

Iniziamo col supporre Γ_1 e Γ_2 coniugati. Ricordando l'osservazione 9.1.8 possiamo scrivere $\Gamma_2 = a\Gamma_1 a^{-1}$ con $a \in A$. Allora per ogni $\gamma \in \Gamma$ è possibile trovare $\gamma' \in \Gamma$ con $(f_2(\gamma), \gamma) = (a,1)(f_1(\gamma'), \gamma')(a,1)^{-1} = (a - {}^{\gamma}a + f_1(\gamma'), \gamma\prime)$ da cui $\gamma = \gamma'$ e $f_1(\gamma) - f_2(\gamma) = {}^{\gamma}a - a$, cioè $f_1 - f_2 \in B^1(\Gamma, A)$.

Viceversa, se esiste $a \in A$ tale che $f_1(\gamma) - f_2(\gamma) = {}^{\gamma}a - a$ per ogni $\gamma \in \Gamma$, il calcolo precedente, che è completamente reversibile, mostra che $\Gamma_2 = a\Gamma_1 a^{-1}$. ■

Possiamo ora tornare al problema della determinazione di condizioni per la suriettività della mappa β^Γ in 9.2.3 e vedere come, in un certo senso, il calcolo di $H^1(\Gamma, A)$ ne sia una soluzione.

Teorema 9.2.11. *Sia $\{0\} \to A \xrightarrow{\alpha} G \xrightarrow{\beta} H \to \{1\}$ una succesione esatta corta di gruppi con un'azione del gruppo Γ ed A abeliano. Allora c'è una successione esatta di gruppi*

$$\{0\} \longrightarrow A^\Gamma \xrightarrow{\alpha^\Gamma} G^\Gamma \xrightarrow{\beta^\Gamma} H^\Gamma \xrightarrow{\delta} H^1(\Gamma, A).$$

Dimostrazione. Come prima cosa dobbiamo definire la mappa δ. Sia $h \in H^\Gamma$. Per suriettività di β, esiste $g \in G$ tale che $\beta(g) = h$. Per ogni $\gamma \in \Gamma$, c'è un'uguaglianza di laterali $Kg = h = {}^{\gamma}h = {}^{\gamma}(Kg) = K{}^{\gamma}g$, cioè $\beta({}^{\gamma}g) = h$. Allora per l'esattezza in G della successione originale ${}^{\gamma}gg^{-1} \in \ker(\beta) = \mathrm{im}(\alpha) = A$ e possiamo considerare la funzione

$$f : \Gamma \longrightarrow A, \qquad f(\gamma) = {}^{\gamma}gg^{-1}$$

che risulta essere un omomorfismo crociato in quanto $f(\gamma\gamma') = {}^{\gamma\gamma'}gg^{-1} = {}^{\gamma}({}^{\gamma'}gg^{-1}){}^{\gamma}gg^{-1} = {}^{\gamma}f(\gamma\prime) + f(\gamma)$ per ogni γ, $\gamma' \in \Gamma$.

Se g' è un altro rappresentante di h in G e se f' è l'omomorfismo crociato a valori in A costruito come sopra a partire da g', scrivendo $g' = ag$ per un opportuno $a \in A$, si ha $f'(\gamma) = {}^{\gamma}g'g'^{-1} = {}^{\gamma}a{}^{\gamma}gg^{-1}a^{-1} = {}^{\gamma}af(\gamma)a^{-1} = f(\gamma) + {}^{\gamma}a - a$ (per l'ultima uguaglianza si ricordi che A è abeliano e la convenzione adottata sullo scambio tra notazione moltiplicativa ed additiva). Il calcolo mostra che $f' \in f + B^1(\Gamma, A)$ e quindi la classe $[f]$ di f in $H^1(\Gamma, A)$ non dipende dalla scelta del rappresentante g. Allora è ben definita la funzione

$$\delta : H \longrightarrow H^1(\Gamma, A), \qquad \delta(h) = [f].$$

Per vedere che δ è un omomorfismo si noti che se g e g' rappresentano rispettivamente h e h', allora gg' rappresenta hh' e allora ${}^{\gamma}gg'(gg')^{-1} = f(\gamma) + f'(\gamma)$.

Bisogna infine controllare che $\mathrm{im}(\beta^\Gamma) = \ker(\delta)$. Se $h = \beta(g)$ con $g \in G^\Gamma$ risulta subito $f(\gamma) = 0$ e quindi $\delta(h) = 0$. Viceversa, se $\delta(h) = 0$, allora l'omomorfismo crociato f associato come sopra alla scelta di un rappresentante g di h deve essere principale, cioè $f(\gamma) = {}^{\gamma}gg^{-1} = {}^{\gamma}a - a$ per un $a \in A$ opportuno. Ma allora ${}^{\gamma}(a^{-1}g) = (a^{-1}g) \in G^\Gamma$ e $h = \beta^\Gamma(a^{-1}g)$. ■

Corollario 9.2.12. *Sia G un gruppo con un'azione $\varphi : \Gamma \to \mathrm{Aut}(G)$ del gruppo Γ sia A un sottogruppo abeliano di G tale che ${}^{\Gamma}A = A$ e $H^1(\Gamma, A) = \{0\}$. Allora $(G/A)^{\Gamma} \simeq G^{\Gamma}/A^{\Gamma}$.*

Dimostrazione. Se $H^1(\Gamma, A) = \{0\}$ si ha, per il teorema precedente, una successione esatta corta

$$\{0\} \longrightarrow A^{\Gamma} \longrightarrow G^{\Gamma} \xrightarrow{\pi^{\Gamma}} (G/A)^{\Gamma} \longrightarrow \{0\}$$

dove π denota la mappa quoziente. ■

Esempi 9.2.13. Riprendiamo ora gli esempi 9.2.4 facendo vedere come, concordamente col corollario appena dimostrato, alla non suriettività della mappa β^{Γ} corrisponde una coomologia non nulla.

1. in questo caso si ha $K = \{0, c\}$ e $\Gamma = \{0, \gamma\}$ con ${}^{\gamma}c = c$. Dunque Γ agisce banalmente su K e per quanto visto nell'esempio 9.2.9
$$H^1(\Gamma, K) = \hom(\Gamma, K) \simeq \mathbb{Z}/2\mathbb{Z}.$$
2. In questo caso si ha $K = 2\mathbb{Z}$ e $\Gamma = \{0, \gamma\}$ con ${}^{\gamma}(2n = -2n.$ per ogni $n \in \mathbb{Z}$ la funzione $f_{2n} : \Gamma \to 2\mathbb{Z}$ definita da
$$f_{2n}(0) = 0, \qquad f_{2n}(\gamma) = 2n$$
definisce un omomorfismo crociato, risultando soddisfatta la relazione $0 = f_{2n}(1) = f_{2n}(\gamma^2) = {}^{\gamma}f_{2n}(\gamma) + f_{2n}(\gamma) = -2n + 2n$. Pertanto $Z^1(\Gamma, 2\mathbb{Z}) = 2\mathbb{Z}$. Inoltre, si verifica immediatamente che l'omomorfismo crociato principale determinato dall'elemento $2n \in 2\mathbb{Z}$ è la funzione f_{-4n}. Dunque
$$H^1(\Gamma, 2\mathbb{Z}) = \frac{2\mathbb{Z}}{4\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Siano A e B gruppi abeliani con azioni $\varphi : \Gamma \to \mathrm{Aut}(A)$ e $\phi : \Gamma \to \mathrm{Aut}(B)$ del gruppo Γ. Un omomorfismo $F : A \to B$ si dice Γ-*equivariante* se

$${}^{\gamma}(f(a)) = f({}^{\gamma}a), \qquad \text{per ogni } a \in A,\ \gamma \in \Gamma.$$

Esempi 9.2.14.
1. Se A è un sottogruppo di B e l'azione definita da φ è la restrizione ad A dell'azione su B definita da ϕ, l'inclusione di A in B è Γ-equivariante.
2. Come abbiamo visto sopra, in presenza di un sottogruppo Γ-invariante l'azione di Γ su un gruppo discende ad un'azione sul gruppo quoziente. in tal caso, la mappa quoziente è sempre Γ-equivariante.

Se $F : A \to B$ è un omomorfismo Γ-equivariante, la composizione con F definisce una mappa

$$F_* : Z^1(\Gamma, A) \longrightarrow Z^1(\Gamma, B), \qquad F_*(f) = F \circ f.$$

Si ha infatti $F_*(f)(\gamma\gamma') = F \circ f(\gamma\gamma') = F({}^{\gamma}f(\gamma') + f(\gamma)) = F({}^{\gamma}f(\gamma')) + F(f(\gamma)) = {}^{\gamma}F(f(\gamma')) + F(f(\gamma)) = {}^{\gamma}F_*(f)(\gamma') + F_*(f)(\gamma)$. Si verifica immediatamente che F_* è un omomorfismo. Se poi f è principale, scritto $f(\gamma) = {}^{\gamma}a - a$ con $a \in A$ risulta $F_*(f)(\gamma) = F({}^{\gamma}a - a) = F({}^{\gamma}a) - F(a) = {}^{\gamma}F(a) - F(a)$, cioè $F_*(f)$ è l'omomorfismo crociato principale associato all'elemento $F(a) \in B$. Pertanto

$$F_*(B^1(\Gamma, A)) \subseteq B^1(\Gamma, B)$$

e allora la mappa F_* induce una mappa

$$F_* : H^1(\Gamma, A) \longrightarrow H^1(\Gamma, B).$$

Teorema 9.2.15. *Sia* $\{0\} \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to \{0\}$ *una succesione esatta corta di gruppi abeliani con un'azione del gruppo* Γ. *Allora c'è una successione esatta di gruppi*

$$\{0\} \longrightarrow A^\Gamma \xrightarrow{\alpha^\Gamma} B^\Gamma \xrightarrow{\beta^\Gamma} C^\Gamma \xrightarrow{\delta} H^1(\Gamma, A) \xrightarrow{\alpha_*} H^1(\Gamma, B) \xrightarrow{\beta_*} H^1(\Gamma, C).$$

Dimostrazione. In virtù del teorema 9.2.11 resta solo da dimostrare l'esattezza in $H^1(\Gamma, A)$ ed in $H^1(\Gamma, B)$.

Iniziamo con $[h] = \delta(c) \in H^1(\Gamma, A)$. Dalla definizione di δ data nella dimostrazione del teorema 9.2.11 si vede che deve essere $h(\gamma) = {}^\gamma b - b \in A$ con $\beta(b) = c$. Applicando α_* l'espressione non cambia, ma questa volta visto a coefficienti in B, l'omomorfismo crociato $\alpha_*(h)(\gamma) = {}^\gamma b - b \in B$ è principale. Dunque $\alpha_*([h]) = 0$ e $\mathrm{im}(\delta) \subseteq \ker(\alpha_*)$.

Sia ora $[h] \in H^1(\Gamma, A)$ tale che $\alpha_*([h]) = 0$. Allora $\alpha_*(h) \in B^1(\Gamma, B)$ e quindi $\alpha_*(h) = {}^\gamma b - b$ per un opportuno $b \in B$. Siccome h è a coefficienti in A deve risultare $\beta({}^\gamma b - b) = 0$. Questo vuol dire che $\beta(b) \in C^\Gamma$ e quindi $h = \delta(\beta(b))$. Dunque $\ker(\alpha_*) \subseteq \mathrm{im}(\delta)$.

Per ogni $[h] \in H^1(\Gamma, A)$ si ha $\beta_* \circ \alpha_*(h)(\gamma) = \beta(\alpha(\gamma)) = 0$ per ogni $\gamma \in \Gamma$ in quanto $\beta \circ \alpha = 0$. Questo mostra che $\mathrm{im}(\alpha_*) \subseteq \ker(\beta_*)$.

Infine, se $[h] \in H^1(\Gamma, B)$ è tale che $\beta_*([h]) = [0]$ allora l'omomorfismo crociato $\beta_*(h)$ deve essere principale. Ciò vuol dire che per un $c \in C$ opportuno $\beta_*(h)(\gamma) = {}^\gamma c - c$ per ogni $\gamma \in \Gamma$. Possiamo allora scrivere

$$h(\gamma) = {}^\gamma b - b + a_\gamma$$

dove $b \in B$ rappresenta c (cioè $\beta(b) = c$) e $a_\gamma \in A$. Si controlla facilmente che la funzione $f(\gamma) = a_\gamma$ è un omomorfismo crociato, di fatto a coefficienti in A. Allora tale scrittura fornisce una decomposizione $[h] = [{}^\gamma b - b] + [f] = [f]$ che rende palese come $[h] \in \mathrm{im}(\alpha_*)$. Dunque $\ker(\beta_*) \subseteq \mathrm{im}(\alpha_*)$ e la dimostrazione è completa. ■

La successione esatta del teorema 9.2.15 può essere utile per la determinazione esplicita dei gruppi H^1. Negli esempi successivi vediamo alcuni casi speciali.

Esempi 9.2.16. Sia $\{0\} \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to \{0\}$ una succesione esatta corta di gruppi abeliani con un'azione del gruppo Γ. Supponiamo che:

1. $C^\Gamma = \{0\}$ e $H^1(\Gamma, C) = \{0\}$. Allora la successione esatta include un segmento

   $$\{0\} \longrightarrow H^1(\Gamma, A) \xrightarrow{\alpha_*} H^1(\Gamma, B) \longrightarrow \{0\},$$

   cioè α_* è un isomorfismo.

2. $H^1(\Gamma, B) = \{0\}$. Allora la successione esatta include un segmento

   $$\{0\} \longrightarrow A^\Gamma \xrightarrow{\alpha^\Gamma} B^\Gamma \xrightarrow{\beta^\Gamma} C^\Gamma \xrightarrow{\delta} H^1(\Gamma, A) \longrightarrow \{0\},$$

   da cui $H^1(\Gamma, A) \simeq \frac{(B/A)^\Gamma}{B^\Gamma/A^\Gamma}$ (vedi problema 9.2). Si confronti questa situazione col corollario 9.2.12.

3. i gruppi A, B, e C siano finiti. Allora, con riferimento ai problemi 9.2 e 9.2, la conoscenza del numero degli elementi in qualcuno dei gruppi della successione esatta fornisce informazioni sugli altri.

PROBLEMI

9.1. Siano C_m e C_n gruppi ciclici di ordine m ed n rispettivamente. Dare condizioni su m ed n affinché ogni prodotto semidiretto di C_m mediante C_n sia isomorfo al prodotto diretto $C_m \times C_n$.

9.2. Determinare tutti i gruppi, a meno di isomorfismi, che sono prodotto semidiretto di $\mathbb{Z}/7\mathbb{Z}$ mediante $\mathbb{Z}/6\mathbb{Z}$.

9.3. Dimostrare in dettaglio che ogni coniugato di H è un complemento di K in $K \times_\varphi H$.

9.4. Verificare tutte le affermazioni fatte nel corso dell'analisi dei gruppi di ordine 12 (Esempio 9.1.10).

9.5. Sia $\{0\} \to A \to B \to C \to D \to \{0\}$ una successione esatta. Mostrare che $D \simeq \frac{C}{B/A}$.

9.6. Sia $\{0\} \to G_1 \to G_2 \to \dots C_{r-1} \to C_r \to \{0\}$ una successione esatta con $|C_i| = n_i$ (finito) per ogni $i = 1, \dots, r$. Si dimostri che $\sum_i = 1^r (-1)^i n_i = 0$.

9.7. Supponiamo che A sia un gruppo abeliano finito con un'azione del gruppo Γ. Si dimostri che $H^1(\Gamma, A)$ è finito.

9.8. Sia $\Gamma = \langle \gamma \rangle$ un gruppo ciclico di ordine 2, e facciamo agire Γ su $\mathbb{Q}$ ponendo ${}^\gamma q = -q$.

1. Dimostrare che $H^1(\Gamma, \mathbb{Q}) = \{0\}$.
2. Determinare il più piccolo sottogruppo $\mathbb{Z} < G < \mathbb{Q}$ tale che $H^1(\Gamma, G) = \{0\}$

9.9. Sia $\Gamma \simeq \mathbb{Z}$ e sia G un gruppo su cui Γ agisce con $G^\Gamma \neq \{0\}$. Si dimostri che $H^1(\Gamma, G^\Gamma) \neq \{0\}$.

Lezione 10

Estensioni, II

10.1 Il secondo gruppo di coomologia

Manteniamo l'ipotesi semplificativa per cui A è un gruppo abeliano.

Definizione 10.1.1. *Sia A un gruppo abeliano e sia Γ un gruppo qualunque. Un'*estensione *di A per Γ è il dato di una successione esatta corta*

$$0 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\beta} \Gamma \longrightarrow 1. \tag{10.1}$$

Il gruppo E si dice elemento centrale *dell'estensione* (10.1).

La nozione di estensione di A per Γ generalizza quella di prodotto semidiretto, come le seguenti osservazioni rendono chiaro.

Osservazioni 10.1.2.

1. Come già osservato nella discussione successiva la definizione 9.2.2 di successione esatta corta, un prodotto semidiretto $A \times_\varphi \Gamma$ da luogo ad un'estensione $0 \to A \to A \times_\varphi \Gamma \to \Gamma \to 1$ di A per Γ.
2. D'altra parte non è vero che per ogni estensione (10.1) il gruppo centrale E ha la struttura di prodotto semidiretto di A mediante Γ perchè in generale non è detto che E contenga un sottogruppo isomorfo a Γ. Ad esempio, si consideri l'estensione

   $$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

   dove la mappa iniettiva è moltiplicazione per 2.

È importante osservare come la definizione 10.1.1 di estensione non si concentri sul solo elemento centrale E, ma consideri l'intera successione esatta nel suo complesso. La ragione di definire le cose in questo modo è che lo stesso gruppo E può definire estensioni diverse, come mostreremo ora. Prima di tutto, però occorre dare una definizione precisa di isomorfismo di estensioni.

Definizione 10.1.3. *Due estensioni del gruppo A per il gruppo Γ con elementi centrali E ed E' si dicono isomorfe se esiste un isomorfismo $f : E \xrightarrow{\sim} E'$ tale che il diagramma*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\alpha} & E & \xrightarrow{\beta} & \Gamma & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_\Gamma} & & \\
0 & \longrightarrow & A & \xrightarrow{\alpha'} & E' & \xrightarrow{\beta'} & \Gamma & \longrightarrow & 0
\end{array}$$

commuti.

È chiaro che questa relazione d'isomorfismo è una relazione d'equivalenza (vedi problema 10.1). Possiamo ora giustificare l'affermazione precedente mostrando come un isomorfismo $f : E \xrightarrow{\sim} E'$ non definisce necessariamente un isomorfismo di estensioni.

Esempio 10.1.4. Sia p un numero primo, $p \neq 2$, e si considerino le $p-1$ estensioni

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\alpha_k} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0, \quad \alpha_k(\bar{1}) = \bar{k}$$

per $k = 1, \ldots, p-1$. Si noti che qualsiasi sia k l'immagine $\alpha_k(\mathbb{Z}/p\mathbb{Z})$ è l'unico sottogruppo di ordine p di $\mathbb{Z}/p^2\mathbb{Z}$ e quindi la mappa β non dipende da k ed è comune a tutte le estensioni. Per ogni scelta di valori distinti r ed s le estensioni corrispondenti alle immersioni α_r ed α_s non sono isomorfe: se lo fossero dovrebbe esistere un isomorfismo $f : \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p^2\mathbb{Z}$ che rende commutativo il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\alpha_r} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\beta} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\ & & \| & & \downarrow f & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\alpha_s} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\beta} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \end{array} .$$

Per la commutatività del rettangolo di sinistra deve aversi $f(\bar{1}) = \bar{h}$ dove $h \neq 1$ soddisfa la relazione $hr \equiv s \pmod{p}$, ma allora $\beta(\bar{1}) \neq \beta(f(\bar{1})$ nega la commutatività del diagramma di destra.

La seguente osservazione completa l'dea di un'estensione come generalizzazione di un prodotto semidiretto e risulterà cruciale per meglio definire il problema di classificazione.

Osservazione 10.1.5. Un'estensione $0 \to A \to E \xrightarrow{\beta} \Gamma \to 1$ definisce un'omomorfismo

$$\Theta : \Gamma \longrightarrow \mathrm{Aut}(A)$$

e quindi un'azione di Γ su A come segue. Dato $\gamma \in \Gamma$ scegliamone un rappresentante $g \in E$ e poniamo $\theta_g : A \to A$ il coniugio per g, cioè $\theta_g(x) = gxg^{-1}$. Se $g' \in E$ è un altro elemento tale che $\beta(g') = \gamma$ si ha $g' = ga$ per un $a \in A$ opportuno e $\theta_{g'}(x) = g'xg'^{-1} = gaxa^{-1}g^{-1} = gxg^{-1} = \theta_g(x)$. Quindi l'automorfismo θ_g dipende solo da γ e può essere denotato θ_γ. Poniamo allora

$$\Theta(\gamma) = \theta_\gamma.$$

Sulla scorta di questa osservazione possiamo supporre che il gruppo abeliano A dato inizialmente sia equipaggiato in partenza con un'azione $\varphi : \Gamma \to \mathrm{Aut}(A)$. Allora, diremo che un'estensione di A per Γ *realizza gli operatori* se $\Theta = \varphi$, cioè se l'azione di Γ su A risultante dalla struttura dell'estensione coincide con quella data preventivamente. Con tale terminologia, possiamo enunciare il problema centrale della teoria:

Problema fondamentale della Teoria delle Estensioni. Assegnati un gruppo abeliano A con un'azione $\varphi : \Gamma \to \mathrm{Aut}(A)$, classificare le estensioni di A per Γ che realizzano gli operatori.

Come primo passo verso la soluzione di questo problema, diamo una caratterizzazione alternativa dei prodotti semidiretti nel linguaggio delle successioni esatte.

Definizione 10.1.6. *Una* sezione *di un'estensione* $0 \to A \to E \xrightarrow{\beta} \Gamma \to 1$ *è una mappa di insiemi*

$$s : \Gamma \longrightarrow E \qquad \textit{tale che } \beta \circ s = \mathrm{id}_\Gamma \textit{ e } s(1) = 1$$

L'estensione si dice spezzata *se esiste una sezione che è un omomorfismo.*

Si noti che in ogni caso una sezione deve essere iniettiva.

Proposizione 10.1.7. *La successione* $0 \to A \to E \xrightarrow{\beta} \Gamma \to 1$ *è spezzata se e soltanto se* E *è prodotto semidiretto di* A *mediante* Γ.

Dimostrazione. Se $E = A \times_\varphi \Gamma$, la sezione $s(\gamma) = (0, \gamma)$ è un omomorfismo.

D'altra parte, se esiste una sezione $s : \Gamma \to E$ che è un omomorfismo, si ha:

- $A \cap s(\Gamma) = \{0\}$, in quanto l'elemento neutro è l'unico elemento di A della forma $(0, \gamma)$,
- $E = As(\Gamma)$, in quanto se $x \in E$ risulta $\beta(xs(\beta(x)^{-1}) = 1$, ovvero $xs(\beta(x))^{-1} \in \ker(\beta) = A$.

Allora E risulta prodotto semidiretto di A mediante $s(\Gamma)$, e quindi l'asserto per l'identificazione tra Γ e $s(\Gamma)$. ■

Definizione 10.1.8. *Sia* A *un gruppo abeliano con un'azione del gruppo* Γ. *Un* sistema di fattori *per* Γ *a coefficienti in* A *è una funzione*

$$\phi : \Gamma \times \Gamma \longrightarrow A$$

tale che

1. $\phi(\gamma, 1) = \phi(1, \gamma)$ *per ogni* $\gamma \in \Gamma$*;*
2. ${}^\gamma\phi(\gamma', \gamma'') - \phi(\gamma\gamma', \gamma'') + \phi(\gamma, \gamma'\gamma'') - \phi(\gamma, \gamma') = 0$ *per ogni* γ, γ', $\gamma'' \in \Gamma$.

Usando la solita definizione di somma di funzioni tra funzioni a valori in un gruppo A, si vede subito che l'insieme $Z^2(\Gamma, A)$ dei sistemi di fattori per Γ a coefficienti in A forma un gruppo abeliano.

Definizione 10.1.9. *Sia* A *un gruppo abeliano con un'azione del gruppo* Γ. *Un* cobordo *per* Γ *a coefficienti in* A *è una funzione* $\phi : \Gamma \times \Gamma \to A$ *per cui esista una funzione* $f : \Gamma \to A$ *con* $f(1) = 0$ *per cui*

$$\phi(\gamma, \gamma') = {}^\gamma f(\gamma') - f(\gamma\gamma') + f(\gamma)$$

per ogni γ, $\gamma' \in \Gamma$.

Anche i cobordi formano un gruppo, denotato $B^2(\Gamma, A)$.

Proposizione 10.1.10. $B^2(\Gamma, A)$ *è un sottogruppo di* $Z^2(\Gamma, A)$.

Dimostrazione. L'asserto si verifica mediante un calcolo diretto. Se ϕ è il cobordo definito dalla funzione f si ha:

- per ogni $\gamma \in \Gamma$, $\phi(\gamma, 1) = {}^\gamma f(1) - f(\gamma) + f(\gamma \cdot 1) = 0$ e $\phi(1, \gamma) = {}^1 f(\gamma) - f(1) + f(1 \cdot \gamma) = 0$;
- per ogni $\gamma, \gamma', \gamma'' \in \Gamma$, ${}^\gamma\phi(\gamma', \gamma'') - \phi(\gamma\gamma', \gamma'') + \phi(\gamma, \gamma'\gamma'') - \phi(\gamma, \gamma') = {}^{\gamma\gamma'} f(\gamma'') - {}^\gamma f(\gamma'\gamma'') + {}^\gamma f(\gamma') - {}^{\gamma\gamma'} f(\gamma'') + f(\gamma\gamma'\gamma'') - f(\gamma\gamma') + {}^\gamma f(\gamma'\gamma'') - f(\gamma\gamma'\gamma'') - {}^\gamma f(\gamma') + f(\gamma\gamma') - f(\gamma) = 0$ perchè i termini dell'ultima espressione si cancellano tutti l'uno con l'altro.

Dunque la funzione ϕ soddisfa le richieste della definizione 10.1.8. ■

Definizione 10.1.11. *Il* secondo gruppo di coomologia *di* Γ *a coefficienti in* A *è il gruppo quoziente*

$$H^2(\Gamma, A) = \frac{Z^2(\Gamma, A)}{B^2(\Gamma, A)}.$$

Il risultato seguente risolve il problema fondamentale della teoria delle estensioni.

Teorema 10.1.12. *Sia A un gruppo abeliano con un'azione del gruppo Γ. C'è una corrispondenza biunivoca canonica*

$$H^2(\Gamma, A) \longleftrightarrow \left\{ \begin{array}{c} \textit{classi di isomorfismo di estensioni di } A \textit{ per } \Gamma \\ \textit{che realizzano gli operatori} \end{array} \right\}.$$

Dimostrazione. Supponiamo assegnata un'estensione $0 \to A \to E \xrightarrow{\beta} \Gamma \to 1$ e scegliamo una sezione $s : \Gamma \to E$. Per ogni γ, $\gamma' \in \Gamma$ poniamo

$$\phi(\gamma, \gamma') = s(\gamma) + s(\gamma') - s(\gamma\gamma').$$

Il calcolo diretto fornisce

- $\phi(\gamma, 1) = s(\gamma) + s(1) - s(\gamma) = 0$ e $\phi(1, \gamma) = s(1) + s(\gamma) - s(\gamma) = 0$ per ogni $\gamma \in \Gamma$;
- $-\phi(\gamma, \gamma') + {}^{\gamma}\phi(\gamma', \gamma'') + \phi(\gamma, \gamma'\gamma'') - \phi(\gamma\gamma', \gamma'') = (s(\gamma\gamma') - s(\gamma') - s(\gamma)) + (s(\gamma) + s(\gamma') + s(\gamma'') - s(\gamma'\gamma'') - s(\gamma)) + (s(\gamma) + s(\gamma'\gamma'') - s(\gamma\gamma'\gamma'')) + (s(\gamma\gamma'\gamma'') - s(\gamma'') - s(\gamma\gamma')) = 0$ perchè i termini si cancellano tutti. Si noti che il riordinamento dei termini ϕ in quest'ultimo calcolo non è causale. Siccome la sezione prende valori in E, che nonostante la notazione additiva non è in generale abeliano, la cancellazione tra elemnto e il suo "opposto"può essere fatta in sicurezza solo quando i termini sono adiacenti.

Per studiare la dipendenza di ϕ dai dati, se $0 \to A \to E' \xrightarrow{\beta'} \Gamma \to 1$ è un'estensione isomorfa alla precedente mediante un isomorfismo $\psi : E \xrightarrow{\sim} E'$ con la scelta di sezione $s' : \Gamma \to E'$ e sistema di fattori ϕ', possiamo passare alla composizione $\psi^{-1} \circ s'$ ed assumere che $E = E'$. Allora se definiamo la funzione

$$f : \Gamma \longrightarrow A, \qquad f(\gamma) = s'(\gamma) - s(\gamma)$$

(che ha veramente immagine in A in quanto $\beta(s'(\gamma)) = \beta(s(\gamma))$) risulta

- $f(1) = s'(1) - s(1) = 0$,
- $s'(\gamma) + s'(\gamma') = f(\gamma) + s(\gamma) + f(\gamma') + s(\gamma') = f(\gamma) + {}^{\gamma}f(\gamma') + s(\gamma) + s(\gamma') = f(\gamma) + {}^{\gamma}f(\gamma') + \phi(\gamma, \gamma') - f(\gamma\gamma') + s'(\gamma\gamma')$ da cui

  $$\phi'(\gamma, \gamma') = \phi(\gamma, \gamma') + f(\gamma) + {}^{\gamma}f(\gamma') - f(\gamma\gamma') \qquad \text{per ogni } \gamma, \gamma' \in \Gamma,$$

  ovvero ϕ e ϕ' definiscono la stessa classe in $H^2(\Gamma, A)$.

Viceversa, assegnato un sistema di fattori $\phi : \Gamma \times \Gamma \to A$ definiamo un'operazione nell'insieme prodotto $E = A \times \Gamma$ ponendo

$$(a, \gamma) + (a', \gamma') = (a + {}^{\gamma}a' + \phi(\gamma, \gamma'), \gamma\gamma')$$

per ogni a, $a' \in A$ e per ogni γ, $\gamma' \in \Gamma$. Con questa operazione E è un gruppo. Infatti:

- vale la proprietà associativa, in quanto per ogni a, a', $a'' \in A$ e γ, γ', $\gamma'' \in \Gamma$ i calcoli $((a, \gamma) + (a', \gamma')) + (a'', \gamma'') = (a + {}^{\gamma}a' + \phi(\gamma, \gamma'), \gamma\gamma') + (a'', \gamma'') = (a + {}^{\gamma}a' + \phi(\gamma, \gamma') + {}^{\gamma\gamma'}a'' + \phi(\gamma\gamma', \gamma''), \gamma\gamma', \gamma'')$ e $(a, \gamma) + ((a', \gamma' + (a'', \gamma''))) = (a, \gamma) + (a' + {}^{\gamma'}a'' + \phi(\gamma', \gamma''), \gamma'\gamma'') = (a + {}^{\gamma}a' + {}^{\gamma\gamma'}a'' + {}^{\gamma}\phi(\gamma', \gamma'') + \phi(\gamma, \gamma'\gamma''), \gamma'\gamma'')$ forniscono il medesimo risultato;
- l'elemento $(0, 1)$ è neutro;

- per ogni $(a, \gamma) \in E$ l'identità

$$(a, \gamma) + (-^{\gamma^{-1}} a - ^{\gamma^{-1}} \phi(\gamma, \gamma'), \gamma^{-1}) = (0, 1)$$

ne definisce l'elemnto inverso.

PROBLEMI

10.1. Verificare che la relazione di isomorfismo di estensioni, definizione 10.1.3, è una relazione d'equivalenza.

Bibliografia

[1] Cameron P. J. e Cohen A. M. On the number of fixed point free elements in a permutation group. *Discrete Math.*, 106:135–138, 1992.

[2] Serre J.-P. On a theorem of Jordan. *Bulletin A. M. S.*, 40:429–440, 2003.

Indice Analitico