Laurea Magistrale in Matematica
Università di Firenze

Teoria dei Gruppi

Carlo Casolo
Corso di Istituzioni di Algebra - a.a. 2013-2014

Indice

Capitolo 1

Richiami

Questo primo capitolo è un elenco (con qualche sparso cenno di dimostrazione) di prerequisiti: ovvero di quei concetti e risultati che il corso assume come noti, e che sono qui riportati per controllo e come riferimento.

1.1 Definizioni, sottogruppi, classi laterali

Un *gruppo* è una coppia $(G, \cdot)$, costituita da un insieme G ed un'operazione binaria $\cdot$ su di esso (cioè un'applicazione $G \times G \to G$, $(a, b) \mapsto a \cdot b$) tale che:

(1) *Per ogni* $a, b, c \in G$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, (proprietà associativa)

(2) *Esiste* $1_G \in G$ *tale che, per ogni* $a \in G$: $a \cdot 1_G = a = 1_G \cdot a$. (esistenza di un elemento neutro)

(3) *Per ogni* $a \in G$ *esiste* $b \in G$ *tale che* $a \cdot b = 1_G = b \cdot a$ (tale b, che è unico, si denota con a^{-1}, e si chiama *inverso* di a).

Nella prassi, trattando di un gruppo generico, non si usa indicare alcun segno di operazione, $a \cdot b$ si scrive semplicemente giustapponendo i due elementi: ab.
Se A è un insieme dotato di un'operazione associativa (quello che si chiama un *semigruppo*), e $a, b, c \in A$, allora possiamo scrivere senza ambiguità abc, intendendo con ciò l'elemento $(ab)c = a(bc)$. Questo fatto si estende ad una qualsiasi stringa finita di elementi. Ad esempio, $a_1a_2a_3a_4 = a_1((a_2(a_3a_4)) = a_1((a_2a_3)\ a_4)) = (a_1a_2)(a_3a_4) =$ etc. elemento che scriviamo semplicemente $a_1a_2a_3a_4$. Più in generale, per ogni $n \geq 1$ ed ogni n-ulpa $(a_1, a_2, \ldots, a_n) \in A^n$, possiamo individuare senza ambiguità l'elemento

$$a_1a_2 \ldots a_n$$

(questa affermazione, che ovviamente vale nei gruppi e che appare ovvia, andrebbe provata con rigore; operazione non difficile ma noiosa; chi è interessato trova una dimostrazione nel testo di M. Artin [1]).

L'unicità dell'elemento neutro in un gruppo G e quella, per ogni $a \in G$, dell'elemento inverso di a, che abbiamo affermato in (2) e in (3), sono immediate conseguenze degli assiomi. Altre immediate conseguenze degli assiomi sono le seguenti.

– *La legge di cancellazione*: se a, b, c sono elementi di un gruppo G tali che $ab = ac$ (o $ba = ca$), allora $b = c$.

– *L'inverso di un prodotto*: se a, b sono elementi di un gruppo G, allora $(ab)^{-1} = b^{-1}a^{-1}$.

Potenze. Sia g un elemento del gruppo G, e $n \in \mathbb{Z}$. La potenza n-esima di g è definita (induttivamente) nel modo seguente:

$$\begin{array}{ll} g^0 = 1_G & \\ g^{n+1} = g^n g & \text{se } n \geq 0 \\ g^n = (g^{-1})^{-n} & \text{se } n < 0. \end{array}$$

In pratica, se $n \geq 0$,

$$g^n = \underbrace{g \cdot g \cdot \cdots \cdot g}_{\text{n volte}}$$

Il seguente Lemma enuncia le regole fondamentali nel trattamento delle potenze di uno stesso elemento; la facile dimostrazione - per induzione su uno degli esponenti (prima il caso di esponente positivo e quindi quello generale) - è lasciata per esercizio (altrimenti, si vedano le dispense di Algebra II [2]).

Lemma 1.1. *Siano G un gruppo, $g \in G$, e $n, m \in \mathbb{Z}$. Allora*

(1) $g^{n+m} = g^n g^m$

(2) $g^{nm} = (g^n)^m$

In generale, la potenza di un prodotto *non è* il prodotto delle potenze; ciò avviene solo in casi molto particolari: vedi esercizio 1.3.

Tipi di gruppi

Gruppi abeliani. Un gruppo G si dice *abeliano*, o *commutativo*, se l'operazione è commutativa, ovvero se $ab = ba$ per ogni $a, b \in G$. Per i gruppi commutativi, si utilizza spesso la *notazione additiva* in cui l'operazione si denota con il simbolo $+$ (mentre la notazione che usiamo in generale, in cui il simbolo dell'operazione è un puntino oppure viene omesso, si dice moltiplicativa). In notazione additiva il simbolo per l'elemento neutro è 0_A (o, semplicemente, 0), mentre se a è un elemento del gruppo abeliano $(A, +)$ il suo inverso si denota con $-a$ (e si chiama "opposto" di a). Infine, se $(A, +)$ è un gruppo abeliano, e $x, y \in A$, si adotta la convenzione di scrivere $x + (-y) = x - y$.
Per gruppi (abeliani) in notazione additiva le potenze assumono naturalmente la forma di multipli. Ad esempio, in notazione additiva la proprietà (1) e (2) si scrivono come $(n+m)g = ng + mg$ e $(nm)g = n(mg)$.
Esempi familiari di gruppoi abeliani sono, con l'usuale operazione di somma, gli insiemi numerici $(\mathbb{Z}, +), (\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$; e, rispetto all'operazione di moltiplicazione, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$, dove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Gruppi lineari. Sia V è uno spazio vettoriale sul campo $\mathbb{K}$, allora l'insieme delle applicazioni lineari $V \to V$ è un anello (l'anello degli endomorfismi di V) rispetto alle operazioni di somma e di composizione, i cui elementi invertibili (le applicazioni lineari invertibili) costituiscono un gruppo (non è commutativo se $\dim_{\mathbb{K}} V \geq 2$) che si denota con $GL(V)$ (vedi sezione 1.5). In generale, se R è un anello, allora l'insieme $U(R)$ degli elementi invertibili di R è un gruppo rispetto alla moltiplicazione indotta da R. Ad esempio, se $R = \mathbb{Z}/12\mathbb{Z}$, allora

$$U(R) = \{\bar{a} = a + 12\mathbb{Z} \mid (a, 12) = 1\} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$$

è un gruppo (moltiplicativo).

Gruppi simmetrici. Esempi fondamentali di gruppi non commutativi sono i gruppi simmetrici. Sia X un insieme. Una *permutazione* di X è un'applicazione biettiva da X in se stesso. L'insieme $(Sym(X), \circ)$ di tutte le permutazioni di X), con l'operazione di composizione è un gruppo, detto il *gruppo simmetrico* su X. Non È facile vedere che se $|X| \geq 3$ allora il gruppo $sym(X)$ non è abeliano (esercizio). Il gruppo simmetrico sull'insieme $I_n = \{1, 2, \ldots, n\}$ si denota abitualmente con S_n e si chiama *gruppo simmetrico di grado n*.

Gruppi finiti. Un gruppo G si dice *finito* se tale è la cardinalità dell'insieme G, *infinito* se la cardinalità dell'insieme G è infinita.

Sottogruppi. Un sottoinsieme H di un gruppo G si dice *sottogruppo* di G (e si scrive $H \leq G$) se soddisfa le seguenti proprietà:

(1) H è *chiuso*; cioè, per ogni $x, y \in H,\ xy \in H$;

(2) $1_G \in H$;

(3) per ogni $x \in G$, se $x \in H$ allora $x^{-1} \in H$.

Un sottogruppo H di un gruppo G è dunque un gruppo rispetto all'operazione indotta da G. Viceversa, si può agevolmente provare che se un sottoinsieme chiuso S di un gruppo G è un gruppo rispetto all'operazione indotta, allora è un sottogruppo di G nel senso della definizione data. Dalla definizione segue immediatamente che se $S \leq H$ e $H \leq G$, allora $S \leq G$. Osserviamo anche che ogni gruppo G ha almeno due sottogruppi: G stesso e $\{1_G\}$. $\{1_G\}$ è detto il *sottogruppo banale* di G, mentre un sottogruppo H si dice *proprio* se $H \neq G$.

Esempio 1.1. Sia $1 \leq n \in \mathbb{N}$, e consideriamo l'insieme delle radici n-esime complesse dell'unità:

$$U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}.$$

Allora U_n è un sottogruppo del gruppo moltiplicativo $\mathbb{C}^*$. Infatti $1 \in U_n$; per ogni $z_1, z_2 \in U_n$, si ha $(z_1 z_2)^n = z_1^n (z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1$ dunque $z_1 z_2 \in U_n$; infine, se $z \in U_n$ allora $(z^{-1})^n = (z^n)^{-1} = 1$ e dunque $z^{-1} \in U_n$. Pertanto, $U_n \leq \mathbb{C}^*$. □

Esempio 1.2. Descriviamo i sottogruppi del gruppo additivo $\mathbb{Z}$ dei numeri interi. Osserviamo, prima di tutto, che se $n \geq 0$, allora l'insieme $n\mathbb{Z}$ dei multipli di n è un sottogruppo di $\mathbb{Z}$. Viceversa, sia $H \leq \mathbb{Z}$. Se $H = \{0\}$, allora $H = 0\mathbb{Z}$. Supponiamo dunque $H \neq \{0\}$; allora, poiché H è chiuso per inversi (opposti - in notazione additiva) si ha $S := -H \cap (\mathbb{N} \setminus \{0\}) \neq \emptyset$. Sia $n = \min S$. Allora $n \in H$ e dunque per definizione di sottogruppo $n\mathbb{Z} \subseteq H$. Sia allora

$h \in H$, e siano $q\, r \in \mathbb{Z}$ con $h = qn + r$ e $0 \leq r \leq n-1$. Si ha che $r = h - nq \in H$; poiché $n \notin S$ (dato che $r < n = \min S$), deve essere $r = 0$, e pertanto $h \in n\mathbb{Z}$. Abbiamo dunque provato il seguente importante fatto:

i sottogruppi del gruppo $(\mathbb{Z}, +)$ sono tutti e soli i sottoinsiemi $n\mathbb{Z}$, al variare di $n \geq 0$. □

Criterio per sottogruppi. Un criterio molto elementare ma anche molto utilizzato per stabilire se un sottoinsieme di un gruppo è un sottogruppo, è il seguente. La dimostrazione, quasi immediata, è lasciata al lettore (che - in caso di necessità - può consultare la dispense di Algebra II [2])

Lemma 1.2. (Criterio per sottogruppi) *Siano G un gruppo e $H \subseteq G$. Sono equivalenti:*

(i) $H \leq G$

(ii) $H \neq \emptyset$ *e* $xy^{-1} \in H$ *per ogni* $x, y \in H$.

Sottogruppo generato. Sia g un elemento di un gruppo G. Le proprietà delle potenze (Proposizione 1.1) implicano che l'insieme di tutte le potenze intere di g,

$$\langle g \rangle = \{g^z \mid z \in \mathbb{Z}\}$$

è un sottogruppo di G. Si chiama il *sottogruppo ciclico generato* da g. Chiaramente, ogni sottogruppo di G contenente l'elemento g deve contenere anche ogni sua potenza. Quindi il sottogruppo ciclico generato da g è il minimo (nel senso dell'inclusione) sottogruppo di G che contiene g. Questa idea, fondamentale, si estende da un singolo elemento ad un qualsiasi sottoinsieme del gruppo G. Si comincia con la seguente Proposizione, la cui facile dimostrazione è lasciata per esercizio.

Proposizione 1.3. *Sia G un gruppo, e siano H, K sottogruppi di G. Allora $H \cap K \leq G$. Più in generale, se $\mathcal{F}$ è una famiglia qualsiasi non vuota di sottogruppi di G, allora $\bigcap_{X \in \mathcal{F}} X$ è un sottogruppo di G.*

Sia ora X un sottoinsieme del gruppo G e considerariamo la famiglia di tutti i sottogruppi di G che contengono X. Essa è non vuota perchè contiene almeno il sottogruppo G, e quindi, per la Proposizione 1.3, ha un elemento minimo (nel senso dell'inclusione) che è l'intersezione di tutti i suoi membri. Tale sottogruppo si denota con $\langle X \rangle$ e si chiama *sottogruppo generato*da X (quando $X = \{x_1, \ldots, x_n\}$ spesso si preferisce scrivere $\langle x_1, \ldots, x_n \rangle$ piuttosto che $\langle \{x_1, \ldots, x_n\} \rangle$). $\langle X \rangle$ è pertanto il minimo sottogruppo di G che contiene X. Se $\langle X \rangle = G$ si dice che X è un *sistema di generatori* di G. Torneremo più ampiamente su questo importantissimo concetto nel capitolo 4.

Classi laterali. Sia H un sottogruppo del gruppo G e sia $x \in G$. La *classe laterale sinistra* di x modulo H è il sottoinsieme di G definito da

$$xH := \{xh \mid h \in H\}.$$

Fissato il sottogruppo H del gruppo G, si definisce una relazione $\sim_H$ su G ponendo, per ogni $x, y \in G$, $x \sim_H y$ se $x^{-1}y \in H$. È molto facile verificare che $\sim_H$ è una relazione d'equivalenza e che, per ogni $x \in G$, la classe di equivalenza di x è

$$[x] = \{a \in G \mid x^{-1}a \in H\} = \{a \in G \mid a = xh \text{ con } h \in H\} = xH.$$

In particolare, quindi, l'nsieme delle classi laterali sinistre modulo H è l'insieme quoziente di G modulo l'equivalenza $\sim_H$, e dunque è una partizione di G.
Poichè due classi di equivalenza coincidono se e solo se i loro rappresentati sono in relazione, si ha il seguente fatto, che è bene avere sempre presente:

$$\textit{per ogni } x, y \in G,\ xH = yH \textit{ se e solo se } x^{-1}y \in H.$$

Un *sistema di rappresentanti* delle classi laterali sinistre di G modulo H è un sottoinsieme S di G tali che ogni classe laterale sinistra modulo H contiene uno ed un solo elemento di S (cioè $|S \cap gH| = 1$ per ogni $x \in G$): questo equivale a dire che $\{gH \mid g \in G\} = \{xH \mid x \in S\}$ e che $x_1H \neq x_2H$ per ogni $x_1, x_2 \in S$ con $x_1 \neq x_2$.

Indice e Teorema di Lagrange. Sia G un gruppo e $H \leq G$. L'*indice* di H in G, che si denota con $[G : H]$, è la cardinalità dell'insieme delle classi laterali (sinistre) di G modulo H:

$$|G : H| = |\{xH \mid x \in G\}|.$$

Ora, per ogni $x \in G$, l'applicazione $\lambda_x : H \to xH$, definita da $\lambda_x(h) = xh\ \forall h \in H$, è - come si dimostra immediatamente - una biezione. Dunque $|xH| = |H|$, per ogni $x \in G$. Poiché l'insieme G è unione disgiunta delle classi laterali distinte modulo H, nel caso finito si deduce il seguente fondamentale risultato.

Teorema 1.4. (Teorema di Lagrange) *Sia G un gruppo finito, e sia $H \leq G$. Allora*

$$|G| = [G : H]|H|.$$

in particolare l'ordine di H divide l'ordine di G.

In modo analogo si definiscono e trattano le classi laterali *destre* di G modulo H. Per ogni $x \in G$ la classe laterale destra di rappresentante x modulo H è l'insieme $Hx = \{hx \mid h \in H\}$. Anche le classi destre modulo H formano una partizione di G, quella associata all'equivalenza $x \sim y \Leftrightarrow xy^{-1} \in H$, quindi, per ogni $x, y \in G$, $Hx = Hy$ se e soltanto se $xy^{-1} \in H$. Mentre, in generale, per $x \in G$, $Hx \neq xH$, si prova (esercizio) che il porre $xH \mapsto Hx^{-1}$ (per ogni $x \in G$) definisce un'applicazione dall'insieme delle classi destre modulo H in quello delle classi sinistre che è una biezione. Dunque, fissato il sottogruppo H di G, la cardinalità dell'insieme di tutte le classi destre modulo H coincide con la cardinalità dell'insieme delle classi sinistre, che è $|G : H|$.

Proposizione 1.5. *Siano H, K sottogruppi di indice finito del gruppo G:*

(1) *Se $K \leq H$ allora $[G : K] = [G : H][H : K]$;*

(2) (Lemma di Poincaré) $[G : H \cap K] \leq [G : H][G : K]$.

Dimostrazione. (1) Sia $K \leq H \leq G$, $|G : H| = n$ e $|H : K| = m$. Siano, rispettivamente, $\{g_1, \ldots, g_n\}$ e $\{h_1, \ldots, h_m\}$ sistemi di rappresentanti delle classi laterali sinistre di G modulo H e di H modulo K. Dato $g \in G$ esistono quindi $i \in \{1, \ldots, n\}$ e $h \in H$ tali che $g = g_ih$. A sua volta, poiché $h \in H$, esistono $j \in \{1, \ldots, m\}$ e $k \in K$ tali che $h = h_jk$. Dunque $g = g_ih_jk \in g_ih_jK$. Questo dimostra che l'insieme $S = \{g_ih_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$

contiene un sistema di rappresentanti delle classi laterali sinistre di G modulo K. Ora, per qualsiasi $1 \leq i, s \leq n$, $1 \leq j, t \leq m$,

$$g_i h_j K = g_s h_t K \;\Rightarrow\; g_s^{-1} g_i h_j \in h_t K \subseteq H \;\Rightarrow\; g_s^{-1} g_i \in H \;\Rightarrow\; g_i H = g_s H \;\Rightarrow\; i = s,$$

da cui segue $h_j K = h_t K$ e quindi $h_t = h_j$ e $j = t$. Pertanto, S è un sistema di rappresentanti delle classi laterali sinistre di G modulo K, e dunque $|G : K| = |S| = |G : H||H : K|$.

(2) Denotiamo con $\mathcal{L}_H$, $\mathcal{L}_K$ e $\mathcal{L}_{H\cap K}$, rispettivamente, l'insieme delle classi laterali sinistre di G modulo H, modulo K e modulo $H \cap K$. Il porre, per ogni $x \in G$, $x(H \cap K) \mapsto (xH, xK)$, definisce un'applicazione da $\mathcal{L}_{H\cap K}$ nel prodotto $\mathcal{L}_H \times \mathcal{L}_K$. Tale applicazione è – come si vede subito – iniettiva, e dunque $|\mathcal{L}_{H\cap K}| \leq |\mathcal{L}_H \times \mathcal{L}_K| = |\mathcal{L}_H||\mathcal{L}_K|$, che è l'enunciato. ∎

Prodotto di sottogruppi. Le classi laterali modulo un sottogruppo sono casi particolari (ma i più importanti) di prodotti di sottoinsiemi di un gruppo. Dati due sottoinsiemi A e B di un gruppo G, il *prodotto* di A e B è il sottoinsieme di G

$$AB = \{ab | a \in A, b \in B\}.$$

Quindi la classe xH non è altro che il prodotto $\{x\}H$. Oltre alle classi laterali, i casi più significativi si hanno quando A e B sono sottogruppi di G: e va subito osservato che, anche in questo caso, il prodotto AB non è necessariamente un sottogruppo, Si ha tuttavia la seguente proposizione.

Proposizione 1.6. *Siano A, B sottogruppi di un gruppo G. Allora AB è un sottogruppo di G se e solo se $AB = BA$.*

Dimostrazione. Sia $AB \leq G$. Allora per ogni $a \in A, b \in B$ si ha $ba = (1_G b)(a 1_G) \in AB$, e quindi $BA \subseteq AB$; per l'inclusione inversa basta osservare che $b^{-1}a^{-1} = (ab)^{-1} \in AB$, quindi $b^{-1}a^{-1} = a'b'$ per qualche $a' \in A$ e $b' \in B$, e dunque

$$ab = (b^{-1}a^{-1})^{-1} = (a'b')^{-1} = b'^{-1}a'^{-1} \in BA$$

Viceversa, supponiamo che $AB = BA$. Chiaramente $AB \neq \emptyset$; siano $x, y \in AB$, possiamo scrivere $x = ab$, $y = b_1 a_1$ con $a, a_1 \in A$ e $b, b_1 \in B$; ora $ba_1^{-1} \in BA = AB$ e dunque esistono $a_2 \in A$, $b_2 \in B$ tali che $ba_1^{-1} = a_2 b_2$; quindi

$$xy^{-1} = (ab)(b_1 a_1)^{-1} = aba_1^{-1}b_1^{-1} = aa_2 b_2 b_1^{-1} \in AB.$$

Per il criterio dei sottogruppi (Lemma 1.2), $AB \leq G$. ∎

Un'altra semplice ma utile osservazione riguarda l'ordine di un prodotto di sottogruppi.

Lemma 1.7. *Siano A e B sottogruppi del gruppo G. Allora*

a) *ogni elemento $g \in AB$ si può scrivere in $|A \cap B|$ modi distinti come prodotto di un elemento di A e di un elemento di B;*

b) $|AB||A \cap B| = |A||B|$. *Se G è finito,* $|AB| = \frac{|A||B|}{|A\cap B|}$

DIMOSTRAZIONE. Per $g \in AB$, sia $U = \{(a,b) \in A \times B \mid ab = g\}$. Fissato un elemento $(a,b) \in U$, sia $\sigma : A \cap B \to U$ l'applicazione definita da $d \mapsto (ad^{-1}, db)$ per ogni $d \in A \cap B$. Chiaramente, σ è iniettiva; sia poi $(a',b') \in U$, allora $ab = g = a'b'$ e quindi $a' = ad^{-1}$, dove $d = b'b^{-1} = a'^{-1}a \in A \cap B$, mostrando che σ è suriettiva. Dunque σ è una biezione, il che prova il punto a).

b) Segue immediatamente dal punto a). ∎

Infine, ancora un'altra osservazione, nota come *regola di Dedekind*, utilizzata - spesso implicitamente - in numerosi argomenti.

Proposizione 1.8. *Siano A, B, U sottogruppi del gruppo G, e sia $U \leq A$ e $UB = BU$. Allora*

$$U(A \cap B) = A \cap UB.$$

DIMOSTRAZIONE. Siano A, B, U come nelle ipotesi. Poiché $U \leq A$, $U(A \cap B) \subseteq A \cap UB$. Viceversa, se $a = ub \in A \cap UB$ (con $u \in U$ e $b \in B$), allora $b = u^{-1}a \in A \cap B$, e dunque $x \in U(A \cap B)$. ∎

Osservazione. Dato un gruppo G, l'insieme $\mathcal{S}(G)$ di tutti i sottogruppi di G ordinato per inclusione (di insiemi) è un insieme parzialmente ordinato. La proposizione 1.3 dice, in particolare, che dati $H, K \leq G$ (cioè $H, K \in \mathcal{S}(G)$), $H \cap K$ è il massimo sottogruppo di G contenuto in H ed in K; cioè $H \cap K$ è l'estremo inferiore di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$. In generale (vedi esercizio sotto), l'unione insiemistica di due sottogruppi non è un sottogruppo. Tuttavia, dati due sottogruppi H, K del gruppo G, la famiglia dei maggioranti di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$ coincide con quella di tutti i sottogruppi di G che contengono $H \cup K$, e quindi ha un minimo, che è $\langle H, K\rangle := \langle H \cup K\rangle$ (pertanto il minimo sottogruppo di G che contiene sia H che K). In altri termini $\langle H, K\rangle$ è l'estremo superiore di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$. Da quanto osservato, risulta quindi che $(\mathcal{S}(G), \subseteq)$ è un reticolo, detto il *reticolo dei sottogruppi* di G.

1.2 Omomorfismi, sottogruppi normali, quozienti

Omomorfismi e isomorfismi. Siano G e G' gruppi. Un *omomorfismo* (di gruppi) di G in G' è un'applicazione $\phi : G \longrightarrow G'$ tale che, per ogni $x, y \in G$,

$$\phi(xy) = \phi(x)\phi(y).$$

Proposizione 1.9. *Sia $\phi : G \longrightarrow G'$ un omomorfismo di gruppi. Allora $\phi(1_G) = 1_{G'}$ e, per ogni $g \in G$, $z \in \mathbb{Z}$, $\phi(g^z) = (\phi(g))^z$ (in particolare $\phi(g^{-1}) = (\phi(g))^{-1}$).*

DIMOSTRAZIONE. Sia $b = \phi(1_G)$. Allora

$$b^2 = \phi(1_G)\phi(1_G) = \phi(1_G 1_G) = \phi(1_G) = b,$$

moltiplicando a destra per b^{-1} si ottiene $b = 1_{G'}$. Sia ora $g \in G$, allora

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(1_G) = 1_{G'}$$

e quindi $\phi(g^{-1}) = (\phi(g))^{-1}$. Fatto questo, procedendo per induzione su z se $z \geq 0$, e applicando poi l'osservazione appena fatta per passare al caso $z < 0$, si dimostra facilmente che $\phi(g^z) = (\phi(g))^z$, per ogni $z \in \mathbb{Z}$. ∎

Un *isomorfismo* dal gruppo G nel gruppo G' è un omomorfismo biettivo di G in G'.

ESEMPIO 1.3. Sia $\mathbb{Z}$ il gruppo additivo dei numeri interi, $n \geq 2$ e $\mathbb{Z}/n\mathbb{Z}$ il gruppo additivo delle classi di congruenza modulo n; allora la riduzione modulo n, $z \mapsto z + n\mathbb{Z}$ ($\forall z \in \mathbb{Z}$) è un omomorfismo suriettivo $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. □

ESEMPIO 1.4. Sia $P = \{x \in \mathbb{R} \mid x > 0\}$. Allora P è un gruppo con l'operazione di moltiplicazione. L'applicazione logaritmo naturale $\ln : P \longrightarrow \mathbb{R}$ definita da, per ogni $x \in P$, $x \mapsto \log_e(x)$ è un isomorfismo del gruppo moltiplicativo $(P, \cdot)$ nel gruppo additivo $(\mathbb{R}, +)$. Infatti, è biettiva e, per ogni $x, y \in P$, $\log_e(xy) = \log_e(x) + \log_e(y)$. L'applicazione inversa è la funzione esponenziale, ed è un isomorfismo da $(\mathbb{R}, +)$ in $(P, \cdot)$ (naturalmente si ottiene un isomorfismo anche considerando il logaritmo in una qualsiasi base positiva $\neq 1$ fissata). □

Proposizione 1.10. *Sia $\phi : G \longrightarrow G'$ un isomorfismo di gruppi. Allora $\phi^{-1} : G' \longrightarrow G$ è un isomorfismo.*

DIMOSTRAZIONE. Siano $a, b \in G'$. Allora, poichè ϕ è un omomorfismo

$$\phi(\phi^{-1}(a)\phi^{-1}(b)) = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = ab = \phi(\phi^{-1}(ab))$$

e, poichè ϕ è iniettiva, si ha $\phi^{-1}(a)\phi^{-1}(b) = \phi^{-1}(ab)$. Quindi ϕ^{-1} è un omomorfismo; poichè è anche biettiva, ϕ^{-1} è un isomorfismo. ■

Un'altra proprietà importante degli omomorfismi e isomorfismi è che la composizione di due di essi è ancora un omomorfismo. La facile dimostrazione è lasciata per esercizio.

Proposizione 1.11. *Siano $\phi : A \longrightarrow B$, $\psi : B \longrightarrow C$ omomorfismi di gruppi. Allora $\psi \circ \phi : A \longrightarrow C$ è un omomorfismo . Se ϕ e ψ sono isomorfismi, $\psi \circ \phi$ è un isomorfismo.*

Gruppi isomorfi. Due gruppi G e G' si dicono *isomorfi* se esiste un isomorfismo da G in G'. Si scrive in tal caso $G \simeq G'$. Dalle proposizioni e osservazioni precedenti segue che $G \simeq G$ (mediante l'applicazione identica), se $G \simeq G'$ allora $G' \simeq G$, e che se $G \simeq G'$ e $G' \simeq G''$ allora $G \simeq G''$.
Due gruppi isomorfi soddisfano le stesse proprietà algebriche, come gruppi. Tutto ciò che, relativamente all'operazione, si può affermare per uno dei due gruppi vale, passando attraverso la corrispondenza biunivoca stabilita dall'isomorfismo, anche per l'altro gruppo.Informalmente, ma convenientemente, si giunge a dire che gruppi isomorfi sono "lo stesso" gruppo.

Automorfismi. Un omomorfismo di un gruppo G in se stesso si dice *endomorfismo* di G; un isomorfismo di G in se stesso si dice *automorfismo* di G. Osserviamo che, per ogni gruppo G, l'applicazione identica ι_G è un automorfismo di G. Dalle Proposizioni 1.10 e 1.11 segue l'importante fatto che l'insieme $Aut(G)$ di tutti gli automorfismi del gruppo G è esso stesso un gruppo rispetto all'operazione di composizione, che guarda caso si chiama *Gruppo degli automorfismi* di G.

Coniugio. Sia G un gruppo e siano $x, g \in G$. Il *coniugato* di x tramite g è l'elemento

$$x^g = g^{-1}xg.$$

Fissato quindi l'elemento $g \in G$, il *coniugio* tramite g è l'applicazione $\sigma_g : G \to G$ definita da $x \mapsto x^g = g^{-1}xg$, per ogni $x \in G$ (si osservi che $x^g = x \Leftrightarrow xg = gx$).

La notazione esponenziale x^g per l'immagine di un elemento si estende nel modo che ci si aspetta all'immagine di un qualsiasi sottoinsieme: se $X \subseteq G$, ovvero

$$X^g = \sigma_g(X) = \{x^g \mid x \in X\}$$

che si chiamerà, ancora, coniugato di X tramite g. La prima osservazione non banale sul coniugio, cioè che è un isomorfismo, è molto semplice e la sua dimostrazione è lasciata per esercizio.

Proposizione 1.12. *Sia G un gruppo, allora per ogni $g \in G$, $\sigma_g \in Aut(G)$.*

Segue in particolare che se $H \leq G$ e $g \in G$ allora $H^g \leq G$, e che la restrizione del coniuguio σ_g ad H determina un isomorfismo $H \to H^g$.

Normalità. Un sottogruppo H di un gruppo G si dice sottogruppo *normale* - e si scrive $H \trianglelefteq G$ - se

$$\text{(n)} \qquad H^g = H \text{ per ogni } g \in G.$$

Una condizione su $H \leq G$, che si riconsce subito essere equivalente ad (n) è la seguente

$$\text{(n}') \qquad x^g \in H \text{ per ogni } x \in H,\ g \in G.$$

Dalla definizione segue immediatamente che in un qualunque gruppo G, il sottogruppo banale $\{1_G\}$ e G sono sottogruppi normali. Un gruppo G si dice *semplice* se $\{1_G\}$ e G sono i soli sottogruppi normali di G. Ad esempio ogni gruppo di ordine primo è semplice (perchè per il Teorema di Lagrange in un gruppo G di ordine primo, $\{1_G\}$ e G sono i soli sottogruppi). Osserviamo inoltre che in un gruppo commutativo ogni sottogruppo è normale. Questo, tranne che per alcune eccezioni (come il gruppo dei quaternioni che definiremo più avanti), non è il caso dei gruppi non commutativi.

Proposizione 1.13. *Siano G un gruppo e $H \leq G$. Allora sono equivalenti:*

(i) $H \trianglelefteq G$

(ii) $Hg = gH$ *per ogni* $g \in G$.

Dimostrazione. Sia $H \trianglelefteq G$ e $g \in G$. Allora, per ogni $x \in H$, $g^{-1}xg = h'$ per qualche $h' \in H$ e dunque $xg = h'g \in Hg$, provando che $Hg \subseteq gH$, Viceversa, per ogni $x \in H$, $gx = gxg^{-1}g = (g^{-1})^{-1}xg^{-1}g \in Hg$, provando che $gH \subseteq Hg$. Dunque $Hg = gH$.

Viceversa, sia $H \leq G$ e supponiamo $Hg = gH$ per ogni $g \in G$. Allora, per ogni $x \in H$, $g \in G$ si ha $xg = gx'$ con $x' \in H$, e di conseguenza $g^{-1}xg = g^{-1}gx' = x' \in H$. ∎

Gruppo quoziente. L'importanza dei sottogruppi normali risiede nel fatto che a partire da essi si definisce la struttura quoziente, Sia G un gruppo e $N \trianglelefteq G$. Denotiamo con G/N l'insieme delle classi laterali di G (destre o sinistre è la stessa cosa per la Proposizione 1.13) modulo N, cioè

$$G/N = \{gN \mid g \in G\}.$$

Su tale insieme si definisce un'operazione (da denotarsi con lo stesso simbolo di quella di G – in generale, quindi, semplicemente accostando gli elementi), ponendo, per ogni $xN, yN \in G/N$:

$$(xN)(yN) = xyN.$$

Si tratta di una buona definizione; infatti se $x_1, y_1 \in G$ sono tali che $x_1N = xN$ e $y_1N = yN$, allora $x^{-1}x_1 \in N$ e $y^{-1}y_1 \in N$; e poichè $N \trianglelefteq G$ si ha: $y^{-1}(x^{-1}x_1)y \in N$, quindi

$$(xy)^{-1}(x_1y_1) = (y^{-1}x^{-1})x_1(yy^{-1})y_1 = (y^{-1}x^{-1}x_1y)(y^{-1}y_1) \in N,$$

e dunque $xyN = x_1y_1N$.
Si prova quindi molto facilmente che G/N con tale operazione è un gruppo, detto *Gruppo quoziente* di G modulo N; più precisamente:

Teorema 1.14. *Sia N un sottogruppo normale del gruppo G. Con l'operazione definita sopra, l'insieme G/N è un gruppo e si ha*

1) $1_{G/N} = 1_GN = N$;

2) per ogni $xN \in G/N, (xN)^{-1} = x^{-1}N$.

Osserviamo che se $N \trianglelefteq G$ allora $|G/N| = |G : N|$. In particolare, per il Teorema di Lagrange, se G è un gruppo finito allora *l'ordine di G/N divide l'ordine di G.*

Lemma 1.15. *Siano $N \trianglelefteq G$ e $B \leq G$; allora $NB = BN$ e $NB \leq G$. In particolare, se N, M sono sottogruppi normali di G, allora NM è un sottogruppo normale di G.*

Dimostrazione. La prima affermazione è una conseguenza piuttosto immediata della definizione di sottogruppo normale e della Proposizione 1.6. La seconda si verifica facilmente usando la definizione di normalità. ∎

Nucleo di un omomorfismo. Sia $\phi : G \to H$ un omomorfismo di gruppi. Il *nucleo* $\ker(\phi)$ di ϕ è l'insieme degli elementi di G la cui immagine tramite ϕ è l'elemento identico:

$$\ker(\phi) = \{x \in G | \phi(x) = 1_{G'}\} = \phi^{-1}(1_{G'}).$$

Lemma 1.16. *Sia $\phi : G \to G'$ un omomorfismo di gruppi.*

(1) *Se $H \leq G$ allora $\phi(H) \leq G'$, in particolare $\phi(G) \leq G'$;*

(2) *se $H \trianglelefteq G$ alllora $\phi(H) \trianglelefteq \phi(G)$;*

(3) *se $T \leq G'$ allora $\phi^{-1}(T) \leq G$;*

(4) *se $T \trianglelefteq G'$ allora $\phi^{-1}(T) \trianglelefteq G$.*

Dimostrazione. Esercizio (oppure, vedi dispense di Algebra II [2]). ∎

Teorema 1.17. *Sia $\phi : G \to H$ un omomorfismo di gruppi; allora*

(1) $\ker(\phi) \trianglelefteq G$;

(2) *ϕ è iniettivo se e solo se* $\ker(\phi) = \{1_G\}$;

(3) *l'applicazione* $\ker(\phi)g \mapsto \phi(g)$ *definisce un isomorfismo da* $G/\ker(\phi)$ *in* $\phi(G)$.

DIMOSTRAZIONE. (1) Posto $K = \ker(\phi)$, si ha $1_G \in K$, e se $a, b \in K$ e $g \in G$, allora $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = 1_{G'}$, e $\phi(g^{-1}ag) = \phi(g)^{-1}\phi(a)\phi(g) = \phi(g)^{-1}\phi(g) = 1_{G'}$ (quindi $ab^{-1} \in K$ e $g^{-1}ag \in K$); dunque $K \trianglelefteq G$ (questo segue anche dal punto (4) del Lemma precedente).
(2) Siano $a, b \in G$; si ha $\phi(a) = \phi(b)$ se e solo se $\phi(ab^{-1}) = 1_{G'}$, ovvero $ab^{-1} \in \ker(\phi)$. Da ciò, (2) segue immediatamente.
(3) Sia $K = \ker(\phi)$. Se $a, b \in G$ allora $Ka = Kb$ se e solo se $ab^{-1} \in K$ e, per quanto appena osservato, ciò avviene se e soltanto se $\phi(a) = \phi(b)$. Quindi è ben definita l'applicazione biettiva $\bar{\phi} : G/K \to \phi(G)$, ponendo , per ogni $Ka \in G/K$, $\bar{\phi}(Ka) = \phi(a)$. Si verifica imediatamente che $\bar{\phi}$ è un omomorfismo; dunque $\bar{\phi}$ è un isomorfismo ∎

ESEMPIO 1.5. l modulo di un numero complesso definisce un omomorfismo $\mu : \mathbb{C}^* \to \mathbb{R}^*$ (di gruppi moltiplicativi: se $z = a + ib \in C^*$, $\mu(z) = |z| = \sqrt{a^2 + b^2}$) . Il nucleo di μ è l'insieme dei complessi sulla circonferenza unitaria di centro l'origine $\ker(\mu) = U = \{z \in \mathbb{C}^* \mid |z| = 1\}$, e l'immagine $\mu(\mathbb{C}^*)$ è l'insieme $\mathbb{R}^+$ dei numeri reali strettamente maggiori di zero. Dunque, per il Teorema 1.17, $\mathbb{C}^*/U \simeq \mathbb{R}^+$. □

Teorema 1.18. (di corrispondenza) *Sia $\phi : G \to G'$ un omomorfismo suriettivo di gruppi e $N = \ker(\phi)$. Allora ϕ definisce una biezione tra l'insieme dei sottogruppi di G che contengono N e l'insieme di tutti i sottogruppi di G'. Tale corrispondenza conserva inclusioni, indici e normalità.*

DIMOSTRAZIONE. Vedi dispense di Algebra II [2]. ∎

Il Teorema di corrispondenza dice in sostanza che, dato un omomorfismo suriettivo di gruppi, il reticolo dei sottogruppi dell'immagine coincide con il reticolo dei sottogruppi del dominio che contengono il nucleo. Un'immediata e importante applicazione riguarda i sottogruppi di un gruppo quoziente: sia N un sottogruppo normale del gruppo G. Si verifica facilmente che

$$\begin{aligned} \pi : G &\to G/N \\ g &\mapsto gN \end{aligned}$$

è un omomorfismo suriettivo di gruppi; si chiama la *proiezione canonica* di G su G/N. Notiamo che $\ker(\pi) = N$. Quest'ultima osservazione, insieme con il Teorema 1.17, ci consente di affermare che *un sottoinsieme di un gruppo è un sottogruppo normale se e solo se è il nucleo di qualche omomorfismo del gruppo.* Inoltre, applicando alla proiezione il Teorema di corrispondenza 1.18, si ha

Teorema 1.19. *Sia G un gruppo e $N \trianglelefteq G$. Allora i sottogruppi del gruppo quoziente G/N sono tutti e soli quelli del tipo H/N al variare di H nell'insieme dei sottogruppi di G che contengono N.*

Teoremi di omomorfismo. Il punto (3) del Teorema 1.17 viene spesso chiamato il *primo Teorema di omomorfismo* per gruppi, lasciando supporre che ve ne siano altri che meritano un numero. E sono infatti il secondo e il terzo, che proviamo qui di seguito. Questi teoremi fanno parte dello strumentario di base nella teoria dei gruppi e sono il più delle volte applicati, quasi automaticamente, senza alcuna menzione.

Teorema 1.20. (secondo T. di omomorfismo) *Siano G un gruppo, $H \leq G$ e $N \trianglelefteq G$. Allora:*

1) $H \cap N \trianglelefteq H$;

2) $\frac{HN}{N} \simeq \frac{H}{H \cap N}$.

Dimostrazione. Consideriamo la restrizione $\eta : H \to G/N$ ad H della proiezione canonica $\pi : G \to G/N$ (quindi $\eta(h) = hN$ per ogni $h \in H$). Allora η è un omomorfismo di gruppi, e

$$\ker(\eta) = \{h \in H \mid \eta(h) = 1_{G/N}\} = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N,$$

in particolare, per il Teorema 1.17, $H \cap N \trianglelefteq H$. Osserviamo ora che, per il Lemma 1.15, $HN \leq G$ e che per ogni $h \in H$, $n \in N$ si ha $hnN = hN$. Dunque

$$\eta(H) = \{\eta(h) \mid h \in H\} = \{hN \mid h \in H\} = \{hnN \mid hn \in HN\ \} = HN/N.$$

L'affermazione 2) segue quindi per per il Primo Teorema di Omomorfismo. ∎

Teorema 1.21. (terzo T. di omomorfismo) *Siano H, K sottogruppi normali del gruppo G e sia $K \leq H$, allora $H/K \trianglelefteq G/K$ e*

$$\frac{G}{H} \simeq \frac{G/K}{H/K}.$$

Dimostrazione. Si applica il Teorema 1.17 all'omomorfismo $\nu : G/K \to G/H$ definito da $\nu(gK) = gH$ per ogni $gK \in G/K$ (si osservi che si tratta infatti di una buona definizione). ∎

Centro di un gruppo. Dato $g \in G$, l'automorfismo σ_g coincide con l'identità se e soltanto se $g^{-1}xg = x$ per ogni $x \in G$, ovvero se $xg = gx$ per ogni $x \in G$. In altre parole, $\sigma_g = \iota_G$ se e soltanto se g commuta con tutti gli elementi di G. È immediato verificare che l'insieme $Z(G)$ degli elementi di questo tipo (che non è vuoto dato che contiene 1) forma un sottogruppo normale del gruppo G, detto il *centro* di G. Dunque,

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

un sottogruppo normale importante, ma che in tanti casi si riduce al sottogruppo banale.

1.3 Prodotti diretti

Dati i gruppi G_1, G_2 si definisce *prodotto diretto* (esterno) di G_1 e G_2 l'insieme

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

dotato dell'operazione naturale per componenti; cioè ponendo, per $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$,

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$$

È chiaro che $G_1 \times G_2$ è un gruppo, con identità $(1_{G_1}, 1_{G_2})$, e $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$ per ogni $(g_1, g_2) \in G_1 \times G_2$, (e, in generale, $(g_1, g_2)^z = (g_1^z, g_2^z)$ per ogni $z \in \mathbb{Z}$).
Ora, in $G = G_1 \times G_2$, consideriamo

$$H_1 = \{(g, 1_{G_2}) \mid g \in G_1\} \quad \text{e} \quad H_2 = \{(1_{G_1}, g) \mid g \in G_2\}.$$

Si osserva che, per ogni $(g_1, g_2) \in G$, si ha $(g_1, g_2) = (g_1, 1)(1, g_2)$, e quindi $G = H_1H_2$. Inoltre, H_1 è il nucleo della proiezione $\pi_2 : G \to G_2$ definita da $\pi_2(g_1, g_2) = g_2$, che è chiaramente un omomorfismo suriettivo; similmente H_2 è il nucleo di $\pi_1 : G \to G_1$, con $\pi_1(g_1, g_2) = g_1$; dunque H_1 e H_2 sono sottogruppi normali di $G_1 \times G_2$. Ricapitolando, sussistono le seguenti proprietà:

D1) $H_1, H_2 \trianglelefteq G_1 \times G_2$;

D2) $G_1 \times G_2 = H_1H_2$;

D3) $H_1 \cap H_2 = \{1_G\}$.

Inoltre, $H_1 \simeq G_1$ e $H_2 \simeq G_2$: anche questo è banale; ad esempio, porre $G_1 \ni g \mapsto (g, 1)$, definisce un isomorfismo $G_1 \to H_1$. Si osservi anche che, per ogni $x \in H_1$ e $y \in H_2$ si ha $xy = yx$. Questa importante osservazione è di fatto una semplicissima conseguenza delle proprietà D1) e D3), che esplicitiamo in generale nel seguente enunciato..

Lemma 1.22. *Siano N, M sottogruppi normali del gruppo G tali che $N \cap M = 1$. Allora $xy = yx$ per ogni $x \in N$ e $y \in M$.*

Dimostrazione. Siano N e M come nell'enunciato, e $x \in N$, $y \in M$. Allora $x^y \in N$ e $(y^{-1})^x \in M$; quindi $x^{-1}y^{-1}xy = x^{-1}x^y = (y^{-1})^x y \in N \cap M = \{1\}$, da cui segue $xy = yx$. ∎

Con l'aiuto di questo Lemma vediamo come le proprietà D1, D2, D3, riferite a due sottogruppi di un gruppo G, caratterizzano quest'ultimo come prodotto diretto.

Teorema 1.23. *Sia G un gruppo e H, K sottogruppi di G tali che*

D1) $H, K \trianglelefteq G$;

D2) $G = HK$;

D3) $H \cap K = \{1_G\}$.

Allora $G \simeq H \times K$.

Dimostrazione. Siano G, H e K come nell'enunciato. Per la condizione D2, l'applicazione

$$\begin{array}{rcl} \phi : H \times K & \to & G \\ (x, y) & \mapsto & xy \end{array}$$

è suriettiva, ed è iniettiva per il punto a) del Lemma 1.7. Per provare che ϕ è omomorfismo, consideriamo $(x, y), (x_1, y_1) \in H \times K$, allora $yx_1 = x_1y$ per il Lemma 1.22 e pertanto:

$$\phi((x, y)(x_1, y_1)) = \phi(xx_1, yy_1) = xx_1yy_1 = xyx_1y_1 = \phi(x, y)\phi(x_1, y_1).$$

Quindi ϕ è un isomorfismo e ciò dimostra il Teorema. ∎

In questa situazione, si dice che G è il *prodotto diretto (interno)* di H e K. Con un abuso di notazione che non produce danni (ma, anzi, aiuta) si scrive ancora $G = H \times K$. Difatti, per quanto osservato dopo la definizione di prodotto diretto esterno, ogni gruppo (isomorfo al) prodotto diretto esterno di due gruppi è prodotto diretto interno di sottogruppi isomorfi ai gruppi dati. Nel seguito, quindi, parleremo semplicemente di prodotto diretto, tralasciando la distinzione tra i casi interno ed esterno.

Un'altra importante caratterizzazione dei prodotti diretti di due sottogruppi è la seguente,

Teorema 1.24. *Sia G un gruppo e $H, K \leq G$. Allora $G = H \times K$ se e solo se:*

a) *ogni elemento di G si scrive in uno ed un solo modo come prodotto di un elemento di H e di un elemento di K;*

b) *per ogni $h \in H$, $k \in K$, $hk = kh$.*

DIMOSTRAZIONE. Esercizio. ∎

L'estensione del concetto di prodotto diretto ad un numero arbitrario e (per il momento) finito di gruppi è piuttosto naturale. Se $H_1, H_2, \ldots, H_n$ sono sottogruppi del gruppo G, il loro prodotto (nell'ordine dato) è l'insieme

$$H_1 H_2 \ldots H_n = \{g \in G |\ g = h_1 h_2 \ldots h_n \text{ con } h_i \in H_i, i = 1, 2, \ldots, n\}$$

Dal Lemma 1.15, mediante una semplice induzione su n, si deduce facilmente che se $H_1, \ldots, H_n$ sono sottogruppi normali di G allora il prodotto $H_1 \ldots H_n$ è un sottogruppo normale di G, che non dipende dall'ordine con cui sono stati considerati i fattori H_i.
Definiamo ora il prodotto diretto (esterno) di n gruppi. Siano $G_1, \ldots G_n$ gruppi; allora il loro *prodotto diretto* è l 'insieme $G_1 \times G_2 \times \cdots \times G_n$ dotato dell'operazione per componenti: per ogni $g_i, h_i \in G_i$ $(i = 1, \ldots, n)$,

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n).$$

È possibile quindi caratterizzare gruppi (isomorfi a un) prodotto diretto di n gruppi in maniera analoga a quella del teorema 1.23. La dimostrazione è lasciata per esercizio.

Proposizione 1.25. *Sia $n \geq 1$ e siano $H_1, \ldots H_n$ sottogruppi del gruppo G tali che*

i) *$H_i \trianglelefteq G$ per ogni $i = 1, \ldots, n$;*

(i) *$G = H_1 H_2 \ldots H_n$*

(iii) *per ogni $i = 1, \ldots, n$, posto $N_i = H_1 \ldots H_{i-1} H_{i+1} \ldots H_n$ (si tratta di un sottogruppo di G per quanto osservato sopra), si ha $H_i \cap N_i = \{1\}$,*

Allora $G \simeq H_1 \times \cdots \times H_n$.

Osserviamo che la condizione (iii) nella Proposizione 1.25 non può essere indebolita richiedendo semplicemente $H_j \cap H_j = \{1\}$ per ogni $i \neq j$. Questo si può vedere prendendo, ad esempio, il gruppo additivo di uno spazio vettoriale di dimensione $n \geq 2$, e considerando sottospazi lineari (che sono in particolare sottogruppi normali) generati da vettori a due a due indipendenti.

Nel seguito non distingueremo, nel linguaggio, tra prodotti diretti esterni ed interni e parleremo semplicemente di "prodotto diretto". Ad esempio, il gruppo additivo di uno spazio vettoriale V di dimensione n sul campo $\mathbb{F}$ *è* il prodotto diretto $\mathbb{F} \times \cdots \times \mathbb{F}$ (n volte).
L'idea di prodotto diretto si estende a famiglie infinite di gruppi; ma su questo ritorneremo più avanti (sezione 2.6). Ricordiamo infine che, nel caso di gruppi abeliani e in notazione additiva, si usa di solito l'espressione "somma diretta" al posto di "prodotto diretto".

1.4 Gruppi ciclici

Abbiamo già osservato che se G è un gruppo e $g \in G$, l'insieme delle potenze intere

$$\langle g \rangle = \{g^z \mid z \in \mathbb{Z}\},$$

è il minimo sottogruppo di G che contiene g e si chiama il sottogruppo *ciclico* generato da g.

Ordine di un elemento. Si dice *ordine* (o periodo) dell'elemento g il numero, che si denota con $|g|$, di potenze distinte di g in G; in altri termini $|g| = |\langle g \rangle|$.

Fissato $g \in G$, le regole sulle potenze (Lemma 1.1) implicano che porre $z \mapsto g^z$, per ogni $z \in \mathbb{Z}$, definisce un omomorfismo $\eta : \mathbb{Z} \to G$ dal gruppo additivo $\mathbb{Z}$ in G. Per definizione si ha $\eta(\mathbb{Z}) = \langle g \rangle$ e (vedi esempio 1.2) esiste $n \geq 0$ tale che $\ker \eta = n\mathbb{Z}$; per il Teorema di omomorfismo si deduce che

$$\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}.$$

Dunque, $|g| = \infty$ se e soltanto se $n = 0$ ovvero se e soltanto se η è iniettivo. Altrimenti, se η non è iniettivo, $n \geq 1$ e di conseguenza $|g| = |\mathbb{Z}/n\mathbb{Z}| = n$ e n è il minimo intero ≥ 1 tale che $g^n = 1_G$. Abbiamo quindi provato il fatto seguente.

Proposizione 1.26. *Siano G un gruppo e $g \in G$. Si verifica allora uno dei casi seguenti.*

(1) $|g| = n < \infty$, $\langle g \rangle = \{g^0 = 1_G,\ g,\ g^2,\ \ldots,\ g^{n-1}\}$, *e* $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

(2) $|g| = \infty$, *tutte le potenze intere di g sono distinte, e* $\langle g \rangle \simeq \mathbb{Z}$

Gruppi ciclici. Un gruppo G si dice *ciclico* se esiste $g \in G$ tale che $G = \langle g \rangle$; in tal caso g è detto un generatore di G. Osserviamo subito che un gruppo ciclico è necessariamente commutativo. Il gruppo additivo $\mathbb{Z}$ è quindi ciclico (e i suoi generatori sono 1 e -1). Un altra importante famiglia di esempi è costituità dai gruppi di radici dell'unità; fissato $n \geq 1$, sia U_n il gruppo moltiplicativo $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Com'è noto, U_n contiene n elementi, che sono i numeri complessi

$$\zeta_i = \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n}$$

con $i = 0, 1, \ldots, n-1$. Posto $\zeta = \zeta_1$, si ha che $\zeta_i = \zeta^i$, per ogni $i = 0, \ldots, n-1$; dunque $U_n = \langle \zeta \rangle$ è un gruppo ciclico e ζ_1 è un suo generatore (ce ne sono altri come vedremo).

È immediato osservare che ogni quoziente di un gruppo ciclico è un gruppo ciclico. La Proposizione 1.26 riconosce che un gruppo è ciclico se e soltento se è (isomorfo a) un quoziente di $\mathbb{Z}$. Si ha quindi il seguente corollario.

Corollario 1.27. *Due gruppi ciclici sono isomorfi se e solo se hanno lo stesso ordine.*

Sottogruppi. Anche i sottogruppi di un gruppo ciclico sono ciclici. La dimostrazione si può ottenere osservando che ciò, come abbiamo osservato, è vero per $\mathbb{Z}$ e quindi (Teorema di corrispondenza) per tutti i suoi quozienti, e concludere applicando la Proposizione 1.26. In modo più diretto, si può riprodurre la dimostrazione già fatta per $\mathbb{Z}$: se H è un sottogruppo del gruppo ciclico $\langle g \rangle$ e $H \neq \{0\}$, allora esiste un minimo intero $m \geq 1$ tale che $g^m \in H$; procedendo come nel caso di $\mathbb{Z}$ si prova quindi che $H = \langle g^m \rangle$. Pertanto

Proposizione 1.28. *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Consideriamo ora un gruppo ciclico $G = \langle g \rangle$ di ordine finito n. Dalla dimostrazione della Proposizione 1.26 segue che, dato $z \in \mathbb{Z}$, $g^z = g^r$ dove r è il resto della divisione di z per n. In particolare evidenziamo l'utilissima osservazione che $g^z = 1_G$ se e soltanto se n divide z. Ora, $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$. Per ogni $0 \leq a \leq n-1$, ci proponiamo di valutare l'ordine del'elemento g^a. Sia quindi $d = |g^a|$ e poniamo $d_1 = n/(a,n)$; allora n divide ad_1, e quindi $(g^a)^{d_1} = g^{ad_1} = 1_G$, da cui segue che d divide d_1; d'altra parte, poiché $1 = (g^a)^d = g^{ad}$, si ha che n divide ad, e dunque $d_1 = \frac{n}{(a,n)}$ divide d (dato che d_1 non ha fattori comuni con $\frac{a}{(a,n)}$). Dunque $d = d_1$; cioè

$$|g^a| = \frac{n}{(a,n)}. \tag{1.1}$$

Da questa identità segue subito che per ogni divisore d di n, $\langle g \rangle$ ha un sottogruppo di ordine esattamente d, quello generato da $g^{n/d}$. Ad esempio, se $\langle g \rangle$ ha ordine 40, allora il sottogruppo $\langle g^5 \rangle$ ha ordine 8, ed è $\langle g^5 \rangle = \{1, g^5, (g^5)^2, \ldots, (g^5)^7\} = \{1, g^5, g^{10}, \ldots, g^{35}\}$.
Viceversa, supponiamo che H sia un sottogruppo di $G = \langle g \rangle$ (con $|G| = n < \infty$) il cui ordine è d. Allora $d|n$ per il Teorema di Lagrange e $H = \langle g^a \rangle$ per la Proposizione 1.28, con $0 \leq a \leq n-1$. Dalla formula (1.1) segue che $(a,n) = n/d$, e quindi a è un multiplo di n/d, da cui $g^a \in \langle g^{n/d} \rangle$ ovvero $H \leq \langle g^{n/d} \rangle$. Pioiché H e $\langle g^{n/d} \rangle$ hanno lo stesso ordine finito, si conclude che $H = \langle g^{n/d} \rangle$. Abbiamo dunque provato la seguente importante proprietà dei gruppi ciclici finiti.

Teorema 1.29. *Sia $G = \langle g \rangle$ un gruppo ciclico di ordine finito n; allora, per ogni divisore positivo d di n, G ha uno ed un solo sottogruppo di ordine d, che è quello generato da $g^{n/d}$.*

Ci fermiamo un istante per ricavare un'informazione utile.

Proposizione 1.30. *Un gruppo abeliano è semplice se e soltanto se è ciclico di ordine primo.*

Dimostrazione. Che un gruppo ciclico di ordine primo sia semplice è un'immediata conseguenza del Teorema di Lagrange. Viceversa, sia A un gruppo abeliano semplice. Poiché ogni suo sottogruppo è normale, A è ciclico. Si deduce allora da 1.28 e 1.29 che A ha ordine primo. ∎

Generatori e funzione di Eulero. Sia $G = \langle g \rangle$ un gruppo ciclcio. Se G è infinito allora le potenze intere di g sono tutte distinte; in particolare, se $a \in \mathbb{Z}$, $g \in \langle g^a \rangle$ se e solo se esiste $b \in \mathbb{Z}$ tale che $g = g^{ab}$ ovvero $ab = 1$;, quindi $a = 1$ oppure $a = -1$. Pertanto, i generatori di G sono solo g e g^{-1}.
Supponiamo ora $|g| = n < \infty$, e sia $0 \leq a \leq n-1$. Allora $\langle g^a \rangle = \langle g \rangle$ se e soltanto se

$$\frac{n}{(a,n)} = |g^a| = |g| = n,$$

e ciò si verifica se e soltanto se $(a,n) = 1$. Pertanto i generatori di un gruppo ciclico $\langle g \rangle$ di ordine finito n sono tutti e soli gli elementi del tipo g^a con $1 \leq a \leq n-1$ tali che $(a,n) = 1$. In altre parole *il numero di generatori distinti di un gruppo ciclico di ordine n coincide con il numero di interi positivi strettamente minori di n e coprimi con n.* Tale numero si denota con $\phi(n)$ dove ϕ è la *funzione di Eulero.* In particolare, in un gruppo ciclico di ordine primo ogni elemento diverso da 1 è un generatore. La dimostrazione delle seguenti proprietà della

funzione di Eulero (che non useremo immediatamente) si può trovare in qualsiasi introduzione alla teoria elementare dei numeri (o nelle dispense di algebra I).

Proposizione 1.31. 1) *Siano p un numero primo e $a \geq 1$, allora*

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).$$

2) *Siano $n, m \geq 1$; se $(n,m) = 1$ allora $\phi(nm) = \phi(n)\phi(m)$.*

3) *Sia $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, con $p_1, p_2, \ldots, p_s$ primi distinti, allora*

$$\phi(n) = \prod_{i=1}^{s} p_i^{a_i - 1}(p_i - 1).$$

Ad esempio, $\phi(40) = \phi(5)\phi(2^3) = (5-1)(2-1)2^2 = 4 \cdot 4 = 16$. Dunque, se $\langle g \rangle$ è un gruppo ciclico di ordine 40, i suoi generatori distinti sono i 16 elementi g^a con $1 \leq a \leq 39$ e $(a, 40) = 1$.

Automorfismi. Sia $G = \langle g \rangle$ un gruppo ciclico, e sia $\phi \in Aut(G)$. È chiaro che allora $G = \phi(G) = \langle \phi(g) \rangle$; dunque $\phi(g)$ è un generatore di G. Viceversa, sia g^a un generatore di G; allora ponendo, per ogni $z \in \mathbb{Z}$

$$\phi(g^z) = (g^a)^z$$

si definisce un automorfismo di G (si noti che, nel caso in cui G è finito occorre provare che quella data sopra è una buona definizione).
Nel caso $|g| = \infty$ concludiamo subito che $Aut(\langle g \rangle)$ contiene solo due elementi: l'identità e l'inversione. Ma anche nel caso finito non è difficile descrivere il gruppo degli automorfismi di un gruppo ciclico. Ricordo che, se R è un anello, con $U(R)$ denotiamo il gruppo moltiplicativo degli elementi invertibioli di R.

Teorema 1.32. *Sia G un gruppo ciclico.*

(i) *Se G è infinito, $Aut(G) \simeq \{1, -1\}$;*

(ii) *se $|G| = n$, $Aut(G) \simeq U(\mathbb{Z}/n\mathbb{Z})$.*

Dimostrazione. Il punto (i) è già stato giustificato sopra. Supponiamo quindi che $G = \langle g \rangle$ abbia ordine finito $n \geq 2$ (il caso $n = 1$ è banale). Dato $a \in \mathbb{Z}$, sia $a + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$; allora, per un fatto ben noto, $(a, n) = 1$, e quindi g^a è un generatore di G, Denotiamo con ϕ_a l'automorfismo di G definito come sopra da $g \mapsto g^a$. ϕ_a dipende solo dalla classe di congruenza $a + n\mathbb{Z}$, ed è quindi possibile definire un'applicazione $\alpha : U(\mathbb{Z}/n\mathbb{Z}) \to Aut(G)$, ponendo $a + n\mathbb{Z} \mapsto \phi_a$ per ogni $a + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$. Poiché, per ogni $a, b \in \mathbb{Z}$, $g^{ab} = g^(ba) = (g^b)^a$, tale applicazione è un omomorfismo del gruppo moltiplicativo $U(\mathbb{Z}/n\mathbb{Z})$ in $Aut(G)$, e siccome – per quanto prima osservato – $|Aut(G)| = \phi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$, si conclude che si tratta di un isomorfismo. ∎

Di fatto, è possibile descrivere con accuratezza la struttura del gruppo moltiplicativo $U(\mathbb{Z}/n\mathbb{Z})$, e quindi del gruppo degli automorfismi di un gruppo ciclico; per il momento ci basta la seguente osservazione.

Corollario 1.33. *Sia G un gruppo ciclico; allora $Aut(G)$ è un gruppo abeliano. Se inoltre G ha ordine primo p, $Aut(G)$ è ciclico di ordine $p-1$.*

Decomposizione primaria dei gruppi ciclici. Sia $n = p_1^{s_1} \dots p_t^{s_t}$, dove $p_1, \dots, p_t$ sono primi distinti e $s_i \geq 1$ per $i = 1, \dots, t$, e sia C_n un gruppo ciclico di ordine n. Per ogni indice $i = 1, \dots t$, C_n contiene un unico sottogruppo P_i di ordine $p_i^{s_i}$. P_i è ciclico ed è normale (poiché C_n è abeliano). Applicando il Lemma 1.15, la formula del Lemma 1.7 e una semplice induzione si vede che per ogni insieme $\{i_1, \dots, i_k\} \subseteq \{1, \dots, t\}$, il prodotto $P_{i_1} \dots P_{i_k}$ è un sottogruppo normale di C_n di ordine $\prod_{j+1}^{k} |P_{i_j}|$. Da ciò segue subito che la famiglia dei sottogruppi $P_1, \dots, P_t$ di C_n soddisfa alle ipotesi della Proposizione 1.25, e dunqe

$$C_n = P_1 \times P_2 \times \dots \times P_t. \tag{1.2}$$

Quindi: *ogni gruppo ciclico finito è prodotto diretto di gruppi ciclici i cui ordini sono potenze di numeri primi distinti.* In particolare (vedi esercizio 1.25) si ha che

$$Aut(C_n) = Aut(P_1) \times \dots \times Aut(P_t).$$

1.5 Gruppi di matrici

Gruppi di matrici. Sia R una anello commutativo con unità, e sia $1 \leq n \in \mathbb{N}$. Denotiamo con $\mathcal{M}_n(R)$ l'insieme di tutte le matrici quadrate di ordine n a coefficienti in R. È noto che, con le operazioni di addizione per componenti e moltiplicazione righe×colonne, $\mathcal{M}_n(R)$ è un anello. In un tale anello si definisce il determinante in modo del tutto analogo a come si fa nel caso, forse più familiare, delle matrici a coefficienti in un campo; e, come in tal caso, si dimostra che $A \in \mathcal{M}_n(R)$ è invertibile se e solo se $\det A$ è invertibile in R. Dunque, con l'operazione di prodotto righe×colonne,

$$GL(n, R) = \{A \in \mathcal{M}_n(R) \mid \det A \in U(R)\}$$

è un gruppo, detto il *gruppo generale lineare* di dimensione n su R. Se $R = \mathbb{F}$ è un campo, allora ogni elemento non zero di $\mathbb{F}$ è invertibile, e quindi

$$GL(n, \mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det A \neq 0\}.$$

Altro caso interessante si ha per $R = \mathbb{Z}$;

$$GL(n, \mathbb{Z}) = \{A \in \mathcal{M}_n(\mathbb{Z}) \mid \det A \in \{1, -1\}\}.$$

Un gruppo G si dice *lineare* se esistono un campo $\mathbb{F}$ ed un intero $n \geq 1$ tali che G è isomorfo ad un sottogruppo di $GL(n, \mathbb{F})$. Mentre ogni gruppo finito è lineare, esistono molti gruppi (infiniti) che non lo sono.

Tornando al caso generale (R è un anello commutativo), l'applicazione determinante, come è noto dall'algebra lineare, induce un omomorfismo suriettivo

$$\det : GL(n, R) \longrightarrow U(R).$$

dal gruppo lineare $GL(n, R)$ nel gruppo moltiplicativo degli elementi invertibili di R. Il nucleo di tale omomorfismo, che è l'insieme delle matrici di determinante 1,

$$SL(n, R) = \{A \in \mathcal{M}_n(R) \mid \det A = 1\}$$

è un sottogruppo normale di $GL(n, R)$ che si chiama *gruppo speciale lineare* (di dimensione n su R). Per il Teorema di omomorfismo:

$$\frac{GL(n, R)}{SL(n, R)} \simeq U(R).$$

Così, ad esempio, $GL(n, \mathbb{Z})/SL(n, \mathbb{Z}) \simeq \{1, -1\}$ e, se $R = \mathbb{F}$ è un campo

$$\frac{GL(n, \mathbb{F})}{SL(n, \mathbb{F})} \simeq \mathbb{F}^*. \tag{1.3}$$

Naturalmente, al di là del determinante, la natura geometrica dei gruppi di matrici è un aspetto fondamentale nel loro studio anche dal punto di vista più strettamente algebrico. Almeno nel caso in cui i coefficienti sono tolti da un campo (caso sul quale, per semplicità, ci concentreremo da qui in avanti), il tramite è ben noto. Dato lo spazio vettoriale n-dimensionale $V = \mathbb{F}^n$ sul campo $\mathbb{F}$, e fissata una base di V (il più delle volte quella canonica), si stabilisce una corrispondenza biunivoca (di fatto un isomorfismo) tra l'anello delle applicazioni lineari da V in sé e quello delle matrici $\mathcal{M}_n(\mathbb{F})$, che ristretto agli automorfismi fornisce un isomorfismo tra il gruppo $GL(V)$ delle applicazioni lineari biettive da V in sé e il gruppo di matrici $GL(n, \mathbb{F})$. Un aspetto importante da tener presente è che, fissata una di queste corrispondenze tra $GL(V)$ e $GL(n, \mathbb{F})$, il cambiamento di base in V corrisponde in $GL(n, \mathbb{F})$ al coniugio mediante la matrice P che descrive il cambiamento della base.

Così, ad esempio, per determinare quale sia il centro del gruppo $GL(n, \mathbb{F})$ (limitiamoci al caso di coefficienti su un campo $\mathbb{F}$) con $n \geq 1$, si possono fare considerazioni di calcolo matriciale, ma si può anche osservare che un elemento A in $G = GL(n, \mathbb{F})$ appartiene al centro di G se e soltanto se $P^{-1}AP = A$ per ogni $P \in G$; ciò significa che l'isomorfisimo $\mathbb{F}^n \to \mathbb{F}^n$ associato ad A non dipende dalla scelta della base su $\mathbb{F}^n$. Si deduce in modo abbastanza ovvio che V deve risultare un autospazio per A relativo ad un unico autovalore, e quindi che A deve essere una matrice scalare (cioè del tipo $A = \lambda I_n$, dove $\lambda \in \mathbb{F}^*$ e I_n la matrice identica). Abbiamo quindi la seguente:

Proposizione 1.34. *Sia $\mathbb{F}$ un campo e $n \geq 1$; allora*

- *$Z(GL(n, \mathbb{F})) = \{\lambda I_n \mid \lambda \in \mathbb{F}^*\}$ è isomorfo al gruppo moltiplicativo $\mathbb{F}^*$;*
- *$Z(SL(n, \mathbb{F})) = \{\lambda I_n \mid \lambda \in \mathbb{F},\ \lambda^n = 1\}$ è isomorfo al gruppo delle radici n-esime dell'unità in $\mathbb{F}^*$.*

(La dimostrazione relativa al caso del gruppo speciale è lasciata per esercizio.). I gruppi quoziente di $GL(n, \mathbb{F})$ e $SL(n, \mathbb{F})$ modulo il loro centro si denotano con $PGL(n, \mathbb{F})$ e $PSL(n, \mathbb{F})$, e si chiamano, rispettivamente, il gruppo *generale proiettivo* e il gruppo *speciale proiettivo* di dimensione $n-1$ sul campo $\mathbb{F}$. Dal punto di vista pi'algebrico, un importante fatto - che non dimostreremo - riguardante i gruppi proiettiviè è il seguente:

Teorema 1.35. *Per ogni $n \geq 2$ il gruppo $PSL(n, \mathbb{F})$ è un gruppo semplice non abeliano tranne nei casi $n = 2$ e $|\mathbb{F}| = 2, 3$.*

Il centro di $G = GL(n, \mathbb{F})$ è dunque contenuto nell'insieme delle matrici diagonali (invertibili), insieme che a sua volta forma un sottogruppo di G, che denotiamo con $D(n, \mathbb{F})$. È immediato constatare che $D(n, \mathbb{F})$ è isomorfo al prodotto diretto $\mathbb{F}^* \times \cdots \times \mathbb{F}^*$ (n volte) e che, tranne nel caso banale $n = 1$, non è normale in G.
A sua volta, $D(n, \mathbb{F})$ è contenuto nell'insieme $T(n, \mathbb{F})$ delle matrici triangolari superiori invertibili, ovvero, le matrici i cui elementi sotto la diagonale principale sono tutti zero, e non vi sono zeri sulla diagonale principale,

$$T(n, \mathbb{F}) = \{(a_{ij}) \in \mathcal{M}_n(\mathbb{F}) \mid a_{ij} = 0 \text{ per } j < i,\ a_{ii} \neq 0\}$$

Anche $T(n, \mathbb{F})$, come si verifica facilmente, è un sottogruppo (non normale) di $GL(n, \mathbb{F})$. Fissati $n \geq 1$ e il campo $\mathbb{F}$, scriviamo $T = T(n, \mathbb{F})$, $D = D(n, \mathbb{F})$ e U l'insieme delle matrici *unitriangolari* (superiori):

$$U = UT(n, \mathbb{F}) = \{(a_{ij}) \in \mathcal{M}_n(\mathbb{F}) \mid a_{ij} = 0 \text{ per } j < i,\ a_{ii} = 1, \forall i = 1, \ldots, n\}$$

Proposizione 1.36. *Con le notazioni di sopra si ha: $U \trianglelefteq T$, $UD = T$ e $U \cap D = \{1\}$.*

Dimostrazione. Esercizio. ∎

Esempio 1.6. Restringiamoci al caso di dimensione $n = 2$; quindi $G = GL(2, \mathbb{F})$ ($\mathbb{F}$ un campo). Allora

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \mathbb{F} \right\}, \qquad D = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{F}^* \right\}$$

e si osserva facilmente che U e D sono isomorfi, rispettivamente, al gruppo additivo $\mathbb{F}$ ed al gruppo moltiplicativo $\mathbb{F}^* \times \mathbb{F}^*$. Consideriamo per un attimo le intersezioni con il gruppo speciale $S = SL(2, \mathbb{F})$; chiaramente $U \leq S$, mentre $D \cap S = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| a \in \mathbb{F}^* \right\}$ è isomorfo al gruppo moltiplicativo $\mathbb{F}$. □

Tornando al caso generale, è utile poter considerare un'interpretazione geometrica dei sottogruppi di $GL(n, \mathbb{F})$ introdotti sopra. Vediamola, ad esempio, per $T = T(n, \mathbb{F})$. Sia $e_1, \ldots, e_n$ la base canonica dello spazio $V = \mathbb{F}^n$, associando ad $A \in GL(n, \mathbb{F})$ la trasformazione lineare di V data per moltiplicazione a sinistra ($\forall \mathbf{v} \in V, \mathbf{v} \mapsto A\mathbf{v}^T$), allora gli elementi di T sono precisamente le matrici che lasciano invariante la catena di sottospazi:

$$\{0\} \leq \langle e_1 \rangle \leq \langle e_1 \rangle \oplus \langle e_2 \rangle \leq \cdots \leq \langle e_1 \rangle \oplus \langle e_2 \rangle \oplus \cdots \oplus \langle e_n \rangle = V.$$

Ordini. Concludiamo questa primo assaggio di gruppi lineari, con alcune considerazioni riguardanti il loro ordine, nel caso che $\mathbb{F}$ sia un campo finito. Sia quindi q una potenza di un numero primo e $\mathbb{F} = GF(q)$ il campo con q elementi. In questo caso, per $n \geq 1$, invece di $GL(n, GF(q))$ o $SL(n, GF(q))$ si scrive $GL(n, q)$ e, rispettivamente, $SL(n, q)$.

Il numero di elementi di $GL(n, q)$ è uguale al numero di basi ordinate $(\mathbf{a_1}, \ldots, \mathbf{a_n})$ dello spazio $V = GF(q)^n$ (una matrice a coefficienti su un campo è invertibile se e soltanto se le

sue colonne, come vettori n-dimesionali, sono linearmente indipendenti). Tale numero può essere calcolato come segue:
- $\mathbf{a_1}$ può essere scelto arbitrariamente tra i $|V| - 1 = q^n - 1$ vettori non nulli di V.
- $\mathbf{a_2}$ può essere scelto arbitrariamente tra i vettori di V che non sono dipendenti con $\mathbf{a_1}$, il numero di scelte è quindi $|V| - |\mathbb{F}\mathbf{a_1}| = q^n - q = q(q^{n-1} - 1)$.
- una volta scelti i primi $\mathbf{a_1}, \ldots, \mathbf{a_i}$, la scelta del successivo vettore della base può essere effettuata arbitrariamente tra i vettori di V che non appartengono al sottospazio generato dai vettori già scelti; quindi il numero di scelte al passo $i + 1$ è

$$|V| - |\mathbb{F}\mathbf{a_1} \oplus \cdots \oplus \mathbb{F}\mathbf{a_i}| = q^n - q^i = q^i(q^{n-i} - 1).$$

Pertanto, l'ordine del gruppo $GL(n, q)$, ovvero il numero di basi ordinate distinte di V, è

$$|GL(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i) = \prod_{i=0}^{n-1} q^i(q^{n-i} - 1) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1) \tag{1.4}$$

Dalla (1.3) segue inoltre

$$|SL(n,q)| = \frac{|GL(n,q)|}{|GF(q)^*|} = \frac{|GL(n,q)|}{q-1}. \tag{1.5}$$

Ad esempio: $|GL(2,q)| = q(q^2-1)(q-1)$ e $|SL(2,q)| = q(q^2-1) = q(q+1)(q-1)$.
Dalla Proposizione 1.34 segue poi $|Z(GL(n,q))| = q-1$. Il caso del gruppo speciale è un poco meno immediato: $GF(q)^*$ è un gruppo ciclico di ordine $q-1$, e le radici n-esime dell'unità in esso contenute costituiscono un suo sottogruppo; dunque il numero di radici n-esime nel campo $GF(q)$ è un divisore di $|GF(q)^*| = q-1$ e di n, quindi è un divisore di $d = (q-1, n)$; d'altra parte, per il Teorema 1.29, $GF(q)^*$ contiene esattamente un sottogruppo di ordine d, i cui elementi sono necessariamente radici n-esime dell'unità. Pertanto, a causa della Proposizione 1.34, si conclude che

$$|Z(SL(n,q))| = (n, q-1). \tag{1.6}$$

1.6 Il gruppo simmetrico

In queste note useremo di preferenza, per le permutazioni, la notazione a destra (o esponenziale): se f è una permutazione dell'insieme X e $x \in X$, scriviamo xf o x^f invece di $f(x)$.

Gruppo simmetrico. Se X è un insieme: con $Sym(X)$ si denota il gruppo, rispetto alla composizione, di tutte le permutazioni su X (detto *gruppo simmetrico* su X).

Osserviamo subito che se X e Y sono insiemi della stessa cardinalità, e $f : X \to Y$ è una biezione, allora porre $\alpha \mapsto f^{-1}\alpha f$, per ogni $\alpha \in Sym(X)$, definisce un isomorfismo $Sym(X) \longrightarrow Sym(Y)$. Quindi,

Proposizione 1.37. *Siano X e Y insiemi. Allora $|X| = |Y| \Rightarrow Sym(X) \simeq Sym(Y)$.*

In particolare, se X è un insieme finito di cardinalità n, possiamo assumere che X coincida con $I_n = \{1, 2, \ldots, n\}$. In tal caso, invece di $Sym(I_n)$, viene usato il simbolo S_n. Ricordiamo il fatto ben noto che, se $n \in \mathbb{N}$, allora $|S_n| = n!$.

Se $\sigma \in Sym(X)$, chiamiamo *supporto* di σ l'insieme degli elementi di X non fissati da σ:

$$supp(\sigma) = \{x \in X \mid x\sigma \neq x\}.$$

Cicli. Sia k intero, $k \geq 1$; una permutazione $\pi \in Sym(X)$ si dice un *ciclo di lunghezza* k (o un k-*ciclo*) se esiste un sottoinsieme di ordine k, $\{i_1, i_2, \ldots, i_k\} \subseteq X$, tale che

(a) $i_1\pi = i_2$, $i_2\pi = i_3$, ..., $i_{k-1}\pi = i_k$, $i_k\pi = i_1$;

(b) $j\pi = j$ per ogni $j \in X \setminus \{i_1, i_2, \ldots, i_k\}$.

In tal caso, scriviamo $\pi = (i_1\ i_2\ \ldots\ i_k)$.

Ad esempio, la permutazione $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix} \in S_5$ è un 4-ciclo: $\sigma = (1\ 3\ 2\ 4)$.

Un ciclo di lunghezza 2, ovvero una permutazione del tipo $\tau = (i_1\ i_2)$, si chiama *trasposizione*. Due cicli σ, ρ si dicono *disgiunti* se $supp(\sigma) \cap supp(\rho) = \emptyset$.

Le seguenti osservazioni si dimostrano con un po' di pazienza, ma facilmente.

Sia $\sigma = (i_1\ i_2\ \ldots\ i_k)$, un k-ciclo. allora

1) $\sigma = (i_k\ i_{k-1}\ \ldots\ i_2\ i_1) = (i_1\ i_k\ \ldots\ ; i_3\ i_2) = \ \ldots$
2) $\sigma^{-1} = (i_2\ i_3\ \ldots\ i_k\ i_1) = (i_3\ i_4\ \ldots\ i_k\ i_1\ i_2)$.
3) Per $1 \leq r \leq k$

$$(i_j)\sigma^r = \begin{cases} i_{j+r} & \text{se} \quad j + r \leq k \\ i_{j+r-k} & \text{se} \quad j + r > k. \end{cases}$$

Si ha poi - sempre piuttosto facilmente - la seguente conseguenza.

Lemma 1.38. *Sia $\sigma \in Sym(X)$ un ciclo di lunghezza k; allora $|\sigma| = k$. Se $\sigma, \rho \in Sym(X)$ sono cicli disgiunti, allora $\sigma\rho = \rho\sigma$.*

L'inverso di un k-ciclo è, come abbiamo visto, un k-ciclo; mentre in generale la potenza di un ciclo non è un ciclo: ad esempio, se $\sigma = (1\ 2\ 6\ 5\ 4\ 3)$, allora $\sigma^2 = (1\ 6\ 4)(2\ 5\ 3)$.
Se X è finito, ogni permutazione (non identica) di X si può fattorizzare come prodotto di cicli a due a due disgiunti:

Teorema 1.39. *Sia X un insieme finito; ogni $\pi \in Sym(X)$, $\pi \neq \iota$, si può fattorizzare come un prodotto*

$$\pi = \sigma_1\sigma_2 \ldots \sigma_t$$

di cicli $\sigma_1, \sigma_2, \ldots, \sigma_t \in S_n$ a due a due disgiunti. A meno dell'ordine dei fattori, tale fattorizzazione di π è unica.

DIMOSTRAZIONE. Vedi dispense di Algebra II, [2]. ∎

Coniugio. Il Teorema 1.39 implica, in particolare, che le lunghezze dei cicli disgiunti che compongono la fattorizzazione di una permutazione finitaria σ sono univocamente individuate (con molteplicità) da σ stessa. La sequenza di tali lunghezze (poste – diciamo – in ordine crescente) si chiama il *tipo ciclico* di σ. Nel caso di permutazioni finite (cioè $\sigma \in S_n$), si contano anche i cicli di lunghezza 1, cioè i punti lasciati fissi da σ, e il tipo ciclico di una permutazione $\sigma \in S_n$ viene rappresentato mediante la sequenza $[a_1, \dots, a_n]$, dove per ogni $1 \leq i \leq n$, a_i indica il numero di cicli di lunghezza i nella decomposizione di σ (ad esempio la permutazione $(1\ 3\ 4)(6\ 8)(2\ 5\ 9) \in S_9$ ha tipo ciclico $[1, 1, 2]$); osserviamo che si ha $a_1 + a_2 + \cdots + a_n = n$. Mediante ecniche di conteggio relativamente semplici si prova che il numero di permutazioni distinte di S_n con tipo ciclico $[a_1, \dots, a_n]$ è

$$\prod_{i=1}^{n} \frac{i}{i^{a_i} a_i!} = \frac{n!}{1^{a_1} 2^{a_2} \cdots n^{a_n} a_1! a_2! \cdots a_n!}. \tag{1.7}$$

La verifica della seguente osservazione è lasciata per esercizio.

Lemma 1.40. *Sia $\sigma = (i_1\ i_2\ \dots\ i_k)$ un k-ciclo in $Sym(X)$ e $\pi \in Sym(X)$. Allora*

$$\sigma^\pi = \pi^{-1}\sigma\pi = (i_1\pi\ i_2\pi\ \dots\ i_k\pi).$$

In particolare, la permutazione coniugata σ^π è un k-ciclo.

Da ciò segue che due permutazioni coniugate di un insieme finito hanno lo stesso tipo ciclico. Questo è abbastanza naturale: un fatto importante è che l'implicazione si inverte.

Teorema 1.41. *Siia X finito; due permutazioni γ e δ di X sono coniugate in $Sym(X)$ se e solo se hanno lo stesso tipo ciclico.*

DIMOSTRAZIONE. Proviamo che se γ e δ hanno lo stesso tipo ciclico, esiste $\pi \in Sym(X)$ tale che $\gamma^\pi = \delta$. Sia $\gamma = (a_1\ a_2\ \dots\ a_h)(b_1\ b_2\ \dots\ b_k)\dots$ e $\delta = (\hat{a}_1\ \hat{a}_2\ \dots\ \hat{a}_h)(\hat{b}_1\ \hat{b}_2\ \dots\ \hat{b}_k)\dots$ e siano $fix(\gamma) = X \setminus supp(\gamma)$ e $fix(\delta) = X \setminus supp(\delta)$ gli insiemi degli elementi fissati da γ e da δ rispettivamente. Chiaramente: $|fix(\gamma)| = |fix(\delta)|$; sia $\beta : fix(\gamma) \to fix(\delta)$ una biezione. Consideriamo quindi la permutazione $\pi \in Sym(X)$ definita da:

$$(a)\pi = \begin{cases} \hat{a} \text{ se } a \in supp(\gamma) \text{ (ovvero } a \in \{a_1, \dots, a_h, b_1, \dots, b_k, \dots\}) \\ (a)\beta \text{ se } a \notin supp(\gamma). \end{cases}$$

Per il Lemma 1.40 segue allora $\delta = \pi^{-1}\gamma\pi$. Si osservi che non è difficile mostrare che anche tale permutazione π può essere presa finitaria ∎

Segno. Sia $\gamma = (i_1\ i_2\ \dots i_k)$ un k-ciclo in $Sym(X)$; allora

$$\gamma = (i_1\ i_2)(i_1\ i_3)\dots(i_1\ i_k).$$

Ogni k-ciclo è dunque il prodotto di $k - 1$ trasposizioni. Unita al Teorema 1.39, questa semplice osservazione implica immediatamente il seguente fatto fondamentale.

Teorema 1.42. *Sia $n \geq 2$, allora ogni elemento di S_n è il prodotto di un numero finito di trasposizioni.*

In altre parole, se X è finito, il gruppo $Sym(X)$ è generato dall'insieme delle sue trasposizioni

$$\{(i\ j) \mid i, j \in X,\ i \neq j\}.$$

Una permutazione γ (di un insieme finito) può essere scritta in modi diversi come prodotto di trasposizioni; quello che tuttavia dipende da γ è la parità o disparità del numero di trasposizioni che costituiscono una qualsiasi fattorizzazione di γ; cioè se $\gamma = \tau_1\tau_2 \dots t_d$, con $\tau_1, \dots \tau_d$ trasposizioni, allora il numero $sgn(\gamma) = (-1)^d$ non dipende dalla specifica fattorizzazione. Tale numero si chiama la *segnatura* della permutazione finitaria γ. Una maniera per calcolarla facilmente consiste nel considerare il tipo ciclico $[d_1, d_2, \dots, d_k]$ di γ e applicare per i singoli cicli l'osservazione di sopra; si ottiene quindi

$$sgn(\gamma) = \prod_{i+1}^{k} (-1)^{d_i - 1}. \tag{1.8}$$

Gruppo alterno. È poi del tutto ovvio che, se X è finito, la segnatura definisce un omomorfismo suriettivo del gruppo $Sym(X)$ nel gruppo moltiplicativo $\{1, -1\}$. Il nucleo di tale omomorfismo si chiama *gruppo alterno* su X e si denota con $Alt(X)$; se $|X| = n$, allora il gruppo alterno si denota con A_n. In altre parole, $Alt(X)$ è costituito da tutte e sole le permutazioni che risultano il prodotto di un numero pari di trasposizioni e sono per questo chiamate permutazioni (di classe) *pari*; mentre le permutazioni appartenenti a $Sym(X) \setminus Alt(X)$ si dicono, ovviamente, (permutazioni di classe) *dispari*. $Alt(X) \trianglelefteq Sym(X)$ e, per il teorema di omomorfismo, $[Sym(X) : Alt(X)| = 2$; in particolare, per $2 \leq n \in \mathbb{N}$,

$$|A_n| = |S_n|/2 = n!/2.$$

I gruppi S_3 e S_4. Il gruppo S_3 ha ordine 6 ed è costituito, oltre che dall'identità ι, dalle permutazioni

$$\gamma = (1\ 2\ 3),\ \gamma^{-1} = (1\ 3\ 2),\ \tau_1 = (2\ 3),\ \tau_2 = (1\ 3),\ \tau_3 = (1\ 2).$$

$A_3 = \langle\gamma\rangle$ è un suo sottogruppo normale ciclico di ordine 3. Inoltre, per ciascun $i = 1, 2, 3$, $\tau_i| = 2$, e $\gamma^{\tau_i} = \gamma^{-1}$..

Il gruppo S_4 ha ordine $4! = 24$. Le permutazioni $\alpha_1 = (1\ 2)(3\ 4),\ \alpha_2 = (1\ 3)(2\ 4)$ commutano tra loro, e $\alpha_1\alpha_2 = (1\ 4)(2\ 3) = \alpha_3$. Poiché $\alpha_1, \alpha_2, \alpha_3$ sono tutte le permutazioni di S_4 con tipo ciclico $[2, 2]$, si conclude che

$$K = \{\iota, \alpha_1, \alpha_2, \alpha_3\}$$

è un sottogruppo normale di S_4; viene detto il *gruppo di Klein*. Per definizione $K \leq A_4 \trianglelefteq S_4$, $|A_4/K| = 12/4 = 3$; posto $\gamma = (1\ 2\ 3)$, si conclude che $A_4 = K \rtimes \langle\gamma\rangle$. Osserviamo che A_4 non ha sottogruppi di ordine 6, perché se H fosse tale, allora $H \trianglelefteq A_4$ e dunque $H \cap K \trianglelefteq A_4$; osservando che deve anche essere $|H \cap K| = 2$, ovvero che $H \cap K \ni a_i$ per qualche $i = 1, 2, 3$, si giunge a una contraddizione dato che, $\{\alpha_i, \alpha_i^{\gamma}, \alpha_i^{\gamma^{-1}}\} = \{\alpha_1, \alpha_2, \alpha_3\}$.

Siano ora $\nu = (1\ 2\ 3\ 4)$, $\tau = (1\ 3)$, e D il sottogruppo di S_4 da essi generato; si trova che $\nu^\tau = \nu^{-1}$ e quindi $D \simeq D_8$ è un sottogruppo di ordine 8. Assieme ai suoi coniugati D^γ e $D^{\gamma^{-1}}$, che sono distinti, costituisce (come si verifica controllando direttamente) l'insieme di tutti i sottogruppi di ordine 8 di S_4. Si osservi che $D \cap K = \langle (1\ 3)(2\ 4) \rangle = Z(D)$.

1.7 Esercizi I

Sezione 1.1

Esercizio 1.1. Sia X un insieme e $\triangle$ l'operazione di differenza simmetrica nell'insieme delle parti $\mathcal{P}(X)$ (definita da $A \Delta B = (A \cup B) \setminus (A \cap B)$ per ogni $A, B \in \mathcal{P}(X)$). Si provi che $(\mathcal{P}(X), \triangle)$ è un gruppo. Non sono invece gruppi (tranne nel caso banale $X = \emptyset$) $(\mathcal{P}(X), \cap)$ e $(\mathcal{P}(X), \cup)$.

Esercizio 1.2. Sia G un gruppo; si provi che se $g^2 = 1$ per ogni $g \in G$, G è abeliano.

Esercizio 1.3. Sia G un gruppo e siano $g, h \in G$. Si provi che sono equivalenti le seguenti proprietà:

(i) $gh = hg$

(ii) $(gh)^z = g^z h^z$ per ogni $z \in \mathbb{Z}$.

Si osservi quindi che In un gruppo commutativo (e solo in un gruppo commutativo) la proprietà (ii) vale per ogni coppia di elementi g, h.

Esercizio 1.4. Sia G un gruppo finito. Si provi che se G ha un numero pari di elementi allora esiste $1 \neq x \in G$, tale che $x^2 = 1$ (un elemento con tale proprietà si chiama *involuzione*).

Esercizio 1.5. Sia G un gruppo e sia $a \in G$ tale che $ag = ga$ per ogni $g \in G$. Su G si definisca una nuova operazione $*$, ponendo, per ogni $x, y \in G$: $x * y = xay$. Si provi che $(G, *)$ è un gruppo, e che è isomorfo a G.

Esercizio 1.6. Sia G un gruppo e $H \leq G$. Si provi che $G \setminus H$ è finito se e soltanto se $G = H$ o G è finito.

Esercizio 1.7. Si provi che il gruppo additivo $\mathbb{Q}$ dei numeri razionali non ha sottogruppi propri di indice finito.

Esercizio 1.8. Sia G un gruppo finito e $H, K \leq G$. Si provi che se $(|G : H|, |G : K|) = 1$, allora $G = HK$.

Sezione 1.2

Esercizio 1.9. Sia G un gruppo. Si dimostri che l'applicazione $f : G \longrightarrow G$ definita da, per ogni $g \in G$, $f(g) = g^{-1}$ è un automorfismo se e solo se G è commutativo.

Esercizio 1.10. Siano ψ e ζ due omomorfismi del gruppo G nel gruppo G'. Si dimostri che l'insieme $\{g \in G \mid \psi(g) = \zeta(g)\}$ è un sottogruppo di G. Si provi quindi che se S è un sistema di generatori di G e $\psi(s) = \zeta(s)$ per ogni $s \in S$, allora $\psi = \zeta$.

Esercizio 1.11. Si descrivano tutti gli automorfismi del gruppo additivo $\mathbb{Z}$.

Esercizio 1.12. Sia p un numero primo e sia $H = \{z/p \mid z \in \mathbb{Z}\}$.
(a) Si provi che H è un sottogruppo del gruppo additivo $\mathbb{Q}$.
(b) Si trovi un sistema di rappresentanti per le classi laterali sinistre di $\mathbb{Q}$ modulo H.
(c) Si provi che H è isomorfo a $\mathbb{Z}$.

Esercizio 1.13. Sia p un numero primo e sia $\mathbb{Q}_p = \{z/p^n \mid z \in \mathbb{Z}, n \in \mathbb{N}\}$.
(a) Si provi che $\mathbb{Q}_p$ è un sottogruppo del gruppo $\mathbb{Q}$.
(b) Si provi che $\mathbb{Q}_p$ non è isomorfo a $\mathbb{Z}$.
(c) Si descrivano gli automorfismi di $\mathbb{Q}_p$.

Esercizio 1.14. Sia H un sottogruppo del gruppo G. Si dimostri che H è normale se e soltanto se, per ogni $x, y \in G$, se $xy \in H$ allora $yx \in H$.

Esercizio 1.15. Sia $H \leq G$ e $g \in G$. Si provi che se $G = HH^g$ allora $H = G$.

Esercizio 1.16. Sia $\phi : G \to G'$ un omomorfismo suriettivo di gruppi e $N = \ker(\phi)$.
1) Si provi che per ogni $H \leq G$, $\phi^{-1}(\phi(H)) = HN$.
2) Si provi che per ogni $N \leq H \leq G$, $[G : H] = [G' : \phi(H)]$.

Esercizio 1.17. Per ogni coppia (a, b) di numeri reali con $a \neq 0$, sia $\sigma_{a,b} : \mathbb{R} \to \mathbb{R}$, l'applicazione definita da $\sigma_{a,b}(x) = ax + b$ per ogni $x \in \mathbb{R}$. Sia $G = \{\sigma_{a,b} \mid a, b \in \mathbb{R}\ a \neq 0\}$.
a) Si dimostri che G, dotato della operazione di composizione di applicazioni, è un gruppo e che il sottoinsieme $T = \{\sigma_{1,b} \mid b \in \mathbb{R}\}$ è un suo sottogruppo normale.
b) Si dimostri che G/T è isomorfo al gruppo moltiplicativo $\mathbb{R}^*$.

Esercizio 1.18. Sia $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ il gruppo moltiplicativo delle radici n-esime dell'unità. Si provi che $\mathbb{C}^*/U_n$ è isomorfo a $\mathbb{C}^*$.

Esercizio 1.19. Sia $\psi : G \to G$ un endomorfismo del gruppo G tale che $\psi \circ \psi = \psi$. Si provi che $G = \psi(G)\ker(\psi)$ e $\psi(G) \cap \ker(\psi) = \{1\}$.

Esercizio 1.20. Sia G un gruppo e $Z = Z(G)$ il suo centro; si provi che per ogni $H \leq G$ si ha $H \trianglelefteq HZ$, e che se $H \leq Z$ allora $H \trianglelefteq G$.

Sezione 1.3

Esercizio 1.21. Sia P l'insieme dei numeri reali strettamente maggiori di 0. Si provi che $\mathbb{R}^* = \{1, -1\} \times P$.

Esercizio 1.22. Sia $G = H \times K$ il prodotto diretto (interno) dei gruppi H e K. Sia $S \leq G$ tale che $S \leq H$.
(a) Si provi che $S \trianglelefteq H \Leftrightarrow S \trianglelefteq G$.
(b) Si provi che $[G : S] = |K|[H : S]$.

Esercizio 1.23. Sia G un gruppo e sia $W = G \times G$. Scriviamo $D = \{(g, g) \in W \mid g \in G\}$.
(a) Si provi che D è un sottogruppo di W isomorfo a G.
(b) Si dimostri che D è normale in W se e solo se G è abeliano.

Esercizio 1.24. Siano H e K gruppi finiti con $(|H|, |K|) = 1$, e sia $G = H \times K$ il loro prodotto diretto. Sia $S \leq G$; si provi che $S = (S \cap H) \times (S \cap K)$.

Esercizio 1.25. Siano H e K gruppi finiti con $(|H|, |K|) = 1$, e sia $G = H \times K$. Si provi che $Aut(G) = Aut(H) \times Aut(K)$.

Esercizio 1.26. Siano, G un gruppo abeliano, $\mathbb{Z}$ il gruppo additivo degli interi, e $W = \mathbb{Z} \times G$. Sia $h \in G$ un elemento fissato e si consideri quindi l'applicazione $\phi : W \longrightarrow G$, definita da, per ogni $(z, g) \in W$, $\phi(z, g) = gh^z$.
(a) Si provi che ϕ è un omomorfismo suriettivo di gruppi.
(b) Sia $K = \ker(\phi)$. Si provi che $|K| = \infty$.
(d) Posto $G_1 = \{(0, g) \mid g \in G\}$, si provi che $W = G_1 \times K$.

Esercizio 1.27. Si descriva il gruppo degli automorfismi del prodotto diretto $\mathbb{Z} \times H$ con H gruppo di ordine 2.

Sezione 1.4

Esercizio 1.28. Sia $D = \mathbb{R} \setminus \{0, 1\}$, e siano $f, g : D \to D$ le applicazioni definite da, per ogni $x \in D$, $f(x) = 1/x$ e $g(x) = (x - 1)/x$. Si determinino gli ordini di f e di g nel gruppo $Sym(D)$.

Esercizio 1.29. Sia G un gruppo. Si dimostri che, per ogni $x, y \in G$ si ha $|xy| = |yx|$.

Esercizio 1.30. Sia G un gruppo, $g \in G$ e H un sottogruppo finito di G. Si provi che se $H \cap \langle g \rangle \neq \{1_G\}$, allora g ha ordine finito.

Esercizio 1.31. Sia G un gruppo. Si provi che se G ha un unico sottogruppo massimale allora G è ciclico finito e il suo rodine è la potenza di un numero primo

Esercizio 1.32. Sia g un elemento di un gruppo, con $|g| = \infty$ e $n, m \in \mathbb{Z}$, si dimostri che $\langle g^n \rangle \leq \langle g^m \rangle$ se e solo se $m|n$.

Esercizio 1.33. Sia G un gruppo di ordine p^2 dove p è un numero primo. Si provi che G è abeliano e contiene al più $p + 3$ sottogruppi.

Esercizio 1.34. Siano C_n e C_m gruppi ciclici finiti di ordine rispettivamente n e m. Si provi che il prodotto diretto $C_n \times C_m$ è un gruppo ciclico se e solo se $(n, m) = 1$.

Esercizio 1.35. Sia C_n un gruppo ciclico di ordine n, dove n è prodotto di primi tutti distinti. Si dica allora per quali n il gruppo $Aut(C_n)$ è ciclico.

Sezione 1.5

Esercizio 1.36. Si provi la Proposizione 1.36.

Esercizio 1.37. a) Dopo aver provato che $G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R},\ (a, b) \neq (0, 0) \right\}$ è un sottogruppo di $GL(2, \mathbb{R})$, si provi che l'applicazione $\phi : \mathbb{C}^* \to G$ definita da

$$\phi(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

per ogni $z = a + bi \in \mathbb{C}^*$, è un isomorfismo di gruppi.
c) Posto $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2, \mathbb{R})$, si provi che, per ogni $z \in \mathbb{C}^*$, si ha $\phi(\overline{z}) = C^{-1}\phi(z)C$.

Esercizio 1.38. Con riferimento all'esempio 1.6, sia

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{F}^* \right\}$$

Si provi che $UH \leq G = GL(2, \mathbb{F})$. Siano quindi $A = UH$ e $B = U(D \cap S)$ (vedi 1.6 per le notazioni); si provi che, se $\mathbb{F}$ è un campo finito, $|A| = |B|$, e che se la caratteristica di $\mathbb{F}$ non è 2, A e B non sono isomorfi.

Esercizio 1.39. Sia $G = SL(2, \mathbb{Q}) \cap T(2, \mathbb{Q})$ e sia $H = \left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \middle| \ z \in \mathbb{Z} \right\}$. Si provi che $H \leq G$. Posto quindi $g = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$, si verifichi che $H^g \subseteq H$, ma che $H^g \neq H$.

Esercizio 1.40. Dati $n \geq 1$ e q la potenza di un numero primo, sia determini l'ordine dei gruppi diagonale $D(n, q)$, triangolare $T(n, q)$, e unitriangolare $UT(n, q)$.

Esercizio 1.41. Sia $n \geq 1$ e $G = GL(n, \mathbb{Z})$.

- Si provi che $Z(G) = \{1, -1\}$ (dove 1 è la matrice identica I_n).
- Si provi che se n è dispari $G = SL(n, \mathbb{Z}) \times Z(G)$.
- Si provi che se n è dispari, $SL(n, \mathbb{Z})$ non è isomorfo a $G/Z(G)$.

Sezione 1.6

Esercizio 1.42. Sia $n \geq 1$ e sia T un sottoinsieme non vuoto di $\{1, ..., n\}$. Si provi che l'insieme H di tutte le permutazioni $\sigma \in S_n$ tali che $\sigma(T) = T$, è un sottogruppo di S_n. Sia quindi $K = \{\sigma \in S_n \mid \sigma(x) = x \text{ per ogni } x \in T\}$; si dimostri che $K \trianglelefteq H$ e che H/K è isomorfo a S_k, dove $k = |T|$.

Esercizio 1.43. Sia $\sigma \in S_n$ un k-ciclo, e sia $a \in \mathbb{Z}$; si provi che σ^a è un k-ciclo se e solo se $(a, k) = 1$.

Esercizio 1.44. Sia $\pi = \sigma_1 \sigma_2 \dots \sigma_t$ con σ_i cicli disgiunti, e per ogni $1 \leq i \leq t$, si σ_i un ciclo di lunghezza k_i. Provare che $supp(\pi) = \bigcup_{i=1}^{t} supp(\sigma_i)$ e che $|\pi| = m.c.m(k_1, k_2, \dots, k_i)$.

Esercizio 1.45. Sia $n \geq 2$. Si provi che S_n è generato dall'insieme $\{(1\ j) \mid 1 < j \leq n\}$.

Esercizio 1.46. Sia $\mathbb{F}$ un campo e sia $\mathcal{B} = \{\mathbf{a_1}, \dots, \mathbf{a_n}\}$ la base canonica dello spazio $V = \mathbb{F}^n$. Poniamo $G = GL(n, \mathbb{F})$, in cui sono le matrici associate alle trasformazioni lineari di V rispetto alla base $\mathcal{B}$. Per ogni permutazione σ di $\{1, \dots, n\}$ si definisce la *matrice di permutazione* P_σ come la matrice associata all'unica trasformazione lineare tale che $\sigma(\mathbf{a_i}) = \mathbf{a}_{\sigma(\mathbf{i})}$ (per ogni $i \in \{1, \dots, n\}$). Sia quindi $H = \langle P_\sigma \mid \sigma \in S_n \rangle \leq G$.

- Si provi che $H \simeq S_n$.
- Posto $D = D(n, \mathbb{F})$ il gruppo delle matrici diagonali, si provi che H normalizza D.
- Si provi che $DH = \mathcal{N}_G(D)$.

Permutazioni finitarie. Sia X un insieme non vuoto; una permutazione $\sigma \in Sym(X)$ si dice *finitaria* se $supp(\sigma)$ è finito. Denotiamo con $FSym(X)$ l'insieme delle permutazioni finitarie di un insieme X.

Esercizio 1.47. Si provi che $FSym(X) \trianglelefteq Sym(X)$.

Una permutazione finitaria si comporta di fatto come una permutazione su un insieme finito; ne segue che quasi tutto quello che si dice per permutazioni finite si estende senza alcun aumento di difficoltà al caso di permutazioni finitarie:

Esercizio 1.48. Si formuli e si dimostri l'analogo per permutazioni finitarie dei Teoremi 1.39, 1.41 e 1.42.

Esercizio 1.49. Si definisca la classe di una permutazione finitaria, ed il sottogruppo normale $Alt(X)$ di $FSym(X)$ costituito dalle permutazioni finitarie di classe pari. Sapendo che per ogni $n \geq 5$, A_n è semplice, si provi che $Alt(\mathbb{N})$ è semplice.

Capitolo 2

Basi

2.1 Coniugio

Automorfismi interni. Sia G è un gruppo e $g \in G$, il *coniugio* tramite g è l'automorfismo σ_g di G, definito da

$$\sigma_g(x) = x^g := g^{-1}xg$$

per ogni $x \in G$; che questo sia un automorfismo di G è immediato, infatti

- $\sigma_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \sigma_g(x)\sigma_g(y)$ per ogni $x, y \in G$ (omomorfismo)
- $1 = \sigma_g(x) = g^{-1}xg \Leftrightarrow 1 = gg^{-1} = x$ (iniettivo); e
- $y = \sigma_g(y^{g^{-1}})$ per ogni $y \in G$ (suriettivo).

Un automorfismo di un gruppo G si dice *interno* se coincide con il coniugio tramite qualche elemento del gruppo G; si denota con $Inn(G)$ l'insieme di tutti gli automorfismi interni di G, cioè $Inn(G) = \{\sigma_G \mid g \in G\}$.

Dato per $g \in G$, è chiaro che l'automorfismo σ_g coincide con l'identità ι_G se e soltanto se $gx = xg$ per ogni $x \in G$, ovvero g appartiene al *centro* di G:

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

Ricordiamo anche che se $H \leq G$ allora H è normale se e soltanto se $H^g = H$ per ogni $g \in G$, ovvero se e soltanto se H è invariante per ogni automorfismo interno di G.

Teorema 2.1. *Sia G un gruppo. Allora*

(1) $Inn(G) \trianglelefteq Aut(G)$*;*

(2) $Inn(G) \simeq G/Z(G)$*.*

Dimostrazione. Abbiamo osservato sopra che $Inn(G)$ è un sottoinsieme (non vuoto) di $Aut(G)$. Definiamo $\phi : G \to Aut(G)$ ponendo, $\phi(g) = \sigma_{g^{-1}}$ per ogni $g \in G$; e verifichiamo che ϕ è un omomorfismo. Infatti, per ogni g, h e x in G,

$$\phi(gh)(x) = \sigma_{(gh)^{-1}}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \sigma_{g^{-1}}(\sigma_{h^{-1}}(x)) = (\phi(g) \circ \phi(h))(x)$$

e dunque $\phi(gh) = \phi(g) \circ \phi(h)$. Ora, per definizione, $Inn(G) = \phi(G)$, e, per quanto osservato prima, $\ker(\phi) = \mathbb{Z}(G)$. Quindi $Inn(G) \leq Aut(G)$ e $Inn(G) \simeq G/Z(G)$ dal Teorema di omomorfismo. Resta da provare $Inn(G) \trianglelefteq Aut(G)$. Siano $\beta \in Aut(G)$ e $\sigma_g \in Inn(G)$; allora, per ogni $x \in G$

$$\sigma_g^\beta(x) = (\beta^{-1} \circ \sigma_g \circ \beta)(x) = \beta^{-1}(\beta(x)^g) = \beta^{-1}(g^{-1}\beta(x)g) = x^{\beta^{-1}(g)}$$

Quindi, $\sigma_g^\beta = \sigma_{\beta^{-1}(g)} \in Inn(G)$, provando che $Inn(G) \trianglelefteq Aut(G)$. ∎

Automorfismi esterni. $Inn(G)$ si chiama il gruppo degli *automorfismi interni* di G; mentre il gruppo quoziente $Aut(G)/Inn(G)$ si denota con $Out(G)$ e si chiama il gruppo degli *automorfismi esterni* di G.
In particolare, dunque, $Aut(G) = Out(G)$ se e soltanto se G è abeliano. All'altro estremo

Centralizzanti. Sia G un gruppo e $X \subseteq G$. Il *centralizzante* di X in G è

$$C_G(X) := \{g \in G \mid xg = gx \text{ per ogni } x \in X\}.$$

(quindi, ad esempio, $C_G(G) = Z(G)$). Si osserva subito che, se X, Y sono sottoinsiemi di G,

1) $C_G(X) \leq G$;
2) $X \subseteq Y \ \Rightarrow \ C_G(Y) \leq C_G(X)$;
3) $\langle X \rangle \leq C_G(C_G(X))$;
4) $C_G(\langle X \rangle) = C_G(X)$.

Infatti, che $C_G(X)$ sia non vuoto e chiuso per prodotti è del tutto evidente; inoltte, se $g \in C_G(X)$ e $x \in X$,

$$g(g^{-1}x) = x = xgg^{-1} = g(xg^{-1}),$$

dunque, per cancellazione, $g^{-1}x = xg^{-1}$ e quindi $C_G(X) \leq G$. Stabilito ciò, il punto 2) segue per definizione. Per il punto 3), basterà osservare che $X \subseteq C_G(C_G(X))$ e applicare 1). Infine, da 3) si deduce $C_G(X) \leq C_G(\langle X \rangle)$, mentre da 2) segue $C_G(\langle X \rangle) \leq C_G(X)$, e dunque vale anche il punto 4).

Normalizzanti. Sia G un gruppo e $H \leq G$. Il *normalizzante* di H in G è

$$\mathcal{N}_G(H) = \{g \in G \mid H^g = H\}.$$

Quindi, un sottogruppo H di G è normale se (e solo se) $\mathcal{N}_G(H) = G$. E, più precisamente, per ogni $H \leq G$ sussistono le proprietà seguenti:

1) $H \trianglelefteq \mathcal{N}_G(H) \leq G$;
2) $C_G(H) \trianglelefteq \mathcal{N}_G(H)$;
3) $\mathcal{N}_G(H)/C_G(H)$ è isomorfo ad un sottogruppo di $Aut(H)$.

È chiaro, infatti, che $H \subseteq \mathcal{N}_G(H)$, e dunque per il punto 1) è sufficiente osservare che $\mathcal{N}_G(H)$ è un sottogruppo di G, e questo è a sua volta facile: se $x, y \in \mathcal{N}_G(H)$ allora $H^x = H = H^y$, quindi

$$H^{xy^{-1}} = (H^x)^{y^{-1}} = (H^y)^{y^{-1}} = H,$$

e dunque $xy^{-1} \in \mathcal{N}_G(H)$. Il punto 2) si dimostra osservando che $g \in \mathcal{N}_G(H)$ implica che la restrizione ad H del coniugio σ_g è un automorfismo di H; quindi, come nella dimostrazione del Teorema 2.1, il porre $g \mapsto \sigma_g|_H$ definisce un omomorfismo da $\mathcal{N}_G(H)$ in $Aut(H)$, il cui nucleo è $C_G(H)$. Dunque $C_G(H) \trianglelefteq \mathcal{N}_G(H)$. Il punto 3) è una estensione del punto (2) del Teorema 2.1, e si dimostra essenzialmente allo stesso modo: infatti, poiché $H \trianglelefteq \mathcal{N}_G(H)$, ogni elemento $b \in \mathcal{N}_G(H)$ induce per coniugio (ristretto ad H) un automorfismo di H, e gli elementi di b tali che $\sigma_b|_H$ è l'identità sono precisamente quelli che appartengono a $C_H(H)$. Ancora, un'osservazione vantaggiosa, la cui dimostrazione è lasciata come esercizio.

Lemma 2.2. *Siano X, Y sottoinsiemi non vuoti di un gruppo G, tali che $x^y \in \langle X \rangle$ per ogni $x \in X$ e $y \in Y$. Allora $\langle Y \rangle \leq \mathcal{N}_G(\langle X \rangle)$.*

I concetti e le notazioni per centralizzanti e normalizzanti si relativizzano a sottogruppi; così, se H e T sono sottogruppi di G, il normalizzante di H in T è

$$\mathcal{N}_T(H) = \{x \in T \mid H^x = H\} = T \cap \mathcal{N}_G(H);$$

e similmente, se $X \subseteq G$, il centralizzante di X in T è $C_T(X) = C_G(X) \cap T$.

Esempio 2.1. Sia $\mathbb{F}$ un campo e $n \geq 1$. Con le notazioni della sezione 1.5, siano $G = GL(n, \mathbb{F})$, $T = T(n, \mathbb{F})$ e $U = UT(n, \mathbb{F})$. Allora, T è il normalizzante in G di U. Un giustificazione geometrica di questa affermazione si può fornire nel modo seguente: sia $e_1, \ldots, e_n$ la base canonica dello spazio F^n, allora per ogni $A \in U$, $Ae_1 - e_1 = 0$ e per ogni $i = 2, \ldots, n$, $Ae_i - e_i \in \langle e_1, \ldots, e_{i-1} \rangle$; da questo, mediante considerazioni lasciate alla lettrice, si deduce che ogni elemento del normalizzante in G di U deve lasciare invariante ciascuno dei sottospazi:

$$\{0\},\ \langle e_1 \rangle,\ \langle e_1 \rangle \oplus \langle e_2 \rangle, \ldots, \langle e_1 \rangle \oplus \langle e_2 \rangle \oplus \cdots \oplus \langle e_n \rangle = \mathbb{F}^n.$$

Come notato nella sezione 1.5, si conclude che $\mathcal{N}_G(U) \leq T$, e l'uguaglianza si verifica direttamente. □

Chiusura normale e cuore di un sottogruppo. Concludiamo con ancora un paio di definizioni. Sia H un sottogruppo del gruppo G; allora, l'intersezione di tutti i sottogruppi normali di G che contengono H è un sottogruppo normale di G che si denota con H^G e si chiama *chiusura normale* di H in G. Quindi, $H \trianglelefteq G \Leftrightarrow H^G = H$, e, per ogni $H \leq G$, H^G è il minimo sottogruppo normale di G contenente H. Si vede facilmente che H^G coincide con il sottogruppo generato da tutti i *coniugati* di H, cioè

$$H^G = \langle \bigcup_{g \in G} H^g \rangle. \tag{2.1}$$

Dualmente, si definisce il *cuore* H_G di un sottogruppo H di un gruppo G come il massimo sottogruppo normale di G che è contenuto in H. Quindi , $H \trianglelefteq G \Leftrightarrow H_G = H$, e, ancora, si vede facilmente che H_G coincide l'intersezione di tutti i coniugati di H, cioè

$$H_G = \bigcap_{g \in G} H^g. \tag{2.2}$$

2.2 Prodotti semidiretti

Sia N un sottogruppo normale del gruppo G; un sottogruppo $H \leq G$ si dice un *complemento* di N in G se

$$\begin{cases} G = NH \\ N \cap H = 1 \end{cases}$$

Non tutti i sottogruppi normali ammettono complementi, ed è anzi un'importante questione quella di stabilire criteri che assicurino che un certo sottogruppo normale N ammette un complemento: alcuni tali criteri li vedremo più avanti.
Per il momento supponiamo che $N \trianglelefteq G$ ammetta complemento H. Allora, essendo normale, N è invariante per ogni coniugio σ_g in G; in particolare lo è per ogni coniugio mediante elementi di H. Quindi, come abbiamo già notato in precedenza, l'applicazione

$$\begin{array}{rccc} \phi: & H & \to & Aut(N) \\ & h & \mapsto & \sigma_h|_N \end{array}$$

è un omomorfismo, il cui nucleo è $C_H(N)$. Si dice allora che il gruppo G è il *prodotto semidiretto (interno)* di N per H, con ϕ omomorfismo associato.

Ad esempio, tornando all'esempio 2.1, e posto $D = D(n, \mathbb{F})$, segue dalla Proposizione 1.36 che T è il prodotto semidiretto del sottogruppo normale U per il complemento D.

Descriviamo ora la corrispondente costruzione "esterna". Siano N, H gruppi e sia dato un omomorfismo $\phi : H \to Aut(N)$. Per ogni $x \in H$ e $a \in N$ scriviamo $a^{\phi(x)}$ per $\phi(x)(a)$. Sull'insieme $N \times H$ si definisce un'operazione ponendo, per ogni $(a, x), (b, y) \in N \times H$,

$$(a, x)(b, y) = (ab^{\phi(x)^{-1}}, xy), \tag{2.3}$$

Si verifica che, con tale operazione, $G = N \times H$ è un gruppo, che si chiama il *prodotto semidiretto* (esterno) di N per H associato all'omomorfismo ϕ, che noi denoteremo con

$$G = N \rtimes_\phi H$$

(semplicemente $N \rtimes H$ quando non ci saranno ambiguità riguardo all'omomorfismo ϕ, o quando ci riferiremo ad un generico prodotto semidiretto dei due gruppi N e H). Si vede facendo direttamente i conti che $1_G = (1_n, 1_H)$, e

$$(a, x)^{-1} = ((a^{-1})^{\phi(x)}, x^{-1}) \tag{2.4}$$

per ogni $a \in N$, $x \in H$. Osserviamo poi che se ϕ è l'omomorfismo banale (cioè $\phi(x) = \iota_N$ per ogni $x \in H$), allora $N \rtimes_\phi H$ non è altro che il prodotto diretto $N \times H$.

Esempio 2.2. Sia $\mathbb{F}$ un campo. Allora, per ogni $0 \neq a \in \mathbb{F}$ la proprietà distributiva assicura che moltiplicazione per a definisce un automorfismo del gruppo additivo $(\mathbb{F}, +)$ che denotiamo con $\phi(a)$ (quindi, $\phi(a)(x) = xa$ per ogni $x \in \mathbb{F}$. Posto $\mathbb{F}^* = \mathbb{F} \setminus \{1\}$ il gruppo moltiplicativo di $\mathbb{F}$, si ha (lo si verifichi) che l'applicazione $\phi : \mathbb{F}^* \to Aut(\mathbb{F})$ è un omomorfismo. Questo consente di definire un prodotto semidiretto $\mathbb{F} \rtimes_\phi \mathbb{F}^*$. □

L'identità tra i concetti interno ed esterno di prodotto semidiretto è data dalla seguente Proposizione, la cui dimostrazione è lasciata per esercizio.

Proposizione 2.3. *Sia $\phi : H \to Aut(N)$ un omomorfismo, e sia $G = N \rtimes_\phi H$ il prodotto semidiretto ad esso associato. In G, siano $N^* = \{(a, 1_H) \mid a \in N\}$ e $H^* = \{(1_N, x) \mid x \in H\}$. Allora $N^* \trianglelefteq G$ e H^* è un suo complemento.*

Con le stesse notazioni, osserviamo anche che, se $a^* = (a, 1) \in N^*$ e $x^* = (1, x) \in H^*$, allora

$$(a^*)^{x^*} = (1, x^{-1})(a, 1)(1, x) = (a^{\phi(x)}, 1) = (a^{\phi(x)})^*,$$

Quindi, l'automorfismo indotto per coniugio da $x^* \in H^*$ su N^* coincide - via isomorfismo $*$ - con $\phi(x)$. Nella prassi, in un prodotto semidiretto esterno G come nella Proposizione 2.3, si identificano N con N^* e H con H^*, e si vede a G come il prodotto NH.

Gruppi diedrali. Una importante famiglia di prodotti semidiretti (definiti da un'azione non banale) è quella dei gruppi diedrali. Sia A un gruppo ciclico (finito o infinito) e sia $H = \langle x \rangle$ un gruppo ciclico di ordine due che opera come l'inversione su A, ovvero si associa ad x l'automorfismo di A definito dall'inversione ($u^x = u^{-1}$ per ogni $u \in A$). Il prodotto semidiretto $A \rtimes H$ si chiama *gruppo diedrale*: se A è ciclico infinito si denota con D_∞ (e si chiama gruppo diedrale infinito); mentre se $|A| = n$ è finito, si denota con D_{2n}. Notiamo che in questo ultimo caso si ha $|D_{2n}| = |A||H| = 2n$, e quindi D_{2n} si chiama gruppo diedrale di ordine $2n$.
Osserviamo che, secondo la definizione, $D_4 \simeq C_2 \times C_2$, $D_6 \simeq S_3$, mentre per $n \geq 2$, D_{2n}, così come D_∞, non è abeliano. (Non è difficile provare che, per $n \geq 3$, il gruppo diedrale D_{2n} è isomorfo al gruppo delle simmetrie di un n-agono regolare sul piano.)

Proposizione 2.4. *Sia G un gruppo e siano $x, y \in G$ con $|x| = 2 = |y|$. Allora il sottogruppo generato da $\{x, y\}$ è un gruppo diedrale.*

Ricordo che un elemento di ordine 2 di un gruppo G si dice *involuzione* di G.

Dimostrazione. Siano x e y involuzioni del gruppo G, sia $a = xy$ e $A = \langle a \rangle$. Sia quindi $\langle x, y \rangle$ il sottogruppo generato da $\{x, y\}$. Si osservi innanzi tutto che $A \leq \langle x, y \rangle$ e che $a^{-1} = yx$. Ora $a^x = x(xy)x = yx = a^{-1}$, quindi $x \in \mathcal{N}_G(A)$. Similmente, $a^y = y(xy)y = yx = a^{-1}$ e $y \in \mathcal{N}_G(A)$. Pertanto $\{x, y\} \subseteq \mathcal{N}_G(A)$ e dunque $\langle x, y \rangle \leq \mathcal{N}_G(A)$; ovvero $A \trianglelefteq \langle x, y \rangle$. A questo punto, si conclude facilmente che $\langle x, y \rangle = A \rtimes \langle x \rangle$, con x che induce per coniugio l'inversione su A. Dunque $\langle x, y \rangle$ è un gruppo diedrale. ∎

Sottogruppi caratteristici. Un sottogruppo di un gruppo G è normale se è invariante per ogni automorfismo interno di G. Questo tipo di requisito può essere rinforzato chiedendo che un sottogruppo H sia invariante per ogni automorfismo del gruppo G. In tal caso si dice che H è sottogruppo *caratteristico* di G e si scrive $H char\, G$. Ripetendo: $H\, char\, G$ se $H \leq G$ e $\beta(H) = H$ per ogni $\beta \in Aut(G)$. Per ogni gruppo G, G e il sottogruppo banale $\{1_G\}$ sono caratteristici. Si vede subito, ad esempio, che anche il centro $Z(G)$ è caratteristico in G. Infatti, siano $z \in Z(G)$ e $\beta \in Aut(G)$; allora, per ogni $g \in G$, $g = \beta(x)$ per qualche $x \in G$ e quindi $\beta(z)g = \beta(z)\beta(x) = \beta(zx) = \beta(xz) = \beta(x)\beta(z) = g\beta(z)$, e dunque $\beta(z) \in Z(G)$.
Notiamo che, per definizione, $H\, char\, G \Rightarrow H \trianglelefteq G$, ma non, chiaramente, il viceversa.

Lemma 2.5. *Siano $K, H \leq G$ e supponiamo $K\, char\, H\, char\, G$. Allora $K\, char\, G$.*

Dimostrazione. Esercizio. ∎

Molto utile è poi la seguente simile osservazione:

Lemma 2.6. *Siano $C, H \leq G$ con C char $H \trianglelefteq G$. Allora $C \trianglelefteq G$.*

DIMOSTRAZIONE. Siano $C, H \leq G$ come nelle ipotesi, e sia $g \in G$. Poiché $H \trianglelefteq G$, per ogni g la restrizione ad H del coniugio σ_g è un automorfismo di H il che significa $y^g = \sigma_g(y) \in C$ per ogni $y \in C$. Poiché ciò vale per ogni $g \in G$, si ha la tesi. ∎

Esempio interessante: Gruppi di isometrie. Sia $n \geq 2$ un numero intero e sia $V = \mathbb{R}^n$ lo *spazio euclideo* delle n-uple di numeri reali, provvisto della *distanza euclidea* d definita nel modo corrente: se $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ e $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ sono elementi di $\mathbb{R}^n$, allora la loro distanza è il numero reale positivo

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}.$$

Una *isometria* di V è un'applicazione $\phi : V \to V$ che conserva le distanze, ovvero tale che, per ogni $\mathbf{x}, \mathbf{y} \in V$:

$$d(\phi(\mathbf{x}), \phi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}).$$

Indichiamo con M_n l'insieme di tutte le isometrie di $V = \mathbb{R}^n$. È chiaro che la composizione di due isometrie è un'isometria. Inoltre, si prova che

Proposizione 2.7. *Ogni isometria è una biezione, e la sua inversa è un'isometria.*

Si deduce quindi che $M = M_n$, con l'operazione di composizione, è un gruppo, detto *Gruppo delle isometrie* di $\mathbb{R}^n$. Un rilievo particolare rivestono due tipi di simmetrie: traslazioni e rotazioni. Per ogni $\mathbf{v} \in V$ definiamo la *traslazione* $t_\mathbf{v}$ modulo $\mathbf{v}$ come l'applicazione di V in se stesso definita da $t_\mathbf{v}(\mathbf{x}) = \mathbf{x} + \mathbf{v}$, per ogni $\mathbf{x} \in V$. Si verifica immediatamente che, per ogni $\mathbf{v} \in V$, $t_\mathbf{v}$ è una isometria. Chiaramente, $t_\mathbf{0}$ è la applicazione identica; inoltre, per ogni $\mathbf{v}, \mathbf{w} \in V$

$$t_\mathbf{v} \circ t_\mathbf{v} = t_{\mathbf{v}+\mathbf{w}} \qquad \text{e} \qquad t_\mathbf{v}^{-1} = t_{-\mathbf{v}}$$

In particolare, il sottoinsieme di tutte le traslazioni di V, $T = \{t_\mathbf{v} \mid \mathbf{v} \in V\}$, è un sottogruppo di M, detto il *gruppo delle traslazioni* di V, e l'applicazione

$$\begin{array}{ccc} \mathbb{R}^n & \to & T \\ \mathbf{v} & \mapsto & t_\mathbf{v} \end{array}$$

è un isomorfismo del gruppo additivo $(\mathbb{R}^n, +)$ in T. Consideriamo ora l'insieme di tutte le isometrie di V che fissano l'origine, cioè

$$R = \{\rho \in M \mid \rho(\mathbf{0}) = \mathbf{0})\} \ .$$

Chiaramente R è un sottogruppo di M, detto *gruppo delle rotazioni* di V. Inoltre non è difficile provare che ogni elemento di R è un'applicazione lineare (invertibile) di $\mathbb{R}^n$ (di fatto, R coincide con l'insieme delle isometrie che sono lineari).

Teorema 2.8. *M è il prodotto semidiretto $M = T \rtimes R$; in particolare, ogni isometria di V si scrive in modo unico come il prodotto di una traslazione per una rotazione.*

DIMOSTRAZIONE. Sia $f \in M$ e sia $\mathbf{v} = f(\mathbf{0})$. Allora, posto $\rho = t_{-\mathbf{v}} \circ f$, si ha

$$\rho(\mathbf{0}) = (t_{-\mathbf{v}} \circ f)(\mathbf{0}) = t_{-\mathbf{v}}(f(\mathbf{0})) = f(\mathbf{0}) - \mathbf{v} = \mathbf{v} - \mathbf{v} = \mathbf{0}$$

quindi ρ è una rotazione, e $f = t_{-\mathbf{v}}^{-1} \circ \rho = t_{\mathbf{v}} \circ \rho$. Dunque, $M = TR$. Inoltre è ovvio che $T \cap R = \{\iota\}$. Rimane da provare che $T \trianglelefteq M$; e per questo basta osservare che ogni rotazione ρ normalizza T. Sia infatti $t_{\mathbf{v}} \in T$ e $x \in \mathbb{R}^n$. Allora , tenendo conto che ρ è lineare:

$$\rho^{-1} t_{\mathbf{v}} \rho(x) = \rho^{-1}(\rho(x) + \mathbf{v}) = x + \rho^{-1}(\mathbf{v}).$$

Quindi $\rho^{-1} t_{\mathbf{v}} \rho = t_{\rho^{-1}(\mathbf{v})} \in T$. ∎

2.3 Serie

Sia G un gruppo. Una *serie* (finita) di sottogruppi di G è una catena

$$1 = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n = G \tag{2.5}$$

di sottogruppi G_i di G tali che $G_{i-1} \trianglelefteq G_i$ per ogni $1 \leq i \leq n$. L'intero $n \geq 0$ si chiama lunghezza della serie, i sottogruppi G_i *termini* della serie, mentre i quozienti G_i/G_{i-1} (per $1 \leq i \leq n$) si dicono *fattori* della serie.
Si deve notare che in una serie ogni termine G_{i-1} è normale nel successivo G_i, ma non necessariamente in G (la normalità non è transitiva). Una serie di G in cui ogni termine è normale in G si dice *serie normale*.

ESEMPIO 2.3. Sia A un gruppo non banale, siano $N = A \times A$ e σ l'automorfismo di N definito da, per ogni $x, y \in A$, $(x, y)\sigma = (y, x)$ (che ciò definisca un automorfismo di N è abbastanza evidente). Consideriamo il prodotto semidiretto $G = N \rtimes \langle\alpha\rangle$. Se $A_1 = \{(a, 1) \mid a \in A\}$, allora $A_1 \trianglelefteq N$, e quindi $1 \leq A_1 \leq N \leq G$ è una serie di G, che non è normale: infatti, in G, $A_1^\sigma = \{(1, a) \mid a \in A\} = A_2$, dunque $A_1 \not\trianglelefteq G$. Osserviamo che i fattori di questa serie sono

$$A_1 \simeq A, \quad N/A_1 \simeq A_2 \simeq A, \quad G/N \simeq \langle\alpha\rangle \simeq C_2.$$

Supponiamo ora che A sia abelano; allora il sottogruppo diagonale $D = \{(a, a) \mid a \in A\}$ è un sottogruppo normale di N (vedi esercizio 1.23). Inoltre $D = C_N(\sigma)$ e dunque in particolare $D^\sigma = D$. Quindi $D \trianglelefteq G$ e la serie $1 \leq D \leq N \leq G$ è normale. I suoi fattori sono gli stessi del caso precedente, ovvero

$$D \simeq A, \quad N/D \simeq DA_1/D \simeq A_1 \simeq A, \quad G/N \simeq \langle\alpha\rangle \simeq C_2.$$

□

Esempi piuttosto scontati di serie normali si possono osservare nei prodotti diretti. Se $n \geq 2$ e $G = G_1 \times G_2 \times \cdots \times G_n$, allora

$$1 \leq G_1 \leq G_1 \times G_2 \leq \cdots \leq G_1 \times \cdots \times G_{n-1} \leq G$$

è una serie normale di G.

Il concetto di serie normale si estende nel modo seguente. Sia G un gruppo e Ω un gruppo di operatori di G (significa che Ω è un gruppo ed esiste, ed è fissato, un omomorfismo $\phi : \Omega \to Aut(G)$); una serie $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ si dice una Ω-serie se per ogni $0 \leq i \leq n$ e ogni $x \in \Omega$, $(G_i)x\phi = G_i$. Le serie normali sono dunque le Ω-serie quando $\Omega = Inn(G)$.

Serie di composizione. Un fattore G_i/G_{i-1} di una serie $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ si dice *raffinabile* se esiste un sottogruppo $G_{i-1} \leq H \trianglelefteq G_i$ tale che $G_{i-1} \neq H \neq G_i$. In tal caso, $1 = G_0 \leq \cdots \leq G_{i-1} \leq H \leq G_i \leq \cdots \leq G_n = G$ è ancora una serie di G (con un termine in più).
Date due serie $\mathcal{S}$ e $\mathcal{S}'$ di un gruppo G, si dice che $\mathcal{S}'$ è un *raffinamento* di $\mathcal{S}$ se ogni termine di $\mathcal{S}$ è un termine di $\mathcal{S}'$. È chiaro quindi che una serie $\mathcal{S}$ ammette un raffinamento proprio se e soltanto se almeno un fattore di $\mathcal{S}$ è raffinabile.
Una serie $\mathcal{S}$ di un gruppo G si dice una *serie di composizione* se ogni suo fattore è non raffinabile; in altri termini se $\mathcal{S}$ non ha raffinamenti propri. Ora, dai teoremi di omomorfismo segue facilmente che un fattore di una serie non è raffinabile se e solo se è un gruppo semplice; quindi,

una serie è una serie di composizione se e solo se ogni suo fattore è un gruppo semplice.

È evidente dalla definizione che ogni gruppo finito ed ogni gruppo prodotto diretto di un numero finito di gruppi semplici ammettono serie di composizione. In generale, però, l'ammettere una serie di composizione è una proprietà piuttosto restrittiva. Ad esempio, già il gruppo ciclico infinito $\mathbb{Z}$ non ha alcuna serie di composizione.

Il concetto di serie di composizione si estende in modo naturale alle Ω–serie. Siano H un gruppo e Ω un gruppo di operatori su H; si dice che H è Ω-semplice se 1 e H sono i soli sottogruppi di H lasciati fissi da Ω. Sia ora Ω un gruppo di operatori di G; allora Ω è in modo naturale un gruppo di operatori su ogni fattore di una Ω-serie di G, e una Ω-serie di G si dice Ω-serie di composizione se ogni suo fattore è un gruppo Ω-semplice.

Teorema di Jordan–Hölder. Diciamo che due serie (in generale, Ω-serie) $1 = G_0 \leq \cdots \leq G_n = G$ e $1 = H_0 \leq \cdots \leq H_m = G$ del gruppo G sono *concordanti* (Ω-concordanti) se $m = n$ ed esiste una permutazione $\pi \in S_n$ tale che $H_{i\pi}/H_{i\pi-1} \simeq G_i/G_{i-1}$ per ogni $1 \leq i \leq n$ (nel caso di Ω-serie si chiede che questi isomorfismi tra fattori siano Ω-isomorfismi - ovvero commutino con gli automorfismi indotti da Ω sui singoli fattori).

Teorema 2.9. (Schreier) *Due qualsiasi Ω-serie di un gruppo G (con l'azione di Ω) ammettono raffinamenti Ω-concordanti.*

Dimostrazione. Vedi [3], 3.1.2. ∎

Il celebre Teorema di Jordan–Hölder, che è un'applicazione del precedente, stabilisce, nella sostanza, che per serie di composizione il concetto di concordanza è pleonastico. Anche di questo Teorema, concettualmente importante ma che utilizzeremo poco in pratica, non daremo la dimostrazione, che si può trovare tra le prime pagine di quasi ogni testo introduttivo alla teoria dei gruppi (ad esempio [3]).

Teorema 2.10. (Jordan–Hölder) *Sia G un gruppo con una serie di composizione $\mathcal{C}$. Allora ogni serie di G può essere raffinata ad una serie di composizione concordante a $\mathcal{C}$. In particolare, tutte le serie di composizione di G sono tra loro concordanti.*

Anche questo risultato si estende senza troppi problemi alle Ω-serie. **Serie principali.**

Quando $\Omega = Inn(G)$ per una Ω-serie di composizione si parla di *serie principale* di G. Quindi una serie $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ si dice principale se è normale e per ogni $1 \leq i \leq n$, i soli sottogruppi $G_{i-1} \leq H \leq G_i$ con $H \trianglelefteq G$ sono i termini stessi della serie G_{i-1} e G_i

Strettamente legato a quello di serie principale è il concetto di sottogruppo *normale minimo*: un sottogruppo normale N del gruppo G è detto normale minimo se $1 \neq N$ e per ogni $K \leq N$ se $K \trianglelefteq G$ allora $K = 1$ oppure $K = N$; in altri termini, un sottogruppo normale $N \neq 1$ di G è minimo se per ogni $1 \neq x \in N$, $\langle x \rangle^G = N$.

Esempio 2.4. Sia $\mathbb{F}$ un campo. Allora, per ogni $\lambda \in \mathbb{F}^*$, la moltiplicazione per λ è un automorfismo del gruppo additivo $(\mathbb{F}, +)$. Sia $G = \mathbb{F} \rtimes \mathbb{F}^*$ (vedi esempio 2.2), e poniamo $N = \{(a, 1) \mid a \in \mathbb{F}\}$ (come sottogruppo normale di G). Ora, per ogni $a, b \in \mathbb{F}$ se $a \neq 0 \neq b$ la moltiplicazione per $a^{-1}b$ manda a in b. Quindi, nel prodotto semidiretto G, $(a, 1)^{(0,a^{-1}b)} = (b, 1)$; e questo significa che $\langle (a, 1) \rangle^G + N$ e dunque, per quanto osservato sopra, N è un sottogruppo normale minimo di G. □

Siano ora $A = G_{i-1} \leq G_i = B$ termini successivi di una serie principale del gruppo G con $A \neq B$; in particolare $A \trianglelefteq G$ e $1 \neq B/A \trianglelefteq G/A$. Per definizione di serie principale e il terzo Teorema di omomorfismo segue quindi che *B/A è un sottogruppo normale minimo di G/A.*

Sia $1 \neq N$ un sottogruppo normale minimo di G, allora, per il Lemma 2.6, i soli sottogruppi caratteristici di N sono 1 e N. Un gruppo G con tale proprietà, ovvero i cui soli sottogruppi caratteristici sono 1 e G, si dice *caratteristicamente semplice*; quindi

Lemma 2.11. *I fattori di una serie principale di un gruppo sono gruppi caratteristicamente semplici.*

Esempio 2.5. Sia $q = 3^3$ e sia $\mathbb{F} = GF(q)$ il campo di ordine q. Nel gruppo $GL(2, q) = GL(2, \mathbb{F})$ consideriamo

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \ a \in \mathbb{F}^*, \ b \in \mathbb{F} \right\}.$$

Si verifica facilmente che $G \leq GL(2, q)$ e che G è il prodotto semidiretto $U \rtimes H$, dove

- $U = UT(2, q) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \ b \in \mathbb{F} \right\}$ è isomorfo al gruppo additivo $\mathbb{F}$
- $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| \ a \in \mathbb{F}^* \right\}$ è isomorfo al gruppo moltiplicativo $\mathbb{F}^*$.

Quindi, U è abeliano elementare di ordine 3^3 e H ciclico di ordine $3^3 - 1 = 26 = 13 \cdot 2$.
Per $a \in \mathbb{F}^*, b \in \mathbb{F}$, poniamo $\bar{a} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ e $\bar{b} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Allora

$$\bar{b}^{\bar{a}} = \bar{a}^{-1}\bar{b}\bar{a} = \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix},$$

quindi $\bar{a}$ opera su $U \simeq \mathbb{F}$ come la moltiplicazione per a^{-1}. Da ciò segue (si completino i dettagli per esercizio) che G è isomorfo ad uno dei gruppi descritti nell'esempio 2.4. In

particolare, U è un sottogruppo normale minimo di G. Sia h un generatore del gruppo ciclico H e poniamo $L = \langle h^2 \rangle$. Allora $|L| = 13$ e $W = UL$ è un sottogruppo normale di G con $|G : W| = 2$. Pertanto, $1 \leq U \leq W \leq G$ è una serie principale di G i cui fattori sono

$$U \simeq C_3 \times C_3 \times C_3, \quad W/U \simeq L \simeq C_{13}, \quad G/W \simeq H/L \simeq C_2. \tag{2.6}$$

Consideriamo ora il gruppo

$$G_1 = T(2,q) \cap SL(2,q) = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| \ a \in \mathbb{F}^*, \ b \in \mathbb{F} \right\}.$$

Il gruppo G trattato prima e G_1 hanno lo stesso ordine, $3^3(3^3 - 1)$, ed anche una struttura simile: infatti $G_1 = U \rtimes H_1$ dove $H_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| \ a \in \mathbb{F}^* \right\}$, che è anch'esso isomorfo al gruppo moltiplicativo $\mathbb{F}^*$. Sia a un generatore di $\mathbb{F}^*$ e sia $b \in \mathbb{F}$; come sopra, poniamo $\bar{a} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ e $\bar{b} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Allora

$$\bar{a}^{-1}\bar{b}\bar{a} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a^{-2}b \\ 0 & 1 \end{pmatrix}.$$

Dunque $\bar{b}$ ha (almeno) 13 coniugati distinti in G_1, quindi, dato che i sottogruppi propri di U hanno ordine al più 9, $\langle \bar{b} \rangle^{G_1} = U$. Ciò significa che U è un sottogruppo normale minimosi G_1. Di conseguenza, posto $W_1 = U\langle \bar{a}^2 \rangle$, si ha che $1 \leq U \leq W_1 \leq G_1$ è una serie principale di G_1, i cui fattori sono ordinatamente isomorfi a quelli in (2.6) per il gruppo G. Tuttavia, $G_1 \not\simeq G$, dato che $Z(G) = 1$ mentre $Z(G_1) = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \neq 1$. □

Non esiste una descrizione generale dei gruppi caratteristicamente semplici. Dall'esempio 2.4 segue che se $\mathbb{F}$ è un campo, allora il suo gruppo additivo è caratteristicamente semplice (questo fatto si estende in modo naturale a gruppi additivi di spazi vettoriali, vedi esercizio 2.14). Ovviamente, poi, ogni gruppo semplice è caratteristicamente semplice. Nel caso finito si può provare che *un gruppo è caratteristicamente semplice se e soltanto se e un prodotto diretto di gruppi semplici tra loro isomorfi* (vedi gli esercizi 2.16–2.18 per una direzione).

2.4 Gruppi abeliani

I gruppi abeliani, la cui teoria forma un ramo a sé, che si è sviluppato e continua a evolversi utilizzando tecniche piuttosto distinte da quelle in uso nelle altre parti della teoria dei gruppi, risulteranno in queste note un poco disseminati in vari capitoli (ad esempio, proveremo l'importante risultato di classificazione dei gruppi abeliani finitamente generati solo nel capitolo 4). In questa sezione ci accontentiamo di qualche osservazione iniziale e quasi banale, in modo da poter in seguito parlare di gruppi abeliani in modo non del tutto generico.
Sia A un gruppo abeliano, e $1 \geq n \in \mathbb{N}$; poniamo

$$A[n] = \{x \in A \mid x^n = 1\} \qquad A^n = \{x^n \mid x \in A\} \tag{2.7}$$

(per abitudine del sottoscritto, usiamo per il momento la notazione moltiplicativa). È cosa immediata verificare che la commutatività di A assicura che, per ogni $n \geq 1$, $A[n]$ e A^n sono sottogruppi caratteristici di A. Per le stesse ragioni, l'insieme degli elementi periodici di A

$$T(A) = \{x \in G \mid |x| < \infty\}$$

è un sottogruppo caratteristico di A, detto sottogruppo di torsione di A. Quindi,

Proposizione 2.12. *Sia A un gruppo abeliano e $T = T(A)$. Allora $TcharA$ e A/T è senza torsione.*

DIMOSTRAZIONE. La prima affermazione è pressoché ovvia. Per la seconda sia xT un elemento periodico di A/T; allora $x^n \in T$ per qualche $n \in \mathbb{N}$, e dunque, per definizione di T, esiste $1 \leq m \in \mathbb{N}$ tale che $1 = (x^n)^m = x^{nm}$. Quindi $x \in T$. ∎

La teoria dei gruppi abeliani si divarica dunque in modo naturale in quella (più difficile) dei gruppi senza torsione ed in quella dei gruppi periodici. Quest'ultima, come nel caso dei gruppi finiti ciclici (1.2), si riduce essenzialmente a quella dei p-gruppi (p un primo). Se π è un insieme di numeri primi, si dice che un intero $n \neq 0$ è un π-numero se ogni suo divisore primo appartiene a π, mentre al, contrario, si dice che è un π'-numero se nessun suo divisore primo appartiene a π

Lemma 2.13. *Sia A un gruppo abeliano periodico e π un insieme di primi. Siano*

$$A_\pi = \{x \in A \mid |x| \text{ un } \pi\text{−numero}\}, \quad A_{\pi'} = \{x \in A \mid |x| \text{ un } \pi'\text{−numero}\}.$$

Allora $A = A_\pi \times A_{\pi'}$.

DIMOSTRAZIONE. Utilizzare la proprietà (1.2) dei gruppi ciclici finiti. ∎

Gruppi divisibili. Un gruppo G si dice radicabile se per ogni $x \in G$ e ogni intero $n \geq 1$, esiste un elemento $y \in G$ tale che $y^n = x$; ma nel caso dei gruppi abeliani si dice che G è *divisibile*. In accordo con questa denominazione, adottiamo in questo paragrafo la notazione additiva; quindi un gruppo abeliano A è divisibile se per ogni $x \in A$ ed ogni $n \geq 1$ esiste $y \in A$ tale che $ny = x$.
Una interessante proprietà dei gruppi divisibile è la seguente.

Lemma 2.14. *Sia A un gruppo abeliano e sia D un sottogruppo divisibile di A. Allora esiste $C \leq A$ tale che $A = D \oplus C$.*

DIMOSTRAZIONE. Siano A e D come nelle ipotesi, e sia $\mathcal{C}$ l'insieme dei sottogruppi H di A tali che $D \cap H = \{0\}$. Poiché, come è chiaro, l'unione dei termini di una qualsiasi catena di elementi di $\mathcal{C}$ appartiene a $\mathcal{C}$, esiste, per il Lemma di Zorn, un sottogruppo C di A massimale in $\mathcal{C}$. Ora, $D \cap C = \{0\}$ per definizione. Proviamo che $D + C = A$. Supponiamo, per contrario, che $B = D + C < A$ e sia $a \in A \setminus B$. Se $|B + a| = \infty$, allora $B \cap \langle A \rangle = \{0\}$ da cui segue facilmente $D \cap (C + \langle a \rangle) = \{0\}$, contro la scelta di C. Supponiamo quindi $|B + a| = n$ per un $1 < n \in \mathbb{N}$; dunque, in particolare, $na = c + x$ con $c \in C$ e $x \in D$. Poiché D è divisibile esiste $y \in D$ tale che $ny = x$; poniamo $b = a - y$, e $C' = C + \langle b \rangle$. Siano $c' \in C$ e $m \in \mathbb{N}$ tali che $D \ni c' + mb = c' + ma - my$; dunque $D \ni c' + ma$ e quindi

$ma = c' + ma - c' \in D + C = B$, ovvero $m(B + a) = B$. Dunque $n|m$, sia $m = kn$ ($k \in \mathbb{N}$); allora $mb = k(na - ny) = k(na - x) = kc \in C$ e $c' + mb \in D \cap C = \{0\}$. Quindi $C' \cap D = \{0\}$ e, per la scelta di C, $C' = C$. Ciò implica la contraddizione $a = b + y \in D + C = B$. ∎

L'esempio ovvio di gruppo divisibile è il gruppo additivo dei razionali. Di fatto, si tratta di qualcosa di più che un esempio come tanti.

Proposizione 2.15. *Sia A un gruppo abeliano divisibile e senza torsione. Allora*

- *per ogni $x \in A$ e $n \geq 1$, esiste un unico $y \in A$ tale che $ny = x$.*
- *A è isomorfo al gruppo additivo di un $\mathbb{Q}$-spazio vettoriale.*

Dimostrazione. Sia A un gruppo abeliano divisibile e senza torsione. Sia $x \in A$, $n \geq 1$, e siano $y_1, y_2 \in A$ tali che $ny_1 = x = ny_2$. Allora $n(y_1 - y_2) = 0$ e dunque, essendo A senza torsione, $y_1 - y_2 = 0$ e $y_1 = y_2$.
Per ogni $1 \leq n \in \mathbb{N}$ e $x \in A$ denotiamo con $\frac{1}{n}x$ l'unico elemento $y \in A$ tale che $ny = x$ (è ben definito per il punto precedente). Ora, porre, per ogni $z \in \mathbb{Z}$, $n \geq 1$ e x in A,

$$\left(\frac{z}{n}, x\right) \mapsto z\left(\frac{1}{n}x\right)$$

definisce un'applicazione $\mathbb{Q} \times A \to A$ che, come si vede facilmente, assieme all'operazione di addizione già presente, definisce una struttura di $\mathbb{Q}$-spazio vettoriale su A ∎

Non è troppo difficile descrivere anche la classe dei gruppi divisibili periodici; occorre prima procurasene i rappresentanti fondamentali (che giocano il ruolo che $\mathbb{Q}$ gioca nel caso senza torsione).

Gruppi di Prüfer. Sia p un numero primo. Si definisce il *p-gruppo di Prüfer*

$$C_{p^\infty} = \{z \in \mathbb{C} \mid z^{p^n} = 1, \text{ per qualche } n \in \mathbb{N}\}.$$

Infatti, è immediato verificare che C_{p^∞} è un sottogruppo del gruppo moltiplicativo $\mathbb{C}^*$ dei numeri compelssi diversi da 0. Se, per ogni $n \geq 0$, e riprendendo una notazione già usata, denotiamo con U_{p^n} l'insieme delle radici p^n-esime dell'unità: U_{p^n} è ciclico per ogni $n \geq 0$ e $U_{p^n} \leq U_{p^m}$ per ogni $0 \leq n \leq m$; infine, riconosciamo che

$$C_{p^\infty} = \bigcup_{n \geq 0} U_{p^n}. \tag{2.8}$$

In particolare, C_{p^∞} è un p-gruppo. Inoltre, C_{p^∞} *è divisibile*. Infatti, siano $a \in C_{p^\infty}$ e $n \geq 1$, allora $|a| = p^j$, $n = kp^i$ con $i, j \geq 0$ e $(k, p) = 1$; sia $b \in C_{p^\infty}$ una radice primitiva p^{i+j}-esima, allora $\langle a \rangle = \langle b^{p^i} \rangle = \langle (b^k)^{p^i} \rangle$ e dunque esiste $c \in \langle b \rangle$ tale che $c^n = a$.

Una interessante proprietà dei gruppi di Prüfer riguarda l'insieme ordinato dei loro sottogruppi. Abbiamo osservato che, per ogni $n \geq 0$, U_{p^n} è un gruppo ciclico di ordine p^n di C_{p^∞}. Viceversa, sia H un sottogruppo di C_{p^∞}; se H è finito dalla (2.8) segue, per semplici ragioni insiemistiche, che H è contenuto inqualche sottogruppo U_{p^n}, e quindi, poiché i soli sottogruppi di U_{p^n} sono gli U_{p^s} con $s \leq n$ si conclude che H coincide con qualche U_{p^s}. Se invece H è infinito, per ogni $n \geq 1$, H contiene un elemento il cui ordine è maggiore di p^n; dunque $U_{p^n} \leq H$ per ogni $n \geq 1$, da cui $H = C_{p^\infty}$. Abbiamo quindi provato

Lemma 2.16. *Ogni sottogruppo proprio di C_{p^∞} è ciclico e coincide con qualche U_{p^n} per $n \geq 0$.*

Si può dimostrare che *un gruppo abeliano periodico è divisibile se e solo se è il prodotto diretto* (nel senso esteso che verrà descritto nella sezione 2.6) *di gruppi di Prüfer*

Esempio importante: il gruppo dei Quaternioni. Nel gruppo moltiplicativo $GL(2, \mathbb{C})$ si considerino gli elementi:

$$x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Allora $xy = x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, e $x^2 = y^2 = (xy)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$; quindi $|x| = |y| = |xy| = 4$. Inoltre $x^y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = x^{-1}$. Si verifica allora facilmente che l'insieme

$$Q_8 = \{1, x^2, x, x^{-1}, y, y^{-1}, xy, (xy)^{-1}\}$$

è un sotogruppo del gruppo $GL(2, \mathbb{C})$. Si chiama *gruppo dei quaternioni* ed ha diverse proprietà peculiari. Q_8 è il prodotto di due gruppi ciclici di ordine 4, infatti $Q_8 = \langle x \rangle \langle y \rangle$. Tutti i sottogruppi propri di Q_8 sono ciclici: sono $\{1\}$, $\langle x \rangle$, $\langle y \rangle$, $\langle xy \rangle$ (quesi tre di ordine 4) e $\langle x^2 \rangle$, che è l'unico sottogruppo di ordine 2 (queste cose si provino per esercizio). Si riconosce quindi che tutti i sottogruppi di Q_8 sono normali; tuttavia Q_8 non è abeliano: infatti $Z(Q_8) = \langle x^2 \rangle$. Di fatto, è possibile dimostrare il seguente risultato.

Teorema 2.17. (R. Dedekind) *Sia G un gruppo finito in cui ogni sottogruppo è normale. Allora G è abeliano o isomorfo ad un prodotto diretto $Q \times A \times D$, dove Q è l gruppo dei quaternioni, A è un 2-gruppo abeliano elementare e D è un gruppo abeliano di ordine dispari.*

2.5 Gruppi risolubili

La nozione di gruppo risolubile è una delle più importanti nella teoria dei gruppi, anche dal punto di vista storico. Il suo atto di nascita, il rivoluzionario lavoro di E. Galois sulla risoluzione delle equazioni polinomiali mediante radicali, coincide infatti con quello della stessa teoria dei gruppi.

Gruppi risolubili. Un gruppo si dice *risolubile* se ammette una serie a fattori abeliani. Una prima osservazione è che la classe dei gruppi risolubile è chiusa per sottogruppi e per quozienti.

Lemma 2.18. *Sia G un gruppo risolubile e $H \leq G$. Allora*

- *H è risolubile;*
- *se $H \trianglelefteq G$, G/H è risolubile.*

DIMOSTRAZIONE. Sia G risolubile e sia $1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$ una serie a fatttori abeliani di G. Utilizzando i Teoremi di omomorfismo (1.20 e 1.21) si verifica più che facilmente che $1 = G_n \cap H \leq G_{n-1} \cap H \leq \cdots \leq G_1 \cap H \leq H$ è una serie a fattori abeliani di H, e che se $H \trianglelefteq G$, $1 = G_nH/H \leq G_{n-1}H/H \leq \cdots \leq G_1H/H \leq G/H$ è una serie a fattori abeliani di G/H. ∎

Nella direzione opposta è anche semplice provare che l'estensione di gruppi risolubili è un gruppo risolubile. Detto con precisione,

Lemma 2.19. *Sia G un gruppo e $N \trianglelefteq G$. Se N e G/N sono risolubili, allora G è risolubile.*

Ad esempio, il prodotto semidiretto di gruppi risolubili è risolubile (esempi più lavorati li vedremo più avanti). Ma un aspetto forse più importante è che l'esistenza, in un gruppo G, di una serie a fattori abeliani, è riconducibile al comportamento di una successione di sottogruppi caratteristici canonicamente definiti.

Commutatori e sottogruppo derivato. Sia G un gruppo; per ogni $x, y \in G$ il *commutatore* di x con y è

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y. \tag{2.9}$$

Osserviamo subito che, per ogni coppia di elementi x, y di un gruppo:

$$xy = yx \;\Leftrightarrow\; [x, y] = 1. \tag{2.10}$$

Se poi $x, y, z \in G$, si pone

$$[x, y, z] = [[x, y], z].$$

Anche se ci saranno utili soprattutto più avanti, enunciamo fin d'ora alcune identità elementari e assai utili per il calcolo con i commutatori. Le dimostrazioni seguono semplicemente sviluppando i commutatori secondo la definizione (2.9).

Lemma 2.20. *Sia G un gruppo e $x, y, z \in G$. Allora*

(1) $[x, y]^{-1} = [y, x]$;

(2) $[xy, z] = [x, z]^y[y, z]$;

(3) $[x, yz] = [x, z][x, y]^z$;

(4) (Identità di Hall-Witt) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

Se X, Y sono sottoinsiemi non vuoti del gruppo G, poniamo

$$[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle.$$

(Quindi $[X, Y]$ è per definizione un sottogruppo di G). Il *sottogruppo derivato* G' di G è il sottogruppo generato da tutti i commutatori di G, ovvero

$$G' = [G, G].$$

Poiché, per ogni $\phi \in Aut(G)$, ed ogni $x, y \in G$, $\phi([x, y]) = [\phi x, \phi y]$, G' risulta un sottogruppo caratteristico, e dunque normale, di G. Più in generale, si ha il seguente fatto,

Lemma 2.21. *Siano X, Y sottogruppi del gruppo G. Allora*

$$[X, Y] \trianglelefteq \langle X, Y \rangle.$$

DIMOSTRAZIONE. Per ogni $x, x_{\in} X$ e $y, y_1 \in Y$, per il punto (2) del Lemma 2.20 si ha $[x, y]^{x_1} = [xx_1, y][x_1, y]^{-1} \in [X, Y]$ e, similmente, $[x, y]^{y_1} = [x, y_1]^{-1}[x, yy_1] \in [X, Y]$. La tesi segue allora dal Lemma 2.2. ∎

Inoltre, da (2.10) segue che G è abeliano se e soltanto se $G' = 1$. Anche questo si relativizza: se X, Y sono sottoinsiemi non vuoti di G allora

$$Y \subseteq C_G(X) \;\Leftrightarrow\; [X, Y] = 1. \tag{2.11}$$

Cose banali forse, ma di primaria importanza, come il prossimo Lemma.

Lemma 2.22. *Sia G un gruppo e $N \trianglelefteq G$. Allora*

- $(G/N)' = NG'/N$;
- *G/N è abeliano se e solo se $G' \leq N$.*

DIMOSTRAZIONE. Sia $N \trianglelefteq G$. Allora per ogni $x, y \in G$, $[Nx, Ny] = N[x, y]$, e da ciò segue facilmente il primo asserto. Per il secondo basterà osservare che G/N è abeliano se e soltanto se $N = [Nx, Ny]$ per ogni $x, y \in G$, e questo avviene se e solo se $[x, y] \in N$ per ogni $x, y \in G$, condizione che, a sua volta, equivale a $G' \leq N$. ∎

Serie derivata. Sia G un gruppo. Poniamo $G^{(0)} = G$, $G^{(1)} = G' = [G, G]$ e, per $n \geq 0$,

$$G^{(n+1)} = [G^{(n)}, G^{(n)}] = (G^{(n)})'.$$

Per un'osservazione fatta prima (e il Lemma 2.5) $G^{(n)}$ *char* G per ogni $n \geq 1$.

ESEMPIO 2.6. Descriviamo la serie derivata dei gruppi diedrali. Sia quindi $G = C \rtimes \langle x \rangle$, con $C = \langle u \rangle$ ciclico, $|x| = 2$ e $a^x = a^{-1}$ per ogni $a \in C$, un gruppo diedrale. Poiché $C \trianglelefteq G$ e $G/C \simeq \langle x \rangle$ è ciclico di ordine 2, dal Lemma 2.22 segue che $G' \leq C$. Poiché C è ciclico (ed in particolare abeliano), $G(2) = [G', G'] = 1$. Ora, per ogni $a \in C$,

$$[a, x] = a^{-1}a^x = a^{-2}. \tag{2.12}$$

Se C è finito di ordine dispari, $a \mapsto a^{-2}$ è una biezione da C in se stesso, e da (2.12) segue $G' = C$. Supponiamo allora che C sia infinito oppure finito di ordine pari; allora $\langle u^2 \rangle$ è l'unico sottogruppo di indice 2 in C, ed è quindi normale in G. Da (2.12) segue che $\langle u^2 \rangle \leq G'$; ma $G/\langle u^2 \rangle$ è un gruppo di ordine 4 e pertanto è abeliano per l'esercizio 1.33. Quindi $G' \leq \langle u^2 \rangle$ e, in conclusione, $G' = \langle u^2 \rangle$. □

Proposizione 2.23. *Un gruppo G è risolubile se e solo se esiste un intero $n \geq 1$ tale che $G^{(n)} = 1$.*

DIMOSTRAZIONE. Poiché, per il Lemma 2.22, i fattori della serie derivata sono abeliani, se $G^{(n)} = 1$ allora G è risolubile per definizione.
Viceversa sia G risolubile e sia $1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$ una serie di G a fatttori abeliani. Si prova, per induzione su n che $G_n \geq G^{(n)}$. Infatti $G_1 \trianglelefteq G$ e G/G_1 è abeliano, quindi $G' \leq G_1$ per il Lemma 2.22. Questo prova il caso $n = 1$. Poi, applicando l'ipotesi induttiva, $G^{(n)} \leq G_1^{(n-1)} \leq G_n = 1$, da cui la tesi. ∎

Proposizione 2.24. *Un gruppo finito è risolubile se e soltanto ha una serie di composizione i cui fattori sono ciclici di ordine primo.*

DIMOSTRAZIONE. In un verso, la tesi segue dalla definizione di gruppo risolubile. Viceversa, supponiamo che G sia un gruppo finito risolubile e proviamo l'affermazione per induzione su $|G|$ (essendo banalmente vera per $|G| = 1$). Sia quindi $|G| > 1$; allora, poiché G è risolubile, $G' < G$. Sia p un divisore primo di $|G/G'|$. Per l'esercizio 2.20 esiste un sottogruppo N/G' di G/G' tale che $|G : N| = |G/G' : N/G'| = p$. Inoltre, poiché G/G' è abeliano, $N \trianglelefteq G$. Per ipotesi induttiva, N ha una serie di composizione i cui fattori sono ciclici di ordine primo; aggiungendo a questa un termine superiore G si ottiene una serie di composizione di G con la medesima proprietà. ∎

Per quanto riguarda le serie principali di un gruppo risolubile osserviamo che i loro fattori sono risolubili e, per il Lemma 2.5, caratteristicamente semplici. Ora, poiché il sottogruppo derivato è caratteristico, un gruppo risolubile e caratteristicamente semplice è abeliano. Applicando l'esercizio 2.15 si deduce quindi la seguente osservazione.

Proposizione 2.25. *Un gruppo finito è risolubile se e soltanto ha una serie principale i cui fattori sono gruppi abeliani elementari (per primi che possono essere diversi).*

Esempio: Gruppi semilineari. In questo paragrafo estendiamo un poco la costruzione dell'esempio 2.2. Siano p un numero primo, $m \geq 2$, $\mathbb{F} = GF(q)$ il campo di ordine $q = p^m$, e $\mathcal{G}$ il gruppo di Galois di $\mathbb{F}$ (su $GF(p)$ (ricordo che $\mathcal{G}$ è un gruppo ciclico di ordine m). Indichiamo con A il gruppo additivo $(\mathbb{F}, +)$, mentre $\mathbb{F}^*$ continua a denotare quello moltiplicativo.
Per ogni $(a, \sigma) \in \mathbb{F}^* \times \mathcal{G}$, sia $\phi(a, \sigma) : A \to A$ definita da

$$x^{\phi(a,\sigma)} = ax^\sigma \quad \forall x \in A. \tag{2.13}$$

Poniamo quindi

$$\Gamma(q) = \{\phi(a, \sigma) \mid (a, \sigma) \in \mathbb{F}^* \times \mathcal{G}\}.$$

Si riconosce facilmente che $\phi(a, \sigma) \in Aut(A)$ e che $(a, \sigma) \neq (a', \sigma') \Rightarrow \phi(a, \sigma) \neq \phi(a', \sigma')$; da cui segue che

$$|\Gamma(q)| = |\mathbb{F}^* \times \mathcal{G}| = m(q - 1)$$

Inoltre, per ogni $(a, \sigma) \neq (b, \tau) \in \mathbb{F}^{ast} \times \mathcal{G}$ e ogni $x \in A$,

$$x^{\phi(a,\sigma)\phi(b,\tau)} = (ax^\sigma)^{\phi(b,\tau)} = ba^\tau x^{\sigma\tau} = x^{\phi(ba^\tau,\sigma\tau)}.$$

Dunque $\Gamma(q)$ è un sottogruppo di $Aut(A)$, nel quale valgono le regole di moltiplicazione

$$\begin{aligned} &\phi(a, \sigma)\phi(b, \tau) = \phi(ba^\tau, \sigma\tau) \\ &\iota_A = \phi(1, \iota) \\ &\phi(a, \sigma)\phi(b, \tau)^{-1} = \phi((a^{-1})^{\sigma^{-1}}, \sigma^{-1}). \end{aligned} \tag{2.14}$$

Poniamo $H = \{\phi(a, \iota) \mid a \in \mathbb{F}^*\}$ e $L = \{\phi(1, \sigma) \mid \sigma \in \mathcal{G}\}$. Dalle formule (2.14), facendo i conti, si trova che H, L sono sottogruppi di $\Gamma(q)$, che H è normale e che $\Gamma(q) = H \rtimes L$. Inoltre

$H \simeq \mathbb{F}^*$ e $L \simeq \mathcal{G}$ sono entrambi gruppi ciclici di ordine, rispettivamente, $q-1$ e m. Sia ρ un generatore di $\mathcal{G}$ e $g = (1, \rho)$; allora $L = \langle g \rangle$. per ogni $\phi(a, \iota) \in H$, applicando le (2.14), si ha

$$\phi(a, \iota)^g = \phi(1, \rho^{-1})\phi(a, \iota)\phi(1, \rho) = \phi(a^\rho, \iota),$$

da cui segue che $C_H(g) = \{\phi(a, \iota) \in H \mid a \in Fix_{\mathbb{F}}(g) \setminus \{0\}\}$. Poiché $Fix_{\mathbb{F}}(g) = GF(p)$, si conclude in particolare che $|C_H(g)| = p - 1$. Ora, per l'esercizio 2.25, $[H, \langle g \rangle]$ (che, lo si verifichi, coincide con il derivato H') è isomorfo a $H/C_H(g)$, dunque è ciclico e

$$|[H, \langle g \rangle]| = \frac{q-1}{p-1} = p^{m-1} + \cdots + p + 1.$$

Il gruppo semilineare affine su $\mathbb{F} = GF(q)$ è definito come il prodotto semidiretto

$$G = A\Gamma(q) = A \rtimes \Gamma(q).$$

Da quanto appena visto (assieme al fatto, vedi esempio 2.4) che A è un sottogruppo normale minimo di G, si ottiene che la serie derivata di G è la seguente

$$G \geq AH' \geq A \geq 1$$

i cui fattori sono (in ordine discendente): $G/AH' \simeq H/H'$ abeliano di ordine $m(p-1)$, $AH'/A \simeq H'$ ciclico di ordine $\frac{q-1}{p-1}$, e A abeliano elementare di ordine p^m.

2.6 Gruppi infiniti (costruzioni)

Prodotto cartesiano e diretto. Sia $(G_n)_{n \in I}$ una famiglia di gruppi, per qualche opportuno insieme di indici I. Denotiamo con W l'insieme di tutte le applicazioni

$$f : I \to \bigcup_{n \in I} G_n$$

tali che $f(n) \in G_n$ per ogni $n \in I$.
Su W si definisce un'operazione $\cdot$ nel modo naturale: date $f, g \in W$, si pone

$$(f \cdot g)(n) = f(n)g(n) \quad \text{per ogni } n \in I.$$

Si prova immediatamente che $(W, \cdot)$ è un gruppo, detto il *prodotto cartesiano* della famiglia $(G_n)_{n \in I}$, e che denoteremo con $Car_{n \in I} G_n$.

Una fondamentale utilizzo del prodotto cartesiano è conseguenza dal seguente risultato.

Proposizione 2.26. *Sia $\mathcal{R}$ una famiglia di sottogruppi normali del gruppo G. Allora l'applicazione*

$$G \to W = Car_{N \in \mathcal{R}} G/N$$

che ad ogni $g \in G$ associa l'applicazione data da

$$N \mapsto Ng, \quad \text{per ogni } N \in \mathcal{R}$$

è un omomorfismo di gruppi il cui nucleo è $\bigcap_{N \in \mathcal{R}} N$. In particolare, se $\bigcap_{N \in \mathcal{R}} N = 1$, allora G è isomorfo ad un sottogruppo di $Car_{N \in \mathcal{R}} G/N$.

DIMOSTRAZIONE. L'enunciato indica in modo abbastanza chiaro la sua dimostrazione. ∎

Sia, come sopra, $(G_i)_{i\in I}$ una famiglia di gruppi e $W = Car_{i\in I}G_i$. Per ogni $i \in I$ si definisce la proiezione $\pi_i : W \to G_i$ ponendo $f \mapsto f(i)$ per ogni $f \in W$. Per definizione di operazione in W, π_i è un omomorfismo suriettivo; il suo nucleo, non è altro che il prodotto cartesiano

$$\ker \pi_i = Car_{i\neq n\in I}G_n. \tag{2.15}$$

Corrispondentemente, si definisce il sottogruppo

$$G_i^* = \{f \in W \mid f(j) = 1_{G_j} \text{ per } j \neq i\}. \tag{2.16}$$

La restrizione a G_i^* della proiezione π_i è un isomorfismo $G_i^* \to G_i$, ed è immediato verificare che $G_i^* \trianglelefteq W$; segue quindi che

$$W \simeq G_i^* \times (\ker \pi_i) \tag{2.17}$$

In particolare, assieme alla (2.15) ed una facile induzione, si ha che se I è finito (diciamo $I = \{1, 2, \ldots, n\}$), allora il prodotto cartesiano $Car_{i=1,\ldots,n}G_i$ coincide col prodotto diretto $G_1 \times G_2 \times \cdots \times G_n$.

Prodotto diretto. Nel caso di famiglia infinita di gruppi, il prodotto diretto è, per come lo stiamo per definire, un sottogruppo proprio del prodotto cartesiano. Sia, come sopra, $(G_n)_{n\in I}$ una famiglia di gruppi, e sia $W = Car_{n\in I}G_n$; per ogni $f \in W$si definisce il *supporto* di f come

$$supp(f) = \{n \in I \mid f(n) \neq 1_{G_n}\}. \tag{2.18}$$

Si prova facilmente che l'insieme delle funzioni a supporto finito,

$$\{f \in W \mid |supp(f)| < \infty\},$$

è un sottogruppo normale di W; questo sottogruppo, che denotiamo con $Dir_{n\in I}G_n$ è, per definizione, il *prodotto diretto* della famiglia $(G_n)_{n\in I}$. Va da sé che se I è finito ($I = \{1, \ldots, n\}$) il prodotto diretto coincide con quello cartesiano che a sua volta, per quanto detto sopra, coincide con la definizione di prodotto diretto $G_1 \times \cdots \times G_n$ data nel primo capitolo.

Limiti diretti. Sia $(P, \leq)$ un insieme parzialmente ordinato *diretto*, ovvero tale che per ogni $x, y \in P$ esiste $z \in P$ con $x \leq z$ e $y \leq z$.
Per ogni $\lambda \in P$ sia G_λ un gruppo, per ogni $\lambda \leq \mu \in P$ sia assegnato un omomorfismo

$$\phi_{\lambda\mu} : G_\lambda \to G_\mu$$

in modo che tali omomorfismi siano soggetti alle seguenti condizioni:

$$\begin{aligned} &\bullet\ \phi_{\lambda\lambda} \text{ coincide con l'identità su } G_\lambda \\ &\bullet\ \phi_{\lambda\mu}\phi_{\mu\nu} = \phi_{\lambda\nu} \text{ per ogni } \lambda \leq \mu \leq \nu \text{ in } P. \end{aligned} \tag{2.19}$$

(dove, cosa che in questo caso rende più grate le notazioni, gli omomorfismi sono scritti "a destra"). L'insieme $\mathfrak{D} = \{G_\lambda, \phi_{\lambda\mu} \mid \lambda, \mu \in P,\ \lambda \leq \mu\}$ si dice un *sistema diretto* di gruppi.

Sull'unione disgiunta (cosa che possiamo assumere senza problemi) $\mathcal{G} = \bigcup_{\lambda\in P} G_\lambda$ definiamo una relazione $\sim$ ponendo, per ogni $g \in G_\lambda$, $h \in G_\mu$, $g \sim h$ se

$$g\phi_{\lambda\nu} = h\phi_{\mu\nu} \text{ per qualche } \nu \in P \text{ con } \lambda \leq \nu,\ \mu \leq \nu. \tag{2.20}$$

Osserviamo che se (2.20) è verificata allora per ogni $\nu \leq \rho \in P$, applicando $\phi_{\nu\rho}$, dalle condizioni (2.19), segue $g\phi_{\lambda\rho} = h\phi_{\mu\rho}$. Si verifica agevolmente che $\sim$ è una equivalenza su $\mathcal{G}$. Denotiamo con D l'insieme quoziente $\mathcal{G}/\sim$, e per ogni $g \in \mathcal{G}$, con $[g]$ la classe di equivalenza di g. Dati $g \in G_\lambda$ e $h \in G_\mu$ si pone

$$[g][h] = [(g\phi_{\lambda\nu})(h\phi_{\mu\nu})] \tag{2.21}$$

dove $\nu \in P$ è tale che $\lambda \leq \nu$ e $\mu \leq \nu$. Verifichiamo che si tratta di una buona definizione. Siano $g' \in G_{\lambda'}$, $h' \in G_{\mu'}$ con $g \sim g'$ e $h \sim h'$; per quanto osservato prima, esiste $\nu \in P$ con $\lambda, \lambda', \mu.\mu' \leq \nu$, tale che

$$g\phi_{\lambda\nu} = g'\phi_{\lambda'\nu},\ h\phi_{\mu\nu} = h'\phi_{\mu'\nu};$$

quindi $(g\phi_{\lambda\nu})(h\phi_{\mu\nu}) = (g'\phi_{\lambda'\nu})(h'\phi_{\mu'\nu})$, il che assicura che la (2.21) è una buona definizione. A questo punto, è semplice provare che, con l'operazione appena definita, l'insieme quoziente D è un gruppo: e che si ha $1_D = [1_{G_\lambda}]$ (qualsiasi $\lambda \in P$), e $[g]^{-1} = [g^{-1}]$ per ogni $g \in \mathcal{G}$.
D si chiama il *limite diretto* del sistema diretto di gruppi $\mathfrak{D}$, e lo denoteremo con

$$D = \varinjlim^{\mathfrak{D}} G_\lambda$$

Fatto questo, per ogni$\lambda \in P$, è possibile definire un omomorfismo $\alpha_\lambda : G_\lambda \to D$, ponendo semplicemente $g\alpha_\lambda = [g]$ per ogni $g \in G_\lambda$. Se, per ogni $\lambda \in P$, denotiamo con G^*_λ l'immagine di α_λ, allora $G^*_\lambda \leq D$; inoltre,

Proposizione 2.27. *Con le notazioni usate sopra si ha*

(i) $D = \bigcup_{\lambda\in P} G^*_\lambda$

(ii) $G^*_\lambda \leq G^*_\mu$ *se* $\lambda \leq \mu$

(iii) α_λ *è iniettivo (cioè* $G^*_\lambda \simeq G_\lambda$*) se e solo se* $\phi_{\lambda\mu}$ *è iniettivo per ogni* $\lambda \leq \mu$.

Dimostrazione. (i) Ovvio per definizione di D.
(ii) Siano $\lambda, \mu \in P$ con $\lambda \leq \mu$, e $g \in G_\lambda$. Allora $g \sim g\phi_{\lambda\mu}$ e quindi

$$g\alpha_\lambda = [g] = [g\phi_{\lambda\mu}] = (g\phi_{\lambda\mu})\alpha_\mu \in G^*_\mu.$$

(iii) Sia $\phi_{\lambda\mu}$ iniettivo per ogni $\lambda \leq \mu$, e siano $g, h \in G_\lambda$ con $g \neq h$; allora $g\phi_{\lambda\mu} \neq h\phi_{\lambda\mu}$ per ogni $\lambda \leq \mu$ e dunque $[g] \neq [h]$ in D. Viceversa, sia α_λ iniettivo e $\lambda \leq \mu$; allora per ogni $g, h \in G_\lambda$, da $g \neq h$ segue $[g] \neq [h]$ e quindi $g\phi_{\lambda\mu} \neq h\phi_{\lambda\mu}$. ∎

Osserviamo come da questa Proposizione segua, in particolare, che il limite diretto di gruppi periodici è periodico, e che se P ha un massimo m, allora $D = G^*_m \simeq G_m$.
Il caso più trasparente di limite diretto è quando tutti le applicazioni $\phi_{\lambda\mu}$ sono iniettive; in tal caso. per $\lambda \leq \mu$, $G_\lambda \simeq G^*_\lambda \leq G^*_\mu \simeq G_\mu$; quindi le applicazioni $\phi_{\lambda\mu}$ possono essere viste come inclusioni e il limite diretto D inteso come l'unione insiemistica dei G_λ.

Ad esempio, sia p un numero primo e, per ogni $1 \leq n \in \mathbb{N}$ sia $U_n = \langle u_n \rangle$ un gruppo ciclico di ordine p^n; per $n \leq m$ sia $\phi_{nm} : U_n \to U_m$ l'omomorfismo definito da $u_n \mapsto u_m^{p^{m-n}}$. Il limite diretto della famiglia (G_n, ϕ_{nm}) è l'unione dei sottogruppi $U_n^* \simeq U_n$ con $1 \leq U_1^* \leq U_2^* \leq \ldots$, e quindi non è altro che il gruppo di Prüfer C_{p^∞}.
Di fatto, se G è un gruppo e $\mathcal{L}$ una famiglia di sottogruppi di G tale che $\bigcup_{H \in \mathcal{L}} H = G$, che formi, rispetto alla relazione d'inclusione, un insieme diretto (cioè, per ogni $H, K \in \mathcal{L}$ esiste $S \in \mathcal{L}$ tale che $\langle H, K \rangle \leq S$); ad esempio $\mathcal{L}$ può essere l'insieme dei sottogruppi finitamente generati di G),e per ogni $H.K \in \mathcal{L}$ con $H \leq K$ si pone ϕ_{HK} l'inclusione di H in K, allora, con le notazioni usate sopra, $g \mapsto [g]$ definisce un isomorfismo da G nel limite diretto $\varinjlim^{\mathcal{L}} H$ (che pertanto si identifica con G). L'interesse della costruzione sta nei casi (che occorrono soprattutto in topologia e omologia) in cui essa da vita a nuovi gruppi.

Esempio 2.7. Sia $\mathbb{F}$ un campo e per ogni $1 \leq n \in \mathbb{N}$ sia $G_n = GL(n, \mathbb{F})$. Per $n \leq m$ l'omomorfismo $\phi_{nm} : GL(n, \mathbb{F}) \to GL(m, \mathbb{F})$ è definito dal porre una matrice quadrata di ordine n come blocco nell'angolo superiore a sinistra (minore principale) di una matrice di ordine m completandone la diagonale con 1. Il limite diretto che si costruisce a partire da questo sistema si chiama talvolta il gruppo stabile lineare su $\mathbb{F}$ (e viene denotato con $GL(\infty, \mathbb{F})$). □

Limiti inversi. Il limite inverso è la costruzione duale (dal punto di vista categorico) a quella di limite diretto, anche se risulta per certi versi più delicata e le sue proprietà, almeno per chi scrive, più difficili da intuire.
Si parte ancora da un insieme parzialmente ordinato diretto $(P, \leq)$ e da una famiglia di gruppi $(G_\lambda)_{\lambda \in P}$, ma gli omomorfismi vanno al contrario. Per ogni $\lambda, \mu \in P$ con $\lambda \leq \mu$ è assegnato un omomorfismo $\pi_{\mu\lambda} : G_\mu \to G_\lambda$, con le seguenti condizioni:

$$\begin{aligned} &\bullet\ \pi_{\lambda\lambda} \text{ coincide con l'}\textit{identità su } G_\lambda \\ &\bullet\ \pi_{\nu\mu}\psi_{\mu\lambda} = \pi_{\lambda\nu} \text{ per ogni } \lambda \leq \mu \leq \nu \text{ in } P. \end{aligned} \tag{2.22}$$

L'insieme $\mathfrak{I} = \{G_\lambda, \pi_{\mu\lambda} \mid \lambda, \mu \in P,\ \lambda \leq \mu\}$ si dice un *sistema inverso* di gruppi.
Si considera poi, nel prodotto cartesiano $W = Car_{\lambda \in P} G_\lambda$ (dove torna conveniente scrivere, per $f \in W$ e $\lambda \in P$, f_λ invece di $f(\lambda)$),

$$\{f \in W \mid f_\mu \pi_{\mu\lambda} = f_\lambda\ \forall \lambda \leq \mu\}. \tag{2.23}$$

Si verifica facilmente che, per effetto delle condizioni (2.22), si tratta di un sottogruppo di W, che si denota con

$$L = \varprojlim^{\mathfrak{I}} G_\lambda$$

e si chiama il *limite inverso* del sistema inverso $\mathfrak{I}$.
Nel caso del limite inverso L, per ogni $\lambda \in P$ è definito in modo naturale un omomorfismo $\beta_\lambda : L \to G_\lambda$, che non è altro che la restrizione a L della proiezione su G_λ del prodotto cartesiano W, cioè: $f\beta_\lambda = f_\lambda$ per ogni $f \in L$. Dalla definizione di L segue che $\beta_\mu \pi_{\mu\lambda} = \beta_\lambda$ per ogni $\lambda \leq \mu$. Per ogni $\lambda \in P$, poniamo $N_\lambda = \ker \beta_\lambda$.

Proposizione 2.28. *Con le notazioni usate sopra si ha*

(i) $\bigcap_{\lambda \in P} N_\lambda = 1$.

(ii) $N_\mu \leq N_\lambda$ *se* $\lambda \leq \mu$.

(iii) β_λ *è suriettivo* (*cioè* $G_\lambda \simeq L/N_\lambda$) *se e solo se* $\pi_{\mu\lambda}$ *è suriettivo per ogni* $\lambda \leq \mu$.

DIMOSTRAZIONE. (i) Chiaro dalla definizione di prodotto cartesiano.
(ii) e (iii) seguono direttamente dal fatto osservato prima che, per $\lambda \leq \mu$, $\beta_\mu \pi_{\mu\lambda} = \beta_\lambda$. ∎

Dualmente alle considerazioni fatte sul limite diretto, consideriamo, in un gruppo G, una famiglia $\mathcal{N}$ di sottogruppi normali tale che $\bigcap_{n\in\mathcal{N}} N = 1$, che sia diretta rispetto alla relazione di inclusione inversa (cioè tale che per ogni $N, M \in \mathcal{N}$ esiste $L \in \mathcal{N}$ con $L \leq N \cap M$). Per ogni $N, M \in \mathcal{N}$ con $N \geq M$ è definita naturalmente la proiezione $\pi_{MN} : G/M \to G/N$ (data da $(Mx)\pi_{MN} = Nx$ per ogni $x \in G$), ed è immediato che $\{G/N, \pi_{nm} \mid N, M \in \mathcal{N}, N \geq M\}$ costituyisce un sistema inverso di gruppi, il cui limite $\overleftarrow{G}_\mathcal{N} = \varprojlim^{\mathcal{N}} G/N$ si chiama il *completamento* di G rispetto a $\mathcal{N}$ (il termine topologico non è casuale: anzi, la teoria dei limiti inversi è più convenientemente trattata nella cornice dei gruppi topologici, cosa che però non rientra negli obiettivi di queste note) e, contrariamente a quanto avviene per limiti diretti di sottogruppi, non è in genere isomorfo a G. Quel che si può dire è che l'immagine dell'immersione naturale di G nel prodotto cartesiano $Car_{N\in\mathcal{N}}(G/N)$ (Proposizione 2.26) è contenuta in $\overleftarrow{G}_\mathcal{N}$, e quindi che G è isomorfo ad un sottogruppo di $\overleftarrow{G}_\mathcal{N}$.

Gruppi residualmente finiti e profiniti. Un gruppo si dice *profinito* se è il limite inverso di un sistema inverso di gruppi finiti.
Ad esempio, sia p un numero primo e, per ogni $1 \leq n \in \mathbb{N}$ sia $G_n = \mathbb{Z}/p^n\mathbb{Z}$ il gruppo ciclico di ordine p^n (questa volta è consigliata la notazione additiva), e per $n \leq m$ sia $\pi_{mn} : G_m \to G_n$ la proiezione naturale $x + p^m\mathbb{Z} \mapsto x + p^n\mathbb{Z}$. Il limite diretto della famiglia (G_n, π_{nm}) è il gruppo additivo dell'anello $\mathbb{Z}_p$ degli interi p-adici (di fatto, la costruzione di limiti inversi funziona in molte altre categorie, in particolare per gli anelli, e si prova - quasi per sua definizione - che $\mathbb{Z}_p$ è *l'anello* limite inverso degli anelli $\mathbb{Z}/p^n\mathbb{Z}$) . Estendendo poi la proiezione mod p^m alle matrici, si definiscono, per ogni $n \leq m$ omomorfismi suriettivi $SL(2, \mathbb{Z}/p^m\mathbb{Z}) \to SL(2, \mathbb{Z}/p^n\mathbb{Z})$; il limite inverso del sistema inverso così ottenuto si dimostra coincidere con il gruppo di matrici $SL(2, \mathbb{Z}_p)$ a coefficienti nell,anello $\mathbb{Z}_p$.

Un caso interessante si ha quando il sistema è definito a partire da quozienti e rispettive proiezioni in un dato gruppo G. Sia G gruppo e sia $\mathcal{F}$ la famiglia dei sottogruppi $N \trianglelefteq G$ tali che G/N è un gruppo finito; il gruppo G si dice si dice *residualmente finito* se

$$\bigcap_{N\in\mathcal{F}} N = 1.$$

Alternativamente, se per ogni $1 \neq x \in G$ esiste un omomorfismo ϕ da G in un gruppo finito F tale che $x\phi \neq 1$ (l'esempio più ovvio di gruppo infinito residualmente finito è il gruppo additivo $\mathbb{Z}$; ma su questa importante classe di gruppi avremo modo di tornare più volte). Se G è un gruppo residualmente finito (e $\mathcal{F}$ come definita sopra) il limite inverso

$$\widehat{G} = \varprojlim^{\mathcal{F}} G/N$$

si chiama il *completamento profinito* di G. Come detto, $\widehat{G}$ è, in generale, molto più grande di G; ad esempio, si dimostra che $\widehat{Z}$ è il prodotto cartesiano dei gruppi additivi $\mathbb{Z}_p$ al variare di p nell'insieme di tutti i numeri primi.

2.7 Esercizi II

Sezione 2.1

Esercizio 2.1. Sia G un gruppo, e poniamo $A = Aut(G)$ e $I = Inn(G)$. Si provi che se $Z(G) = 1$ allora $C_A(I) = 1$.

Esercizio 2.2. Siano $\mathbb{F}$ un campo, $n \geq 1$ e $G = GL(n, \mathbb{F})$. Allora l'applicazione "inversa della trasposta" $A \mapsto (A^{\mathrm{T}})^{-1}$ $(\forall A \in G)$ è un automorfismo di G. Si provi che non è un automorfismo interno.

Esercizio 2.3. Siano G un gruppo finito e $H \leq G$. Si dimostri che $G = \bigcup_{g \in G} H^g$ se e soltanto se $H = G$. [sugg.: contare gli elementi dell'unione]

Esercizio 2.4. Sia G un gruppo finito. Si provi che se G contiene uno ed un solo sottogruppo di ordine d per ogni divisore d di $|G|$, allora G è ciclico.

Sezione 2.2

Esercizio 2.5. Sia S sottogruppo del prodotto semidiretto $N \rtimes H$. Si provi che $S/(N \cap S)$ è isomorfo ad un sottogruppo di H.

Esercizio 2.6. Sia $n \geq 2$ e D_{2n} il gruppo diedrale di ordine $2n$. Si provi che le seguenti condizioni sono equivalenti:
(1) n è dispari;
(2) le involuzioni di D_{2n} sono a due a due coniugate.

Esercizio 2.7. Si provi che ogni gruppo diedrale è isomorfo a un quoziente di D_∞. Siano poi $2 \leq n, m \in \mathbb{N}$; si provi che esiste un omomorfisfmo suriettivo $D_{2n} \to D_{2m}$ se e soltanto se m divide n.

Esercizio 2.8. Sia G un gruppo infinito tale che esiste $A \trianglelefteq G$ con A ciclico e $|G : A| = 2$. Si provi che G è isomorfo ad uno dei seguenti gruppi: $\mathbb{Z}$, $\mathbb{Z} \times C_2$, D_∞.

Esercizio 2.9. Sia $T(2, \mathbb{Z})$ il gruppo delle matrici triangolari superiori invertibili su $\mathbb{Z}$ (vedi sezione 1.5). Si provi che $T(2, \mathbb{Z}) \simeq D_\infty \times C_2$.

Sezione 2.3

Esercizio 2.10. Sia G un gruppo con una serie di composizione. Si provi che ogni sottogruppo ed ogni quoziente di G hanno una serie di composizione.

Esercizio 2.11. Sia G un gruppo ciclico di ordine $n < \infty$. Si trovi una maniera per determinare a partire solo da n il numero di fattori in una qualunque serie di composizione di G.

Esercizio 2.12. Si provi che un gruppo abeliano ha una serie di composizione se e soltanto se è finito.

Esercizio 2.13. Si provi che un gruppo che ha una serie di composizione ha anche una serie principale. (Il viceversa non vale: vedi esercizio 3.31)

Esercizio 2.14. Si provi che il gruppo additivo di uno spazio vettoriale (su un campo) è caratteristicamente semplice.

Esercizio 2.15. Sia A un gruppo abeliano caratteristicamente semplice. Si provi che A è un p-gruppo abeliano elementare per un primo p (quindi isomorfo al gruppo additivo di uno spazio vettoriale su $\mathbb{Z}/p\mathbb{Z}$, di dimensione eventualmente infinita) oppure è isomorfo al gruppo additivo di uno spazio vettoriale su $\mathbb{Q}$.

Gruppi caratteristicamente semplici. Una prima osservazione riguarda i sottogruppi normali di un prodotto diretto di gruppi semplici:

Esercizio 2.16. Sia $n \geq 1$ e per ogni $i = 1, \ldots, n$ sia S_i un gruppo semplice non abeliano. Si provi che i sottogruppi normali del prodotto $G = S_1 \times \cdots \times S_n$ sono tutti e soli quelli del tipo

$$S_{i_1} \times \cdots \times S_{i_k} \tag{2.24}$$

con $\{s_1, \ldots, s_k\} \subseteq \{1, \ldots, n\}$.
[sugg.: la parte difficile è provare che ogni sottogruppo $1 \neq N \trianglelefteq G$ è del tipo (2.24). Sia Sia $J = \{1 \leq j \leq n \mid S_j \leq N\}$; si provi che se $i \notin J$ allora $S_i \cap N = 1$, da cui $\pi_i(N) \leq Z(S_i) = 1$ (dove $\pi_i : G \to S_i$ è la proiezione naturale); si concluda che se $i \notin J$, allora $\pi_i(N) = 1 \ldots$]

Passiamo quindi ai prodotti diretti di gruuppi semplici isomorfi.

Esercizio 2.17. Sia p un primo e $S = C_p$ un gruppo ciclico di ordine p. Si provi che per ogni $n \geq 1$, il prodotto diretto di n-copie di S, $S^n = S \times \cdots \times S$ è un gruppo caratteristicamente semplice.

Esercizio 2.18. Sia S un gruppo semplice e $n \geq 1$. Allora il prodotto diretto di n-copie di S, $S^n = S \times \cdots \times S$ è un gruppo caratteristicamente semplice. [sugg.: se S non è abeliano si ricorra all'esercizio 2.16]

Sezione 2.4

Esercizio 2.19. Sia A un gruppo abeliano e sia T il suo sottogruppo di torsione. Si provi che esiste un sottogruppo C di A tale che $T \cap C = 1$ e A/C è periodico.

Esercizio 2.20. Sia A un gruppo abelano finito. Si provi che per ogni divisore d di $|A|$ esiste $B \leq A$ con $|B| = d$.

Esercizio 2.21. Sia A un gruppo abeliano. Si provi che esiste un massimo sottogruppo divisibile D di A (cioè A è divisibile ed ogni sottogruppo divisibile di A è contenuto in D).

Esercizio 2.22. Sia π un insieme di primi; diciamo che un gruppo abeliano A è π-divisibile se per ogni $x \in A$ ed ogni π-numero $n \geq 1$, esiste $y \in A$ tale che $n = x$.

- Si provi che se A è un gruppo abeliano periodico e $A = A_{\pi'}$, allora A è π-divisibile.
- Sia D un sottogruppo π-divisibile di un gruppo abeliano A tale che A/D non contiene π-elementi. Si provi che esiste $C \leq A$ tale che $A = D \oplus C$.

- Sia p un numero primo. Si descriva un gruppo abelaino privo di torsione che sia p-divisibile ma non divisibile.

Esercizio 2.23. Sia p un numero primo e sia $G = C_{p^\infty}$ il p-gruppo di Prüfer.

- Sia H un sottogruppo proprio di G; si provi che $G/H \simeq G$.
- Sia $\mathbb{Q}_p$ come definito nell'esercizio 1.13. Si provi che $\mathbb{Q}_p/\mathbb{Z} \simeq C_{p^\infty}$.

Esercizio 2.24. Un gruppo abeliano G è detto *iniettivo* se per ogni gruppo abeliano A ed ogni $B \leq A$, ogni omomorfismo $B \to G$ si estende ad un omomorfismo $A \to G$. Si provi che un gruppo abeliano iniettivo è divisibile (vale anche il viceversa, ed è un esercizio più difficile). [sugg. per $n \geq 1$ si consideri $A = \mathbb{Z}$ e $B = n\mathbb{Z} \dots$]

Esercizio 2.25. Sia A un sottogruppo normale e abeliano del gruppo G.

- Si provi che per ogni $x \in G$, l'applicazione definita da $a \mapsto [a, x]$ $(\forall a \in A)$ è un omomorfismo di A in se stesso, il cui nucleo è $C_A(g)$; si concluda che $[A, \langle g \rangle] \simeq A/C_A(g)$.
- Si provi che se $[a, x, y] = 1$ per ogni $a \in A$ ed ogni $x, y \in G$, allora $G' \leq C_G(A)$.

Sezione 2.5

Esercizio 2.26. Un gruppo risolubile ha una serie di composizione se e solo se è finito.

Esercizio 2.27. Siano H, K sottogruppi normali del gruppo $G = HK$. Si provi che se H e K sono risolubili allora G è risolubile. Si deduca che in un gruppo finito G esiste un massimo sottogruppo normale risolubile $S(G)$ (cioè $S(G) \trianglelefteq G$ è risolubile e tale che ogni sottogruppo normale e risolubile di G è contenuto in esso; $S(G)$ si chiama il *radicale risolubile* di G).

Esercizio 2.28. Sia $\mathbb{F}$ un campo. Si determini la serie derivata del gruppo delle matrici unitriangolari superiori

$$U = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \Big| a, b, c \in \mathbb{F} \right\}$$

Si determini quindi la serie derivata del grupp $T(3, \mathbb{F})$ delle matrici triangolari superiori.

Esercizio 2.29. Si provi che se G è un gruppo risolubile finito e H un sottogruppo massimale di G, allora $|G : H|$ è la potenza di un numero primo. Se inoltre $H \trianglelefteq G$ allora $|G : H|$ è un numero primo.

Esercizio 2.30. Sia G un gruppo finito tale che per ogni coppia H, K di sottogruppi massimali si ha: $H \neq K \Rightarrow H \cap K = 1$. Si provi che si verifica uno dei seguenti casi:

- G è abeliano: allora G è ciclico di ordine p^n oppure ha ordine pq, dove p, q sono numeri primi (non necessariamente distinti).
- G non è abeliano e se H, K sono due sottogruppi massimali di G tra loro non coniugati, allora $H \trianglelefteq G$ oppure $K \trianglelefteq G$; quindi G ha due classi di coniugio di sottogruppi massimali, e $G = K \rtimes H$ dove H, K sono sottogruppi massimali con $K \trianglelefteq G$.

[sugg. se G non è abeliano, si provi che deve esistere un sottogruppo massimale $H \not\trianglelefteq G$; quindi $H = N_G(H)$. Applicando l'esercizio 2.3, si deduce che esiste un sottogruppo massimale K di G che non è coniugato ad H. Stimando il numero di elementi di $(\bigcup_{g\in G} H^g) \cup (\bigcup_{g\in G} K^g)$ (che è limitato superiormente da $|G|$) concludere che $K \trianglelefteq G$.]

Esercizio 2.31. Si provi che un gruppo finito in cui ogni sottogruppo proprio è abeliano è risolubile ed ha lunghezza derivata al più 2. [sugg. Provare che un controesempio di ordine minimo alla prima affermazione soddisfa le ipotesi dell'esercizio precedente]

Esercizio 2.32. Siano $X = \langle x\rangle$, $Y = \langle y\rangle$, due gruppi ciclici di ordine 4, e sia dato l'omomorfismo $\phi : X \to Y$ definito assegnando $\phi(x)$ l'automorfismo di inversione su Y (quindi $\phi(x^2)$ è l'identità su Y). Nel prodotto semidiretto $G = Y \rtimes_\phi X$ sia $Z = \langle (y^2, x^2)\rangle$. Si provi che $|Z| = 2$, $Z \trianglelefteq G$ e che $G/Z \simeq Q_8$.

Esercizio 2.33. Sia G un gruppo di ordine 8. Si provi che G è isomorfo ad uno dei seguenti gruppi

$$C_2 \times C_2 \times C_2, \quad C_4 \times C_2, \quad C_8, \quad D_8, \quad Q_8.$$

Esercizio 2.34. Sia $G = GL(2, 3)$. Si provi che $G' = SL(2, 3)$, $G^{(2)} = Q$ e $G^{(3)} = Z(Q)$. Si descrivano quindi i fattori della serie derivata.

Esercizio 2.35. Sia $q = p^m$ la potenza di un numero primo, $\mathbb{F} = GF(q)$, e $\mathcal{G}$ il gruppo di Galois di $\mathbb{F}$ su $GF(p)$. Per ogni $(u, a, \sigma) \in \Omega = \mathbb{F} \times \mathbb{F}^* \times \mathcal{G}$, si denoti con $\phi(u, a, \sigma)$ l'applicazione $\mathbb{F} \to \mathbb{F}$ definita da $x \mapsto u + ax^\sigma$ (per ogni $x \in \mathbb{F}$). Si provi che $G = \{\phi(u, a, \sigma) \mid (u, a, \sigma) \in \Omega\}$ è un sottogruppo di $Sym(\mathbb{F})$ e che è isomorfo a $A\Gamma(q)$.

Sezione 2.6

Esercizio 2.36. Sia $(G_n)_{n\in I}$ una famiglia di gruppi periodici. Si provi che

- $Dir_{i\in I} G_i$ è periodico;
- $Car_{i\in I} G_i$ è periodico se e solo se esiste $n \geq 1$ tale che $|g|\,|n$ per ogni $i \in I$ e $g \in G_i$.

Esercizio 2.37. Si provi che il prodotto cartesiano (o diretto) di una famiglia $(G_n)_{n\in I}$ di gruppi risolubili è risolubile se e soltanto se esiste $d \geq 1$ tale che la lunghezza derivata di ciascun G_i non supera d.

Esercizio 2.38. (Proprietà universale del prodotto cartesiano) Sia $(G_n)_{n\in I}$ una famiglia di gruppi, e sia $C = Car_{i\in I} G_i$ il suo prodotto cartesiano. Per ogni $i \in I$ denotiamo con π_i la proiezione $C \to G_i$. Sia H un gruppo e per ogni $i \in I$ sia assegnato un omomorfismo $\phi_i : H \to G_i$. Si provi che esiste un unico omomorfismo $\phi : H \to C$ tale che $\phi\pi_i = \phi_i$ per ogni $i \in I$.

Esercizio 2.39. Sia p un numero primo e, per ogni $n \geq 1$, sia $H_n = C_{p^n}$ un gruppo ciclico di ordine p^n. Siano $G = Car_{n\geq 1} H_n$ e $D = Dir_{n\geq 1} H_n$. G è abeliano, sia $T = T(G)$ il suo sottogruppo di torsione. Si provi che T è un p-gruppo, che $D \leq T$ e che T/D è divisibile.

Esercizio 2.40. Per ogni $1 \leq n \in \mathbb{N}$ sia $\langle x_n\rangle$ un gruppo ciclico infinito (scritto additivamente). Per ogni $1 \leq n, m \in \mathbb{N}$ con $n|m$ sia ϕ_{nm} l'omomorfismo $\langle x_n\rangle \to \langle x_m\rangle$ definito da $x_n \mapsto \frac{m}{n} x_m$. Si provi che $\{\langle x_n\rangle,\ \phi_{nm} \mid 1 \leq n, m \in \mathbb{N},\ n|m\}$ è un sistema diretto di gruppi e che il suo limite diretto è isomorfo al gruppo additivo $\mathbb{Q}$.

Esercizio 2.41. Si provi che il gruppo diedrale infinito è residualmente finito.

Esercizio 2.42. Si provi che ogni sottogruppo di un gruppo residualmente finito è residualmente finito. Fissato un primo p, sia H_p il sottogruppo del gruppo additivo dei razionali definito da $H_p = \{m/p^n \mid m \in Z,\ n \in \mathbb{N}\}$. Si provi che H_p è residualmente finito ma ha un quoziente che non lo è.

Capitolo 3

Azioni

3.1 Definizioni

Un'*azione* di un gruppo G su un insieme non vuoto S è un omomorfismo

$$\Phi : G \to Sym(S). \tag{3.1}$$

Un'azione (3.1) è *fedele* quando è iniettiva, ovvero il suo *nucleo* $\ker \Phi$ è banale (cioè $\ker \Phi = \{1_G\}$); in tal caso l'immagine $\Phi(G)$ è un sottogruppo di $Sym(S)$ isomorfo a G, e si dice (identificando G con $\Phi(G)$) che G è un *gruppo di permutazioni* su S.
Sia $\Phi : G \to Sym(S)$ un'azione di G su S e, per ogni $g \in G$ e ogni $s \in S$, sia $s \cdot g = s^{\Phi(g)}$
Sussistono allora le seguenti proprietà: per ogni $g, h \in G$ e ogni $s \in S$:

$$s \cdot (gh) = (s \cdot g) \cdot h, \qquad s \cdot 1_G = s. \tag{3.2}$$

Ciò suggerisce una maniera equivalente per definire il concetto di azione: se G è un gruppo e S un insieme, una azione di G su S è un'applicazione $S \times G \to S$ data da $(s, g) \mapsto s \cdot g$, tale che soddisfa (3.2) per ogni $s \in S$ ed ogni $g, h \in G$. Se ciò avviene, per ciascun $g \in G$

$$\begin{array}{rccc} \phi(g) : & S & \to & S \\ & s & \mapsto & s \cdot g \end{array}$$

è una permutazione di S, e questo definisce un omomorfismo di G in $Sym(S)$.

Esempio 3.1. Sia $\mathbb{F}$ un campo e sia $G = \mathbb{F} \rtimes \mathbb{F}^*$ il gruppo definito nell'esempio 2.2. Il porre, per ogni $(a, b) \in G$ ed ogni $s \in \mathbb{F}$,

$$s \cdot (a, b) = a + sb,$$

definisce una azione del gruppo G su $\mathbb{F}$. Infatti, per ogni $s \in \mathbb{F}$: $s \cdot 1_G = s \cdot (0, 1) = 0 + s1 = s$, e, per ogni $(a, b), (c, d) \in G$:

$$(s \cdot (a, b)) \cdot (c, d) = (a + sb) \cdot (c, d) = c + ad + sbd = s \cdot (c + ad, bd) = s \cdot ((a, b)(c, d)).$$

Si osservi che questo esempio può essere più convenientemente descritto identificando subito G come l'insieme delle biezioni di $\mathbb{F}$ del tipo $x \mapsto bx+a$ ($\forall x \in \mathbb{F}$), al variare di (a,b) in $\mathbb{F} \times \mathbb{F}^*$. Tale insieme di biezioni è un gruppo e la sua azione su $\mathbb{F}$ è allora quella naturale. □

Orbite e stabilizzatori. Data una azione del gruppo G su S, per ogni $s \in S$ si definiscono:
- l'*orbita* $O_G(s)$ di s (rispetto alla azione di G), come l'insieme dei trasformati di s tramite tutti gli elementi di G:

$$O_G(s) = \{s \cdot g |\ g \in G\},$$

- lo *stabilizzatore* G_s (o anche $Stab_G(s)$) di s in G, come l'insieme degli elementi di G la cui permutazione fissa s:

$$G_s = \{g \in G |\ s \cdot g = s\}$$

Prima di proseguire, si osservi il fatto elementare ma fondamentale che, data una azione del gruppo G sull'insieme S, le G-orbite distinte costituiscono una partizione di S.

Teorema 3.1. *Sia data una azione del gruppo G sull'insieme S, e sia $s \in S$. Allora:*

1) *G_s è un sottogruppo di G.*

2) *$|O_G(s)| = [G : G_s]$.*

Dimostrazione. 1) Poichè $s \cdot 1_G = s$, si ha $1_G \in G_s$ per qualunque $s \in S$. Fissato ora un tale punto s, siano $g, h \in G_s$. Allora $s \cdot g = s = s \cdot h$ e quindi

$$s \cdot (g^{-1}h) = (s \cdot g) \cdot (g^{-1}h) = s \cdot (gg^{-1}h) = s \cdot h = s,$$

dunque $g^{-1}h \in G_s$ e, per il criterio dei sottogruppi, $G_s \leq G$.

2) Sia $\mathcal{C} = \{G_s x \mid x \in G\}$ e consideriamo l'applicazione $\eta : \mathcal{C} \to O_G(s)$ descritta da $G_s x \mapsto s \cdot x$, per ogni $x \in G$.
Se, per $x, y \in G$, $G_s x = G_s y$, allora $xy^{-1} \in G_s$, cioè $s \cdot (xy^{-1}) = s$ e quindi $s \cdot x = s \cdot (xy^{-1}y) = (s \cdot (xy^{-1})) \cdot y = s \cdot y$. Dunque η è ben definita.
Proviamo ora che η è biettiva. Essa è suriettiva per definizione di orbita di s. Siano ora $G_s x, G_s y \in \mathcal{C}$ tali che $s \cdot x = s \cdot y$, allora

$$s \cdot x(y^{-1}) = (s \cdot x) \cdot y^{-1} = (s \cdot y) \cdot y^{-1} = s \cdot (yy^{-1}y) = s\ ;$$

dunque $xy^{-1} \in G_s$, cioè $G_s x = yG_s y$. Quindi η è iniettiva e pertanto è una biezione.
In particolare si ha $[G : G_s] = |\mathcal{C}| = |O_G(s)|$, come si voleva. ∎

Corollario 3.2. *Se il gruppo finito G opera sull'insieme S, allora per ogni $s \in S$, $|O_G(s)|$ divide $|G|$.*

Consideriamo ora il caso in cui sia G che S sono finiti, ed è data una azione di G su S. Siano $O_G(s_1),\ O_G(s_2),\ \ldots,\ O_G(s_n)$ le orbite distinte di G su S (l'insieme $\{s_1, s_2, \ldots, s_n\}$ si dice un insieme di rappresentanti per le orbite di G su S). Per quanto osservato, esse costituiscono una partizione di S, quindi

$$|S| = |O_G(s_1)| + |O_G(s_2)| + \cdots + |O_G(s_n)|\ .$$

Ora, per il Teorema 3.1, per ogni $i = 1, \ldots, n$, si ha $|O_G(s_i)| = [G : G_{s_i}]$; si deduce quindi l'importante:

Equazione delle orbite. *Sia* $\{s_1, s_2, \ldots, s_n\}$ *un insieme di rappresentanti per le orbite di* G *su* S. *Allora*

$$|S| = \sum_{i=1}^{n} [G : G_{s_i}] \ .$$

Punti fissi. Se G opera sull'insieme S ed $s \in S$ è tale che $O_G(s) = \{s\}$, allora s si dice un *punto fisso* per l'azione di G su S. In altri termini, $s \in S$ è un punto fisso se e solo se $s \cdot g = s$ per ogni $g \in G$, ovvero se e solo se $G_s = G$. L'insieme (possibilmente vuoto) dei punti fissi lo denoteremo con $Fix_S(G)$.

Come applicazione dell'equazione delle orbite, vediamo un criterio sufficiente all'esistenza di un punto fisso. Sia p un numero primo, sia P un gruppo di ordine p^m e sia data una azione di P su un insieme finito S. Sia $\{s_1, s_2, \ldots, s_n\}$ un insieme di rappresentanti per le orbite di G su S, e sia $F = Fix_S(P)$ l'insieme dei punti fissi. Per il teorema di Lagrange, per ogni $i = 1, \ldots, n$, l'indice $[G : G_{s_i}]$ divide $|P| = p^m$. Allora, per ogni $i = 1, \ldots, n$, o s_i è un punto fisso, cioè $s_i \in F$, oppure G_{s_i} è un sottogruppo proprio di P e quindi $[G : G_{s_i}] = p^{k(i)}$ con $k(i) \geq 1$; in particolare p divide $[G : G_{s_i}]$. Applicando la formula delle orbite si ha che p divide $\sum_{i=1}^{n} [G : G_{s_i}] = |S| - |F|$. Abbiamo quindi dimostrato

Proposizione 3.3. *Sia* P *un* p*-gruppo finito che opera su un insieme* S*; allora*

$$|Fix_S(P)| \equiv |S| \pmod{p}.$$

In particolare, si ha:

Corollario 3.4. *Sia* P *un* p*-gruppo finito che opera su un insieme* S. *Se* $(|S|, p) = 1$ *allora esiste almeno un punto fisso di* P *su* S.

Proviamo ora un altro risultato di carattere combinatorio che risulta spesso utile: dice che - nel caso di azioni di un gruppo finito - il numero di orbite è la media sugli elementi del gruppo del numero di punti fissi. Spesso è ancora chiamato *lemma di Burnside* anche se è noto che Burnside non fu il primo a notarlo.

Lemma 3.5. *Sia* G *un gruppo finito e sia data una azione del gruppo* G *sull'insieme finito* S. *Sia* t *il numero di orbite distinte e, per ogni* $g \in G$ *denotiamo con* $Fix(g)$ *l'insieme dei punti fissi per* g *su* S. *Allora*

$$t|G| = \sum_{g \in G} |Fix(g)|.$$

Dimostrazione. Sia $\mathcal{F} = \{g, s) \in G \times S \mid s \cdot g = s\}$. Calcolando la cardinalità di $\mathcal{F}$ facendo variare la prima componente g, si ha

$$|\mathcal{F}| = \sum_{g \in S} |Fix(g)|; \tag{3.3}$$

mentre, calcolando la stessa cardinalità facendo variare la seconda componente si ottiene:

$$|\mathcal{F}| = \sum_{s \in S} |G_s| \tag{3.4}$$

Ora, è chiaro che se s e r appartengono alla stessa orbita allora $|G_s| = |G_r|$; dunque, se $s_1, \ldots, s_t$ sono rappresentanti delle diverse orbite per G su S, dalla (3.4) segue:

$$|\mathcal{F}| = \sum_{i=1}^{t} |O_G(s_i)||G_{s_i}| = \sum_{i=1}^{t} |G : G_{s_i}||G_{s_i}| = t|G| \tag{3.5}$$

che confrontata con (3.3) dà la formula cercata. ∎

Azioni transitive. Una azione di G sull'insieme S si dice *transitiva* se esiste $s \in S$ tale che $O_G(s) = S$; ciò avviene se per ogni $t \in S$ esiste $g \in G$ tale che $g \cdot s = t$. Si osservi in particolare che se G è finito e l'azione di G su S è transitiva allora $|S|$ divide $|G|$.

Esempio 3.2. Si vede facilmente che l'azione descritta nell'esempio 3.1 è transitiva: infatti, per ogni $a \in K$: $0_K \cdot (a, 1)) = a + 0 = a$ se $a \neq 0$, e quindi $O_G(0_K) = K$. Calcoliamo lo stabilizzatore di un punto $s \in K$. Sia $(a, b) \in G$; allora $(a, b) \in G_s$ se e solo se $s = (s \cdot a, b) \cdot = a + sb$, se e solo se $a = s(b-1)$; quindi $G_s = \{(s(b-1), b) \mid b \in \mathbb{R}^*\}$ (ad esempio, $G_1 = \{(b-1, b) \mid b \in \mathbb{R}^*\}$). □ □

Azioni su classi laterali. Descriviamo ora una classe fondamentale di azioni transitive di un gruppo G. Sia H un sottogruppo fissato di G e denotiamo con $G\backslash H$ l'insieme delle classi laterali destre di G modulo H; su questo insieme definiamo una azione di G ponendo, per ogni $g \in G$ e ogni $Hx \in G\backslash H$,

$$Hx \cdot g = Hxg.$$

Si verifica immediatamente che ciò definisce una azione. Tale azione è transitiva: infatti, per ogni $Hx, Hy \in G\backslash H$ si ha

$$Hx \cdot (x^{-1}y) = Hxx^{-1}y = Hy.$$

Supponiamo ora che l'indice $|G : H| = n$ sia finito. Allora $|G\backslash H| = [G : H] = n$, e l'azione di G su $G\backslash H$ sopra descritta da luogo ad un omomorfismo $G \to Sym(G\backslash H) = S_n$. Sia N il nucleo di questo omomorfismo, allora

$$N = \{g \in G \mid Hxg = Hx \ \forall Hx \in G\backslash H\} = \{g \in G \mid Hxgx^{-1} = H \ \forall x \in G\}$$

osservando che

$$Hxgx^{-1} = H \quad \Leftrightarrow \quad xgx^{-1} \in H \quad \Leftrightarrow \quad g \in x^{-1}Hx = H^x$$

possiamo concludere che

$$N = \{g \in G \mid g \in H^x \ \forall x \in G\} = \bigcap_{x \in G} H^x.$$

Quind, $N = H_G$, il massimo sottogruppo normale di G contenuto in H. Inoltre, per il Teorema di omomorfismo, G/H_G risulta isomorfo ad un sottogruppo di S_n; in particolare $[G : H_G]$ divide $n!$.

Nel caso particolare in cui $H = 1$, l'azione sulle classi laterali coincide con quella per moltiplicazione a destra sugli elementi. Tale azione è sicuramente fedele, e ciò mostra come ogni gruppo si possa rappresentare come un gruppo di permutazioni (transitivo): che è il cosiddetto teorema di Cayley.

Teorema 3.6. (Cayley) *Sia G un gruppo. Allora G è isomorfo ad un sottogruppo del gruppo simmetrico $Sym(G)$.*

DIMOSTRAZIONE. Per ogni $g \in G$, la moltiplicazione a destra $\rho_g : G \to G$, definita da $x \mapsto xg$ (per ogni $x \in G$), è una biezione (quindi un elemento di $Sym(G)$); e l'applicazione $\Phi : G \to Sym(G)$ deinita da $x \mapsto \rho_g$ (per ogni $g \in G$), è un omomorfismo iniettivo da G nel gruppo $Sym(G)$. Da ciò si conclude che $G \simeq \Phi(G) \leq Sym(G)$. ∎

3.2 Teoremi di Sylow

Iniziamo con una applicazione del Corollario 3.4.

Proposizione 3.7. *Siano p un primo e P un gruppo con $|P| = p^n$, per $n \geq 1$. Allora*

(1) *$Z(P) \neq 1$;*

(2) *per ogni $0 \leq t \leq n$, P ha un sottogruppo di ordine p^t.*

DIMOSTRAZIONE. (1) Consideriamo l'azione per coniugio di P su se stesso. Quindi $Z(P)$ coincide con l'insieme dei punti fissi. Per la Proposizione 3.3

$$|Z(P)| \equiv |P| \pmod{p}.$$

Poiché $1 \leq |Z(P)|$ si ha la conclusione.

(2) Procediamo per induzione su t, l'asserto essendo banalmente vero per $t = 0$. Sia $t \geq 1$ e poniamo $Z = Z(P)$. Per il punto (1), $|Z| \neq 1$. Sia $1 \neq x \in Z$, allora l'ordine di x è una potenza p^s con $s \geq 1$, e $\langle x \rangle$ ha un sottogruppo A di ordine p. Se $t = 1$, A è il sottogruppo di P cercato. Altrimenti, osserviamo che, poiché è contenuto nel suo centro, A è normale in P. Per ipotesi induttiva P/A ammette un sottogruppo H/A di ordine p^{t-1}, dove $A \leq H \leq P$. Ma allora, $|H| = |H/A||A| = p^t$, così completando l'induzione e la dimostrazione. ∎.

Sottogruppi e teorema di Sylow. Sia G un gruppo finito e sia p un numero primo; un p-sottogruppo di G è un sottogruppo il cui ordine è una potenza di p, mentre un p-sottogruppo di Sylow di G è un p-sottogruppo P tale che p non divide l'indice $|G : P|$. Dal Teorema di Lagrange segue immediatamente che se p^m è la massima potenza di p che divide l'ordine di G (ovvero, $|G| = p^m a$ con $(p, a) = 1$), allora un sottogruppo P di G è un p-sottogruppo di Sylow se e soltanto se $|P| = p^m$.

Insieme al Teorema di Lagrange, i Teoremi di Sylow (che garantiscono l'esistenza di p-sottogruppi di Sylow, assieme a diverse altre informazioni) sono il primo strumento fondamentale per lo studio dei gruppi finiti. La dimostrazione che daremo non è quella originaria di L. Sylow (1832 - 1918), ma è ispirata a quella scoperta molti anni più tardi (1959) da H. Wielandt, ed è una ingegnosa applicazione della teoria di base per le azioni. Cominciamo con un Lemma numerico.

Lemma 3.8. *Sia p^n la massima potenza del numero primo p che divide $1 \leq k \in \mathbb{N}$. Allora p non divide $\binom{k}{p^n}$*

DIMOSTRAZIONE. Dato un numero intero $n \geq 1$ ed un primo p denotiamo con $\tau_p(n)$ l'esponente della massima potenza di p che divide n; è chiaro che $\tau_p(nm) = \tau_p(n)\tau_p(m)$, per ogni $1 \leq n, m \in \mathbb{N}$. Sia ora $k \geq 1$, $n = \tau_p(k)$ e $k = p^n a$, con $(p, a) = 1$; allora per ogni $0 \leq i \leq p^n - 1$ si ha

$$\tau_p(k - i) = \tau_p(i) = \tau_p(p^n - i). \tag{3.6}$$

poiché

$$\binom{k}{p^n} = \frac{k(k-1)\dots(k-(p^n-1))}{p^n!} = \frac{(k-1)\dots(k-(p^n-1))}{1 \cdot 2 \cdot \dots (p^n-1)} = \prod_{i=1}^{n} \frac{k-i}{p^n-i}$$

da (3.6) segue immediatamente l'asserto. L'uguaglianza (3.6) si dimostra facilmente tenendo conto che, per $0 \leq i \leq p^n$, $\tau_p(k-i) \leq n$. ∎

Possiamo ora dimostrare il Teorema di Sylow.

Teorema 3.9. *Sia G un gruppo finito, p un numero primo, $|G| = p^m a$, con $m \in \mathbb{N}$ e $(p, a) = 1$. Allora*

(i) *G ammette sottogruppi di ordine p^m (i p-sottogruppi di Sylow);*

(ii) *posto $n_p(G)$ il numero di p-sottogruppi di Sylow di G, si ha $n_p(G)|a$, ed inoltre*

$$n_p(G) \equiv 1 \pmod{p}$$

(iii) *i p-sottogruppi di Sylow sono tutti tra loro coniugati in G;*

(iv) *per ogni p-sottogruppo H di G esiste un p-sottogruppo di Sylow P di G tale che $H \leq P$.*

DIMOSTRAZIONE. Sia $|G| = p^n a$, con $(p, a) = 1$. Sia Ω l'insieme di tutti i sottoinsiemi di G di cardinalità p^n. Per il Lemma precedente

$$p \text{ non divide } |\Omega| \tag{3.7}$$

Il gruppo G agisce su Ω mediante moltiplicazione a destra: per ogni $X \in \Omega$ e $g \in G$, $X \cdot g = \{xg \mid x \in X\}$. Per (3.7) e la formula delle orbite, esiste $X \in \Omega$ tale che, posto G_X lo stabilizzatore in G di X per tale azione, si ha che p non divide $|G : G_X|$. Ora, G_X opera a sua volta su X per moltiplicazione a destra, e in questa azione gli stabilizzatori sono tutti banali; quindi X è un unione di orbite per moltiplicazione a destra di G_X, e tali orbite sono classi laterali sinistre modulo G_X. Dunque X è unione di classi laterali sinistre di G_X e pertanto

$$|G_X| \text{ divide } |X| = p^n \tag{3.8}$$

Per quanto osservato a proposito della scelta di X, da ciò segue $|G_X| = p^n$. Dunque G_X è un p-sottogruppo di Sylow di G, il che dimostra il punto (i).

Denotiamo con $\mathfrak{S}$ l'insieme dei p-sottogruppi di Sylow di G (che, per quanto appena visto, non è vuoto) e sia $P \in \mathfrak{S}$. P agisce per coniugio si $\mathfrak{S}$; chiaramente P è un punto fisso per se stesso in tale azione. Sia Q un (altro) punto fisso, allora siccome P normalizza Q, si ha che PO è un sottogruppo di G contenente P, e per la formula per l'ordine di un prodotto

(Lemma 1.7) ha cardinalità una potenza di p. Pertanto $PQ = P$, cioè $Q = P$. Quindi P è l'unico punto fisso per l'azione del p-gruppo P su $\mathfrak{S}$; per la Proposizione 3.3

$$n_p(G) = |\mathfrak{S}| \equiv 1 \pmod{p} \tag{3.9}$$

il che dimostra una parte del punto (ii).

Consideriamo ora l'azione di tutto G per coniugio su $\mathfrak{S}$; per quanto appena dimostrato e per la formula delle orbite, esiste un'orbita $\mathfrak{O}$ (cioè una classe di coniugio) per tale azione la cui cardinalità non è divisa dal primo p. Sia $P \in \mathfrak{S}$; per il corollario 3.4, P ha un punto fisso su $\mathfrak{O}$, cioè esiste un $Q \in]\mathfrak{O}$ tale che P normalizza Q. Ma allora, come sopra, $|QP| = |P|$, e quindi $Q = P$. In particolare, $P \in \mathfrak{O}$. Dunque $\mathfrak{O} = \mathfrak{S}$, e anche il punto (iii) è provato.
Da questo punto segue che, se P è un p-sottogruppo di Sylow di G, allora $n_p(G)$ coincide col numero di coniugati di P e quindi con $|G : \mathcal{N}_G(P)|$. Poiche $P \leq \mathcal{N}_G(P) \leq G$, si ha che $n_p(G)$ divide $|G : P| = a$, completando la dimostrazione del punto (ii).

Infine, sia H un p-sottogruppo di G. Allora, nell'azione per coniugio su $\mathfrak{S}$, H ha un punto fisso P. Come prima PH è allora un p-sottogruppo di G, il che comporta $PH = H$ e dunque $H \leq P$. La dimostrazione del Teorema è conclusa ∎

Dal punto (2) della Proposizione 3.7 e dal Teorema di Lagrange seguono immediatamente i seguenti corollari.

Corollario 3.10. *Siano p un primo e $m \geq 0$. Se p^m divide l'ordine del gruppo G, allora G ha un sottogruppo di ordine p^m.*

Corollario 3.11. *Siano p un primo. Un gruppo finito G è un p-gruppo se e solo il suo ordine è una potenza di p.*

Prima di passare ad alcuni esempi di applicazione del Teorema di Sylow, osserviamo il seguente fatto generale.

Proposizione 3.12. *Sia G un gruppo finito, $N \trianglelefteq G$ e p un divisore primo dell'ordine di G. Sia P un p-sottogruppo di Sylow di G. Allora, che NP/N è un p-sottogruppo di Sylow di G/N, e $P \cap N$ è un p-sottogruppo di Sylow di N.*

Dimostrazione. Sia $|G| = p^n a$ con $(p, a) = 1$, sia P un p-sottogruppo di Sylow di G, $N \trianglelefteq G$ e $|N| = p^k b$ con $k \leq a$ e $b|a$. Allora $NP \leq G$ e quindi $|NP| = p^n c$ con $c|a$. Ora

$$p^n c = |NP| = \frac{|N||P|}{|N \cap P|} = \frac{p^{k+n} b}{|N \cap P|}$$

per cui $|P \cap N| = p^k$, e dunque $P \cap N$ è un p-sottogruppo di Sylow di N; inoltre $|NP/N| = p^{n-k}$ e dunque NP/N è un p-sottogruppo di Sylow di G/N. ∎

Se p è un numero primo e G un gruppo finito, denotiamo con $Syl_p(G)$ l'insieme dei p-sottogruppi di Sylow di G. Vediamo quindi alcune prime applicazioni del Teorema di Sylow, che ne illustrano la forza anche se non ancora la portata.

Esempio 3.3. Siano p, q primi distinti, con $p > q$, e sia G un gruppo di ordine pq. Per il teorema di Sylow $n_p(G) \equiv 1 \pmod{p}$ e per quanto osservato sopra, $n_p(G)$ divide q. Poiché $q < p$ la sola possibilità è $n_p(G) = 1$, e dunque G ha un unico p-sottogruppo di Sylow P (e $P \trianglelefteq G$). Sia Q un q-sottogruppo di Sylow di G, e distinguiamo due casi:

- q non divide $p-1$. In questo caso, $p \not\equiv 1 \pmod{q}$ e dunque $n_q(G)$, che deve dividere p, è anch'esso uguale a 1; pertanto $Q \trianglelefteq G$, e $G = P \times Q$ è un gruppo ciclico di ordine pq.

- $q \mid p-1$. In questo caso $n_q(G) \in \{1, p\}$. Se $n_q(G) = 1$ allora, come prima, G è il gruppo ciclico di ordine pq; altrimenti $n_q(G) = p$ e G è il prodotto semidiretto $P \rtimes Q$, dove se $Q = \langle y \rangle$, y agisce su P come un automorfismo di ordine q. Osserviamo che, in un tale gruppo, ogni elemento $\neq 1$ appartiene a P oppure ad un unico coniugato di Q.

□

Esempio 3.4. Analizziamo il caso in cui $|G| = p^2 q$, dove p e q sono primi distinti. In questo caso, $n_p(G) \in \{1, q\}$ e $n_q(G) \in \{1, p, p^2\}$. Siano P e Q, rispettivamente, un p-sottogruppo di Sylow e un q-sottogruppo di Sylow di G. Distinguiamo due casi.

- p non divide $q-1$. Allora, come nell'esempio precedente, $n_p(G) = 1$ e $P \trianglelefteq G$. Ne segue che G è (isomorfo a) un prodotto semidiretto $P \rtimes Q$. se inoltre q non divide $p^2 - 1$ allora anche Q è normale e si ha $G = P \times Q$.

- Sia $p|q-1$. Allora $p < q$, e dunque $n_q(G) \neq p$ (dato che $p \not\equiv 1 \pmod{q}$). Se $n_q(G) = 1$, allora $Q \trianglelefteq G$ e G è il prodotto semidiretto $Q \rtimes P$ (che diventa diretto se anche $n_p(G) = 1$). Se invece $n_q(G) = p^2$, allora q divide $p^2 - 1 = (p-1)(p+1)$, e siccome q è primo ed è maggiore di p, il solo caso possibile è $p = 2$ e $q = 3$; dunque $|G| = 12$.

□

Esempio 3.5. Sia $q = p^m$ dove p è un primo e $n \geq 1$, e sia $n \geq 1$. Sia quindi (vedi sezione 1.5) $U = UT(n, q)$ l'insieme delle matrici unitriangolari superiori in $GL(n, q)$. Sappiamo che $U \leq G$ e si verifica facilmente (esercizio 1.40) il suo ordine è

$$|UT(n, q)| = q^{\frac{n(n-1)}{2}}. \tag{3.10}$$

poiché $|GL(n, q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1)$, si conclude che U è un p-sottogruppo di Sylow di $GL(n, q)$. Posto $G = GL(n, q)$, si ha $\mathcal{N}_G(U) = T$ dove T è il gruppo delle matrici triangolari superiori (esempio 2.1). Tenendo conto che $|T| = |U|(q-1)^n$, si ricava

$$n_p(GL(n, q)) = \frac{|GL(n, q)|}{|T|} = \frac{\prod_{i=1}^{n} (q^i - 1)}{(q-1)^n}.$$

□

Passiamo ad un lemma davvero molto apprezzato da chiunque studi gruppi finiti.

Lemma 3.13. (Argomento di Frattini) *Sia G un gruppo finito, e siano $N \trianglelefteq G$, p un numero primo e P un p-sottogruppo di Sylow di N. Allora*

$$G = N\mathcal{N}_G(P).$$

DIMOSTRAZIONE. Nelle ipotesi dell'enunciato, sia $g \in G$. Allora, poiché $N \trianglelefteq G$, P^g è un p-sottogruppo di Sylow di N. Dunque, per il Teorema di Sylow, esiste $a \in N$ tale che $P^g = P^a$. Da ciò segue $P^{ga^{-1}} = P$, cioè $ga^{-1} \in \mathcal{N}_G(P)$. Dunque $g \in \mathcal{N}_G(P)N = N\mathcal{N}_G(P)$, come si voleva. ∎

Un concetto utile è il seguente. Sia G un gruppo finito e p un numero primo; poniamo

$$O_p(G) = \bigcap_{P \in Syl_p(G)} P.$$

Poiché i p-sottogruppi di Sylow di G sono tra loro coniugati, $O_p(G) \trianglelefteq G$ (ed infatti se $P \in Syl_p(G)$ allora $O_p(G) = P_G$). Sia ora B un p-sottogruppo normale di G; allora $B \leq P$ per qualche $P \in Syl_p(G)$ e dunque, poiché $B \trianglelefteq G$, $B \leq O_p(G)$. Pertanto:

$O_p(G)$ *è il massimo p-sottogruppo normale di G.*

Ad esempio $O_2(S_4) = K$ (il gruppo dii Klein), mentre $O_3(S_4) = 1$.

3.3 Gruppi di permutazioni

Azioni equivalenti. Sia G un gruppo. Due azioni di G su insiemi S e S' si dicono *equivalenti* se esiste una biezione $f : S \to S'$ tale che, per ogni $g \in G, s \in S$

$$f(s \cdot g) = f(s) \cdot g. \tag{3.11}$$

In tal caso è immediato verificare che risulta $O_G(f(s)) = f(O_G(s))$ e $G_{f(s)} = G_s$, per ogni $s \in S$ (lo si provi per esercizio).
La seguente osservazione è fondamentale: insieme con quanto visto nella sezione 3.1, mostra che le azioni transitive di un gruppo G sono a meno di equivalenza, tutte e sole quelle per moltiplicazione a destra sull'insieme della classi laterali di un sottogruppo.

Proposizione 3.14. *Data una azione transitiva del gruppo G sull'insieme S, e fissato $s \in S$, sia $H = G_s$. Allora l'azione di G su S è equivalente all'azione per moltiplicazione di G sull'insieme delle classi laterali destre modulo H.*

DIMOSTRAZIONE. Fissato un $s \in S$, siano $H = G_s$ e $G\backslash H$ l'insieme delle classi laterali destre di G modulo H. Sia $f : G\backslash H \to S$ l'applicazione definita da $f(Hx) = s \cdot x$ per ogni $x \in G$. Sappiamo dal Teorema 3.1 che f è una biezione. Basta quindi verificare che vale (3.11). Il che è vero: infatti, per ogni $x, g \in G$ si ha

$$f(Hx \cdot g) = f(Hxg) = s \cdot xg = (s \cdot x) \cdot g = f(Hx) \cdot g.$$

Questo completa la dimostrazione. ∎

Un'altra istanza di equivalenza di azioni, di carattere più tecnico, ma molto utile è la seguente.

Proposizione 3.15. *Data un'azione transitiva di G su Ω sia $H = G_x$ lo stabilizzatore di un punto $x \in \Omega$. Sia N un sottogruppo normale di G tale che $N \cap H = 1$ e $NH = G$. Allora l'azione di H su Ω è equivalente all'azione per coniugio di H su N. In particolare l'azione di H su $\Omega \setminus \{x\}$ è equivalente all'azione per coniugio su $N \setminus \{1\}$.*

DIMOSTRAZIONE. Siano $x \in \Omega$, H e N come nell'enunciato. Allora l'applicazione $\beta : N \to \Omega$ definita da $\beta)x) = x^a$ (per ogni $a \in N$), è una biezione. Infatti, per $a, b \in N$, se $x^a = x^b$ allora $ab^{-1} \in N \cap H = 1$, dunque $a = b$, provando che β è iniettiva. D'altra parte se $y \in \Omega$ esiste, per l'ipotesi di transitività, $g \in G$ tale che $y = x^g$; poiché $G = HN$, $g = ha$ per qualche $h \in H$ e $a \in N$, dunque $y = x^{ha} = (x^h)^a = x^a$; quindi β è surriettiva (e N opera transitivamente su Ω). Vediamo ora che β realizza l'equivalenza tra l'azione di H su Ω indotta da quella di G e l'azione per coniugio di H su N. Infatti, per ogni $h \in H$ e ogni $a \in N$:

$$\beta(a^h) = x^{h^{-1}ah} = (x^{h^{-1}})^{ah} = (x^a)^h = (\beta(a))^h.$$

Poiché $\beta(1) = x$, l'ultima asserzione segue immediatamente. ∎

Transitività multipla. Sia $1 \leq k \in \mathbb{N}$. Un'azione di un gruppo G su un insieme Ω si dice *k-transitiva* se, per ogni coppia di k-uple $(x_1, \ldots, x_k), (y_1, \ldots, y_k)$ di elementi distinti di Ω esiste $g \in G$ tale che

$$(x_1, \ldots, x_k)^g = (x_1 \cdot g, \ldots, x_k \cdot g) = (y_1, \ldots, y_k).$$

Ad esempio, per ogni $n \geq 2$, l'azione naturale di S_n su $\{1, \ldots, n\}$ è n-transitiva. Altri significativi esempi di azioni 2-transitive li vedremo tra poco. Per il momento diamo la seguente osservazione, che è importante anche se la sua dimostrazione non è difficile.

Proposizione 3.16. *Sia $n \geq 2$ e sia data un'azione transitiva del gruppo G su Ω. Sia $x \in \Omega$. Allora l'azione di G su Ω è n-transitiva se e solo se l'azione di G_x su $\Omega \setminus \{x\}$ è $(n-1)$-transitiva.*

DIMOSTRAZIONE. Supponiamo che l'azione di G su Ω sia n-transitiva con $n \geq 2$, e siano $(x_1, \ldots x_{n-1}), (y_1, \ldots, y_{n-1})$ $(n-1)$-uple a elementi distinti di $\Omega \setminus \{x\}$. Allora, per definizione, esiste $g \in G$ tale che

$$(x_1, \ldots x_{n-1}, x)^g = (x_1^g, \ldots, x_k^g, x^g) = (y_1, \ldots, y_{n-1}, x).$$

In particolare, $(x_1, \ldots x_{n-1})^g = (y_1, \ldots, y_{n-1})$ e $x^g = x$; dunque $g \in G_x$ e ciò prova che G_x agisce $(n-1)$-transitivamente su $\Omega \setminus \{x\}$.
Viceversa, supponiamo G_x sia $(n-1)$-transitivo su $\Omega \setminus \{x\}$ e siano $(x_1, \ldots x_n), (y_1, \ldots, y_n)$ due n-uple a elementi distinti di Ω. Per transitività, esistono $g, h \in G$ tali che $x_n^g = x$ e $y_n^h = x$. Allora $(x_1, \ldots x_n)^g$ e $(y_1, \ldots, y_n)^h$ sono a elementi distinti, dunque $(x_1, \ldots x_{n-1})^g$ e $(y_1, \ldots, y_{n-1})^h$ sono $(n-1)$-uple a elementi distinti di $\Omega \setminus \{x\}$. Per ipotesi esiste $t \in G_x$ tale che $(x_1, \ldots x_{n-1})^{gt} = (y_1, \ldots, y_{n-1})^h$; poiché $x_n^{gt} = x^t = x = y_n^h$, da ciò segue $(x_1, \ldots x_n)^{gth^{-1}} = (y_1, \ldots, y_n)$, provando così che G è n-transitivo su Ω. ∎

Si deduce subito il seguente corollario

Corollario 3.17. *Sia $k \geq 1$ e G un gruppo. Se G ammette un'azione k-transitiva su un insieme Ω con $|\Omega| = n \geq k$, allora $n(n-1)\ldots(n-k+1)$ divide $|G|$.*

DIMOSTRAZIONE. Per induzione su k, applicando per il passo induttivo la Proposizione precedente. ∎

Proposizione 3.18. *Sia $n \geq 3$ e $I_n = \{1, 2, \ldots, n\}$. Allora S_n è n-transitivo nella sua azione naturale su I_n e A_n è $(n-2)$-transitivo su I_n.*

DIMOSTRAZIONE. Per esercizio. ∎

ESEMPIO 3.6. Sia $\mathbb{F}$ un campo, e $G = \mathbb{F} \rtimes \mathbb{F}^*$ (esempio 2.2). L'azione di G su $\Omega = \mathbb{F}$ definita nell'esempio 3.1 è 2-transitiva. Infatti, come abbiamo osservato, tale azione è transitiva e lo stabilizzatore di $0_{\mathbb{F}}$ è $G_0 = \{(0, b) \mid b \in \mathbb{F}^*\}$, che è un sottogruppo di G isomorfo a al gruppo moltiplicativo $\mathbb{F}^*$. Ora per ogni $0 \neq a \in \mathbb{F}$, si ha $a \cdot (0, a^{-1}b) = b$, quindi G_0 opera transitivamente su $\Omega \setminus \{0\} = \mathbb{F}^*$ e dunque, per la Proposizione 3.16, l'azione di G su Ω è 2-transitiva. □

ESEMPIO 3.7. Sia V una spazio vettoriale di dimensione $n \geq 2$ sul campo $\mathbb{K}$. Fissata una base di V, il gruppo $W = SL(n, \mathbb{K})$ delle matrici invertibili di determinante 1 opera nel modo naturale su V; per ogni $v \in V, A \in W$, $(v, A) \mapsto vA$, dove $\mathbf{v}$ è la n-upla dei coefficienti di v rispetto alla base data. (questa azione non è transitiva dato che $\{0\}$ e $V \setminus \{0\}$ sono le orbite). Sia $\Omega = \mathbb{P}(n-1, \mathbb{K})$ l'insieme dei sottospazi 1-dimensionali di V, cioè $\Omega = \{\mathbb{K}v \mid 0 \neq v \in V\}$ (su tratta dello spazio proiettivo $(n-1)$-dimensionale su $\mathbb{K}$). Ora, l'azione di W su V induce nel modo naturale un'azione di W su Ω, ponendo $\mathbb{K}v \cdot A = \mathbb{K}(\mathbf{v}A)$, per ogni $\mathbb{K}v \in \Omega$ e $A \in W$. Il nucleo di tale azione è l'insieme delle matrici scalari $Z = \{\lambda I_n \mid 0 \neq \lambda \in \mathbb{K}\}$, che è il cdentro di $GL(n, \mathbb{K})$. Il gruppo quoziente $GL(n, \mathbb{K})/Z$, che pertanto opera fedelmente su Ω, si denota con $PGL(n, \mathbb{K})$ e, come già detto, si chiama il gruppo proiettivo generale di rango $n-1$ su $\mathbb{K}$; il sottogruppo determinato dall'immagine inversa di $SL(n, \mathbb{K})$ (cioè $G = SL(n, \mathbb{K})Z/Z$) si chiama gruppo *speciale proiettivo* e si denota con $PSL(n, \mathbb{K})$. A questo punto osserviamo finalmente che l'azione di $PSL(n, \mathbb{K})$ su Ω è 2-transitiva. Infatti se Ku, Kv sono elementi distinti di Ω allora u, v sono vettori di V linearmente indipendenti; se $\mathbb{K}u_1$ e $\mathbb{K}v_1$ sono due altri elementi distinti di Ω esiste allora una matrice $A \in GL(n, \mathbb{K})$ tale che $\mathbf{u}A = \mathbf{u_1}$ e $\mathbf{v}A = \mathbf{v_1}$. Sia $d = \det A$ e $B = dA$; allora $B \in SL(n, \mathbb{K})$ e $(\mathbb{K}u) \cdot B = \mathbb{K}u_1$, $(\mathbb{K}v) \cdot B = \mathbb{K}v_1$. □

Azioni primitive. Sia data un'azione del gruppo G sull'insieme Ω. Una partizione $\mathcal{F}$ di Ω si dice G-invariante se $X \cdot g = \{x \cdot g \mid x \in X\} \in \mathcal{F}$ per ogni $X \in \mathcal{F}$ e $g \in G$. Si osservi che ciò significa che l'azione di G su Ω induce un'azione di G su $\mathcal{F}$.

Fissata un'azione di G su Ω esistono sempre due partizioni che sono certamente G-invarianti, dette *partizioni banali*, che sono
- quella costituita dai sottoinsiemi con un singolo elemento: $\mathcal{F} = \{\{x\} \mid x \in \Omega\}$,
- quella costituita da tutto Ω: $\mathcal{F} = \{\Omega\}$.

Un'azione di G su Ω si dice *primitiva* se le sole partizioni G-invarianti sono quelle banali.

Poiché le orbite in Ω costituiscono chiaramente una partizione G-invariante, un'azione primitiva è transitiva (a meno che Ω non sia costituito da due soli elementi entrambi punti fissi per G). Un'azione si dice *imprimitiva* se non è primitiva. Osserviamo il seguente fatto:

Lemma 3.19. *Un'azione transitiva di G su Ω, con $|\Omega| \geq 2$, è imprimitiva se e soltanto se esiste $X \subseteq \Omega$ con $X \neq \Omega$ e $|X| \geq 2$, tale che, per ogni $g \in G$:*

$$X^g \neq X \;\Rightarrow\; X^g \cap X = \emptyset. \tag{3.12}$$

DIMOSTRAZIONE. Esercizio. ∎

Il seguente teorema raggruppa due fatti fondamentali riguardanti le azioni primitive.

Teorema 3.20. *Sia data un'azione transitiva del gruppo G sull'insieme Ω, con $|\Omega| > 2$.*

(1) *l'azione è primitiva se e soltanto se lo stabilizzatore di un punto è un sottogruppo massimale di G.*

(2) *se l'azione è 2-transitiva è anche primitiva.*

DIMOSTRAZIONE. (1) Data un'azione transitiva di G su Ω, sia $H = G_x$ lo stabilizzatore di un punto $x \in \Omega$. Poiché $|\Omega| \geq 2$, H è un sottogruppo proprio. Proviamo che l'azione è imprimitiva se e solo se H non è massimale.
Supponiamo che l'azione sia imprimitiva. Allora esiste $X \subseteq \Omega$ con $|X| \geq 2$ e $X \neq \Omega$ tale che (3.12) è soddisfatta per ogni $g \in G$. Per la transitività dell'azione possiamo assumere $x \in X$. Sia $K = G_X$ lo stabilizzatore globale di X (cioè $K = \{g \in G \mid X^g = X\}$). Se $h \in H$, allora $x \in X \cap X^h$ e dunque $X^h = X$; questo significa $H \leq K$. Sia $x \neq y \in X$ (esiste perché $|X| \geq 2$); per transitività esiste $g \in G$ tale che $y = x^g \in X \cap X^g$; ed allora, per la (3.12), $g \in K$, Siccome $g \notin H$ si conclude che H è propriamente contenuto in K. Assumiamo $K = G$, allora X contiene l'intera G-orbita di x e dunque, sempre per la transitività, $X = \Omega$, che non è. Quindi $H < K < G$, e H non è massimale.

Viceversa, supponiamo che H non sia massimale e sia $K \leq G$ tale che $H < K < G$. Poniamo $X = x^K$, la K-orbita di x. Poiché $H < K$, lo stabilizzatore in K di x è H, pertanto $|X| = |K : H| \geq 2$. Sia poi $g \in G \setminus K$; se $x^g \in X$ allora esiste $t \in K$ tale che $x^g = x^t$, da cui segue $gt^{-1} \in H < K$, che è assurdo. Dunque $x^g \notin X$ e $X \neq \Omega$. Mostriamo che X soddisfa (3.12). Sia $g \in G$ tale che $X^g \cap X \neq \emptyset$. Allora esistono $u, v \in K$ tali che $x^u = (x^v)^g x^{vg}$, da cui $vgu^{-1} \in H < K$ e di conseguenza $g \in K = G_X$, che significa $X^g = X$. Per il Lemma 3.19, si conclude che l'azione è imprimitiva.

(2) Supponiamo che l'azione di G su Ω sia 2-transitiva, e sia $X \subseteq \Omega$ con $|X| \geq 2$ che soddisfa la proprietà (3.12). Proviamo che $X = \Omega$ (segue allora dal Lemma 3.19 che l'azione è primitiva). Chiaramente, possiamo supporre $|\Omega| \geq 3$. Siano $x, y \in X$ con $x \neq y$ e sia $z \in \Omega$ con $x \neq z \neq y$. Per la 2-transitività, esiste $g \in G$ tale che $x^g = x$ e $y^g = z$. Allora $x \in X \cap X^g$; dunque, per (3.19), $X = X^g$ e quindi $z \in X^g = X$, il che dimostra che $X = \Omega$, e di conseguenza che l'azione è primitiva. ∎

Nel seguito di queste note, con "gruppo di permutazioni" intenderemo un sottogruppo di un gruppo simmetrico $Sym(\Omega)$ nella sua azione naturale sull'insieme Ω. O, in altri termini, un gruppo G assieme ad un'azione *fedele* di G su un insieme Ω. Osserviamo che in questo caso l'intersezione degli stabilizzatori degli elementi di Ω è il sottogruppo banale. Sempre in questo caso, attribuiremo al gruppo le proprietà dell'azione: diremo cioè che G è transitivo, primitivo, etc.

Sottogruppi normali regolari. Un gruppo di permutazioni G su Ω si dice *regolare* se è transitivo e lo stabilizzatore di un punto è il sottogruppo identico $\{1\}$. In questo caso, per 3.1, $|\Omega| = |G|$, e, per la Proposizione 3.14, l'azione di G su Ω è equivalente a quella per moltiplicazione a destra su se stesso (dunque, a meno di equivalenza, ogni gruppo ammette una ed una sola azione regolare).

Lemma 3.21. *Ogni gruppo di permutazioni abeliano e transitivo è regolare.*

DIMOSTRAZIONE. Sia A un gruppo permutazioni transitivo su Ω, allora gli stabilizzatori degli elementi di Ω sono tra loro coniugati; se inoltre A è abeliano, essi coincidono tra loro, dato che in un gruppo abeliano ogni sottogruppo è normale, e dunque - per la fedeltà dell'azione - coincidono con il sottogruppo identico. ∎

Lemma 3.22. *Siano G un gruppo di permutazioni transitivo su Ω, con $|\Omega| \geq 2$, e G_x, con $x \in \Omega$, lo stabilizzatore di un punto. Sia N un sottogruppo normale di G. Se N è regolare (su Ω) allora $G = N \rtimes G_x$, e l'azione per coniugio di H su $N \setminus \{1\}$ è equivalente all'azione di H su $\Omega \setminus \{x\}$.*

DIMOSTRAZIONE. Poiché N è per ipotesi regolare su Ω sia ha $N \cap G_x = N_x = 1$. Inoltre, per ogni $g \in G$, poiché N è transitivo, esiste $a \in N$ tale che $x^g = x^a$. Da cui $ga^{-1} \in G_x$ e quindi $g \in NG_x$, provando che $G = N \rtimes G_x$. L'ultima affermazione discende immediatamente dal Lemma 3.15. ∎

Teorema 3.23. *Sia G un gruppo finito di permutazioni n-transitivo su Ω, con $|\Omega| \geq 2$. Sia N un sottogruppo normale e regolare di G. Sia $H = G_x$, con $x \in \Omega$, lo stabilizzatore di un punto. Allora:*

(1) *se $n = 2$, N è un p-gruppo abeliano elementare;*

(2) *se $n = 3$, N è un 2-gruppo abeliano elementare, oppure $G = S_3$ e $N = A_3$ è ciclico di ordine 3;*

(3) *se $n = 4$, $G = S_4$ e N è il gruppo di Klein.*

DIMOSTRAZIONE. Sia $x \in \Omega$ e poniamo $H = G_x$; osserviamo che, poiché N è regolare, $N \cap H = 1$.

(1) Sia G 2-transitivo. Allora, per la Proposizione 3.16, H è transitivo su $\Omega \setminus \{x\}$, e dunque, per il Lemma 3.22, H opera transitivamente per coniugio su $N \setminus \{1\}$. Sia p un divisore primo di $|N|$; allora esiste $a \in N$ di ordine p, e per ogni $1 \neq b \in N$ esiste $h \in H$ tale che $b = a^h$. Ne segue che tutti gli elementi di $N \setminus \{1\}$ hanno ordine p. Per il teorema di Sylow N è un p-gruppo, e siccome non è banale il suo centro $Z = Z(N)$ non è banale (Proposizione 3.7). In particolare $H < ZH \leq G$. Poiché, per il Teorema 3.20, H è un sottogruppo massimale di G, si ha $ZH = G$, e per la legge di Dedekind, $Z = Z(H \cap N) = ZH \cap N = N$. Dunque $N = Z$ è abeliano elementare.

(2) Sia G 3-transitivo. N è un p-gruppo abeliano elementare per il punto (1). Se $|N| = \Omega| = 3$ allora - come si vede facilmente - $G = S_3$ e $N = A_3$. Supponiamo quindi $|N| \geq 4$. Allora esistono $x, y \in N \setminus \{1\}$ tali che $x \neq y \neq x^{-1}$. Ora, per la Proposizione 3.16, H opera per coniugio 2-transitivamente su N; se fosse $x \neq x^{-1}$, esisterebbe quindi $h \in H$ tale che $(x^{-1})^h = y$ e $x^h = x$, il che implica la contraddizione $y = (x^{-1})^h = (x^h)^{-1} = x^{-1}$. Dunque $x = x^{-1}$, da cui segue $|x| = 2$ e N è un 2-gruppo abeliano elementare.

(3) Sia G 4-transitivo. Sappiamo, per il punto (2), che N è un 2-gruppo abeliano elementare. Supponiamo per assurdo, $|N| = |\Omega| = 2^s > 5$. Esistono allora $x, y, z \in N \setminus \{1\}$ tali che $x \neq y$ e $z \neq x, y, xy$. Poiché, per la Proposizione 3.16, H opera per coniugio 3-transitivamente su

N, esiste $h \in H$ tale che $x^h = x,\ y^h = y$ e $(xy)^h = z$, da cui la contraddizione $xy = x^h y^h = (xy)^h = z$. Quindi $|N| = \Omega| = 4$, e allora - come si vede facilmente - $G = S_4$ e N è il gruppo di Klein. ∎

Lemma 3.24. *Sia G un gruppo di permutazioni primitivo su Ω, con $|\Omega| \geq 2$, e sia A un sottogruppo normale abeliano non-banale di G. Allora A è regolare.*

Dimostrazione. Sia A un sottogruppo normale non banale di un gruppo di permutazioni primitivo G su Ω, e sia $H = G_x$ lo stabilizzatore di un punto $x \in \Omega$. Ora $H \not\geq A$ perché altrimenti A, essendo normale, sarebbe contenuto in tutti i coniugati di H (che, dato che G transitivo sono gli stabilizzatori degli elemetni di Ω) e quindi nel nucleo dell'azione che è banale, contro l'ipotesi che A non lo sia. Dunque, $H < AH \leq G$;e quindi, poiché H è massimale per il Teorema 3.22, $AH = G$. Ora, $A \cap H \trianglelefteq H$, dato che $A \trianglelefteq G$ e $A \cap H \trianglelefteq A$ poiché A è abeliano. Pertanto $A \cap H \trianglelefteq AH = G$; quindi $A \cap H = 1$ per la stessa ragione per cui di sopra abbiamo escluso il caso $A \leq H$. Da ciò segue $|A| = \frac{|AH|}{|H||A \cap H|} = |AH : H| = |G : H| = |\Omega|$. Inoltre $A \cap H = A_x$ (lo stabilizzatore in A del punto x); quindi A è transitivo su Ω e dunque, per il Lemma 3.21, regolare. ∎

Da questo Lemma e dal Teorema 3.23 segue il seguente corollario.

Corollario 3.25. *Sia G un gruppo di permutazioni n-transitivo con $n \geq 4$. Se G ha un sottogruppo normale abeliano non banale, allora $n = 4$ e $G \simeq S_4$.*

3.4 Esempi (gruppi semplici)

Gruppi alterni. Iniziamo provando la semplicità di A_5.

Lemma 3.26. *Sia G un gruppo di ordine 60. Sono equivalenti:*

(i) *$n_5(G) \neq 1$;*

(ii) *G è semplice;*

(iii) *$G \simeq A_5$.*

Dimostrazione. Cominciamo provando che se H è un gruppo di ordine $5, 10, 15, 20, 30$ allora $n_5(H) = 1$.
I casi $|G| = 5, 10, 15, 20$ sono ovvi o conseguenze immediate del teorema di Sylow. Supponiamo quindi $|H| = 30$ e assumiamo, per assurdo, $n_5(H) \neq 1$; allora, per il teorema di Sylow, $n_5(H) = 6$. Ora, i 5-sottogruppi di Sylow di H sono ciclici di ordine 5, dunque hanno a due a due intersezione banale, ed ogni loro elemento non identico ha ordine 5; ne segue che il numero di elementi di ordine 5 di H è $4 \cdot n_5(H) = 4 \cdot 6 = 24$. Supponiamo inoltre, $n_3(H) = 10$; allora, lo stesso argomento porta a concludere che il numero di elementi di ordine 3 di H è $2 \cdot n_3(H) = 2 \cdot 10 = 20$; poiché $24 + 20 = 44 > 30 = |H|$ si ha un assurdo. Dunque $n_3(H) \neq 10$ e, per il Teorema di Sylow si ha $n_3(H) = 1$; e quindi H ha un unico 3-sottogruppo di Sylow T, che è normale. Ora $|H/T| = 10$ e quindi $n_5(H/T) = 1$, cioè H/T ha un 5-sottogruppo di Sylow normale C/T. Ma allora $C \trianglelefteq H$ e $|C| = 15$; dunque C contiene tutti i 5-sottogruppi di Sylow di G, il che è assurdo.

$(i) \Rightarrow (ii)$. Sia G un gruppo di ordine 60 e supponiamo che G non sia semplice. Sia $N \neq 1$ un sottogruppo normale proprio di G. Se 5 divide $|N|$ allora, poiché $N \trianglelefteq G$, N contiene tutti i 5-sottogruppi di Sylow di G, cioè $n_5(G) = n_5(N)$; per quanto provato sopra $n_5(N) = 1$. Se 5 non divide $|N|$ allora divide $|G/N$, dunque, ancora per quanto provato prima $n_5(G/N) = 1$. Sia C/N l'unico 5-sottogruppo di Sylow di G/N; allora, $C \trianglelefteq G$ e $n_5(C) = n_5(G)$. Se $C < G$, per quanto visto sopra, si conclude $n_5(G) = 1$.
Rimane il caso $C = G$, cioè $|N| = |G|/5 = 12$. Sia $T \in Syl_3(N)$; per l'argomento di Frattini, $G = N\mathcal{N}_G(T)$, da cui, per considerazioni sull'ordine, si deduce che 5 divide $|\mathcal{N}_G(T)|$, il che significa che $\mathcal{N}_G(T)$ contiene 5-sottogruppo di Sylow P di G; dunque P normalizza T e quindi $H = TP$ è un sottogruppo di ordine 15 di G. Ora, gruppi di ordine 15 sono abeliani (segue dall'Esempio 3.3, o da quanto provato all'inizio della dimostrazione), in particolare, dunque, $P \trianglelefteq H$, ovvero $H \leq \mathcal{N}_G(P)$. Da ciò segue $n_5(G) = |G : \mathcal{N}_G(P)| \leq |G : H| = 4$, e dunque, per il Teorema di Sylow, $n_5(G) = 1$.

$(ii) \Rightarrow (iii)$. Sia G un gruppo semplice di ordine 60. Sia $Q \in Syl_2(G)$; allora $|Q| = 4$ e $|G : Q| = 15$. Sia $Q \leq H \leq G$, con $H \neq Q$; poiché $|G : H|$ divide $|G : Q| = 15$, si ha $|G : H| \in \{1, 3, 5\}$. Se $|G : H| = 3$, l'azione di G sulle classi laterali modulo H definisce un omomorfismo non banale $G \to S_3$, il cui nucleo è un sottogruppo normale $\neq 1$, contraddicendo la semplicità di G. Se $|G : H| = 5$ allora, allo stesso modo, esiste un omomorfismo non banale $\phi : G \to S_5$; poiché G è semplice tale omomorfismo è iniettivo quindi $\phi(G) \simeq G$ è semplice e dunque $\phi(G) \cap A_5 = \phi(G)$; in conclusione $G \simeq \phi(G) = A_5$.

Rimane il caso in cui se $Q \leq H \leq G$ e $H \neq Q$ allora $H = G$ (cioè il caso in cui Q è sottogruppo massimale). Allora in particolare, poiché $Q \leq \mathcal{N}_G(Q)$ e $Q \not\trianglelefteq G$, si ha $Q = \mathcal{N}_G(Q)$ e dunque $n_2(G) = |G : \mathcal{N}_G(Q)| = 15$. Sia Q_1 un altro 2-sottogruppo di Sylow di G con $Q_1 \neq Q$ e supponiamo, per assurdo, che $Y = Q \cap Q_1 \neq 1$. Allora $|Y| = 2$ e poch'e Q e Q_1 sono abeliani, $Q \cup Q_1 \subseteq C_G(Y) \leq G$ e dunque $C_G(Y) = G$; in particolare $Y \trianglelefteq G$ che è una contraddizione. Dunque $Q \cap Q_1 = 1$ per ogni coppia di 2-sottogruppi di Sylow distinti Q e Q_1. Ne segue che, posto $\mathcal{U}_2$ l'unione di tutti i 2-sottogruppi di Sylow di G, si ha $|\mathcal{U}_2| = 15 \cdot 3 + 1 = 46$. Poiché il numero di elementi di ordine 5 di G è (come già visto) $4 \cdot n_5(G)$, deve risultare $4 \cdot n_5(G) \leq |G| - |\mathcal{U}_2| = 60 - 46 = 14$. e dunque $n_5(G) = 1$; ma allora esiste un unico 5-sottogruppo di Sylow di G, contro la semplicità.

$(iii) \Rightarrow (i)$. Questo è chiaro: infatti, come si può verificare direttamente, $n_5(A_5) = 6$ ∎

Veniamo alla dimostrazione della semplicità dei gruppi alterni di grado almeno 5.

Teorema 3.27. *Per ogni $n \geq 5$ il gruppo alterno A_n è semplice.*

Dimostrazione. Procediamo per induzione su n. Il caso $n = 5$ è stato provato col Lemma 3.26; supponiamo quindi $n \geq 6$ e consideriamo $G = A_n$ nella sua azione naturale su $I_n = \{1, \ldots, n\}$. Sia H lo stabilizzatore di un punto (ad esempio $H = G_1$); osserviamo che - poihcé $G + A_n$ è primitivo su I_n (Lemma 3.18 e Teorema 3.22) H è un sottogruppo massimale di G; inoltre $H \simeq A_{n-1}$ è semplice per ipotesi induttiva.
Sia $N \trianglelefteq G$; allora $N \cap H \trianglelefteq H$ e dunque $N \cap H = 1$ o $N \cap H = H$. Nel secondo caso, poiché H non è normale, $H < N$ e dunque, poiché H è massimale, $N = G$. Supponiamo dunque $N \cap H = 1$ e assumiamo, per assurdo, $N \neq 1$. Allora $H < NH \leq G$ e quindi $G = NH$. Poiché $N \cap H = 1$, segue che $|N| = n$ e N opera regolarmente su I_n. Poiché G è $(n - 2)$

transitivo, con $n \geq 6$, dal Teorema 3.23 segue $G \simeq S_4$, una contraddizione. Questo prova che $N = 1$ oppure $N = G$, e dunque che G è semplice. ∎

Gruppi speciali proiettivi. Sia $\mathbb{F}$ un campo, $n \geq 2$, e $1 \leq i, j \leq n$; denotiamo con e_{ij} la matrice in $M_n(\mathbb{F})$ i cui elementi sono tutti zero tranne quello al posto (i, j) che è $1_{\mathbb{F}}$. Una matrice del tipo

$$t_{ij}(b) = 1 + be_{ij}$$

con $b \in \mathbb{F}^*$, $i \neq j$ (con 1 si intende la matrice identica I_n), si chiama matrice elementare, o *trasvezione*. È chiaro che ogni trasvezione ha determinante 1 e quindi appartiene a $SL(n, \mathbb{F})$. Tenendo conto che $e_{ij}e_{rs} = \delta_{jr}e_{is}$ (δ_{jr} è il simbolo di Kronecker), si osservano la seguenti regole per la composizione di trasvezioni

$$\begin{aligned} &t_{ij}(a)^{-1} = t_{ij}(-a) \\ &t_{ij}(a)t_{rs}(b) = 1 + ae_{ij} + be_{rs} + \delta_{jr}abe_{is}. \end{aligned} \tag{3.13}$$

Usando le tecniche di riduzione di una matrice in forma diagonale (moltiplicare a destra o a sinistra una matrice A per una trasvezione sottopone A a quelle che si chiamano trasformazioni elementari, sulle righe o sulle colonne), si dimostra il seguente fatto,

Lemma 3.28. *Per $n > 1$, $SL(n, \mathbb{F})$ è generato dalle sue trasvezioni.*

Un gruppo G si dice *perfetto* se coincide con il suo derivato, cioè se $G = G'$.

Lemma 3.29. *Per $n \geq 2$, tranne i casi $n = 2$ e $|\mathbb{F}| = 2, 3$, $SL(n, \mathbb{F})$ è un gruppo perfetto.*

Dimostrazione. Per il lemma 3.28 è sufficiente provare che ogni trasvezione è prodotto di commutatori in $SL(n, \mathbb{F})$.
Sia $n \geq 3$ e $1 \leq i, j \leq n$ con $i \neq j$; allora esiste $1 \leq k \leq n$ con $i \neq k \neq j$. Dalle formule (3.13) si ricava, per ogni $0 \neq a \in \mathbb{F}$,

$$[t_{ik}(a), t_{kj}(1)] = t_{ik}(-a)t_{kj}(-1)t_{ik}(a)t_{kj}(-1) = t_{ij}(a).$$

sia $n = 2$ e $|\mathbb{F}| > 3$. Allora esiste $0 \neq b \in \mathbb{F}$ con $b^2 \neq 1$. Dato $a \in \mathbb{F}$, sia $c = a(b^2 - 1)^{-1}$; allora

$$\left[\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c(b^2-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

quindi $t_{12}(a) \in SL(2, \mathbb{F})'$; similmente si verifica $t_{21}(a) \in SL(2, \mathbb{F})'$, e la dimostazione è completa. ∎

Teorema 3.30. *Per ogni campo $\mathbb{F}$, se $n > 2$ oppure $n = 2$ e $|\mathbb{F}| > 3$, allora il gruppo $PSL(n, \mathbb{F})$ è semplice.*

Proviamo il caso $n = 2$, lasciando quello generale, con gli argomenti preparatori, agli esercizi (esercizi 3.23, 3.24, 3.25 e 3.26). Quindi

Teorema 3.31. *Tranne nei casi $|\mathbb{F}| = 2, 3$, $PSL(2, \mathbb{F})$ è un gruppo semplice.*

DIMOSTRAZIONE. Sia $|\mathbb{F}| \geq 4$ e $G = PSL(2,\mathbb{F})$. Sappiamo (esempio 3.7) che l'azione naturale di $SL(2,\mathbb{F})$ sullo spazio vettoriale $V = \mathbb{F}^2$ induce un'azione fedele e 2-transitiva di G sulla retta proiettiva $\mathbb{P}(1,\mathbb{F}) = \{\mathbb{F}v \mid 0 \neq v \in V\}$. In tale azione, lo stabilizzatore H del punto $\mathbb{F}(0,1)$ è l'insieme (modulo il centro $Z = Z(G)$ delle matrici

$$\begin{pmatrix} a^{-1} & b \\ 0 & a \end{pmatrix}$$

con $a \in \mathbb{F}^*$ e $b \in \mathbb{F}$; ovvero $H = (T(2,\mathbb{F}) \cap SL(2,\mathbb{F}))/Z$. Abbiamo osservato in precedenza che $T(2,\mathbb{F})$ è risolubile; di conseguenza, anche H è risolubile. Sia $1 \neq N \trianglelefteq G$; poiché l'azione di G su $\mathbb{P}(1,\mathbb{F})$ è fedele $N \not\leq H$ e dunque $H < NH \leq G$. Ma, per il teorema 3.20, H è un sottogruppo massimale di G, e dunque $NH = G$. In particolare, passando alle controimmagini modulo Z, $NH = SL(2,\mathbb{F})$. Poiché H è risolubile, $|G/N = HN/N \simeq H/H \cap N$ è risolubile; per contro, G è perfetto e dunque ogni suo quoziente è tale ($(G/N)' = G'N/N = G/N$). Quindi, $HN = N$, ovvero $H \leq N$ e dunque, poiché H è massimale e non è normale $N = G$. Questo prova che G è semplice. ∎

Osserviamo che $|PSL(2,4)| = |PSL(2,5)| = 60 = |A_5|$; quindi, per il Lemma 3.26,

$$PSL(2,4) \simeq A_5 \simeq PSL(2,5).$$

Ancora, $|PSL(2,7)| = 168 = |PSL(3,2)|$ (si osservi che $PSL(3,2) = GL(3,2)$) e anche in questo caso si dimostra che $PSL(2,7) \simeq PSL(3,2)$.
Si prova inoltre che $PSL(2,9) \simeq A_6$. Oltre a quelli appena citati, non ci sono altri casi di isomorfismo tra gruppi semplici del tipo PSL e alterno. Il più piccolo ordine per il quale esistono due gruppi semplici non isomorfi è $20.160 = \frac{8!}{2}$: infatti, A_8 e $PSL(3,4)$ sono gruppi semplici di ordine 20.160 che non sono isomorfi (vedi esercizio 3.27).

3.5 Prodotti intrecciati

Date azioni di permutazione dei gruppi H, K sugli insiemi Δ, Ω rispettivamente, non è difficile immaginare come definire un'azione del gruppo prodotto diretto $H \times K$ sull'insieme $\Delta \times \Omega$; basta operare "per componenti"

$$(x,y)^{(h,k)} = (x^h, y^k)$$

per ogni $(x,y) \in \Delta \times \Omega$ e $(h,k) \in H \times K$. Ed è immediato verificare che tale azione è fedele (transitiva) se e solo se le azioni di H su Δ e di K su Ω sono fedeli (transitive). Questa azione prodotto è utile in molti casi, ma non è la maniera più efficace di introdurre - a partire da due gruppi di permutazioni sugli insiemi Δ e Ω - un gruppo un gruppo di permutazioni su $\Delta \times \Omega$. La maniera più interessante è quella del *prodotto intrecciato*, che definiamo qui di seguito.

Prodotto intrecciato permutazionale. Siano H, K gruppi di permutazioni non banali sugli insiemi Δ, Ω rispettivamente. Sia

$$B = \{f \mid f : \Omega \to H,\ supp(f) \text{ finito}\}$$

(ricordo che in questo caso - vedi sezione 1.6 - $supp(f)$ è l'insieme degli elementi $x \in \Omega$ tali che $f(x) \neq 1_H$). B è un gruppo rispetto all'operazione naturale

$$(ff_1)(x) = f(x)f_1(x),$$

per ogni $f, f_1 \in B$ e $x \in \Omega$; come gruppo, B è isomorfo al prodotto diretto di copie del gruppo H indicizzate sull'insieme Ω. Ora, K opera su B nel modo seguente

$$f^g(x) = f(x^{g^{-1}}) \tag{3.14}$$

per ogni $f \in B$, $g \in G$ e $x \in \Omega$. La verifica che si tratta di un'azione è lasciata al lettore; di più, ogni $g \in K$ agisce come un automorfismo di B; infatti, per ogni $x \in \Omega$,

$$(ff_1)^g(x) = (ff_1)(x^{g^{-1}}) = f(x^{g^{-1}})f_1(x^{g^{-1}}) = f^g(x)f_1^g(x) = f^g f_1^g(x)$$

e dunque $(ff_1)^g = f^g f_1^g$, per ogni $f, f_1 \in B$. Questo definisce un'omomorfismo iniettivo

$$\phi : K \to Aut(B)$$

(che ϕ sia initettivo segue dalla definizione dell'azione (3.14) e dal fatto che K è un gruppo di permutazioni di Ω e $H \neq 1$. Sia

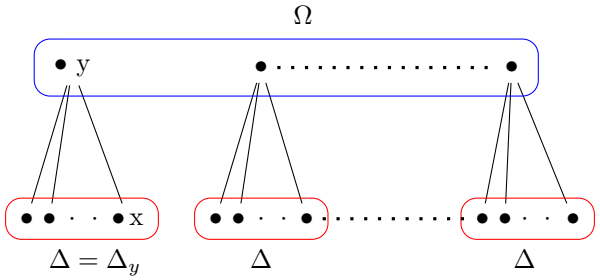
$$W = B \rtimes_\phi K$$

il prodotto semidiretto definito da tale omomorfismo; e denotiamo i suoi elementi come fg dove $f \in B$ e $g \in K$ (ricordo che allora la scrittura di ogni elemento di W è unica, e che la regola di moltiplicazione è: $fg \cdot f_1 g_1 = ff_1^{g^{-1}} gg_1$).
Definiamo ora un'azione di W su $\Delta \times \Omega$ ponendo, per ogni $(x, y) \in \Delta \times \Omega$, $f \in B$, $g \in K$,

$$(x, y)^{fg} = (x^{f(y)}, y^g). \tag{3.15}$$

Il *prodotto intrecciato permutazionale* $H \wr K$ dei gruppi (di permutazioni) H e K è il gruppo W come gruppo di permutazioni di $\Delta \times \Omega$. IN particolare, nel caso finito, si avrà che se $H \leq S_n$ e $K \leq S_m$, allora $H \wr K \leq S_{nm}$.

Promemoria visuale e imprimitività. Per comprendere l'azione del prodotto $H \wr K$ appena definita, è conveniente vedere l'insieme $\Delta \times \Omega$ come l'unione disgiunta degli insiemi $\Delta_y = \Delta \times \{y\}$, al variare di $y \in \Omega$. La cosa si può visualizzare con un diagramma come quello seguente.



Se $f \in B$ è un elemento della base di $W = H \wr K$, f fissa tutti gli insiemi Δ_y ed agisce su ciascun Δ_y come l'elemento $f(y) \in H$ agisce su Δ; mentre gli elementi $g \in K \leq W$ agiscono permutando i sottoinsiemi Δ_y ($y \in \Omega$), al modo in cui y permuta Ω, cioè $\Delta_y^g = \Delta_{y^g}$. In particolare, quindi, $\{\Delta_y \mid y \in \Omega\}$ è una partizione W-invariante di $\Delta \times \Omega$, e l'azione del prodotto intrecciato non è primitiva. 'E anche utile osservare come a W si possa associare in modo immediato un gruppo di automorfismi delll'insieme parzialmente ordinato descritto dal diagramma di sopra.

Viceversa, sia data un'azione transitiva e non primitiva di un gruppo G su un insieme X, e sia Ω una partizione non banale G-invariante di X. Denotiamo con N il nucleo dell'azione di G su Ω e poniamo $K = G/N$ (dunque K opera fedelmente su Ω); quindi, fissato $\Delta \in \Omega$, poniamo $H = G_\Delta$ (lo stabilizzatore in G di Δ), che consideriamo nella sua azione su Δ (osserviamo che $H \geq N$). Dalla transitività di G su X segue la transitività di K su Ω e quella di H su Δ; osserviamo anche che Δ è una H-orbita in X. In particolare, quindi, l'azione di K su Ω è equivalente a quella di K sulle classi laterali modulo H/N (che è lo stabilizzatore di Δ in K). Dunque, se T è un trasversale di $H \in G$, Ω risulta l'insieme dei Δ^g, e X l'unione disgiunta dei Δ^g ($g \in T$). Possiamo perciò identificare X con $\Omega \times T$, che come G-insieme è equivalente a $\Delta \times \Omega$, e - con un po' di lavoro supplementare - concludere che G è isomorfo (come gruppo di permutazioni) ad un sottogruppo del prodotto intrecciato $H \wr K$ nella sua azione su $\Delta \times \Omega$.

Struttura astratta e ordine. Prima di vedere un'interessante applicazione, soffermiamoci sulla struttura astratta di un prodotto intrecciato. Con le notazioni di sopra, sia $G = H \wr K$. Con le identificazioni solite $G = BK$ dove il sottogruppo normale B è detto *base* del prodotto intrecciato e K un complemento. Come detto, B è isomorfo al prodotto diretto di $|\Omega|$ copie di H. Precisamente, per ogni $x \in \Omega$, sia

$$H_x = \{f \in H^\Omega \mid f(y) = 1 \text{ per ogni } x \neq y \in \Omega\};$$

allora $H_x \trianglelefteq B$ e $B = Dir_{x\in\Omega} H_x$; chiaramente poi $H_x \simeq H$. Per $g \in K$, l'azione di g - per coniugio - su B è definita permutando i sottogruppi H_x allo stesso modo in cui g permuta gli elementi di Ω (più esattamente, si ha $H_x^g = H_{x^{g^{-1}}}$ per ogni $x \in \Omega$).
Quanto all'ordine di un prodotto intrecciato nel caso finito, si ha chiaramente:

$$|H \wr K| = |H|^{|\Omega|}|K|. \tag{3.16}$$

Sottogruppi di Sylow dei gruppi simmetrici. Applicheremo ora la costruzione del prodotto intrecciato per descrivere i sottogruppi di Sylow dei gruppi simmetrici S_n. Per prima cosa, vogliamo trovare l'ordine di tali sottogruppi.

Sia $n \geq 1$ un intero positivo, e p un numero primo. Denotiamo con $r_p(n)$ il massimo intero s (maggiore o uguale a zero) tale che p^s divide n. Ovvero $p^{r_p(n)}|n$ e $p^{r_p(n)+1} \not| n$ Dalla definizione si ha subito le seguente ovvia osservazione:

$$\forall n, m, \geq 1 : \quad r_p(nm) = r_p(n) + r_p(m). \tag{3.17}$$

Meno evidente, ma importante, è la formula seguente.

Lemma 3.32. *Sia $n \geq 1$, e sia p un numero primo. Allora*

$$r_p(n!) = \sum_{i \geq 1} \left[\frac{n}{p^i} \right] = \sum_{i=1}^{[\log_p n]} \left[\frac{n}{p^i} \right].$$

DIMOSTRAZIONE. Siano $n \geq 1$ e p un numero primo. Sia $I = \{1, 2, \ldots, n\}$ ed $E = \{1, 2, \ldots, [\log_p n]\}$ (l'insieme dei numeri compresi tra 1 e $[\log_p n]$). Consideriamo l'insieme delle coppie,

$$S = \{(i, m) \in E \times I | p^i \text{ divide } m\}.$$

Sia $i \in E$; allora il numero di elementi di S che hanno i come prima componente è uguale al numero di interi minori o uguali ad n che sono multipli di p^i, cioè $[n/p^i]$. Dunque, sommando per ogni $i \in I$ il numero di coppie di cui essa è la prima componente,

$$|S| = \sum_{i=1}^{[\log_p n]} \left[\frac{n}{p^i} \right] .$$

Viceversa, fissato un $m \in I$, il numero di elementi di S che hanno m come seconda componente è il numero di potenze di p che dividono m, cioè $r_p(m)$; quindi, tenendo conto di (3.14)

$$|S| = \sum_{m=1}^{n} r_p(m) = r_p \left(\prod_{m=1}^{n} m \right) = r_p(n!)$$

Da cui l'enunciato. ∎

Lemma 3.33. *Siano $n \geq 1$ e p un numero primo ($p \leq n$). Sia $P \in Syl_P(S_n)$; allora $|P| = p^{r_p(n!)}$, dove $r_p(n!)$ è dato dalla formula del Lemma 3.32; in particolare, se $n = p^m$ (con $m \geq 1$), si ha*

$$|P| = p^{\frac{p^m - 1}{p-1}}.$$

DIMOSTRAZIONE. Segue ovviamente dal lemma 3.32, osservando, per quanto riguarda l'ultima affermazione, che se $n = p^m$ allora $[n/p^i] = p^{m-i}$ per ogni $1 \leq i \leq m$: quindi $r_p(p^m) = p^{m-1} + \cdots + p + 1 = \frac{p^m - 1}{p-1}$. ∎

Per descrivere i p-sottogruppi di Sylow dei un gruppi simmetrici S_n, iniziamo col definire induttivamente la seguente famiglia di gruppi di permutazioni. Il primo p è fissato.

- Si pone $W_1 = C_p$ il gruppo ciclico di ordine p nella sua azione regolare su $\Omega = C_p$: quindi $C_p \leq S_p$;
- $W_2 = W_1 \wr C_p = C_p \wr C_p$, come sottogruppo di S_{p^2}.
- avendo definito W_n come sottogruppo di S_{p^n} si pone $W_{n+1} = W_n \wr C_p$ che è quindi un sottogruppo di $S_{p^n p} = S_{p^{n+1}}$.

In sostanza, W_n è il prodotto intrecciato (permutazionale) iterato $((C_p \wr C_p) \wr \dots) \wr C_p$ dove il gruppo ciclico C_p, nella sua rappresentazione regolare, appare n volte. L'ordine dei gruppi W_n si determina facilmente; si ha, per ogni $n \geq 1$:

$$|W_n| = p^{\frac{p^m-1}{p-1}} \tag{3.18}$$

Tale uguaglianza sussiste, infatti, per $n = 1$, e supposta valida per $n \geq 1$, per come è definito W_{n+1}, si ricava dalla (3.16):

$$|W_{n+1}| = |W_n|^p p = \left(p^{\frac{p^n-1}{p-1}}\right)^p p = p^{\frac{p^{n+1}-p}{p-1}+1} = p^{\frac{p^{n+1}-1}{p-1}}$$

Ora, per costruzione, per ogni $n \geq 1$, $W_n \leq S_{p^n}$; quindi, per il Teorema di Sylow, $W_n \leq P$ per qualche $P \in Sylow_p(S_{p^n})$. Ma, dal Lemma 3.33 e l'uguaglianza (3.18) segue $|P| = |W_n|$, e dunque $P = W_n$. Abbiamo così dimostrato il seguente:

Teorema 3.34. *Siano p un primo e $n \geq 1$. Allora i p-sottogruppi di Sylow di S_{p^n} sono isomorfi (come gruppi di permutazioni) a W_n.*

Per enunciare il caso generale, la cui dimostrazione lasciamo - se lo vuole - alla lettrice, fissiamo la seguente convenzione: se G è un gruppo e $n \geq 1$, denotiamo cono G^n il prodotto diretto di n copie di G; poniamo inoltre $G^0 = \{1\}$.

Teorema 3.35. *Siano p un primo e $n \geq 2$. Sia $n = a_0 + a_1 p + \dots + a_m p^m$ la rappresentazione di n in base p (quindi $m = [\log_p n]$, $0 \leq a_i \leq p-1$ e $a_m \neq 0$). Sia $P \in Syl_p(S_n)$; allora*

$$P \simeq W_1^{a_1} \times \dots \times W_m^{a_m}.$$

Prodotto intrecciato standard. La costruzione del prodotto intrecciato è molto utilizzata anche al di fuori della teoria dei gruppi di permutazioni. Ed in genere, quando si parla di prodotto intrecciato di due gruppii, si intende il prodotto standard che ora definiremo - che è un caso particolare di prodotto intrecciato permutazionale.
Siano dunque H e K due gruppi. Il *prodotto intrecciato standard* $HwrK$ è il prodotto costruito come nel caso permutazionale quando K è inteso nella sua rappresentazione regolare su se stesso per moltiplicazione a destra. La base del prodotto intrecciato è quindi il gruppo B, insieme delle applicazioni a supporto finito da $K \to H$; l'azione di K su B è la seguente: per ogni $f \in B$, $g \in K$, f^g è definita da

$$f^g(x) = f(xg^{-1}) \text{ per ogni } x \in K. \tag{3.19}$$

Ciò definisce un omomorfismo (evidentemente iniettivo) $\phi : K \to Aut(K)$. Il prodotto intrecciato standard è quindi il prodotto semidiretto

$$HwrK = B \rtimes_\phi K.$$

Gli elementi di $HwrK$ si possono perciò scrivere i modo unico nella forma fx con $f \in B$, $x \in K$ (una volta fatte le abituali identificazioni per prodotti semidiretti), e la regola di moltiplicazione è: $(fx)(f_1 x_1) = f f_1^{x^{-1}} x x_1$, dove, per ogni $y \in K$, $f^{x^{-1}}(y) = f(yx)$.

Un caso relativamente semplice ma che ha particolare importanza anche nelle applicazioni è il cosiddetto gruppo del lampionaio (*Lamplighter group*), che è definito come il prodotto intrecciato standard

$$(\mathbb{Z}/2\mathbb{Z})wr\mathbb{Z},$$

dove $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ è il gruppo ciclico di ordine 2 e $\mathbb{Z}$ il gruppo additivo degli interi (ciclico infinito).

3.6 Esercizi III

Sezione 3.1

Esercizio 3.1. Data una azione del gruppo G su S, siano $s \in S$, $g \in G$ e $t = g \cdot s$. Si provi che $G_s = (G_t)^g$.

Esercizio 3.2. (1) Sia A un gruppo abeliano, e sia data un'azione fedele di A su un insieme Ω. Si provi che se tale azione è transitiva allora $A_x = \{1_G\}$ per ogni $x \in \Omega$; si concluda che $|A| = |\Omega|$.
(2) Sia data un'azione fedele del gruppo G su Ω e sia A un sottogruppo abeliano di G. Si supponga inoltre che la restrizione ad A dell'azione di G su Ω sia transitiva. Si provi che, per ogni $x \in \Omega$, $G = AG_x$ e $A \cap G_x = 1$.

Esercizio 3.3. Determinare un sottogruppo del gruppo simmetrico S_8 isomorfo al gruppo Q_8 dei quaternioni di ordine 8. Provare che 8 è il più piccolo intero positivo n tale che S_n contiene un sottogruppo isomorfo a Q_8.

Esercizio 3.4. Si provi che $PGL(2,3) = GL(2,3)/Z$ è isomorfo a S_4 [sugg. si consideri l'azione naturale di $GL(2,3)$ sull'insieme dei sottospazi unidimensionali di $GF(3)^2$].

Esercizio 3.5. Sia G un gruppo finito e ϕ un automorfismo di G il cui ordine è un numero primo p. Sia $N \trianglelefteq G$ un sottogruppo normale e ϕ-invariante di G. Allora ϕ induce un automorfismo $Nx \mapsto Nx^\phi$ di G/N. Si assuma ora $(|N|, p) = 1$ e sia $x \in G$; si provi che se $(Nx)^\phi = Nx$, allora $Nx \cap C_G(\phi) \neq 1$ (quindi esiste $a \in G$ con $a^\phi = a$ e $Nx = Na$). [sugg.: si consideri l'azione di $\langle\phi\rangle$ su $\Omega = Nx$]

Esercizio 3.6. Si provi che il numero di classi di coniugio di un gruppo finito G è

$$\frac{1}{|G|}\sum_{x\in G}|C_G(x)|$$

Esercizio 3.7. Sia G un gruppo finito, e sia p il minimo numero primo che divide $|G|$. Si provi che se $H \leq G$ e $[G : H] = p$, allora $H \trianglelefteq G$.

Sezione 3.2

Esercizio 3.8. Sia p un primo, e sia P un p-sottogruppo di Sylow del gruppo finito G. Si provi che per ogni $\mathcal{N}_G(P) \leq H \leq G$, si ha $\mathcal{N}_G(H) = H$.

Esercizio 3.9. Siano p, q, r numeri primi (distinti). Si provi che un gruppo di ordine pqr non è semplice.

Esercizio 3.10. Siano p un numero primo dispari, $2 \leq m \in \mathbb{N}$, e G un gruppo di ordine $2(p+1)p^m$; si provi che G non è semplice.

Esercizio 3.11. Siano p, q numeri primi distinti, con $p > q$. Sia G un gruppo di ordine p^2q^2, e P è un p-sottogruppo di Syolw di G. Si provi che $P \trianglelefteq G$ oppure $p = 3$ e $|Z(G)| = 3$.

Esercizio 3.12. Sia G un gruppo di ordine 72; si provi che $O_3(G) \neq 1$.

Esercizio 3.13. Sia G un gruppo finito con $|G| \leq 100$ e $|G|$ è multiplo 5. Si provi che se $O_5(G) \neq 1$ allora $|G| \in \{55, 60, 80\}$. Si provi che se inoltre G è semplice, allora $|G| = 60$.

Esercizio 3.14. Siano G un gruppo finito e p un primo. Sia $H \leq G$ tale che $|G : H|$ è una potenza di p; si provi che $O_p(H) \leq O_p(G)$.

Sezione 3.3

Esercizio 3.15. Sia G un gruppo di permutazioni transitivo su Ω. Sia $N \trianglelefteq G$ e sia $\Delta = \{x^N \mid x \in \Omega\}$ l'insieme delle orbite di N. Si provi che G opera transitivamente su Δ. Si concluda che tutte le N-orbite su Ω hanno la stessa lunghezza.

Esercizio 3.16. Sia q la potenza di un numero primo. Si provi che il gruppo $G = A\Gamma(q)$ (vedi sezione 2.5), nella sua azione su $GF(q)$ (esplicitamente descritta nell'esercizio 2.35) è 2-transitiva, ed è 3-transitiva se e solo se $q = 3, 4$ (nei quali casi G è rispettivamente S_3 e S_4). Sim provi che, in ogni caso, se H è lo stabilizzatore di due punti allora le orbite di H sull'insieme dei rimanenti punti hanno tutte la stessa lunghezza.

Esercizio 3.17. Sia $G = GL(3, 2)$ il gruppo delle matrici invertibili di ordine 3 su un campo con due elementi. Si provi che esiste un omomorfismo iniettivo $G \to S_7$. Si provi che G è semplice.

Esercizio 3.18. Sia G un gruppo finito e p un numero primo che divide $|G|$. Si provi che

$$|\{g \in G \mid g^p = 1\}| \equiv 0 \pmod{p}.$$

[sugg. posto S un p-sottogruppo di G che sia massimale per essere abeliano elementare (vedi sezione 1.7) si consideri l'azione di coniugio di S sull'insieme $\{g \in G \mid g^p = 1\} \ldots$]

Esercizio 3.19. Sia G un gruppo di permutazioni primitivo e non regolare su Ω con $|\Omega| \geq 2$ Si provi che per ogni $x, y \in \Omega$, se $x \neq y$ allora $G_x \neq G_y$.

Esercizio 3.20. Sia p un primo e G un p-gruppo finito di permutazioni primitivo su un insieme Ω. Si provi che $|\Omega| = p = |P|$.

Esercizio 3.21. Sia G un gruppo di permutazioni primitivo su Ω, con $|\Omega| = n \geq 2$, e sia $x \in \Omega$. Supponiamo inoltre che G_x sia abeliano. Si provi che $|G_x| | n - 1$. Nel caso in cui $n = p^m$ sia la potenza di un numero primo, si provi che $G = PG_x$, dove $P \in Syl_p(G)$, $P \trianglelefteq G$ e P è abeliano elementare.

Sezione 3.4

Esercizio 3.22. Si dimostri che, a meno di isomorfismo, il solo gruppo semplice non abeliano di ordine ≤ 120 è A_5.

Esercizio 3.23. Sia $n \geq 3$, $\mathbb{F}$ un campo e $n \geq 3$. Si provi che due trasvezioni di G sono coniugate in G; in particolare, se $t = t_{ij}(a)$ è una trasvezione, $\langle t \rangle^G = G$ [sugg. guardare alla dimostrazione (nel caso $n \geq 3$) del Lemma 3.29].

Esercizio 3.24. Sia $G = SL(n, \mathbb{F})$, con $n \geq 2$. Si provi che il sottogruppo A generato da

$$\{t_{ni}(a) \mid 1 \leq i \leq n-1,\ a \in \mathbb{F}\}$$

è un sottogruppo abeliano dello stabilizzatore H (in G) del vettore $\mathbf{e}_n = (0, \ldots, 0, 1)$. Si provi quindi che $A \trianglelefteq H$ [sugg. per la seconda parte si descriva un omomorfismo ϕ da H in $GL(n-1, \mathbb{F})$ tale che $A = \ker \phi$].

Esercizio 3.25. (Iwasawa) Sia G un gruppo di permutazioni primitivo, sia H lo stabilizzatore di un punto e A un sottogruppo abeliano di H. Supponiamo che

1. G è perfetto (cioè $G = G'$)
2. $A \trianglelefteq H$
3. $A^G = G$.

Allora G è semplice [sugg. Sia $1 \neq N \trianglelefteq G$ e si assuma per assurdo $N \neq G$, allora (primitività) $NH = G$; dalle assunzioni 1 e 2 segue $NA = G$ e dalla 3 si conclude].

Esercizio 3.26. Utilizzando gli esercizi precedenti, si dimostri il Teorema 3.30.

Esercizio 3.27. Si mostri che lo spazio proiettivo $\mathbb{P}(3, 4)$ contiene 21 punti. Si provi che un elemento di ordine 5 in $SL(3, 4)$ stabilizza uno ed un solo punto di $\mathbb{P}(3, 4)$; si provi quindi che $PSL(3, 4)$ non contiene elementi di ordine 15. Si deduca che $PSL(3, 4) \not\simeq A_8$.

Sezione 3.5

Esercizio 3.28. Si provi che $C_2 \wr C_2$ è isomorfo al gruppo diedrale D_8.

Esercizio 3.29. Si dimostri il Teorema 3.35.

Esercizio 3.30. Siano H, K gruppi di permutazioni sugli insiemi Δ, Ω rispettivamente, con $|\Omega| \geq 2$. Sia $G = H \wr K$ il loro prodotto intrecciato. Si determini il centro $Z(G)$, mostrando, in particolare, che $Z(G) \simeq Z(H)$ se Ω è finito, mentre $Z(G) = 1$ se Ω è infinito.

Esercizio 3.31. Sia H un gruppo semplice infinito (ad esempio $Alt(\mathbb{N})$). Si provi che il prodotto intrecciato standard $G = HwrH$ ha una serie principale ma non ha alcuna serie di composizione.

Esercizio 3.32. Sia $G = C_2 wr C_3$. Si provi che $G/Z(G)$ è isomorfo ad A_4.

Esercizio 3.33. Sia P un 3-sottogruppo di Sylow di S_6. Si provi che $N_G(P) \simeq S_3 \wr C_2$.

Esercizio 3.34. Con le notazioni dell'esercizio 1.46, si provi che $DH \simeq \mathbb{F}^* \wr S_n$.

Capitolo 4

Gruppi liberi

4.1 Gruppi liberi

Ricordiamo che se X un sottoinsieme di un gruppo G si denota con $\langle X\rangle$ il *sottogruppo generato* da X, ovvero il minimo (per la relazione di inclusione) sottogruppo di G contenente X, $\langle X\rangle$ è dunque l'intersezione di tutti i sottogruppi di G che contengono X. In particolare, $\langle\emptyset\rangle = \{1\}$, mentre se X non è vuoto è facile verificare che, posto $X^{-1} = \{x^{-1} \mid x \in X\}$,

$$\langle X\rangle = \{x_1^{\beta_1} \dots x_n^{\beta_n} \mid 1 \leq n \in \mathbb{N},\ x_1, \dots, x_n \in X \cup X^{-1}\}. \tag{4.1}$$

Poiché, in un prodotto $x_1 \dots x_n$ termini consecutivi che siano uguali o inversi possono essere moltiplicati senza cambiare l'elemento, la (4.1) si può riscrivere come

$$\langle X\rangle = \{x_1^{\beta_1} \dots x_n^{\beta_n} \mid 1 \leq n \in \mathbb{N},\ x_1, \dots, x_n \in X,\ \beta_1, \dots, \beta_n \in \mathbb{Z}\}. \tag{4.2}$$

X si dice un *sistema di generatori* del gruppo G se $G = \langle X\rangle$. Quindi, un sottoinsieme non vuoto X del gruppo G è un suo sistema di generatori se e soltanto se ogni $g \in G$ si scrive nelle forma

$$g = x_1^{\beta_1} \dots x_n^{\beta_n} \tag{4.3}$$

con $n \geq 1$, $x_i \in X$ e $\beta_i \in \mathbb{Z}$ per ogni $i = 1, \dots, n$.

Un gruppo G si dice *finitamente generato* (a volte scriveremo f.g.) se ammette un sistema finito di generatori. Quando sarà necessario essere più precisi, si dirà che un gruppo è n-generato se ammette un sistema di generatori X con $|X| = n$; in particolare, un gruppo è 1-generato se e soltanto se è ciclico.

Un sistema di generatori di un gruppo G è minimale se nessun suo sottoinsieme proprio è un sistema di generatori di G. Anche per gruppi finitamente generati, sistemi di generatori minimali distinti non hanno necessariamente la stessa cardinalità. Ad esempio, $\mathbb{Z} = \langle 1\rangle$ (la notazione è additiva), ma si osservi che se n, m sono interi coprimi allora $\{n, m\}$ è un sistema minimale di generatori di $\mathbb{Z}$; in effetti, se $p_1, \dots, p_k$ sono primi distinti e, per ogni $i = 1, \dots, k$, $n_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k$, allora $\{n_1, \dots, n_k\}$ è un sistema minimale di generatori di $\mathbb{Z}$ (lo si dimostri per esercizio).

Il gruppo (additivo) $\mathbb{Q}$ non è finitamente generato; un suo sistema di generatori è, ad esempio, $X = \{1/n \mid 1 \leq n \in \mathbb{N}\}$, che non è minimale (si dimostrino queste affermazioni). Altri esempi di gruppi non f.g. sono i gruppi di Prüfer C_{p^∞}; anche questi - come il gruppo additivo dei razionali - non ammettono sistemi minimali di generatori.

Osserviamo infine che se G è finitamente generato allora esiste un minimo per le cardinalità dei suoi sistemi di generatori che denoteremo con $d(G)$.

Generatori liberi. Sia X un sistema di generatori del gruppo G; dato $g \in G$, la scrittura di g come in (4.3) non è in generale univocamente determinata. Ad esempio, per $x, y \in X$, $xx^{-1} = x^{-1}x = yy^{-1} = 1$. Potremmo cercare di aggirare queste e simili situazioni richiedendo che, in (4.3), si abbia, per $g \neq 1$, che $x_i \neq x_{i+1}$ $(i = 1, \ldots, n-1)$ e che nessun esponente β_i sia 0. Ma è facile fornire esempi per i quali anche imponendo ciò non si ha unicità nella (4.3).

Un sistema di generatori X del gruppo G si dice *libero*, se per ogni $n \geq 1$, $x_1, \ldots x_n \in X$, con $x_i \neq x_{i+1}$ (per $i = 0, \ldots, n-1$) e $\beta_1, \ldots, \beta_n \in \mathbb{Z} \setminus \{0\}$ si ha

$$x_1^{\beta_1} \ldots x_n^{\beta_n} \neq 1. \tag{4.4}$$

È facile verificare (lo si faccia per esercizio) che X è un sistema libero di generatori per G se e soltanto se ogni $1 \neq g \in G$ si scrive in modo unico nella forma $g = x_1^{\beta_1} \ldots x_n^{\beta_n}$ con $x_1, \ldots x_n \in X$, $x_i \neq x_{i+1}$ e $\beta_1, \ldots, \beta_n \in \mathbb{Z} \setminus \{0\}$.

Un gruppo G si dice un *gruppo libero* se ammette un sistema libero di generatori. Più in generale, dato un insieme X, si dice che il gruppo G è libero su X se esiste una applicazione iniettiva $\tau : X \to G$ tale che $X\tau$ è un sistema libero di generatori di G.

La definizione di gruppo libero appena data non garantisce da sé l'esistenza di gruppi del genere. In questa sezione vedremo la costruzione astratta dei gruppi liberi (un argomento di fondamentale importanza), mentre nel prossimo forniremo alcuni esempi "in natura".

Costruzione di gruppi liberi. Sia X un insieme non vuoto. Si considera un insieme X^{-1}, disgiunto da X e della sua stessa cardinalità, assieme ad una biezione $X \to X^{-1}$, per cui denotiamo con x^{-1} l'imagine di ciscun elemento $x \in X$.
Sia W l'insieme di tutte le *parole* nell'alfabeto $X \cup X^{-1}$, ovvero di tutte le stringhe finite $x_1 x_2 \ldots x_n$, con $x_i \in X \cup X^{-1}$, alle quali si deve aggiungere la parola (stringa) vuota, che denotiamo col simbolo 1. L'insieme W è in modo naturale un semigruppo, dove il prodotto di due parole consiste nelle loro giustapposizione: se $w_1 = x_1 x_2 \ldots x_n$ e $w_2 = x_1' x_2' \ldots x_m'$ sono elementi di W (quindi $x_1, \ldots, x_n, x_1', \ldots, x_m' \in X \cup X^{-1}$), allora

$$w_1 \cdot w_2 = x_1 x_2 \ldots x_n x_1' x_2' \ldots x_m'. \tag{4.5}$$

Inoltre, la parola vuota 1 può essere aggregata come elemento neutro, ottenendo quindi che W è un monoide.

Sugli elementi w di W definiamo i seguenti due tipi di operazioni:

(1) inserimento in w di una coppia di termini consecutivi xx^{-1} oppure $x^{-1}x$, con $x \in X$;
(2) cancellazione in w di una coppia di termini consecutivi del tipo xx^{-1} oppure $x^{-1}x$, con $x \in X$

(dove si intende che l'inserimento o la cancellazione possono avvenire anche all'inizio o alla fine della parola). Una parola w si dice *ridotta* se $w = 1$ oppure w non include alcuna coppia consecutiva del tipo xx^{-1} oppure $x^{-1}x$, con $x \in X$. Diciamo poi che due parole $w_1, w_2 \in W$ sono *equivalenti*, e scriviamo $w_1 \sim w_2$, se w_2 si ottiene da w_1 mediante una successione finita di operazioni del tip (1) o (2). Che $\sim$ definisca effettivamente un'equivalenza su W è immediato; per ogni $w \in W$ denotiamo con $[w]$ la sua classe di equivalenza. Ad esempio, se x, y sono elementi distinti di X allora $[xx^{-1}] = [yy^{-1}] = [1][$; un altro esempio è $1 \sim w = xyx^{-1}xy^{-1}yy^{-1}x^{-1}$, infatti una successione di operazioni del tipo (2) dà:

$$w = xy(x^{-1}x)y^{-1}yy^{-1}x^{-1} \sim x(yy^{-1})yy^{-1}x^{-1} \sim x(yy^{-1})x^{-1} \sim xx^{-1} \sim 1 \tag{4.6}$$

dove abbiamo indicato con paretesi le coppie che via via sono cancellate. Osserviamo che quella descritta da (4.6) non è l'unica serie di riduzioni che è possibile condurre a partire da w; ad esempio, un 'altra è la seguente:

$$w = xyx^{-1}xy^{-1}(yy^{-1})x^{-1} \sim xy(x^{-1}x)y^{-1}x^{-1} \sim x(yy^{-1})x^{-1} \sim xx^{-1} \sim 1 \tag{4.7}$$

Si osservi che però la parola di arrivo (in questo caso la parola vuota 1) è la stessa, ed è una parola ridotta.. Infatti con un po' di pazienza si dimostra che

Lemma 4.1. *Ogni classe di equivalenza in W modulo $\sim$ contiene una ed una sola parola ridotta.*

Se $w \in W$, denotiamo con $\overline{w}$ l'unica parola ridotta tale che $w \sim \overline{w}$.

Sia $F = W/\sim$ l'insieme quoziente. Su F definiamo quindi un prodotto ponendo, per ogni $w_1, w_2 \in W$,

$$[w_1] \cdot [w_2] = [w_1 w_2]. \tag{4.8}$$

Che si tratti di una buona definizione è piuttosto immediato dalla definizione di $\sim$, e lo lasciamo comunque per esercizio.

Proposizione 4.2. *Con l'operazione definita in (4.8), F è un gruppo, ed è libero nel sistema di generatori $\{[x] \mid x \in X\}$.*

Dimostrazione. Che l'operazione in (4.8) sia associativa discende immediatamente dal fatto che tale è l'operazione nel monoide delle parole W. Per la stessa ragione si riconosce subito che [1] (dove 1 rappresenta la parola vuota) è l'elemento neutro in F, che denoteremo ancora con 1.
Ora, per ogni $x \in X$, $xx^{-1} \sim 1 \sim x^{-1}x$, e quindi, in F, $[x^{-1}] = [x]^{-1}$. Infine, sia $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in W$, con $x_1, \dots, x_n \in X$ e $\epsilon_1, \dots, \epsilon_n \in \{1, -1\}$ (dove, ovviamente, per $x \in X$, si intende $x^1 = x$); allora

$$[w]^{-1} = [x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}].$$

Pertanto, F è un gruppo, e chiaramente $X\tau = \{[x] \mid x \in X\}$ è un suo sistema di generatori (qui $\tau : X \to F$ è la proiezione $x \mapsto [x]$, che, per il Lemma 4.1 è un'applicazione iniettiva). Proviamo che tale sistema di generatori è libero. Per $x \in X$ e $0 \neq \beta \in \mathbb{Z}$, scriviamo (nel monoide W) $x^\beta = x \cdots x$ (β volte) se $\beta > 0$, e $x^\beta = x^{-1} \cdots x^{-1}$ (-β volte) se $\beta < 0$. Chiaramente, per ogni $x \in X$ ed ogni $0 \neq \beta \in \mathbb{Z}$, x^β è una parola ridotta; inoltre, in

F, si ha $[x]^\beta = [x^\beta]$. Quindi, se $x_1, \dots x_n \in X$, con $x_{i+1} \neq x_i$ (per $i = 1, \dots, n-1$) e $\beta_1, \dots, \beta_n \in \mathbb{Z} \setminus \{0\}$, allora $x_1^{\beta_1} \dots x_n^{\beta_n}$ è una parola ridotta; conseguentemente,

$$[x_1]^{\beta_1} \dots [x_n]^{\beta_n} = [x_1^{\beta_1} \dots x_n^{\beta_n}] \neq [1].$$

Questo prova che $\{[x] \mid x \in X\}$ è un sistema libero di generatori di F (la cui cardinalità coincide con quella di X). ∎

4.2 Presentazioni di gruppi

Proprietà universale dei gruppi liberi. I gruppi liberi sono caratterizzati dal soddisfare una importante proprietà di tipo universale. Questo è il contenuto della Proposizione seguente. Un gruppo F è detto libero sull'insieme X se esiste una applicazione iniettiva $\tau : X \to F$ tale che $X\tau$ è un sistema libero di generatori di F.

Proposizione 4.3. *Siano X un insieme ed F un gruppo. Allora F è libero su X se e soltanto se esiste $\tau : X \to F$, con la proprietà che per ogni gruppo G ed ogni applicazione $f : X \to G$, esiste un unico omomorfismo $\alpha : F \to G$ tale che $\tau\alpha = f$; in altri termini, esiste uno ed un solo omomorfismo α che rende commutativo il diagramma:*

$$\begin{array}{ccc} X & \xrightarrow{\tau} & F \\ {\scriptstyle f}\downarrow & \swarrow_{\alpha} & \\ G & & \end{array} \tag{4.9}$$

Dimostrazione. Sia F un gruppo libero su X, e $\tau : X \to F$ tale che $X\tau$ è un sistema libero di generatori di F. Ogni elemento $g \neq 1$ di F si scrive allora in maniera unica come una parola ridotta $g = (x_1\tau)^{\epsilon_1} \dots (x_n\tau)^{\epsilon_n}$, con $x_i \in X$ e $\epsilon_i \in \{-1, 1\}$. Sia G un gruppo e $f : X \to G$ un'applicazione; ponendo

$$g\alpha = (x_1 f)^{\epsilon_1} \dots (x_n f)^{\epsilon_n} \tag{4.10}$$

si definisce un omomorfismo $\alpha : F \to G$. Poiché F è generato da $X\tau$ e per ogni $x \in X$, per definizione, $x\tau\alpha = xf$, si conclude che $\tau\alpha = f$. Che una tale omomorfismo α sia unico discende anche immediatamente dal fatto che, per ogni $x \in X$, $x\tau\alpha = xf$ e $X\tau$ genera F.

Viceversa, supponiamo che F sia un gruppo e che sia data $\tau : X \to F$ tali che sussiste la proprietà universale descritta in (4.9). Sia $F(X)$ il gruppo libero definito a partire da X come nella costruzione di sopra; per cui possiamo interpretare univocamente gli elementi di $F(X)$ come le parola ridotte in $X \cup X^{-1}$. Per la proprietà ipotizzata su F, esiste un omomorfismo $\alpha : F \to F(X)$ tale che $\tau\alpha = \iota$, dove ι è l'inclusione di X in $F(X)$. D'altra parte, per quanto provato sopra, esiste un omomorfismo $\beta : F(X) \to F$ tale che $\iota\beta = \tau$. Dunque, per ogni $x \in X \subseteq F(X)$, $x\beta\alpha = (x\iota\beta)\alpha = x\tau\alpha = x\iota = x$. Poiché $F(X)$ è generato da X e $\beta\alpha$ è un omomorfismo, si conclude che $\beta\alpha$ è l'identità su $F(X)$. Allo stesso modo, $\alpha\beta$ risulta un omomorfismo $F \to F$ che fissa ogni $x\tau$. Per l'unicità dell'applicazione che completa il diagramma (4.9) quando $G = F$ e $f = \tau$, si deduce che $\alpha\beta$ è l'identità su F. Quindi $\alpha : F \to F(X)$ è una biezione e dunque un isomorfismo. ∎

La proprietà universale descritta da questa Proposizione è spesso assunta come definizione di un gruppo libero, e in questo senso trova corrispettivi in teorie che riguardano altri tipi di strutture algebriche (e anche noi la adotteremo più avanti per definire gruppi liberi ristretti a particolari classi di gruppi).
La seconda parte della dimostrazione precedente si può applicare quasi nell'identica maniera per provare che gruppi liberi sullo stesso insieme X sono isomorfi. Più in generale,

Proposizione 4.4. *Siano F e G gruppi liberi su, rispettivamente, gli insiemi X e Y. Se $|X| = |Y|$, allora F e G sono isomorfi.*

DIMOSTRAZIONE. Sia $g : X \to Y$ una biezione; siano F e G gruppi liberi, rispettivamente su X e su Y, con $\tau : X \to F$ e $\sigma : Y \to G$ le immersioni dei generatori. Applicando la (4.9) a $f = g\sigma$ si deduce l'esistennza di un omomorfismo $\alpha : F \to G$ tale che $\tau\alpha = g\sigma$; applicandola a $f' = g^{-1}\tau$, quella di un omomorfismo $\beta : G \to F$ tale che $g^{-1}\tau = \sigma\beta$. Allora $\tau\alpha\beta = g\sigma\beta = gg^{-1}\tau = \tau$, e quindi (come nella dimostrazione di 4.3), $\alpha\beta = 1_F$. Allo stesso modo $\beta\alpha = 1_G$. Dunque α è un isomorfismo. ∎

Quindi, dato un insieme X, si parla *del* gruppo libero su X, che denoteremo con $F(X)$. Anzi, poiché il tipo di isomorfismo di $F(X)$ dipende solo dalla cardinalità di X, se $|X| = \lambda$, diremo che $F(X)$ è il *gruppo libero di rango* λ. Nel caso particolare in cui $n < \infty$, denoteremo con F_n il gruppo libero di rango n. Di fatto la Proposizione 4.4 ammette una formulazione inversa (che vedremo più avanti), nel senso che gruppi liberi di rango diverso (non necessariamente finito) non sono isomorfi.

Presentazioni. Sia G un gruppo; siano X un sistema di generatori di G, e $F(X)$ il gruppo libero su X. Applicando la Proposizione 4.3 con $f : X \to G$ l'immersione di X in G, si conclude che esiste un unico omomorfismo

$$\phi : F(X) \to G \ \text{ tale che } \ (x\tau)\phi = x. \tag{4.11}$$

dove, al solito, τ è l'immersione $X \to F(X)$. Poiché G è generato da X, ϕ è suriettivo e, per il Teorema di omomorfismo,

$$G \simeq F(X)/\ker(\phi). \tag{4.12}$$

Quindi, in particolare: *ogni gruppo è immagine omomorfa di un gruppo libero.* Un isomorfismo come in (4.12) è ciò che si chiama una *presentazione* del gruppo G, e gli elementi di $\ker(\phi)$ sono dette le *relazioni* della presentazione.

Illustriamo ora il modo con cui viene in genere definita una presentazione. Sia ϕ come in (4.11) e sia R un sottoinsieme di $\ker(\phi)$ tale che $\langle R\rangle^{F(X)} = \ker(\phi)$, allora la presentazione (4.12) si descrive come

$$G = \big\langle X\tau \mid R\big\rangle. \tag{4.13}$$

Nella pratica, spesso - e noi così faremo - si identifica x con $x\tau$ (per ogni $x \in X$) e si specificano gli elementi di R in quanto inducenti relazioni nel gruppo G, ovvero invece di (4.13), si preferisce scrivere la presentazione come

$$G = \big\langle X \mid \phi(r) = 1,\ r \in R\big\rangle. \tag{4.14}$$

Ad esempio, per ogni $n \geq 1$, $\big\langle x \mid x^n = 1\big\rangle$ è una presentazione del gruppo ciclico di ordine n, mentre $\big\langle x, y \mid xy = yx\big\rangle = \big\langle x, y \mid xyx^{-1}y^{-1} = 1\big\rangle$ è una presentazione del prodotto diretto $\mathbb{Z} \times \mathbb{Z}$.

Teorema 4.5. (von Dyck) *Siano G e H due gruppi con presentazioni $G = \langle X \mid R\rangle$ e $H = \langle X \mid S\rangle$. Se $R \subseteq S$ allora H è isomorfo ad un quoziente di G.*

Dimostrazione. Sia $F = F(X)$ e siano $\phi : F \to G$ e $\psi : F \to H$ gli omomorfismi sottesi dalle due presentazioni nell'enunciato. Allora $\ker(\phi) = R^F \leq S^F = \ker(\psi)$ e dunque H è isomorfo $F/\ker(\psi)$ che è isomorfo ad un quoziente di $F/\ker(\phi) \simeq G$. ∎

Esempio 4.1. Il gruppo $D_\infty = \langle x, y \mid x^2 = 1,\ y^2 = 1\rangle$ è il gruppo diedrale infinito. Ponendo $a = xy$, allora $D_\infty = \langle a, x\rangle$ e $a^x = x^{-1}xyx = a^{-1} = a^y$. Quindi $\langle a\rangle \trianglelefteq D_\infty$, e possiamo identificare D_∞ con il prodoitto semidiretto $\langle a\rangle \rtimes \langle x\rangle$, con $|a| = \infty,\ |x| = 2$, e $a^x = a^{-1}$. In effetti, un'altra presentazione per D_∞ è $\langle x, y \mid x^2 = 1,\ y^x = y^{-1}\rangle$.
Sia $n \geq 2$ un intero. Allora (lo si dimostri) $\langle x, y \mid x^2 = 1,\ y^2 = 1,\ (xy)^n = 1\rangle$ e $\langle x, y \mid x^2 = 1,\ y^n = 1,\ y^x = y^{-1}\rangle$, sono due presentazioni del gruppo diedrale di ordine $2n$. □

Esempio 4.2. Siano $a, b \in \mathbb{N}$ diversi da 0 e coprimi, e sia

$$G = \langle x, y \mid x^{-1}y^{-1}xy^{a+1} = 1,\ y^{-1}x^{-1}yx^{b+1} = 1\rangle.$$

dalle relazioni segue $y^x = y^{a+1}$ e $x^y = x^{b+1}$; quindi

$$z := x^b = x^{-1}x^y = (y^{-1})^x y = y^{-a}.$$

Ora,

$$z = z^y = (x^b)^y = (x^y)^b = (x^{b+1})^b = (x^b)^{b+1} = z^b z,$$

da cui $z^b = 1$. Allo stesso modo $z^a = 1$. Poiché $(a, b) = 1$, risulta $z = 1$. Quindi

$$x^b = 1 = y^a,\quad x^y = x,\quad y^x = y.$$

Dunque $[x, y] = 1$, e pertanto $G = \langle x\rangle \times \langle y\rangle \simeq C_b \times C_a$. □

Dato un gruppo non è in genere facile trovare una sua presentazione; e viceversa, non è facile dedurre le proprietà di un gruppo a partire da una sua presentazione. il ricorso al Teorema 4.5 è efficace quando, data una presentazione $G = \langle X \mid R\rangle$ si riesce a trovare un gruppo H ed un suo sistema di generatori in modo che le relazioni R siano soddisfatte; allora si deduce che H è (isomorfo a) un quoziente di G.

Esempio 4.3. Consideriamo il gruppo $G = \langle x, y \mid y^x = y^2\rangle$. Sia $Q = H \rtimes \langle\alpha\rangle$ dove H è il gruppo dei razionali il cui denominatore è una potenza di 2 e α la moltiplicazione per 2; allora Q soddisfa la presentazione con $y = 1$, $x = \alpha$ (e messo in notazione moltiplicativa); quindi Q è un quoziente di G; detto meglio, esiste un omomorfismo suriettivo $\pi : G \to Q$ tale che $y\pi = 1$ e $x\pi = \alpha$; in particolare $|x| = |y| = \infty$. Ora, per ogni $n \in \mathbb{N}$ si ha $y^{x^n} = y^{2^n}$, quindi, per ogni $n, m \in \mathbb{Z}$, con $n \geq m$,

$$[y^{x^n}, y^{x^m}] = [y^{x^{n-m}}, y]^{x^m} = [y^{2^{n-m}}, y]^{x^m} = 1$$

e quindi $N = \langle y\rangle^G = \langle y^{x^z} \mid z \in \mathbb{Z}\rangle$ è abeliano., e $G = N \rtimes \langle x\rangle$. Ogni numero razionale in H si scrive in modo unico nella forma $z2^i$ con $z, i \in \mathbb{Z}$ e z dispari; si pone $z2^i \mapsto (y^z)^{x^i}$ e si verifica senza difficoltà che ciò stabilisce un omomorfismo $\phi : H \to N$, la cui immagine $\phi(H)$ contiene y ed è normalizzata da x. Quindi, $N = \phi(H)$, e ϕ si estende ad un omomorfismo suriettivo $Q \to G$ con $x\phi = \alpha$. A questo punto si trova che ϕ e π sono uno inverso dell'altro, e che dunque $G \simeq Q$. □

4.3 Esempi (gruppi liberi, presentazioni)

Per ogni insieme X abbiamo costruito in modo astratto un gruppo libero su X. Vediamo ora, mediante alcuni esempi, come i gruppi liberi non ciclici si trovino (e anche con una certa frequenza) "in natura". Per provare che un certo gruppo è libero, un criterio semplice ma molto efficace è il *Lemma del Ping–Pong*, che fu sostanzialmente applicato già da Felix Klein. Quella che vediamo è la sua versione basica.

Lemma 4.6. *Sia G un gruppo che agisce sull'insieme Ω, e siano $x, y \in G$. Supponiamo esistano sottoinsiemi non vuoti Ω_1, Ω_2 di Ω tali che $\Omega_1 \not\subseteq \Omega_2$, e*

$$\Omega_1 x^z \subseteq \Omega_2$$
$$\Omega_2 y^z \subseteq \Omega_1$$

per ogni $0 \neq z \in \mathbb{Z}$. Allora $\langle x, y\rangle$ è un gruppo libero su $\{x, y\}$.

Dimostrazione. Nel gruppo $\langle x, y\rangle$ consideriamo un prodotto del tipo (4.3), dove quindi, per ogni indice $i = 1, \dots, n$, $x_i \in \{x, y\}$. Distinguiamo vari casi, cominciando da quello in cui il primo e l'ultimo generatore che compaiono nel prodotto sia x; ovvero, $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_{n-1}} y^{\beta_{n-1}} x^{\alpha_n}$, con $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{n-1} \in \mathbb{Z} \setminus \{0\}$. Allora

$$\Omega_1 w = (\Omega_1 x^{\alpha_1}) y^{\beta_1} \dots x^{\alpha_n} \subseteq (\Omega_2 y^{\beta_1}) \dots x^{\alpha_n} \subseteq \dots \subseteq \Omega_1 x^{\alpha_n} \subseteq \Omega_2$$

e poiché, per ipotesi, $\Omega_1 \not\subseteq \Omega_2$, si conclude che w non può agire come l'identità, e quindi che $w \neq 1$. Supponiamo ora che $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_n} y^{\beta_n}$; allora scelto un intero $0 \neq z \neq \alpha_1$, si ha che $w^{x^z} = x^{-z} w x^z$ è un elemento del tipo analizzato sopra. Quindi $w^{x^z} \neq 1$ e dunque $w \neq 1$. Nei casi rimanenti, ovvero, $w = y^{\beta_1} \dots y^{\beta_{n-1}} x^{\alpha_n}$ e $w = y^{\beta_1} \dots x^{\alpha_n} y^{\beta_n}$ si procede in modo analogo. ∎

Esempio 4.4. Il gruppo $G = GL(2, \mathbb{R})$ opera in modo naturale sull'insieme dei punti di $\mathbb{R}^2$; se $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ e $(\alpha, \beta) \in \mathbb{R}^2$,

$$(\alpha, \beta)A = (\alpha a + \beta c, \alpha b + \beta d) \tag{4.15}$$

In G consideriamo gli elementi

$$x = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Si verifica facilmente che, per ogni $z \in \mathbb{Z}$, $x^z = \begin{pmatrix} 1 & 2z \\ 0 & 1 \end{pmatrix}$, e $y^z = \begin{pmatrix} 1 & 0 \\ 2z & 1 \end{pmatrix}$.
Posto $\Omega_1 = \{(\alpha, \beta) \in \mathbb{R}^2 \mid |\alpha| > |\beta|\}$ e $\Omega_2 = \{(\alpha, \beta) \in \mathbb{R}^2 \mid |\alpha| < |\beta|\}$, sia $(\alpha, \beta) \in \Omega_1$ e $0 \neq z \in \mathbb{Z}$. Allora, per (4.15), $(\alpha, \beta)x^z = (\alpha, 2z\alpha + \beta)$, e si ha

$$|2z\alpha + \beta| > ||2z\alpha| - |\beta|| = 2|z||\alpha| - |\beta| > (2|z1)|\alpha| > |\alpha|,$$

e dunque $(\alpha, 2z\alpha + \beta) \in \Omega_2$. Quindi $\Omega_1 x^z \subseteq \Omega_2$. In maniera analoga si prova che, per ogni $0 \neq z \in \mathbb{Z}$, $\Omega_2 y^z \subseteq \Omega_1$. Per il Lemma del Ping–Pong si conclude che il gruppo $\langle x, y\rangle$ è libero nei generatori x e y. □

In questo ambito citiamo un importante risultato generale dovuto a J. Tits.

Teorema 4.7. (Tits alternative) *Siano F un campo, $1 \leq n \in \mathbb{N}$ e G un sottogruppo di $GL(n, F)$. Allora G contiene un sottogruppo libero di rango almeno due oppure un sottogruppo risolublie di indice finito.*

Il nostro prossimo esemplare è un sottogruppo del gruppo degli omeomorfismi della retta reale o, anche, del gruppo degli automorfismi $Aut(\mathbb{R}, \leq)$ dell'insieme ordinato dei reali, ed è tratto da un articolo di C. Bennett [4].

ESEMPIO 4.5. Si consideri la funzione lineare a tratti $\phi : [0, 1] \to [0, 1]$, definita da

$$\phi(x) = \begin{cases} 4x & \text{se} \quad 0 \leq x \leq 1/5 \\ x/4 + 3/4 & \text{se} \quad 1/5 \leq x \leq 1 \end{cases}$$

(le funzioni di variabile reale le scriviamo a sinistra). Sia quindi $f : \mathbb{R} \to \mathbb{R}$ definita da, per ogni $x \in \mathbb{R}$,

$$f(x) = [x] + \phi(x - [x]),$$

dove $[x]$ è la parte intera di x. Infine sia $g = \tau f \tau$ dove τ è la traslazione, $x \mapsto x - 1/5$ (per ogni $x \in \mathbb{R}$); cioè

$$g(x) = f(x - 1/5) - 1/5.$$

Allora $\{f, g\} \subseteq Aut(\mathbb{R}, \leq)$. Siano

$$\Omega_1 = \bigcup_{u \in \mathbb{Z}} \Big(u + \frac{3}{10}, u + \frac{7}{10}\Big) \quad \text{e} \quad \Omega_2 = \bigcup_{u \in \mathbb{Z}} \Big(u - \frac{1}{5}, u + \frac{1}{5}\Big).$$

Allora, per ogni $0 \neq z \in \mathbb{Z}$ si ha

$$f^z(\Omega_1) \subseteq \Omega_2 \qquad \text{e} \qquad g^z(\Omega_2) \subseteq \Omega_1$$

(lascerei al lettore che lo desideri svolgere le relativamente laboriose verifiche, oppure consultare [4]). Per il Lemma del Ping–Pong si conclude quindi che $\langle f, g \rangle$ è un gruppo liberamente generato da f e g. □

Presentazione del gruppo simmetrico. In certi casi, se, data una presentazione di un gruppo G, si riesce a provare che $|G| \leq n$, e si trova un gruppo H che soddisfa le stesse relazioni ed è tale che $|H| = n$, si deve concludere che $H \simeq G$. Questa procedura è applicata nella seguente proposizione, che fornisce una presentazione dei gruppi simmetrici finiti.

Proposizione 4.8. *Sia $n \geq 2$. Allora*

$$S_n = \big\langle x_1, \ldots, x_{n-1} \mid x_i^2 = (x_j x_{j+1})^3 = (x_k x_\ell)^2 = 1 \big\rangle. \tag{4.16}$$

dove $1 \leq i \leq n-1$, $1 \leq j \leq n-2$ e $1 \leq \ell < k - 1 < n - 1$.

DIMOSTRAZIONE. Sia G il gruppo la cui presentazione è il termine a destra di (4.16). Proviamo, per induzione su n, che $|G| \leq n!$. Per $n = 2$ si ha che $G = \langle x_1, x_2 \mid x_1^2 = x^2 = (x_1 x_2)^3 = 1 \rangle$ è il gruppo diedrale di ordine 6, ovvero S_3. Sia $n \geq 3$ e sia H il sottogruppo di G generato da $\{x_1, \ldots, x_{n-2}\}$. Per ipotesi induttiva, $H| \leq (n-1)!$. È dunque sufficiente

provare che $|G : H| \leq n$. Consideriamo l'azione di G per moltiplicazione a destra sull'insieme della classi laterali destre di H in G. Siano $i, j \in \{1, \ldots, n-1\}$.
- Se $j < i - 1$ allora $(x_s x_j)^2 = 1$, dunque $x_s x_j = x_j x_s$ per ogni $s \geq i$, e quindi (poiché $j < n - 1$ e dunque $x_j \in H$),

$$(Hx_{n-1} \ldots x_i)x_j = Hx_j x_{n-1} \ldots x_i = Hx_{n-1} \ldots x_i.$$

- Se $j > i$, allora $x_k x_j = x_j x_k$ per $|j - k| > 1$, inoltre $(x_{j-1}x_j)^3 = 1$ da cui segue subito $x_{j-1}x_j x_{j-1} = x_j x_{j-1} x_j$; quindi

$$\begin{aligned}(Hx_{n-1} \ldots x_i)x_j &= Hx_{n-1} \ldots x_{j+1}(x_j x_{j-1} x_j)x_{j-2} \ldots x_i = \\ &= Hx_{n-1} \ldots x_{j+1}(x_{j-1} x_j x_{j-1})x_{j-2} \ldots x_i \\ &= Hx_{j-1}x_{n-1} \ldots x_i = Hx_{n-1} \ldots x_i.\end{aligned}$$

- Infine, nei casi $j + i$ e $j = i - 1$ si ha, rispettivamente,

$$(Hx_{n-1} \ldots x_i)x_j = Hx_{n-1} \ldots x_{i+1} \qquad e \qquad (Hx_{n-1} \ldots x_i)x_j = Hx_{n-1} \ldots x_i x_{i-1}.$$

Tenendo conto che gli elementi x_j $(j = 1, \ldots, n-1)$ generano G, si conclude che l'insieme di classi laterali $\Omega = \{H, Hx_{n-1}, Hx_{n-1}x_{n-2}, \ldots, Hx_{n-1}x_{n-2} \ldots x_1\}$ è invariante per l'azione di G; siccome tale azione è transitiva, si conclude che Ω è l'insieme di tutte le classi laterali destre di H in G. Quinbdi $|G : H| = |\Omega| \leq n$, che è quel che si voleva. Dunque, $|G| \leq n!$.
A questo punto si nota che posto, nel gruppo simmetrico S_n, $x_i = (i\ i{+}1)$, per $i = 1, \ldots, n{-}1$,, allora $S_n = \langle x_1, \ldots, x_{n-1} \rangle$ e gli elementi x_i soddisfano le relazioni che definiscono G. Per il Teorema 4.5, si deduce che S_n è isomorfo ad un quoziente di G. Poiché $|S_n| = n! \geq |G|$, si conclude che $|G| = n!$ e $G \simeq S_n$. ∎

4.4 Prodotti liberi

Il *prodotto libero* di gruppi è una generalizzazione dell'idea di gruppo libero. Noi tratteremo il caso del prodotto libero di due gruppi: l'estensione al prodotto di famiglia arbitraria di gruppi dovrebbe riuscire comunque abbastanza naturale (ed è lasciata per esercitazione al lettore laborioso). Procedendo contromano rispetto a quanto abbiamo fatto nell'introdurre i gruppi liberi, iniziamo con la proprietà universale che caratterizza il prodotto libero.

Proprietà universale dei prodotti liberi. Siano H e K gruppi; un gruppo G e omomorfismi $\alpha_H : H \to G$, $\alpha_K : K \to G$ si dice un *prodotto libero* di H e K, se è soddisfatta la seguente proprietà universale

Per ogni gruppo W ed omomorfismi $\phi_H : H \to W$, $\phi_K : K \to W$, esiste uno ed un unico omomorfismo $\phi : G \to W$ tale che $\phi_H = \alpha_H \phi$ e $\phi_K = \alpha_K \phi$. Ovvero risulta commutativo il diagramma

$$\begin{array}{ccccc} H & \xrightarrow{\alpha_H} & G & \xleftarrow{\alpha_K} & K \\ & \searrow^{\phi_H} & \downarrow \phi & \swarrow_{\phi_K} & \\ & & W & & \end{array} \tag{4.17}$$

Prima di dimostrare l'esistenza dei prodotti liberi, facciamo alcune osservazioni fondamentali che si deducono facilmente dalla proprietà universale.

Proposizione 4.9. *Siano H e K gruppi:*
(1) se (G, α_H, α_K) è prodotto libero di H e K allora α_H e α_K sono iniettive;
(2) se G e G' sono prodotti liberi dei gruppi H e K, allora $G \simeq G'$.

Dunque, se esiste, il prodotto libero di H e K è unico (a meno di isomorfismi) e lo si denota con

$$H * K.$$

ESEMPIO 4.6. Siano $H = \langle a \rangle$ e $K = \langle b \rangle$ gruppi ciclici di ordine 2 e D_∞ il gruppo diedrale infinito. D_∞ è generato da due involuzioni a', b' con $|a'b'| = \infty$; definiamo α_H e α_K ponendo $a\alpha_H = a'$ e $b\alpha_K = b'$. Se ϕ_H, ϕ_K sono omomorfismi, rispettivamente, di H e di K in un gruppo G allora $x = a\phi_H$ e $y = b\phi_K$ sono involuzioni di G (il caso in cui ϕ_H e ϕ_K non sono entrambi iniettivi è facile e lo lascio al lettore), dunque $\langle x, y \rangle$ e un gruppo diedrale ed esiste un omomorfsmo $\phi : D_\infty \to G$ (la cui immagine è $\langle x, y \rangle$) tale che $a'\phi = x$ e $b'\phi = y$. Allora $\alpha_H\phi = \phi_H$, $\alpha_K\phi = \phi_K$, e $D_\infty = H * K$. □

Dalla proprietà universale (e la Proposizione 4.9) discende anche che se H, K e T sono gruppi allora

$$(H * K) * T \simeq H * (K * T)$$

per cui si scrive senza ambiguità $H * K * T$; e $H_1 * H_2 * \cdots * H_n$ per una famiglia finita $H_1, H_2, \ldots, H_n$ di gruppi.

La seguente immediata osservazione rende conto dell'affermazione che il prodotto libero sia una generalizzazione del concetto di gruppo libero.

ESEMPIO 4.7. Siano F_n e F_m due gruppi liberi di rango n e m rispettivamente; allora

$$F_n * F_m = F_{n+m}.$$

In particolare, per ogni $n \geq 1$, $F_n \simeq \mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}$ (n volte). □

Osservazione. Analogamente a quello che vale per i gruppi liberi, una conseguenza pressoché immediata della proprietà universale è ce se H e K sono gruppi allora per ogni gruppo G che sia generato da due sottogruppi isomorfi, rispettivamente, ad H e a K, esioste un omomorfismo suriettivo $H * K \to G$ (dunque G è isomorfo ad un quoziente del prodotto libero $H * K$).

Proviamo ora l'esistenza del prodotto libero $H * K$. Siano H e K dati mediante presentazioni, diciamo $H = \langle X \mid R \rangle$ e $K = \langle Y \mid S \rangle$, con $X \cap Y = \emptyset$ (si può, ad esempio, prendere $H = \langle H \mid T_H \rangle$ dove T_H è l'insieme delle relazioni dato dalla tavola di moltiplicazione di H e fare lo stesso per K); mostreremo che il gruppo

$$G = \langle X \cup Y \mid R \cup S \rangle$$

è prodotto libero di H e K. Innanzi tutto definiamo gli omomorfismi α_H e α_K: per il primo si pone $\alpha_H : H \to G$ l'omomorfismo ottenuto componendo l'immersione $H \to \langle X \cup Y \mid R \rangle$ con la proiezione $\langle X \cup Y \mid R \rangle \to G$ (quindi $x\alpha_H = x$ per ogni $x \in X$); osserviamo che ponendo $\eta : G \to H$ l'omomorfismo tale che $x\eta = x$ per ogni $x \in X$ e $y\eta = 1$ per $y \in Y$

(l'unico omomorfismo da $F(X \cup Y) \to H$ dato da $x \mapsto x$ per $x \in X$, e $y \mapsto 1$ per $y \in Y$, contiene $R \cup S$ nel suo nucleo e dunque induce un'omomorfismo - η appunto - da G in H), allora $\alpha_H \eta$ è l'identità su H e pertanto α_H è iniettiva; similmente si definisce e si ragiona per $\alpha_K : K \to G$.

Passiamo quindi a provare la proprietà universale. Siano W un gruppo, $\phi_H : H \to W$ e $\phi_K : K \to W$ omomorfismi; definiamo $\phi : G \to W$ ponendo $x\phi = x\phi_H$ per ogni $x \in X$, e $y\phi = y\phi_K$ per ogni $y \in Y$, ed estendendo ad un omomorfismo: allora $\phi_H = \alpha_H\phi$, $\phi_K = \alpha_K\phi$, come vuole la proprietà universale, e ϕ è chiaramente unico per tale condizione.

L'esempio 4.6 illustra quanto appena detto: in quel caso $H = \langle x \mid x^2 \rangle$, $K = \langle y \mid y^2 \rangle$, ed infatti $D_\infty = \langle x, y \mid x^2, y^2 \rangle$; quindi $D_\infty = C_2 * C_2$. Un poco più sbalorditivo è il seguente classico esempio.

Esempio 4.8. $PSL(2,\mathbb{Z}) = C_2 * C_3$ (Felix Klein e Robert Fricke, $\sim$1890).

Dopo aver ricordato che $G = PSL(2,\mathbb{Z})$, detto *gruppo modulare*, è il quoziente $SL(2,\mathbb{Z})/\{\pm I\}$, dove I è la matrice identica, e $\{\pm I\} = Z(SL(2,\mathbb{Z}))$, consideriamo in $SL(2,\mathbb{Z})$ le matrici

$$x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

Facendo i calcoli si trova $x^2 = y^3 = -I$; quindi, detti $\bar{x}$ e $\bar{y}$ i corrispondenti elementi in $G := PSL(2,\mathbb{Z})$ si ha $|\bar{x}| = 2$ e $|\bar{y}| = 3$. Il passo successivo è quello di provare che x, y generano $SL(2,\mathbb{Z})$ e quindi che $\langle \bar{x}, \bar{y} \rangle = G$ (cosa che lasciamo come esercizio 4.19).

Per quanto osservato sinora, $C_2 * C_3 = \langle a, b \mid a^2, b^3 \rangle$ ed esiste un omomorfismo suriettivo $\phi : C_2 * C_3 \to G$ tale che $a\phi = \bar{x}$ e $b\phi = \bar{y}$. Sia $N = \ker\phi$; vogliamo provare che $N = 1$. Per farlo, adattiamo un analogo del metodo del Ping-Pong. Osserviamo innanzi tutto che, come si vede ragionando come nell'esempio3.7, G agisce fedelmente sulla "retta proiettiva" $\Omega = \mathbb{P}(1,\mathbb{Z}) = \{(a,b)\mathbb{Z} \mid (a,b) \in \mathbb{Z} \times \mathbb{Z}\}$. Poniamo

$$\Omega_1 = \{(a,b)\mathbb{Z} \mid (a,b) \in \mathbb{Z} \times \mathbb{Z},\ ab > 0\}, \qquad \Omega_2 = \{(a,b)\mathbb{Z} \mid (a,b) \in \mathbb{Z} \times \mathbb{Z},\ ab < 0\};$$

si verifica direttamente che $\Omega_1\bar{x} \subseteq \Omega_2$, e $\Omega_2\bar{y}^i \subseteq \Omega_1$ $(i = 1, 2)$. Sia ora, con le notazioni di sopra, $1 \neq g \in C_2 * C_3$, allora $g = x_1 x_2 \dots x_n$, con $x_i \in \{a, b, b^2\}$ e, per $i = 1, \dots, n-1$,

$$x_i = a \Rightarrow x_{i+1} \in \{b, b^2\}, \quad x_i \in \{b, b^2\} \Rightarrow x_{i+1} = a.$$

Supponiamo, per assurdo, $g \in \ker\phi$; allora, a meno di coniugio, possiamo assumere $x_1 = a$ e $x_n \in \{b, b^2\}$ oppure $x_1 \in \{b, b^2\}$ e $x_n = a$. Nel primo caso si avrebbe la contraddizione

$$\Omega_1 = \Omega_1\bar{g} = \Omega_1\bar{x} \cdots \bar{x}\bar{y}^i \subseteq \Omega_2,$$

nel secondo $\Omega_2 = \Omega_2\bar{g} \subseteq \Omega_1$. □

Credo che quest'ultimo esempio e l'argomento della sua dimostrazione possano suggerire la seguente e naturale caratterizzazione "interna" del prodotto libero:

Proposizione 4.10. *Sia G un gruppo e H, K sottogruppi di G tali che $G = \langle H, K \rangle$; allora $G = H * K$ se e solo se ogni elemento $g \in G$ si scrive in modo unico nella forma*

$$g = a_1 b_1 \cdots a_n b_n \tag{4.18}$$

con $a_1, \dots, a_n \in H$, $b_1, \dots, b_n \in K$, $a_i \neq 1 \neq b_j$ per $i = 2, \dots, n$ e $j = 1, \dots, n-1$.

DIMOSTRAZIONE. Siano $H, K \leq G$ e $G = \langle H, K \rangle$. Allora esiste un omomorfismo suriettivo $\phi : H * K \to G$ tale che $x = x\alpha_H\phi$ per ogni $x \in H$ e $y = y\alpha_K\phi$ per ogni $y \in K$ (α_H e α_K sono, rispettivamente, le immersioni di H e di K in $H * K$). Se per ogni $1 \neq g \in G$ è soddisfatta la richiesta (4.18) allora $\ker\phi = 1$ e dunque ϕ è un isomorfismo.

Viceversa, sia $G = H * K$ e identifichiamo per ogni $x \in H$ ed ogni $y \in K$, x con $x\alpha_H$ e y con $y\alpha_K$. È facile convincersi che, per provare che la (4.18) vale per ogni $g \in G$, è sufficiente dimostrare che per ogni $n \geq 1$, $a_1, \ldots, a_n \in H \setminus \{1\}$, $b_1, \ldots, b_n \in K \setminus \{1\}$

$$a_1 b_1 \cdots a_n b_n \neq 1 \tag{4.19}$$

(infatti, mediante un eventuale coniugio per opportuni elementi di H o di K, ci si pu ricondurre ad una forma del genere).

Sia Ω l'insieme di tutte le sequenze finite $(u_1, u_2, \ldots, u_n)$ ($n \in \mathbb{N}$) con $u_i \in K \cup H \setminus \{1\}$, e

$$\begin{cases} u_i \in H \Rightarrow u_{i+1} \in K \\ u_i \in K \Rightarrow u_{i+1} \in H, \end{cases}$$

insieme alla sequenza vuota. Ora, il porre, per ogni $\mathbf{u} = (u_1, \ldots, u_n) \in \Omega$ e $1 \neq a \in H$,

$$\mathbf{u} \cdot a = \begin{cases} (u_1, \ldots, u_k, a) & \text{se} \quad u_n \in K \\ (u_1, \ldots, u_{k-1}) & \text{se} \quad u_n = a^{-1} \\ (u_1, \ldots, u_k a) & \text{se} \quad a^{-1} \neq u_n \in A \end{cases}$$

definisce, come si vede facilmente, un'azione di H su Ω. In modo analogo si definisce un'azione di K su Ω. Tali azioni sono fedeli; dunque possiamo vedere H e K come sottogruppi di $Sym(\Omega)$. Per la proprietà universale esiste un omomorfismo suriettivo da $H * K$ nel sottogruppo $S = \langle H, K \rangle$ di $Sym(\Omega)$; e questo solleva l'azione su Ω da S a $H * K$. Sia $g \in H * K$ il membro di sinistra di (4.19), ed $\mathbf{e} \in \Omega$ la parola vuota; allora (come si dimostra subito per induzione sulla lunghezza n di g),

$$\mathbf{e} \cdot g = (a_1, b_1, \ldots, a_n, b_n) \neq \mathbf{e}$$

e dunque $g \neq 1$. ∎

La scrittura, per $g \in H * K$, $g = a_1 b_1 \ldots a_n b_n$ come in (4.18) si dice *forma normale* dell'elemento g. Alcune immediate ma basilari conseguenze della Proposizione 4.10 sono descritte negli esercizi 4.21 e 4.22. Va da sé che, da qui in avanti (ad esempio negli esercizi) adotteremo come nella seconda parte della dimostrazione precedente, la convenzione di identificare, in un prodotto libero (interno o esterno) $G = H * K$, gli elementi di H e di K con le loro immagini in G (cioè, per $h \in H$, scriveremo h per $\alpha_H(h)$, etc.)

4.5 Varietà

Sia $w = w(x_1, \ldots, x_n)$ un elemento del gruppo libero F_n generato da $\{x_1, \ldots, x_n\}$, e sia G un gruppo fissato. Per ogni n-upla ordinata $\bar{g} = (g_1, \ldots, g_n)$ di elementi $g_i \in G$, esiste allora un unico omomorfismo $\phi_{\bar{g}} : F \to G$ tale che $x_i\phi_{\bar{g}} = g_i$ per ogni $i = 1, \ldots, n$; scriviamo

$$w(\bar{g}) = w(g_1, \ldots, g_n) = w\phi_{\bar{g}} \tag{4.20}$$

(quindi, $w(\bar{g})$ non è altro che la "sostituzione" di $g_1, \dots g_n$ in w e la sua conseguente valutazione nel gruppo G). Il *sottogruppo verbale* $w(G)$ di G associato alla parola w è il sottogruppo generato dall'insieme di tutti i valori (4.20) che la parola w assume in G, ovvero

$$w(G) = \langle w(\bar{g}) \mid \bar{g} = (g_1, \dots, g_n),\ g_i \in G \rangle. \tag{4.21}$$

Ad esempio, se $w = [x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2 \in F_2$, allora, per ogni gruppo G, $w(G)$ è il sottogruppo derivato G'.
La definizione (4.21) si estende in modo naturale al caso di un insieme di più parole: sia F_ω il gruppo libero su un insieme numerabile $\{x_1, x_2, \dots\}$ di generatori e sia $\emptyset \neq W \subseteq F_\omega$; osservando che ogni parola $w \in W$ coinvolge un numero finito di generatori x_i, per ogni gruppo G, si definisce il sottogruppo verbale associato a W come

$$W(G) = \langle w(G) \mid w \in W \rangle. \tag{4.22}$$

Sia W come sopra e $w = w(x_{i_1}, \dots, x_{i_n}) \in W$. Sia G un gruppo e $\alpha \in Aut(G)$, allora per ogni n-upla $\bar{g} = (g_1, \dots, g_n)$ di elementi di G, posto $\bar{g}\alpha = (g_1\alpha, \dots, g_n\alpha)$, risulta $w(\bar{g}\alpha) = w(\bar{g})\alpha$. Si ha dunque immediatamente la seguente osservazione.

Proposizione 4.11. *Per ogni $W \subseteq F_\omega$ ed ogni gruppo G, il sottogruppo verbale $W(G)$ è un sottogruppo caratteristico di G.*

Sia $W \subseteq F_\omega$ come sopra; la **varietà** $\mathcal{V}(W)$ definita da W è la classe di tutti i gruppi G tali che $W(G) = 1$. Cioè la classe di tutti i gruppi G che soddisfano alla famiglia di "equazioni"

$$w(g_1, \dots, g_n) = 1 \qquad \forall g_1, \dots, g_n \in G \text{ e } \forall w \in W.$$

Ad esempio, la classe dei gruppi abeliani è la varietà definita da $W = \{[x_1, x_2]\}$. Dalla definizione, segue immediatamente che se $W \subseteq W_1 \subseteq F_\omega$ allora la varietà $\mathcal{V}(W_1)$ è contenuta in $\mathcal{V}(W)$. Inoltre, ogni varietà $\mathcal{V}(W)$ è chiaramente chiusa per sottogruppi e per immagini omomorfe, ed è facile provare che è chiusa per la formazione di prodotti cartesiani (ovvero, se $(G_i)_{i\in I}$ è una famiglia di gruppi appartenenti a $\mathcal{V}(W)$, allora $Car_{i\in I}G_i$ appartiene a $\mathcal{V}(W)$). Un fondamentale Teorema di Birkhoff mostra che queste proprietà di chiusura caratterizzano le classi di gruppi che sono varietà.

Teorema 4.12. (Birkhoff) *Una classe di gruppi è una varietà se e soltanto se è chiusa per sottogruppi, per quozienti e per prodotti cartesiani.*

Da ciò segue, ad esempio, che la classe dei gruppi periodici non è una varietà (dato che il prodotto cartesiano dei gruppi ciclici C_n con $n \in N$ non è un gruppo periodico). Un interessante tipo di varietà si definisce mediante il concetto di esponente. *L'esponente* di un gruppo G è, se esiste, il minimo intero $n \geq 1$ tale che $g^n = 1$ per ogni $g \in G$; altrimenti si dice che G ha esponente infinito. È chiaro che se G ha esponente finito n allora G è periodico e n è il minimo comune multiplo degli ordini dei suoi elementi. La classe dei gruppi di esponente finito non costituisce una varietà; fissato però un numero intero $n \geq 1$ la classe dei gruppi di esponente che divide n è la varietà definita dalla parole x^n. Come già accennato alla fine del capitolo precedente, per ogni gruppo G il sottogruppo verbale definito da x^n si denota con G^n ed ìl sottogruppo di G generato dall'insieme di tutte le potenze n-esime $G^n = \langle \{g^n \mid g \in G\} \rangle$.

Gruppi liberi in una varietà. Tornando al caso generale, per ogni insieme di parole $W \subseteq F_\omega$ ed ogni gruppo G, il quoziente $G/W(G)$ appartiene alla varietà $\mathcal{V}(W)$. Questa osservazione ci consente di formulare la nozione seguente.
Fissata una classe $\mathcal{B}$ di gruppi, un gruppo F si dice *libero nella classe* $\mathcal{B}$, con sistema di generatori X se F appartiene alla classe $\mathcal{B}$ e la proprietà universale (4.9) è soddisfatta per ogni gruppo G nella classe $\mathcal{B}$. Come nel caso generale (un gruppo è libero se è libero nella classe di tutti i gruppi), il tipo di isomorfismo dei gruppi $\mathcal{B}$-liberi, quando esistono, dipende solo dalla cardinalità del sistema di generatori X. Il punto è che non tutte le classi contengono gruppi liberi con sistema di generatori di qualsiasi cardinalità. In effetti questa proprietà è appannaggio delle varietà.
Sia, infatti, $\mathcal{V} = \mathcal{V}(W)$ la varietà definita da $W \subseteq F_\omega$, e sia $U = F(X)$ il gruppo libero su X, con immersione $\tau : X \to U$. Allora $F = U/W(U)$ appartiene a $\mathcal{V}$. Poniamo $\bar{\tau} : X \to F$ la composizione di τ con la proiezione $\pi : U \to U/W(U)$. Chiaramente $\langle X\bar{\tau}\rangle = F$. Sia G un gruppo nella varietà $\mathcal{V}$ e $f : X \to G$ un'applicazione. Per la Proposizione 4.3 esiste un omomorrfismo $\alpha : U \to G$ tale che $\tau\alpha = f$; poiché G appartiene a $\mathcal{V}$, $W(G) = 1$ e quindi $W(U) \leq \ker(\alpha)$: dunque α si fattorizza come $\alpha = \pi\bar{\alpha}$ con $\bar{\alpha} : U \to G$ omomorfismo. Allora

$$\bar{\tau}\bar{\alpha} = \tau\pi\bar{\alpha} = \tau\alpha = f \tag{4.23}$$

inoltre, poiché $X\bar{\tau}$ genera F, $\bar{\alpha}$ è l'unico omomorfismo $F \to G$ che realizza (4.23). Abbiamo pertanto provato la seguente

Proposizione 4.13. *Fissato un insieme di parole $W \subseteq F_\omega$, sia X un insieme e U il gruppo libero su X. Allora $U/W(U)$ è un gruppo libero su X nella varietà $\mathcal{V}(W)$.*

Ad esempio, ed è un caso semplice in apparenza in realtà complicatissimo, sia $n \geq 1$: la varietà definita dalla parola x^n'e quella costituita da tutti i gruppi il cui esponente divide n; per ogni $1 \leq r \in \mathbb{N}$, il gruppo libero di rango r in tale varietà si chiama *gruppo di Burnside* e si denota con $B(r, n)$. Il problema se $B(r, n)$ sia un gruppo finito per ogni $r, n \in \mathbb{N}$ ([problema di Burnside) è rimasto aperto per diversi decenni da quando fu formulato da Burnside nel 1902; la ripsoste è on generale negativa, ma ancora aperte sono molte questioni riguardanti i gruppi $B(r, n)$, ad esempio, se $B(2, 5)$ sia o meno finito (su questo argomento torneremo nella sezione 7.4).

Gruppi abeliani. Un caso molto più abbordabile è invece quello della varietà dei gruppi abeliani (definita dalla parola $[x_1, x_2]$). Osserviamo, per cominciare, che in ogni gruppo G il sottogruppo verbale rispetto alla varietà dei gruppi abeliani è il sottogruppo derivato G'; quindi, a norma della Proposizione 4.13, i gruppi liberi in tale varietà sono i quozienti F/F' con F gruppo libero. Osserviamo anche che se A è un gruppo abeliano e X un suo sistema di generatori allora gli elementi di A, già prodotti del tipo (4.3), per via della commutatività possono essere riscritti (non necessariamente in modo unico) "raccogliendo" i termini con la stessa base, nella forma

$$g = x_1^{\beta_1} \dots x_n^{\beta_n} \tag{4.24}$$

con $x_1, \dots x_n$ elementi *distinti* di X, e $\beta_1, \dots, \beta_n \in \mathbb{Z}$.

Dato un insieme X sia $F = F(X)$ il gruppo libero su X, $A(X) = F/F'$ e

$$\mathbb{Z}^{(X)} = Dir_{x\in X}\mathbb{Z}_x$$

dove, per ogni $x \in X$, $\mathbb{Z}_x \simeq \mathbb{Z}$. Per $x \in X$ si consideri la funzione $\delta_x \in \mathbb{Z}^{(X)}$ definita da

$$\delta_x(y) = \begin{cases} 1 & \text{se} \quad y = x \\ 0 & \text{se} \quad y \neq x \end{cases}$$

Poiché $\{\delta_x \mid x \in X\}$ è un sistema di generatori di $\mathbb{Z}^{(X)}$, esiste un omomorfismo dal gruppo libero $F = F(X)$ in $\mathbb{Z}^{(X)}$, tale che $x \to \delta_x$. Il nucleo di tale omomorfismo contiene F', quindi, posto per ogni $x \in X$, $\bar{x} = xF'$, c'è un omomorfismo suriettivo $\alpha : A(X) \to \mathbb{Z}^{(X)}$ tale che $\bar{x} \to \delta_x$ per ogni $x \in X$. Ora, ogni elemento di A si scrive nella forma (4.24): $g = \bar{x}_1^{\beta_1} \dots \bar{x}_n^{\beta_n}$ con $x_1, \dots x_n$ elementi distinti di X; se $g \in \ker \alpha$,

$$1 = g\alpha = \delta_1^{\beta_1} \dots \delta_n^{\beta_n}$$

da cui segue $\beta_i = 0$ per ogni $i = 1, \dots, n$ e quindi $g = 1$. Pertanto, α è un isomorfismo.

Convenendo di denominare *gruppo abeliano libero* un gruppo libero nella varietà dei gruppi abeliani, abbiamo quindi provato la seguente proposizione.

Proposizione 4.14. *Sia X un insieme e F il gruppo libero su X. Allora F/F' è un gruppo abeliano libero su X, ed è isomorfo al prodotto diretto $\mathbb{Z}^{(X)}$. In particolare, se F ha rango finito $n \geq 1$, allora $F/F' \simeq \mathbb{Z}^n$.*

Un fatto che (alla fine del prossimo capitolo) vedremo esteso a varietà definite da commutatori iterati.

4.6 Esercizi IV

Sezione 4.1

Esercizio 4.1. Sia F un gruppo libero. Si provi che ogni $1 \neq g \in F$ ha ordine infinito, e che se F ha rango almeno 2, $Z(F) = 1$.

Esercizio 4.2. (Proprietà Proiettiva dei gruppi liberi) Siano G, H gruppi ed F un gruppo libero. Si provi che se $\phi : G \to H$, $\alpha : F \to H$ sono omomorfismi tali che $Im(\alpha) \leq Im(\phi)$, allora esiste un omomorfismo $\beta : F \to G$ tale che $\alpha = \beta\phi$.

Esercizio 4.3. Sia G un gruppo e sia $N \trianglelefteq G$ tale che G/N è un gruppo libero. Si provi che esiste un complemento H di N in G.

Esercizio 4.4. Sia X un insieme, $\emptyset \neq Y \subseteq X$, e sia $F = F(X)$ il gruppo libero su X. Si provi che F/Y^F è libero su $X \setminus Y$.

Esercizio 4.5. Sia F un gruppo libero su X. Per ogni $g \in F$ e $x \in X$ sia $\delta_x(g)$ la somma degli esponenti con cui compare il generatore x nell'espressione di g come parola.

(a) Si provi che per ogni $g, h \in F$, $\delta_x(gh) = \delta_x(g) + \delta_x(h)$.

(b) Si provi che $F' = \{g \in F \mid \delta_x(g) = 0 \ \forall x \in X\}$.

Esercizio 4.6. Sia F un gruppo libero su $\{x, y\}$. Si provi che esiste un unico automorfismo ϕ di F tale che $x\phi = x$ e $y\phi = yx$; si provi quindi che ϕ non è un automorfismo interno.

Sezione 4.2

Esercizio 4.7. Si provi che il gruppo simmetrico S_3 e il gruppo alterno A_4 hanno, rispettivamente, presentazioni,

$$S_3 = \langle x, y \mid y^3 = x^2 = (xy)^2 = 1 \rangle \qquad A_4 = \langle x, y \mid y^3 = x^2 = (xy)^3 = 1 \rangle.$$

Esercizio 4.8. Sia p un primo, si provi che il gruppo con presentazione

$$\langle x, y \mid x^p = y^p = x^{-2}y^{-1}xy = 1 \rangle$$

è il gruppo ciclico di ordine p.

Esercizio 4.9. Siano $G = \langle X \mid R \rangle$ e $H = \langle Y \mid S \rangle$ due gruppi con rispettive presentazioni. Si descriva una presentazione del gruppo $G \times H$.

Esercizio 4.10. Sia $p \geq 3$ un primo. Si provi che il gruppo

$$G = \langle x, y \mid x^p = y^p = (xy)^p = 1 \rangle$$

è infinito (mentre, per $p = 2$, il gruppo è abeliano di ordine 4). [sugg. Detta $\omega = 2^{\frac{2\pi i}{p}}$ una radice primitiva p-esima dell'unità, si considerino le trasformazioni del piano complesso f, g definite da, per ogni $z \in \mathbb{C}$, $f : z \mapsto \omega z$ e $g : z \mapsto \omega z + 1$ e sia $H + \langle f, g \rangle$. Si provi che $f^p = g^p = (fg)^p = 1$, quindi $H \ldots$]

Esercizio 4.11. Si descriva (ad esempio come prodotto semidiretto di gruppi altrimenti noti) il gruppo

$$\langle a, b, c \mid a^2 = b^2 = c^2 = (abc)^2 = 1 \rangle.$$

Esercizio 4.12. Si provi che il gruppo dato dalla presentazione

$$\langle x_1, x_2, x_3, \ldots \mid x_{n+1}^{n+1} = x_n, \forall n \geq 1 \rangle$$

è il gruppo additivo $(\mathbb{Q}, +)$.

Sezione 4.3

Esercizio 4.13. Si provi che il sottogruppo di $SL(2, \mathbb{R})$,

$$G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$$

non è un gruppo libero.

Esercizio 4.14. Sia Z il gruppo delle matrici scalari non nulle di $SL(2, \mathbb{C})$. Allora, il gruppo $G = PSL(2, \mathbb{C}) = SL(2, \mathbb{C})/Z$ opera sulla sfera $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, mediante

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az + b}{cz + d}.$$

Applicando il Lemma del Ping–Pong a tale azione, sii trovi in G un sottogruppo libero di rango 2.

Esercizio 4.15. Generalizzando in modo opportuno il Lemma del Ping–Pong, se ne trovi un sottogruppo di $PSL(2,\mathbb{C})$ che sia libero di rango 3.

Esercizio 4.16. Sia F_2 il gruppo libero di rango due. Si trovino tre elementi di F_2 tali che il sottogruppo da essi generato sia libero di rango 3.

Esercizio 4.17. Sia G un gruppo una cui presentazione ha n generatori e s relazioni. Si provi che se $s < n$, G è infinito.

Esercizio 4.18. Sia F un gruppo libero di rango finito. Si provi che F non è isomorfo ad un suo quoziente proprio.

Sezione 4.4

Esercizio 4.19. Siano $x,\ y$ le matrici definite nell'esempio 4.8. Si provi che $\langle x, y\rangle = SL(2,\mathbb{Z})$.

Esercizio 4.20. Si enunci e si dimostri un Lemma del Ping–Pong (del tipo del lemma 4.6) per il prodotto libero di due gruppi.

Esercizio 4.21. Siano $H,\ K$ gruppi e sia $g \in H * K$; si provi che $H \cap H^g \neq 1$ se e solo se $g \in H$. Si provi che se $H \neq 1 \neq K$ allora $Z(H * K) = 1$.

Esercizio 4.22. Sia $G = H * K$. Si provi che ogni elemento periodico di G è coniugato ad un elemento di $H \cup K$. Si deduca che se H e K sono senza torsione allora $H * K$ è senza torsione.

Esercizio 4.23. Si provi che se H e K sono gruppi residualmente finiti allora anche $H * K$ è residualmente finito.

Esercizio 4.24. Siano H e K gruppi finiti di ordine coprimo; si provi che

$$Out(H * K) \simeq Aut(H) \times Aut(K).$$

Esercizio 4.25. Siano $H,\ K$ gruppi e $G = H * K$; si provi che $G/G' \simeq H/H \times K/K'$.

Esercizio 4.26. Siano H e K gruppi non banali e $G = H * K$; si provi che il sottogruppo $[H, K]$ di G è un gruppo libero nel sistema di generatori $\{[x, y] \mid x \in H,\ y \in K\}$.

Sezione 4.5

Esercizio 4.27. Sia $G = C_{p^\infty}$, il p-gruppo di Prüfer. Si provi che $\{1\}$ e G sono i soli sottogruppi verbali di G.

Esercizio 4.28. (B.H. Neumann) Sia F un gruppo libero e sia N un sottogruppo di F tale che $\phi(N) \leq N$ per ogni endomorfismo ϕ di F (un sottogruppo con questa proprietà si dice *pienamente invariante*). Si provi che N è un sottogruppo verbale di F.

Nei seguenti esercizi F_ω è il gruppo libero di rango numerabile $F[x_1, x_2, \dots]$.

Esercizio 4.29. Siano $w, u \in F_\omega$ Si provi che $\mathcal{V}(w) = \mathcal{V}(w^u)$.

Esercizio 4.30. Sia $w \in F_\omega$ una parola in cui il generatore x_1 ha una sola occorrenza e x_1^{-1} non compare. Si provi che $\mathcal{V}(w)$ è la varietà banale (cioè quella che comprende il solo gruppo banale).

Esercizio 4.31. Siano $w, w_1 \in F_\omega$ e $\mathcal{V} = \mathcal{V}(w)$ la varietà definita da w. Si provi che la classe dei gruppi G tali che $w_1(G) \in \mathcal{V}$ è una varietà.

Esercizio 4.32. Sia $W \subseteq F_\omega$ tale che $W \not\subseteq F'_\omega$. Si provi che esiste un $1 \leq n \in \mathbb{N}$ tale che $\{g^n \mid g \in G\} = 1$ per ogni $G \in \mathcal{V}(W)$. [sugg. ricordarsi dell'esercizio 4.5].

Esercizio 4.33. Si generalizzi il risultato dell'esercizio 4.27 provando che in ogni gruppo abeliano divisibile D i soli sottogruppi verbali sono 1 e D.

Esercizio 4.34. Si descrivano tutte le varietà $\mathcal{V}$ tali che ogni gruppo in $\mathcal{V}$ è abeliano.

Capitolo 5

Gruppi nilpotenti

5.1 Gruppi abeliani finitamente generati

Riprendiamo, prima di concentrarci sul caso finitamente generato, le considerazioni intorno ai gruppi liberi nella varietà dei gruppi abeliani, che chiamiamo *gruppi abeliani liberi*, iniziate al termine del capitolo precedente. Abbiamo provato che i gruppi abeliani liberi sono isomorfi al prodotto diretto di copie di $\mathbb{Z}$; più precisamente, il gruppo abeliano libero sull'insieme X è isomorfo al prodotto diretto $\mathbb{Z}^{(X)}$ (l'insieme della funzioni quasi ovunque zero da X in $\mathbb{Z}$).

Un sottoinsieme X di un gruppo abeliano A si dice *libero* se avviene che per ogni sottoinsieme finito $\{x_1, \dots x_n\}$ di elementi distinti di X, ed ogni n-upla $(\beta_1, \dots, \beta_n) \in \mathbb{Z}^n$

$$x_1^{\beta_1} \dots x_n^{\beta_n} = 1 \quad \Leftrightarrow \quad \beta_1 = \dots = \beta_n = 0. \tag{5.1}$$

Da tale definizione segue facilmente che se X è un sottoinsieme libero di generatori del gruppo abeliano A allora ogni elemento $a \in A$ si scrive in modo unico nella forma:

$$a = \prod_{x \in X} x^{\beta_x} \tag{5.2}$$

con $\beta_x \in \mathbb{Z}$ per ogni $x \in X$, e $\beta_x = 0$ tranne che per un numero finito di $x \in X$. Dunque, in questo caso, ad ogni $a \in A$ è associata naturalmente un'applicazione $\phi_a : X \to \mathbb{Z}$ data da $x\phi_a = \beta_x$ per ogni $x \in X$, e ciò, definisce a sua volta una biezione $A \to \mathbb{Z}^{(X)}$, che si verifica immediatamente essere un isomorfismo. Quindi, un gruppo abeliano che ammette un sistema libero di generatori è un gruppo libero; viceversa, è pressoché ovvio che un gruppo abeliano libero su X ammette proprio X come sistema libero di generatori. Abbiamo dunque provato il fatto segeuente.

Teorema 5.1. *Sia A un gruppo abeliano; sono equivalenti*

1. *A è libero;*
2. *A ammette un sistema libero di generatori;*
3. *A è libero se e solo se è prodotto diretto di copie di $\mathbb{Z}$.*

A questo punto, un'importante proprietà dei gruppi abeliani liberi.

Proposizione 5.2. (Proprietà proiettiva dei gruppi abeliani liberi) *Sia A un gruppo abeliano e $B \leq A$ tale che A/B è libero. Sia $X \subseteq A$ tale che $\{Bx \mid x \in X\}$ è un sistema libero di generatori di A/B. Allora $A = B \times \langle X \rangle$.*

DIMOSTRAZIONE. Poiché $\{Bx \mid x \in X\}$ è un sistema di generatori di A/B, è chiaro che $A = B\langle X \rangle$. Dato che $\langle X \rangle$ è normale in A (che è abeliano), basta provare che $B \cap \langle X \rangle = 1$. Sia dunque $g \in B \cap \langle X \rangle$; allora $g = x_1^{\beta_1} \dots x_n^{\beta_n}$, con $x_1, \dots x_n$ elementi distinti di X, e $\beta_1, \dots, \beta_n \in \mathbb{Z}$. Ma allora, passando al quoziente,

$$1_{A/B} = B = Bg = Bx_1^{\beta_1} \dots x_n^{\beta_n} = (Bx_1)^{\beta_1} \cdots (Bx_n)^{\beta_n}$$

e poiché $\{Bx \mid x \in X\}$ è un sistema libero di generatori di A/B, dalla definizione segue $g = 1$. ∎

Ricordiamo ancora che un gruppo G si dice *senza torsione* se ogni suo elemento non banale ha ordine infinito; cioè se

$$\forall x \in G : \ |x| < \infty \Rightarrow x = 1.$$

Abbiamo già notato (Proposizione 2.12) che se A è un gruppo abeliano, allora l'insieme $T(A) = \{a \in A \mid |a| \neq \infty\}$ degli elementi periodici di A è un sottogruppo (detto il *sottogruppo di torsione* di A) e che $A/T(A)$ è un gruppo abeliano senza torsione.

Struttura dei gruppi abeliani f.g. Passiamo ora ai gruppi abeliani finitamente generati, iniziando proprio dal caso senza torsione. Ricordo che se G è un gruppo finitamente generato, $d(G)$ indica la cardinalità minima di un sistema di generatori di G.

Lemma 5.3. *Sia A un gruppo abeliano finitamente generato; le seguenti proprietà sono equivalenti*

(1) *$A = \langle x_1 \rangle \times \cdots \times \langle x_d \rangle$, con $\langle x_1 \rangle$ ciclico infinito e $d = d(A)$; cioè $A \simeq \mathbb{Z}^d = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{d}$;*

(2) *A è libero;*

(3) *A è senza torsione.*

DIMOSTRAZIONE. (1) ⇒ (2) e (2) ⇒ (3) seguono dal Teorema 5.1.

(3) ⇒ (1). Sia A gruppo abeliano f.g. e senza torsione. Procediamo per induzione su $d(A)$. Se $d(A) = 1$, A è ciclico e isomorfo a $\mathbb{Z}$. Sia $d = d(A) \geq 2$ e sia $\{x_1, \dots, x_d\}$ un sistema di generatori di A; poniamo

$$B = \{a \in A \mid a^t \in \langle x_1 \rangle, \text{per qualche t} \geq 1\}.$$

Si verifica facilmente che $B \leq A$. Inoltre A/B è senza torsione: se infatti $(Ba)^k = B$, per qualche $k \geq 1$ ed $a \in A$, allora $a^k \in B$ e quindi $(a^k)^t = a^{kt} \in \langle x_1 \rangle$ per qualche $t \geq 1$ da cui segue $a \in B$ e pertanto $Ba = B = 1_{A/B}$. Ora, A/B è generato da $\{Bx_2, \dots, Bx_n\}$; possiamo quindi applicare l'ipotesi induttiva e concludere che A/B è isomorfo ad un prodotto diretto di un numero finito di gruppi ciclici infiniti. In particolare, per il passo (1)⇒(2) è libero e dunque, dalla Proposizione 5.2, deriva che $A = B \times C$, dove $C \simeq A/B$. Da ciò segue,

anche, che $B \simeq A/C$ è f. g. dunque $B/\langle x_1\rangle$ è f.g. e siccome è - per definizione - periodico, per il lemma 5.4, $B/\langle x_1\rangle$ è finito, diciamo $|B/\langle x_1\rangle| = k$. Allora, porre $b \mapsto b^k$ definisce un omomorfismo $\phi : B \to \langle x_1\rangle$. Poiché B è senza torsione, $\ker\phi = \{b \in B \mid b^k = 1\} = \{1\}$, dunque ϕ è iniettivo e B è isomorfo ad un sottoogruppo di $\langle x_1\rangle$; pertanto B è ciclico infinito. In conclusione $A = B \times C \simeq B \times A/B$ è un prodotto diretto di un numero finito di gruppi ciclici infiniti. È chiaro che il numero di tali fattori coincide con $d(G)$. ∎

Osserviamo che, mentre le implicazioni (1)⇒(2)⇒(3) valgono anche nel caso di un gruppo abeliano non finitamente generato (in tal caso d è un cardinale qualsiasi), il gruppo additivo $\mathbb{Q}$ dei razionali, ovvio esempio, mostra che l'implicazione (3)⇒(1) non vale quando A non è finitamente generato.

Il passo successivo è rappresentato dal caso periodico: e questo si riduce al caso dei gruppi abeliani finiti. Un'immediata conseguenza dell'osservazione (4.24) è infatti il seguente

Lemma 5.4. *Sia $X = \{x_1, \dots, x_n\}$ un sistema di generatori di un gruppo abeliano A. Se, per $i = 1, \dots, n$, $|x_i| \neq \infty$, allora $|A| \leq |x_1| \cdots |x_n|$.*

Lemma 5.5. *Sia A un gruppo abeliano finito, e $g \in A$ tale che $|g|$ è massimo. Allora*

1. *$|g| = m.c.m.\{|a| \mid a \in A\}$;*
2. *esiste $B \leq A$ tale che $A = \langle g\rangle \times B$.*

Dimostrazione. 1) Basta dimostrare che $|a|$ divide $|g|$ per ogni $a \in A$. Supponiamo che, per $a \in A$, ciò non sia vero; allora esiste un primo p tale che $|a| = p^n t$, $|g| = p^m s$, con $(p,t) = 1 = (p,s)$ e $m < n$. Posto $a_1 = a^t$ e $g_1 = g^{p^m}$, si ha $|a_1| = p^n$ e $|g_1| = s$, e quindi, in particolare $\langle a_1\rangle \cap \langle g_1\rangle = \{1\}$. Ne segue che $|a_1 g_1| = m.c.m.\{|a_1|, |g_1|\} = p^n s > p^m s = |g|$, 1. contro la scelta di g.

2) Se $A = \langle g\rangle$ basta porre $B = \{1\}$. Supponiamo ora $|A/\langle g\rangle| = p$, con p primo e sia a un elemento di ordine minimo in $A \setminus \langle g\rangle$. Allora $a^p \in \langle g\rangle$ e se q è un divisore primo di $|a|$ si ha $a^q \in \langle g\rangle$; dunque $q = p$, e pertanto $|a| = p^t$ per $t \geq 1$. Per il punto *1.* p^t divide $|g|$; quindi $\langle g\rangle$ ha un unico sottogruppo $\langle g_1\rangle$ di ordine p^t, e $\langle g_1^p\rangle = \langle a^p\rangle$. Allora esiste $s \geq 1$ tale che $a^p = g_1^{sp}$. Posto $b = a^{-1} g_1^s$, si ha $b^p = (a^p)^{-1} g_1^{sp} = 1$ e $b \notin \langle g\rangle$. Dunque, per la scelta di a, $b = 1$; da ciò segue $\langle g\rangle \cap \langle a\rangle = 1$ e, di conseguenza, $A = \langle g\rangle \times \langle a\rangle$.
Procediamo ora per induzione su $n = |A/\langle g\rangle|$. Sia $n > 1$ e sia p un divisore primo di n; allora esiste un sottogruppo $C/\langle g\rangle$ di $A/\langle g\rangle$ di ordine p. Per il caso provato sopra, esiste $D \leq C$ tale che $C = \langle g\rangle \times D$. Poniamo $\overline{A} = A/D$. Allora, poiché in tal caso, $|Dg| = |g|$, Dg è un elemento di ordine massimo di $\overline{A}$. Ora, $|\overline{A} : \langle Dg\rangle| = |\overline{A} : C/D| = |A : C| = n/p$ e, per ipotesi induttiva, esiste $B/D \leq \overline{A}$ (con $D \leq B \leq A$) tale che $\overline{A} = \langle Dg\rangle/D \times B/B = C/D \times B/D$. Questo implica $\langle g\rangle B = BD\langle g\rangle = BC = A$ e $\langle g\rangle \cap B = C \cap B \cap \langle g\rangle = D \cap \langle g\rangle = 1$. Dunque $A = \langle g\rangle \times B$, e ciò completa la dimostrazione. ∎

Possiamo ora provare il fondamentale teorema che descrive i gruppi abeliani finitamente generati. Lo enunciamo in notazione additiva, perché si tratta di un risultato che ha molte applicazioni anche al di fuori della teoria dei gruppi astratti, dove in genere viene appunto utilizzato in notazione additiva.

Teorema 5.6. *Sia A un gruppo abeliano finitamente generato. Esistono $n, m \in \mathbb{N}$, e $d_1, \dots, d_m \geq 1$ con $d_{i+1}|d_i$ (il caso $m = 0$, indica che A è senza torsione e che i d_i non ci sono) tali che*

$$A \simeq \mathbb{Z}^n \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}.$$

Inoltre i parametri $n, m, d_1, \dots, d_m$ con le proprietà sopraddette sono univocamente determinati da A.

Dimostrazione. Sia A un gruppo abeliano finitamente generato e T il suo sottogruppo di torsione. Per la Proposizione 2.12, A/T è senza torsione ed è finitamente generato; dunque, per il Lemma 5.3, $A/T \simeq Z^n$ per un intero $n \geq 0$ univocamente determinato ($n = d(G/T)$, con $n = 0$ se $A = T$). Per la Proposizione 5.2, $A = T \oplus C$ con $C \simeq A/T \simeq \mathbb{Z}^n$. In parrticolare, $T \simeq A/C$ è finitamente generato e quindi (Lemma 5.4) è finito. Dunque

$$A \simeq T \oplus Z^n$$

e possiamo limitarci al caso di un gruppo abeliano finito $A = T$. Si procede per induzione su $|T|$. Sia g_1 un elemento di ordine massimo in T, sia $d_1 = |g_1|$ (dunque $\langle g_1 \rangle \simeq \mathbb{Z}/d_1\mathbb{Z}$) ed osserviamo che, per il punto *1.* del Lemma 5.5, d_1 è univocamente determinato da T (quindi da A); inoltre, per il punto *2.* del medesimo Lemma, $T = \langle g_1 \rangle \oplus A_1$. Per ipotesi induttiva, A_1 è la somma diretta di gruppi ciclici $A_1 = \langle g_2 \rangle \oplus \cdots \oplus \langle g_m \rangle$, con $d_{i+1} = |g_{i+1}|$ che divide $d_i = |g_i|$ per $i = 2, \dots, m-1$. Poichè d_2 divide d_1 per il Lemma 5.5, si conclude che

$$A = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \cdots \oplus \langle g_m \rangle \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

con $d_{i+1}|d_i$ per ogni $i = 1, \dots, m-1$. La conclusione della dimostrazione che i d_i sono univocamente determinati è lasciata al lettore. ∎

5.2 Gruppi nilpotenti

Quello di gruppo nilpotente è un'estensione piuttosto naturale (qualsiasi cosa possa significare questo in matematica) del concetto di gruppo abeliano.
Per ogni $n \geq 1$ si definisce induttivamente la parola $\gamma_n \in F_\omega$, ponendo $\gamma_1 = x_1$,

$$\gamma_2 = [x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$$

e, per ogni $n \geq 3$,

$$\gamma_n = \phi_2(\gamma_{n-1}, x_n) = [\gamma_{n-1}, x_n]$$

L'elemento γ_n è detto *commutatore semplice* di peso n, e di solito si conviene di scrivere

$$\gamma_n = [x_1, x_2, \dots, x_n].$$

Quindi, γ_2 è la parola che definisce come varietà i gruppi abeliani: cioè - con le notazioni della sezione precedente - la varietà $\mathcal{V}(\gamma_2)$ coincide con la famiglia di tutti i gruppi abeliani, e per ogni gruppo G il sottogruppo verbale $\gamma_2(G)$ è il sottogruppo derivato G'.
Allo stesso modo, per ogni gruppo G ed ogni $n \geq 1$, risulta definito il sottogruppo verbale

$$\gamma_n(G) = \langle [g_1, \dots, g_n] \mid g_1, \dots g_n \in G \rangle,$$

ed è chiaro che, per $1 \leq n$, $\gamma_{n+1}(G) \leq \gamma_n(G)$. La serie

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \geq \cdots$$

si chiama *serie centrale discendente* di G e, per ogni $n \geq 1$, il sottogruppo $\gamma_{n+1}(G)$ si chiama n–esimo termine della serie centrale discendente di G (ovviamente, $\gamma_2(G)$ continua a chiamarsi sottogruppo derivato). Per quanto osservato nella sezione 4.5, $\gamma_n(G)$ è un sottogruppo caratteristico di G. Inoltre, per ogni $N \trianglelefteq G$ e $n \geq 1$ si ha $\gamma_n(G/N) = \gamma_n(G)N/N$, e per ogni $H \leq G$, $\gamma_n(H) \leq H \cap \gamma_n(G)$..

Un gruppo G si dice *nilpotente* se esiste $n \geq 1$ tale che $\gamma_n(G) = 1$. Se G è nilpotente, la *classe di nilpotenza* di G è il minimo $c \geq 0$ tale che $\gamma_{c+1}(G) = 1$.

Esempio 5.1. Descriviamo la serie centrale discendente di un gruppo diedrale $D = \langle y, x\rangle$, con $|x| = 2$ e $y^x = y^{-1}$. Per ogni $n \geq 1$,

$$[y^n, x] = y^{-n}(y^n)^x = y^{-n}y^{-n} = y^{-2n}.$$

Da ciò segue (come abbiamo già visto nell'esempio 2.6) che $D' = \gamma_2(D) = \langle y^2\rangle$, ed anche che, per $c \geq 2$

$$\gamma_c(D) = \langle y^{2^{c-1}}\rangle.$$

Sia $D = D_{2n}$ finito, e $n = 2^d m$ con m dispari; poniamo $A = \langle y^{2^d}\rangle$ e $B = \langle y^m\rangle$; da quanto appena visto, si conclude che $\gamma_c(D) = A \times B^{2^{c+1}} = A \times \langle (y^m)^{2^{c+1}}\rangle$. Quindi, D_{2n} è nilpotente se e soltanto se $n = 2^d$ ed in tal caso la sua classe di nilpotenza è proprio d.
Se invece $D = D_\infty$, D non è nilpotente ma si ha $\bigcap_{c\geq 1} \gamma_c(D) = 1$ □

È conveniente richiamare cosa si intende per commutatore tra sottogruppi: se $H.K \leq G$,

$$[H, K] = \langle [x, y] \mid x \in H,\ y \in K\rangle.$$

È anche utile ricordare (Lemma 2.21) che, per ogni $H, K \leq G$, $[H, K] \trianglelefteq \langle H, K\rangle$.
Per definizione, $[G, G] = \gamma_2(G)$; vedremo tra poche righe come questo si generalizza.

Serie centrali. Sia G un gruppo e $H \trianglelefteq K \leq G$: il fattore K/H si dice una *sezione centrale* di G se $[K, G] \leq H$. Osserviamo che, in tal caso, $[H, G] \leq [K, G] \leq H \leq K$, quindi $H, K \trianglelefteq G$; inoltre, per ogni $a \in K$ e $g \in G$, $[aH, gH] = [a, g]H = H = 1_{G/H}$, e dunque $K/H \leq Z(G/H)$. Provare il viceversa è altrettanto immediato. In conclusione, per ogni sezione $H \trianglelefteq K \leq G$,

$$K/H \text{ centrale } \Leftrightarrow\ H \trianglelefteq G \text{ e } K/H \leq Z(G/H). \tag{5.3}$$

Lemma 5.7. *Sia G un gruppo e $n \geq 1$. Allora $\gamma_{n+1}(G) = [\gamma_n(G), G]$.*

Dimostrazione. Per $n \geq 1$, sia $T = \gamma_{n+1}(G)$ e siano $g_1, \ldots, g_n, g_{n+1} \in G$. Allora

$$[\gamma_n(g_1, \ldots, g_n), g_{n+1}] = [[g_1, \ldots, g_n], g_{n+1}] = \gamma_{n+1}(g_1, \ldots, g_{n+1}) \in T$$

quindi $\gamma_n(g_1, \ldots, g_n)T \leq Z(G/T)$, e dunque

$$\frac{\gamma_n(G)T}{T} = \frac{\langle \gamma_n(g_1, \ldots, g_n) \mid g_1, \ldots, g_n \in G\rangle T}{T} \leq Z\Big(\frac{G}{T}\Big),$$

e pertanto $[\gamma_n(G), G] \leq T = \gamma_{n+1}(G)$. ∎

Una serie (finita) di un gruppo G

$$1 = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n$$

si dice *centrale* se, per ogni $i = 1, \ldots, n$, $[G_i, G] \leq G_{i-1}$.

Il Lemma 5.7 assicura che, se G è nilpotente, la serie $1 = \gamma_{c+1} \leq \cdots \leq \gamma_2() \leq G$ è centrale. Dualmente, per ogni gruppo G si definisce la *serie centrale ascendente* come la serie formata dai sottogruppi $\zeta_i(G)$, i quali sono definiti ricorsivamente come segue: $\zeta_0(G) = 1$ e, per $i \geq 1$,

$$\frac{\zeta_i(G)}{\zeta_{i-1}(G)} = Z\Big(\frac{G}{\zeta_{i-1}(G)}\Big).$$

In particolare, quindi, $\zeta_1(G) = Z(G)$ (e per ogni $i \geq 2$ il termine $\zeta_i(G)$ si chiama il centro n-esimo di G). L'osservazione (5.3) garantisce che se, per qualche $n \geq 1$, $\zeta_n(G) = G$, allora la serie $(\zeta_i(G))_{i=1,\ldots,n}$ è centrale.

Lemma 5.8. *Sia $1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n$ una serie centrale del gruppo G. Allora, per ogni $0 \leq i \leq n$,*

$$\gamma_{n-i+1}(G) \leq G_i \leq \zeta_i(G).$$

Dimostrazione. Sia $1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n$ una serie centrale di G.
Proviamo $G_i \leq \zeta_i(G)$ per induzione su i. Se $i = 0$ è per definizione. Per $i \geq 1$ si ha, applicando l'ipotesi induttiva, $[G_i, G] \leq G_{i-1} \leq \zeta_i(G)$, e quindi, come in (5.3),

$$\frac{G_i\zeta_{i-1}(G)}{\zeta_{i-1}(G)} \leq Z\Big(\frac{G}{\zeta_{i-1}(G)}\Big) = \frac{\zeta_i(G)}{\zeta_{i-1}(G)}$$

da cui $G_i\zeta_{i-1}(G) \leq \zeta_i(G)$, e quindi l'asserto.
Proviamo $\gamma_{n-i+1}(G) \leq G_i$ per induzione su $n - i$. Poiché $\gamma_1(G) = G = G_n$ l'affermazione è vera per $i = n$. Sia $n - i \geq 1$. Allora, applicando l'ipotesi induttiva e il Lemma 5.7,

$$G_i \geq [G_{i-1}, G] \geq [\gamma_{n-i}(G), G] = \gamma_{n-i+1}(G),$$

il che completa la dimostrazione. ∎

Proposizione 5.9. *Sia G un gruppo. Allora sono equivalenti:*

(1) *G è nilpotente;*

(2) *G ha una serie centrale;*

(3) *$\zeta_n(G) = G$ per qualche $n \geq 1$.*

Dimostrazione. (1) ⇒ (2) Immediato dalla definizione (e Lemma 5.7).
(2) ⇒ (3) Segue dal lemma 5.8.
(3) ⇒ (1) Segue ancora dal Lemma 5.8: poiché la serie $1 \leq \zeta_1(G) \leq \cdots \leq \zeta_n(G) = G$ è centrale, si ha $\gamma_{n-i}(G) \leq \zeta_i(G)$ per ogni $1 \leq i \leq n$, in particolare $\gamma_n(G) \leq \zeta_0(G) = 1$. ∎

Osserviamo che dal Lemma 5.8 discende che G è un gruppo nilpotente di classe c se e solo se c è il minimo intero positivo tale che $\zeta_c(G) = G$.

Oltre ai gruppi abeliani, esempi fondamentali di gruppi nilpotenti sono (come vedremo nelle prossime sezioni) i p-gruppi finiti e i gruppi di matrici unitriangolari.

Alcune proprietà dei gruppi nilpotenti. La prima che osserviamo è fondamentale ma piuttosto ovvia, e discende dal fatto che i sottogruppi $\gamma_n(G)$ sono verbali.

Proposizione 5.10. *La classe dei gruppi nilpotenti è chiusa per sottogruppi, quozienti e prodotti diretti.*

Le prossime proprietà che proviamo sono invece molto più specifiche dei gruppi nilpotenti.

Proposizione 5.11. *Sia G un gruppo nilpotente. Allora*

1. *se $1 \neq N \trianglelefteq G$, allora $N \cap Z(G) \neq 1$;*
2. *se H è un sottogruppo massimale di G, allora $H \trianglelefteq G$ e $|G/H| = p$ per un primo p.*

Dimostrazione. 1. Sia $G \neq 1$ nilpotente e sia $n \geq 1$ tale che $\zeta_n(G) = 1$.

1. Se $n = 1$, $G = Z(G)$ e non c'è nulla da provare. Sia $n \geq 2$, $1 \neq N \trianglelefteq G$, e sia $1 \leq k \leq n$ minimo tale che $N \cap \zeta_k(G) \neq 1$. Supponiamo per assurdo $k > 1$. Si ha allora

$$[N \cap \zeta_k(G), G] \leq N \cap \zeta_{k-1}(G) = 1,$$

quindi $1 \neq N \cap \zeta_k(G) \leq \zeta_1(G)$, una contraddizione.

2. Sia H un sottogruppo massimale di G e $1 \leq k \leq n$ massimo tale che $\zeta_k(G) \not\leq H$. Dunque $H \geq \zeta_{k-1}(G)$ e, per la massimalità di H, $H\zeta_k(G) = G$. Si ha allora

$$[H, G] = [H, H\zeta_k(G)] \leq H[H, \zeta_k(G)] \leq H\zeta_{k-1}(G) \leq H$$

e dunque $H \trianglelefteq G$. Infine, poiché H è massimale in G, G/H è un gruppo privo di sottogruppi propri non banali, quindi è un gruppo di ordine p per qualche primo p. ∎

Un lemma molto utile quando si ha a che fare con commutatori di sottogruppi è una conseguenza abbastanza diretta dell'identità di Hall-Witt per commutatori (punto (4) del Lemma 2.20):

Lemma 5.12. (Lemma dei tre sottogruppi). *Siano A, B, C sottogruppi del gruppo G, e sia $N \trianglelefteq G$ tale che $[A, B, C] \leq N$ e $[B, C, A] \leq N$. Allora $[C, A, B] \leq N$.*

Dimostrazione. Siano $a \in A$, $b \in B$ e $c \in G$. Per il Lemma 2.20, appunto, e le nostre ipotesi (tra le quali la normalità di N), si ha

$$([c, a^{-1}, b]^a)^{-1} = [a, b^{-1}, c]^b [b, a^{-1}, c]^a \in N.$$

Quindi $[c, a^{-1}, b] \in N$, per ogni $c \in C, a \in A$ e $b \in B$; il che significa che ogni $b \in B$ centralizza modulo il sottogruppo normale N ogni generatore di $[C, B]$. Dunque $[[C, A]N/N, BN/N] = 1$, il che equivale alla tesi $[C, A, B] = [[C, A], B] \leq N$. ∎

Il prossimo risultato serve a illustrare in che modo si può applicare il lemma dei 3 sottogruppi nello studio delle serie centrali.

Lemma 5.13. *Sia G un gruppo e $m, n \in \mathbb{N} \setminus \{0\}$. Allora*

1. $[\gamma_n(G), \gamma_m(G)] \leq \gamma_{n+m}(G)$;.
2. $\gamma_m(\gamma_n(G)) \leq \gamma_{mn}(G)$;
3. *se $n \geq m$, $[\gamma_m(G), \zeta_n(G)] \leq \zeta_{n-m}(G)$ (in particolare $[\gamma_n(G), \zeta_n(G)] = 1$).*

DIMOSTRAZIONE. (1) Per induzione su n. Se $n = 1$, $\gamma_1(G) = G$ e l'asserto è i Lemma 5.7. Sia $n \geq 2$, allora, per ipotesi induttiva

$$[G, \gamma_m(G), \gamma_{n-1}(G)] = [\gamma_{n-1}(G), \gamma_{m+1}(G)] \leq \gamma_{n+m}(G),$$

e inoltre, sempre per ipotesi induttiva,

$$[\gamma_m(G), \gamma_{n-1}(G), G] \leq [\gamma_{n+m-1}(G).G] = \gamma_{n+m}(G).$$

Per il Lemma dei tre sottogruppi, si conclude che

$$[\gamma_n(G), \gamma_m(G)] = [\gamma_{n-1}(G), G, \gamma_m(G)] \leq \gamma_{n+m}(G).$$

(2) Induzione su n. Per $m = 1$, si ha per definizione l'uguaglianza. Sia $m \geq 1$ e $N = \gamma_n(G)$; allora, applicando l'ipotesi induttiva e il punto precedente,

$$\gamma_m(N) = [\gamma_{m-1}(N), N] \leq [\gamma_{(m-1)n}(G), \gamma_n(G)] \leq \gamma_{(m-1)n+n}(G) = \gamma_{mn}(G).$$

(3) Induzione su m. Se $m = 1$, $\gamma_1(G) = G$ e l'asserto segue dalla definizione di $\zeta_n(G)$. Sia $m \geq 2$; allora, per le definizioni e l' ipotesi induttiva

$$[G, \zeta_n(G), \gamma_{m-1}(G)] \leq [\zeta_{n-1}(G), \gamma_{m-1}(G)] \leq \zeta_{(n-1)-(m-1)}(G) = \zeta_{n-m}(G).$$

Similmente, $[\zeta_n(G), \gamma_{n-1}(G), G] \leq [\zeta_{n-(m-1)}(G), G] \leq \zeta_{n-m}(G)$. Per il Lemma dei tre sottogruppi,

$$[\gamma_n(G), \zeta_n(G)] = [\gamma_{n-1}(G), G, \zeta_n(G)] \leq \zeta_{n-m}(G)$$

come si voleva. ∎

Dal punto (1) del lemma 5.13 e mediante una semplice induzione su n, si deduce il seguente importante fatto.

Corollario 5.14. *Per ogni gruppo G ed ogni $1 \leq n \in \mathbb{N}$, $G^{(n)} \leq \gamma_{2^n}(G)$. In particolare un gruppo nilpotente di classe c è risolubile con lunghezza derivata al più $[\log_2 c] + 1$.*

5.3 Gruppi nilpotenti finiti

Subito un'osservazione che da lungo tempo aspetta di essere provata.

Proposizione 5.15. *Sia p un numero primo. Un p-gruppo finito è nilpotente.*

DIMOSTRAZIONE. Sia P un p-gruppo finito, e $|P| = p^n$. Procediamo per induzione su n. Se $n = 0$, $P = 1$ e non c'è nulla da provare. Sia $n \geq 1$. Allora, per la Proposizione 3.7, $Z = Z(P) \neq 1$. Dunque $|P/Z| < p^n$ e, per ipotesi induttiva P/Z è nilpotente; ovvero esiste $c \geq 1$ tale che $\gamma_c(P)Z/Z = \gamma_c(P/Z) = 1$, quindi $\gamma_c(P) \leq Z$. Ma allora $\gamma_{c+1}(P) = 1$ e P è nilpotente. ∎

Un sottogruppo H di un gruppo G si dice *subnormale* in G (e si scrive $H \lhd\lhd G$) se H è un termine di una serie di G. cioè se esiste una catena finita

$$H = H \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G. \tag{5.4}$$

Sia $H \lhd\lhd G$ con $H \neq G$; allora, considerando una serie del tipo (5.4) in cui tutte i termini sono distinti, si ha in particolare $H \trianglelefteq H_1 > H$ e $G > H_{n-1} \trianglelefteq G$. Quindi, se H è un sottogruppo subnormale proprio di G, $H < \mathcal{N}_G(H)$ e $H^G < G$.

Lemma 5.16. *Sia G un gruppo nilpotente, allora ogni sottogruppo di G è subnormale. In particolare se H è un sottogruppo proprio di G, allora $H < \mathcal{N}_G(H)$ e $H^G < G$.*

DIMOSTRAZIONE. Sia G nilpotente, e $G = \zeta_n(G)$ con $n \geq 1$. Sia $H \leq G$; allora, come si verifica immediatamente, $\zeta_{i-1}(G)H \trianglelefteq \zeta_i(G)H$ per ogni $i = 1, \ldots, n$. Poiché $H = \zeta_0(G)H$ si conclude che H è subnormale in G. ∎

Corollario 5.17. *Siano G nilpotente e $H \leq G$ tale $\gamma_2(G)H = G$; allora $H = G$.*

DIMOSTRAZIONE. Siano G, H come nelle ipotesi. Si ha allora

$$\gamma_2(G/H^G) = \gamma_2(G)H^G/H^G = \gamma_2(G)H/H^G = G/H^G,$$

e dunque (per la nilpotenza di G/H^G), $G = H^G$ e $G = H$ dal Lemma 5.16. ∎

Vediamo ora la basilare e multipla caratterizzazione dei gruppi nilpotenti finiti.

Teorema 5.18. *Sia G un gruppo finito. Sono allora equivalenti le seguenti proprietà:*

(i) *G è nilpotente;*

(ii) *ogni sottogruppo di G è subnormale;*

(iii) *per ogni sottogruppo proprio H di G, $H < N_G(H)$;*

(iv) *ogni sottogruppo massimale di G è normale;*

(v) *G è il prodotto diretto dei suoi sottogruppi di Sylow.*

DIMOSTRAZIONE. (i)⇒(ii). È un caso particolare del Lemma 5.16.

(ii)⇒(iii). Supponiamo che G soddisfi (ii) e sia H un sottogruppo proprio di G; allora $H \lhd\lhd G$ e dunque $N_G(H) > H$.

(iii)⇒(iv). È chiaro che se H è un sottogruppo massimale di un gruppo G che soddisfa (iii) allora $N_G(H) = G$.

(iv)⇒(v). Sia G un gruppo che soddisfa (iv). È sufficiente provare che ogni sottogruppo di Sylow è normale. Sia dunque p primo che divide $|G|$ e sia P un p-sottogruppo di Sylow di

G. Assumiamo, per assurdo, $N_G(P) < G$; allora esiste un sottogruppo massimale M di G con $N_G(P) \leq M$. Per l'ipotesi su G, $M \trianglelefteq G$ e quindi, per l'argomento di Frattini (Lemma 3.13), $G = MN_G(P) = M$, una contraddizione. Quindi, $N_G(P) = G$ che è ciò che si voleva.

(v)⇒(i). Segue in modo diretto dalla Proposizione 5.15 e dall'esercizio 5.5. ∎

Come si vede dalle dimostrazioni, le implicazioni (i)⇒(ii), (ii)⇒(iii) e (iii)⇒(iv) valgono anche per gruppi infiniti, mentre si dimostra che nessuna di esse si inverte un generale (diremo qualcosa di più nella prossima sezione).

Sottogruppo di Frattini. Il Teorema 5.18 riconduce, nella sostanza, lo studio dei gruppi nilpotenti finiti a quello (in verità tutt'altro che agevole) dei p-gruppi finiti. Di questa importante parte della teoria dei gruppi finiti riportiamo solo un risultato, il Teorema della Base di Burnside, che ne è una delle basi. Per poterlo enunciare occorre introdurre il concetto di sottogruppo di Frattini.

Un sottogruppo H di un gruppo G si dice massimale se H è un elemento massimale nell'insieme parzialmente ordinato per inclusione di tutti i sottogruppi propri di G, ovvero se $H \neq G$ e per ogni $K \leq G$, $H \leq K \ \Rightarrow \ K = H$ o $K = G$. Il *sottogruppo di Frattini* $\Phi(G)$ è definito come l'intersezione di tutti i sottogruppi massimali di G, nel caso ce ne siano[1], mentre si pone $\Phi(G) = G$ se G non ha sottogruppi massimali. Chiaramente, $\Phi(G)$ è un sottogruppo caratteristico di G,

Esempio 5.2. I sottogruppi massimali di $\mathbb{Z}$ sono tutti e soli i $p\mathbb{Z}$ con p un numero primo. Di conseguenza

$$\Phi(\mathbb{Z}) = \bigcap_{p \text{ primo}} p\mathbb{Z} = \{0\}.$$

Similmente nel gruppo diedrale infinito $D_\infty = \langle a \rangle \rtimes \langle x \rangle$, con $|a| = \infty$ e $a^x = a^{-1}$, si riconosce che $\langle a \rangle$ è un sottogruppo massimale, così come ogni sottogruppo $\langle a^p, x \rangle$ con p un numero primo. Quindi $\Phi(D_\infty) = \langle a \rangle \cap \bigcap_{p \text{ primo}} \langle a^p, x \rangle = \bigcap_{p \text{ primo}} \langle a^p \rangle = 1$. □

Esempio 5.3. Siano p un primo, $C = C_{p^\infty}$ e x l'automorfismo di C che inverte ogni elemento. C è un sottogruppo massimale (e normale) del prodotto semidiretto $G = C \rtimes \langle x \rangle$. Supponiamo H sia un sottogruppo proprio di G, con $H \neq C$; allora $H \cap C < C$, quindi $H \cap C$ è ciclico finito ed esiste $K \leq C$ con $H \cap C < K < C$, per quanto osservato $K \trianglelefteq G$ e dunque $KH \leq G$, e $KH \cap C = k(H \cap C) = K$, dunque HK è sottogruppo proprio che propriamente contiene H. Quindi C è l'unico sottogruppo massimale di G, cioè $\Phi(G) = C$. □

In un gruppo finito G ogni sottogruppo proprio H è contenuto in un sottogruppo massimale M; dunque $\Phi(G)H \leq M < G$. Eleviamo al rango di lemma questa semplice osservazione:

Lemma 5.19. *Sia G un gruppo finito e $H \leq G$. Se $G = \Phi(G)H$ allora $H = G$.*

Teorema 5.20. *Sia G un gruppo finito; allora*

1. *$\Phi(G)$ è nilpotente;*
2. *G è nilpotente se e solo se $G/\Phi(G)$ è nilpotente.*

[1] Non tutti i gruppi ammettono sottogruppi massimali, ad esempio il gruppo additivo dei razionali $\mathbb{Q}$, i gruppi di Prüfer C_{p^∞} non hanno sottogruppi massimali.

DIMOSTRAZIONE. (1) Se $G = 1$ non c'è nulla da provare. Sia $G \neq 1$, sia p un divisore primo di $|\Phi(G)|$, e sia P un p-sottogruppo di Sylow di $Phi(G)$. Per l'argomento di Frattini,

$$G = \Phi(G)N_G(P),$$

e quindi, per il Corollario 6.1, $N_G(P) = G$. Dunque, a maggior ragione, $P \trianglelefteq \Phi(G)$. Ciò vale per ogni divisore primo di $|\Phi(G)|$ e pertanto $\Phi(G)$ è nilpotente.

(2) In una direzione l'affermazione è ovvia. Viceversa, supponiamo che $G/\Phi(G)$ sia nilpotente, e sia M un sottogruppo massimale di G; allora $M \geq \Phi(G)$ e quindi $M/\Phi(G)$ è un sottogruppo massimale di $G/\Phi(G)$. Per il Teorema 5.18, $M \trianglelefteq G$. Ciò vale per ogni sottogruppo massimale di G e dunque, sempre per 5.18, G è nilpotente. ∎

Teorema 5.21. *Sia P un p-gruppo finito. Allora $P/\Phi(P)$ è abeliano elementare e*

$$|P/\Phi(P)| = p^{d(P)}.$$

DIMOSTRAZIONE. Sia H un sottogruppo massimale del p-gruppo finito P. Allora, per la Proposizione 5.11 (e il Teorema di Lagrange) $H \trianglelefteq G$ e P/H è ciclico di ordine p. Quindi $\Phi(P) \geq P'$ e $P/\Phi(P)$ è un gruppo abeliano di esponente p; dunque un p-gruppo abeliano elementare.
Poniamo $|P/\Phi(P)| = p^n$. Poiché $P/\Phi(P)$ è un quoziente di P, $n = d(P/\Phi(P)) \leq d(P)$. Viceversa, siano $a_1, \dots a_n \in P$ tali che $a_1\Phi(P), \dots, a_n\Phi(P)$ è un sistema minimo di generatori di $P/\Phi(P)$ (ovvero una base di $P/\Phi(P)$ come spazio vettoriale su $GF(p)$), e sia $A = \langle a_1, \dots, a_n\rangle$. Allora $\Phi(P)A = P$ e dunque, per il Corollario 6.1, $A = P$ e dunque $d(P) \leq n$. ∎

Concludiamo questa sezione provando un risultato che non è fra quelli esattamente centrali, ma serve ad illustrare a livello elementare l'utilizzo del Teorema 5.18. Chi non fosse particolarmente interessato al lato tecnico dei gruppi finiti può tranquillamente passare alla sezione successiva.

Proposizione 5.22. *Sia G un gruppo finito in cui ogni sottogruppo proprio è nilpotente. Allora si verifica uno dei casi seguenti:*

- *G è nilpotente;*
- *$|G| = p^a q^b$ con p, q primi distinti e $G = P \rtimes Q$ dove $P \trianglelefteq G$ è un p-sottogruppo di Sylow, e Q un q-sottogruppo di Sylow; inoltre $Q = \langle x\rangle$ è ciclico e $\langle x^q\rangle \leq Z(G)$.*

DIMOSTRAZIONE. Sia G un gruppo finito in cui ogni sottogruppo proprio è nilpotente. Procedendo per induzione su $|G|$, proviamo innanzi tutto che G è risolubile.
Se $|G| = 1$ la cosa è banale. Sia $|G| \geq 1$. Sia M un sottogruppo massimale di G, allora M è nilpotente; se $M \trianglelefteq G$, G/M ha ordine primo quindi è risolubile e pertanto G è risolubile. Possiamo dunque supporre che nessun sottogruppo massimale di G sia normale. Siano ora L, M sottogruppi massimali distinti e tali che $A = M \cap L$ abbia ordine massimo possibile. Supponiamo che $\mathcal{N}_G(A)$ sia un sottogruppo proprio di G; allora esiste un sottogruppo massimale $U \geq \mathcal{N}_G(A)$. Ora, poiché M, L sono nilpotentti e A è un sottogruppo proprio di entrambi, dal Lemma 5.16 segue che $U \cap L > A$ e dunque, per la scelta di M, L, $U = L$; ma allo stesso modo $U = M$, che è assurdo. Dunque $\mathcal{N}_G(A) = G$. Se $A \neq 1$, G/A è risolubile per ipotesi induttiva e dunque (essendo A nilpotente) si conclude che G è risolubile.

Possiamo quindi supporre che $M \cap L = 1$ per ogni coppia di sottogruppi massimali distinti di G. Sia M un sottogruppo massimale. Poiché $\bigcup_{g\in G} M^g \neq G$ (esercizio 2.3), esiste un altro sottogruppo massimale L di G che non è coniugato a M. Poichè sottogruppi massimali distinti si intersecano banalmente, ed osservando che dato che assumiamo che né M né L sia normale, il numero di coniugati distinti di M (rispettivamente, di L) è $|G : M|$ (rispettivamenet, $|G : L|$), si ha

$$|G| > \Big|\bigcup_{g\in G}(M^g \setminus \{1\}) \cup \bigcup_{g\in G}(L^g \setminus \{1\})\Big| \geq |G : H|(|H| - 1) + |G : L|(|L| - 1)$$

da cui

$$|G| > |G| - \frac{|G|}{|H|} + |G| - \frac{|G|}{|L|} = 2|G| - |G|\Big(\frac{1}{|M|} + \frac{1}{|L|}\Big)$$

e l'assurdo

$$\frac{1}{|M|} + \frac{1}{|L|} > 1.$$

Questo conclude la dimostrazione che G è risolubile.

In qualità di gruppo risolubile, G ammette un sottogruppo massimale N che è normale e il cui indice è un numero primo q (esercizio 2.29). Inoltre, N è nilpotente per ipotesi. Se N è un q-gruppo, G è un q-gruppo e quindi è nilpotente. Possiamo quindi supporre che esiste un primo $p \neq q$ che divide $|G|$ e di conseguenza divide $|N|$. Sia P un p-sottogruppo di Sylow di G; allora $P \leq N$, quindi, per il Teorema 5.18, $P \trianglelefteq N$ e pertanto P è normale in G. Sia Q un q-sottogruppo di Sylow di G e supponiamo che l'insieme dei divisori primi di $|G|$ diversi da q sia $\{p = p_1, \ldots, p_t\}$ con $t \geq 2$; allora (come nel caso di p) per ogni $i = 1, \ldots, t$, G ha un unico p_i-sottogruppo di Sylow $P_i \leq N$ e $P_iQ < G$. Dunque, per ipotesi, P_iQ è nilpotente e quindi, per il Teorema 5.18, $P_i \leq C_G(Q)$ per ogni $i = 1, \ldots t$. da questo segue che anche Q è normale in G e quindi che $G + P_1 \times \times P_t \times Q$ è nilpotente.
Ci resta il caso in cui p e q sono i soli divisori primi di $|G|$ (e quindi che $|G| = p^a q^b$ per qualche $a, b \geq 1$). Allora $PQ = G$ e $G = P \rtimes Q$. Supponiamo che Q non sia ciclico, allora per ogni $x \in Q$, $P\langle x\rangle < G$ e dunque, come sopra, $x \in C_G(P)$, ovvero $Q \leq C_G(P)$; il che comporta ancora $G = P \times Q$ che è nilpotente.
Dunque, se $G = P \rtimes Q$ non è nilpotente, deve essre $G = \langle x\rangle$ per qualche $x \in Q$; ed anche $x^q \in C_Q(P)$ dato che $P\langle x^q\rangle < G$. Poiché x^q commuta sia con Q che con P, si conclude $\langle x^q\rangle \leq Z(G)$, e anche la dimostrazione. ∎

L'enunciato della Proposizione precedente non è una caratterizzazione dei gruppi finiti in cui ogni sottogruppo proprio è nilpotente, dato che esistono prodotti semidiretti $P \rtimes Q$ con le proprietà dell'enunciato che hanno sottogruppi propri non nilpotenti. D'altra parte, il gruppo $SL(2, 3)$ è un esempio di gruppo in cui ogni sottogruppo proprio è nilpotente nel quale $P \simeq Q_8$ non è abeliano.

5.4 Esempi

Condizioni (non)-equivalenti. Le equivalenze logiche nell'enunciato del Teorema 5.20 non valgono quando il gruppo non è assunto essere finito.

ESEMPIO 5.4. Consideriamo il prodotto $G = H \rtimes \langle x \rangle$ dove x è una involuzione che agisce come l'inversione su $H = C_{2^\infty}$. Come al solito, per $n \in \mathbb{N}$, denotiamo con U_n l'unico sottogruppo di ordine 2^n di H. Risolvendo l'esercizio 5.8 avete provato che $\gamma_2(G) = H = \gamma_n(G)$ per ogni $n \geq 2$, quindi in particolare che G non è nilpotente; mentre $\zeta_n(G) = U_n$, per ogni $n \geq 0$. Verifichiamo che G soddisfa la propietà (iii) del Teorema 5.20 (proprietà detta, a volte, *condizione del normalizzante*), ma non la (ii). Sia $S \leq G$, $S \neq G$; se $S \leq H$ allora $S = H$ oppure $S = U_n$ per qualche n e dunque $S \trianglelefteq G$. Assumiamo dunque $S \not\leq H$; poiché S è un sottogruppo proprio di G, $S \cap H = U_n = \zeta_n(G)$ per qualche $n \geq 0$ e, come nella dimostrazione del Lemma 5.9, $U_{n+1} = \zeta^G_{n+1}) \leq \mathcal{N}_G(S)$, provando che $\mathcal{N}_G(S) > S$. Quindi, G soddisfa (iii). Per convincersi che G non soddisfa (ii) si consideri il sottogruppo $S = \langle x \rangle$: si ha $[G, S] = H$, dunque (esercizio 5.17) $S^G = [G, S]S = HS = G$, il che esclude che S possa essere subnormale. □

Provare che, per gruppi non finiti, la proprietà (ii), cioè l'avere tutti i sottogruppi subnormali, non implica la nilpotenza, richiede la costruzione di esempi molto più complicati, ed è cosa che non faremo. I primi esempi del genere furono trovati da Heineken e Mohamed nel 1968: essi anzi provarono che esistono p-gruppi infiniti U in cui ogni sottogruppo è subnormale ma tali che $Z(U) = 1$.

ESEMPIO 5.5. Sia $G = H \rtimes \langle x \rangle$, dove x è ancora una involuzione che agisce come l'inversione su H ma, questa volta,

$$H = \left\{ \frac{n}{r} \mid n, r \in \mathbb{Z},\ 2 \not| r \right\}$$

è il gruppo additivo dei razionali con denominatore dispari. Poiché x opera come l'inversione, ogni sottogruppo di H è normale in G. Si osserva poi che $2H = \{2n/r \mid n, r \in \mathbb{Z}, r \text{ dispari}\}$ è un sottogruppo di indice 2 in H; quindi è un sottogruppo massimale di H. Non solo, $2H$ è l'unico sottogruppo massimale di H (esercizio). Proviamo quindi che $2H = \phi(G)$. Da $|G : H| = |x| = 2$ segue che H è un sottogruppo massimale di G; similmente, posto $L = (2H)\langle x \rangle$, si ha $HL = G$ e $H/2H = H/(H \cap L)$ da cui segue $|G : L| = 2$. Dunque L è massimale e quindi $\Phi(G) \geq H \cap L = 2H$. D'altra parte, se $M \neq H$ è un sottogruppo massimale di G; allora (poiché ogni sottogruppo di H è normale in G) $M \cap H$ è un sottogruppo massimale di H e quindi $M \geq 2H$.
Dunque $2H = \Phi(G)$ e $G/\Phi(G)$ è abeliano di ordine 4 (un gruppo di Klein); di conseguenza ogni sottogruppo massimale di G è normale. Ma G non soddisfa la condizione del normalizzante; infatti $\mathcal{N}_G(\langle x \rangle) \cap H = C_H(x) = 1$, quindi $\mathcal{N}_G(\langle x \rangle) = \langle x \rangle$. □

Osservazioni. (a) Si può dimostrare che, per gruppi finitamente generati, le proprietà (ii) e (iii) sono equivalenti alla nilpotenza, ma non la (iv).
(b) Agli scopi dell'esempio 5.5 anche il prodotto semidiretto $\mathbb{Q} \rtimes \langle x \rangle$, dove x è sempre l'automorfiamo di inversione, sarebbe andato bene, dato che il suo unico sottogruppo massimale è $\mathbb{Q}$; ho scelto un esempio leggermente più complicato perché, diversamenete da $\mathbb{Q} \rtimes \langle x \rangle$, soddisfa un'ulteriore proprietà che, ma solo apparentemente, lo avvicina ancor di più alla nilpotenza (esercizio 5.21).

Matrici unitriangolari. Esempi molto significativi di gruppi nilpotenti sono i i gruppi di matrici unitriangolari ad elementi in un anello commutativo con identità R; per $n \geq 1$, posto,

come al solito, $UT(n,R)$ il gruppo moltiplicativo delle matrici unitriangolari superiori $n \times n$ a coefficienti in R, si prova infatti che $UT(n,R)$ è nilpotente di classe $n-1$.
Questi gruppi unitriangolari possono essere visti, a loro volta, come istanze di un fenomeno più generale, che illustriamo brevemente. Sia E un anello con identità; un elemento $u \in E$ si dice *nilpotente* se $u^n = 0$ per qualche $n \geq 0$: ed è ben noto che se u è nilpotente allora l'elemento $1+u$ è invertibile (infatti, se $u^n = 1$ allora $(1+u)(1-u+\cdots+(-1)^{n-1}u^{n-1}) = 1$). Un sottoanello S di E (dove non richiediamo che $1 \in S$) si dice *nilpotente* se esiste $1 \leq n \in \mathbb{N}$ tale che $x_1 \cdots x_n = 0$ per ogni $x_1, \ldots, x_n \in S$ In particolare ogni elemento di un sottoanello nilpotente è nilpotente, dunque, ogni elemento di $T = \{1 + x \mid x \in S\}$ è invertibile, e si verifica facilmente che T è un sottogruppo del gruppo moltiplicativo degli invertibili di E.
Quasi altrettanto facilmente, dalla nilpotenza di S segue che $\gamma_n(T) = 1$. Più esattamente, per $1 \leq i \in \mathbb{N}$, si denota con S^i il sottoanello di E i cui elementi sono tutte le somme finite del tipo $\sum a(x_1 \cdots x_i)x_1 \cdots x_i$ con $a(x_1 \cdots x_i) \in \mathbb{Z}$, $x_1, \ldots, x_i \in S$, e si pone quindi $T_i = \{1 + y \mid y \in S^i\}$. Sia n il più piccolo intero positivo per il quale $S^n = 0$; allora, $1 = T_n \leq T_{n-1} \leq \cdots \leq T_2 \leq T_1 = T$ è una serie centrale di T.; in particolare T è un gruppo nilpotente di classe al più $n-1$.

I gruppi di matrici unitriangolari sono ottenuti in questo modo considerando $E = M_n(R)$ l'anello di tutte le matrici all $n \times n$ a coefficienti nell'anello commutativo R, ed S il sottoanello di tutte le matrici i cui elementi su e sotto la diagonale principale sono 0: queste sono somme di matrici del tipo ae_{ij}, con $a \in R$, $1 \leq i < j \leq n$ e le e_{ij} matrici elementari come definite nella sezione 3.4. Il gruppo $U = UT(n,R) = \{1 + s \mid s \in S\}$ è quindi generato dall'insieme di tutte le trasvezioni $t_{ij}(a)$, con $a \in R$ e $1 \leq i < j \leq n$. Essendo stati abbastanza sbrigativi nel trattare sopra il caso generale, vediamo con un poco di dettaglio la determinazione dei termini della serie centrale di U. Siano $i < j$, $r < s$ e (cosa che possiamo sempre assumere) $i \leq r$; dalle formule (3.13) segue la seguente regola di commutazione

$$[t_{ij}(a), t_{rs}(b)] = \begin{cases} t_{is}(ab) & \text{se } j = r \\ 1 & \text{se } j < r. \end{cases} \tag{5.5}$$

Applicando questa regola, si trova immediatamente

$$\gamma_2(U) = U' = \langle t_{ij}(a) \mid a \in R,\ j \geq i+2 \rangle,$$

che è l'insieme delle matrici unitriangolari superiori in cui la prima diagonale sopra quella principale è composta da 0. Per $c \geq 2$, anticipando il contenuto della Proposizione 5.23 e con una semplice induzione, si ottiene

$$\gamma_c(U) = \langle t_{ij}(a) \mid a \in R,\ j \geq i+c \rangle.$$

Quindi, in particolare, $\gamma_{n-1}(U) = \langle t_{1n}(a) \mid a \in R \langle$ (un sottogruppo isomorfo al gruppo additivo $(R,+)$), e $\gamma_n(U) = 1$. Pertanto U è nilpotente di classe $n-1$.

Algebre libere nilpotenti. Oltre ai gruppi di matrici, un'altro caso molto importante è quello delle algebre libere. Sia $\mathbb{F}$ un campo (va bene anche un anello commutativo, ma per semplicità descriviamo il caso del campo), e $n \geq 1$; denotiamo con $\mathbb{F}[x_1, \ldots, x_d]$ l'anello dei polinomi su $\mathbb{F}$ nelle indeterminate *non commutative* $x_1, \ldots, x_d$ (in sostanza, si tratta dello spazio vettoriale su $\mathbb{F}$, con base l'insieme di tutti i monomi non commutativi nelle indeterminate

$x_1, \ldots, x_d$, con la moltiplicazione definita tra monomi come la semoplice giustapposizione e quindi estesa per distributività.
Ad ogni monomio in $x_1, \ldots, x_d$ è associata un grado (la lunghezza della parola che si ottiene trascurando il coefficiente in $\mathbb{F}$), e ad ogni elemento dell'algebra $\mathbb{F}[x_1, \ldots, x_d]$ è associato un *grado*, come la massima tra le lunghezze dei monomi che lo compongono. Denotiamo con A la sottoalgebra generata dai monomi di grado positvo (≥ 1), ovvero la sottoalgebra di tutti i polinomi il cui termine noto è zero, e per ogni $i \geq 1$, con A_i lo $\mathbb{F}$-sottospazio di A generato da tutti i monomi di grado i. Quindi, come $\mathbb{F}$-spazio vettoriale, $\mathbb{F}[x_1, \ldots, x_d] = 1\mathbb{F} \oplus A$ e

$$A = A_1 \oplus A_2 \oplus A_3 \oplus \ldots$$

Si osservi che, per ogni $i \geq 1$, $\dim A_i = d^i$.
Fissato $c \geq 1$, consideriamo l'ideale N_c generato da A_{c+1}; chiaramente i suoi elementi sono tutti gli elementi di $\mathbb{F}[x_1, \ldots, x_d]$ che sono somma di monomi di grado $\geq c+1$; in altri termini, $N_c = A_{c+1} \oplus A_{c+2} \oplus \ldots$. Il quoziente $E = \mathbb{F}[x_1, \ldots, x_d]/N_c$ è un'algebra su $\mathbb{F}$ che contiene la sottoalgebra nilpotente $\mathcal{A} = A/N_c$ (di fatto, possiamo vedere E come ottenuto uguagliando a zero i monomi di grado $\geq c+1$, verificare quindi che, in E, il prodotto di $c+1$ monomi di grado positivo è 0 diventa quasi immediato). Quindi, per quanto detto sopra, l'insieme $1 + \mathcal{A}$ è un sottogruppo nilpotente (di classe c) del gruppo moltiplicativo degli invertibili di E. L'algebra $\mathcal{A} = A/N_c$ si chiama la $\mathbb{F}$-algebra nilpotente libera d-generata di classe c. Torneremo più avanti su questo oggetto.

5.5 Gruppi nilpotenti finitamente generati

Proposizione 5.23. *Sia G un gruppo e X un suo sistema di generatori. Allora, per ogni $n \geq 1$,*

$$\gamma_n(G) = \langle [x_1, \ldots, x_i] \mid i \geq n,\ x_1, \ldots, x_i \in X \rangle \tag{5.6}$$

Dimostrazione. Dato un gruppo G, per ogni $n \geq 1$, denotiamo con D_n il termine di destra nell'uguaglianza (5.6). Osserviamo, innanzi tutto, che $D_n \trianglelefteq G$ per ogni $n \geq 1$. Infatti, per ogni $i \geq n$ e $x, x_1, \ldots, x_i \in X$

$$[x_1, \ldots, x_i]^x = [x_1, \ldots, x_i][x_1, \ldots, x_i, x] \in D_n;$$

quindi $X \subseteq \mathcal{N}_G(D_n)$, e poiché $\langle X \rangle = G$, si deduce $D_n \trianglelefteq G$.
Procediamo per induzione su n. Poiché $D_1 = G = \gamma_1(G)$, sia $n \geq 1$, ed assumiamo $\gamma_n(G) = D_n$. Allora, per definizione di D_n, $\gamma_n(G)/D_{n+1}$ è generato dalle immagini dei commutatori $a = [x_1, \ldots, x_n]$ con $x_j \in X$. Sia a un tale commutatore, e sia $x \in X$; si ha $[a, x] \in D_{n+1}$, il che significa che ogni elemento di X centralizza la sezione $\gamma_n(G)/D_{n+1}$. Siccome X genera G si conclude che $\gamma_{n+1}(G) = [\gamma_n(G), G] \leq D_{n+1}$. Poiché, chiaramente, $D_{n+1} \leq \gamma_{n+1}(G)$, si ha $D_{n+1} = \gamma_{n+1}(G)$, il che conclude la dimostrazione. ∎

Corollario 5.24. *Un gruppo $G = \langle X \rangle$ è nilpotente di classe al più c se e soltanto se $[x_1, \ldots, x_{c+1}] = 1$ per ogni $x_1, \ldots, x_{c+1} \in X$.*

Un'altra conseguenza della Proposizione 5.23 riguarda il caso in cui G è noto essere nilpotente, di classe diciamo c; allora tutti i commutatori di lunghezza $\geq c+1$ sono banali; segue

quindi dalla Proposizione che se G è finitamente generato, ogni termine della serie centrale discendende di G è anche finitamente generato. In effetti, si può dire di pù:

Lemma 5.25. *Sia G un gruppo nilpotente. Sono equivalenti*

1. *$G/\gamma_2(G)$ è finitamente generato.*
2. *G è finitamente generato.*
3. *Ogni sottogruppo di G è finitamente generato.*

Dimostrazione. 1. $\Rightarrow$ 2. Sia G un gruppo nilpotente ed assumiamo G/G' finitamente generato ($G' = \gamma_2(G)$). Siano $x_1, \dots, x_n$ elementi di G tali che $\langle G'x_1, \dots, G'x_n\rangle = G/G'$, e sia $H = \langle x_1, \dots, x_n\rangle$; allora $G = G'H$. Dunque, per il Corollario 5.17, $G = H$ è finitamente generato.

2. $\Rightarrow$ 3. Sia G un gruppo nilpotente finitamente generato e sia $X = \{x_1, \dots, x_n\}$ un suo sistema di generatori. Per la Proposizione 5.23, $\gamma_n(G)$ è finitamente generato per ogni $n \geq 1$. Procediamo ora per induzione sulla classe di nilpotenza c di G. Se $c = 1$, G è abeliano finitamente generato e dunque ogni suo sottogruppo è finitamente generato (esercizio 5.2). Sia $c \geq 2$; allora ogni sottogruppo di $G/\gamma_c(G)$ è finitamente generato per ipotesi induttiva; ed anche ogni sottogruppo di $\gamma_c(G)$ è finitamente generato perché $\gamma_c(G)$ è abeliano e, per quanto osservato, finitamente generato. Pertanto, se $H \leq G$, si ha che sia $\gamma_c(G) \cap H$ che $H/(\gamma_c(G) \cap H) \simeq H\gamma_c(G)/\gamma_c(G)$ sono finitamente generati; quindi H è finitamente generato.

3. $\Rightarrow$ 1. Ovvio ∎

Facciamo ora un'osservazione molto elementare, ma anche molto utile:

Lemma 5.26. *Siano x, g elementi di un gruppo G tali che $[x, g] \in C_G(g)$. Allora $[x, g^n] = [x, g]^n$ per ogni $n \in \mathbb{Z}$.*

Dimostrazione. Se $n = 0, 1$, non c'è nulla da provare. Procedendo per induzione, per $n \geq 1$ si ha

$$[x, g^{n+1}] = [x, gg^n] = [x, g]^{g^n}[x, g^n] = [x, g][x, g]^n = [x, g]^{n+1}.$$

Dunque l'asserto è provato per $n \geq 0$. Per $n < 0$ basterà notare che

$$1 = [x, gg^{-1}] = [x, g]^{g^{-1}}[x, g^{-1}] = [x, g][x, g^{-1}]$$

e quindi $[x, g^{-1}] = [x, g]^{-1}$. ∎

Il Lemma 5.25 è, in particolare, un'istanza di come, in un gruppo nilpotente G, il primo fattore della serie centrale discendente, $G/\gamma_2(G)$, eserciti una notevole influenza sulle proprietà dell'intero gruppo; ecco un altro caso semplice (per un altro ancora si veda l'esercizio 5.27).

Lemma 5.27. *Sia G un gruppo nilpotente. Se $G/\gamma_2(G)$ è finito, allora G è finito.*

Dimostrazione. Induzione sulla classe di nilpotenza c di G. Se $c = 1$ allora $\gamma_2(G) = 1$, quindi G è finito per ipotesi. Sia $c \geq 1$ e $A = \gamma_c(G)$. Poiché $\gamma_2(G/A) = \gamma_2(G)/A$ e $\gamma_c(G/A) = 1$, G/A è finito per ipotesi induttiva; inoltre A è abeliano ed è finitamente generato per il Lemma 5.25. Per concludere che G è finito basta provare che A è periodico.

Siano $a \in \gamma_{c-1}(G)$ e $g \in G$. Allora (dato che G/A è finito) esiste $n \geq 1$ tale che $a^n \in A$. Poiché $[g, a] \in A \leq Z(G)$, possiamo applicare il Lemma 5.26, ottenendo $[g, a]^n = [g, a^n] = 1$. Dunque A è generato da elementi periodici e pertanto è finito. ∎

Corollario 5.28. *Un gruppo nilpotente finitamente generato e periodico è finito.*

DIMOSTRAZIONE. Sia G un gruppo nilpotente finitamente generato e periodico. Allora $G/\gamma_2(G)$ è un gruppo abeliano finitamente generato e periodico, dunque è finito. Per il Lemma 5.27, G è finito. ∎

Proposizione 5.29. *Sia G un gruppo nilpotente e $T(G) = \{x \in G \mid |x| < \infty\}$ l'insieme degli elementi periodici di G. Allora*

1. *$T(G) \trianglelefteq G$ e $G/T(G)$ è senza torsione.*
2. *Se G è finitamente generato, $T(G)$ è finito.*

DIMOSTRAZIONE. Sia G un gruppo nilpotente e $T = T(G)$. Se $x, y \in T$ e $H = \langle x, y \rangle$, allora $H/\gamma_2(H)$ è un gruppo abeliano finitamente generato e periodico, pertanto è finito. Per il Lemma 5.27, H è finito e quindi $H \subseteq T(G)$. Questo dimostra che $T(G)$ è un sottogruppo. Che sia normale (e anzi caratteristico) in G è ora ovvio. Che infine $G/T(G)$ sia un gruppo senza torsione si dimostra, assai facilmente, come nel caso abeliano (Proposizione 2.12).
Se G è finitamente generato, allora $T(G)$ è finitamente generato per il Lemma 5.25, e dunque è finito per il Corollario 5.28. ∎

Il punto 1 della Proposizione mostra che la studio dei gruppi nilpotenti si riconduce in modo naturale allo studio dei casi periodico e senza torsione.

Lemma 5.30. *Sia G un gruppo nilpotente. Sono equivalenti*

1. *G è senza torsione;*
2. *$Z(G) = \zeta_1(G)$ è senza torsione;*
3. *per ogni $i \geq 0$, $G/\zeta_i(G)$ è senza torsione.*

DIMOSTRAZIONE. 1. $\Rightarrow$ 2. Ovvio.

2. $\Rightarrow$ 3. Sia G un gruppo nilpotente tale che $Z = Z(G)$ è senza torsione; proviamo, procedendo per induzione su $i \geq 0$ che $\zeta_{i+1}(G)/\zeta_i$ è senza torsione. Il caso $i = 0$ è l'ipotesi. Sia $g \in \zeta_2(G)$ e supponiamo che esista $n \geq 1$ con $g^n \in Z$. Allora per ogni $x \in G$, poiché $[x, g] \in Z$, segue dal Lemma 5.26 che $[x, g]^n = [x, g^n] = 1$. Ma, appunto, $[x, g] \in Z$ che è senza torsione per ipotesi; dunque $[x, g] = 1$ per ogni $x \in G$, cioè $g \in Z$. Questo dimostra che $\zeta_2(G)/Z = \zeta_2(G)/\zeta_1(G) = Z)G/\zeta_1(G))$ è senza torsione. Segue allora per ipotesi induttiva che $\zeta_{i+1}(G)/\zeta_i(G)$ è senza torsione per ogni $i \geq 0$. Da ciò è immediato dedurre che $G/\zeta_i(G)$ è senza torsione per ogni $i \geq 0$.

3. $\Rightarrow$ 1. Ovvio. ∎

Proposizione 5.31. *Sia G un gruppo nilpotente finitamente generato, allora G ha una serie centrale i cui fattori sono ciclici; se, inoltre, G è senza torsione allora ha una serie centrale a fattori ciclici infiniti.*

DIMOSTRAZIONE. Procediamo per induzione su $|T(G)| = n$ (che è finito per la Proposizione 5.29). Se $n = 1$, G è senza torsione; ragioniamo allora per induzione sulla classe c di G. Se $c = 1$, G è abeliano, quindi, per il Teorema 5.6 , $G = C_1 \times \dots C_n$ con C_1 gruppi ciclici infiniti e $n \geq 1$. Ponendo, per ogni $1 \leq i \leq n$, $G_i = C_1 \times \cdots \times C_i$ si ottiene una serie $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$, che è certamente centrale (dato che G è abeliano) e tale che, per ogni $i = 1, \dots n$, il fattore $G_i/G_{i-1} \simeq C_i$ è ciclico infinito. Assumiamo quindi $c \geq 2$. Ora, $Z(G)$ è finitamente generato per il Lemma 5.25, e quindi, come nel caso precedente, esiste una serie $1 \leq C_1 \leq \cdots \leq C_k = Z(G)$ tale che ogni fattore è ciclico e centrale in G (dato che è collocato dentro il centro stesso di G). Ora, $G/Z(G)$ ha classe $c-1$ e, per il Lemma 5.30, è senza torsione. Per ipotesi induttiva esiste una serie centrale $1 = Z(G)/Z(G) \leq D_1/Z(G) \leq \cdots \leq D_s/Z(G) = G/Z(G)$ a fattori ciclici. Allora la serie

$$1 \leq C_1 \leq \cdots \leq C_k = Z(G) \leq D_1 \leq \cdots \leq D_s = G$$

è una serie centrale di G a fattori ciclici infiniti.
Sia ora $|T(G)| > 1$. Allora (Lemma 5.11), $N = T(G) \cap Z(G) \neq 1$. Esistono quindi un primo p ed un elemento $1 \neq a \in N$ tale che $A = \langle a \rangle$ è ciclico di ordine p. Ora, $A \trianglelefteq G$ e $|T(G/A)| = |T(G)/A| < |T(G)|$. Per ipotesi induttiva esiste una serie centrale $1 = A/A \leq G_2/A \leq \cdots \leq G_n/A = G/A$ a fattori ciclici; ma allora, come prima, $1 \leq A \leq G_2 \leq \cdots \leq G_n = G$ è una serie centrale di G a fattori ciclici. ∎

5.6 Anelli di Lie

Abbiamo iniziato questo capitolo affermando che il concetto di gruppo nilpotente è un'estensione di quello di gruppo abeliano, e in effetti abbiamo poi provato come questi due tipi di gruppo condividano diverse proprietà non comuni. L'associare ad un gruppo nilpotente un anello o un algebra di Lie, ed il conseguente processo di "linearizzazione" del primo, rende tecnicamente precisa questa affermazione, ma soprattutto costituisce uno strumento imprescindibile nello studio dei gruppi nilpotenti ad un livello più avanzato. Esistono diverse maniere per collegare gruppi nilpotenti e anelli di Lie; qui illustreremo quella più semplice e basica, che può essere applicata a tutti i gruppi nilpotenti.

Anelli di Lie. Un *anello di Lie* è una struttura algebrica costituita da un insieme $\mathfrak{L}$ dotato di due operazioni: una somma $(a, b) \mapsto a + b$ rispetto alla quale L è un gruppo abeliano, ed un *prodotto di Lie* $(a, b) \mapsto [ab]$ che è "bilineare", nel senso che, per ogni $a, b, x \in \mathfrak{L}$,

$$[(a + b)x] = [ax] + [bx], \qquad [x(a + b)] = [xa] + [xb] \tag{5.7}$$

e soddisfa le seguenti proprietà:

$$\begin{aligned} &[xx] = 0 \\ &[[xy]z] + [[yz]x] + [[zx]y] = 0 \qquad \text{(identita}' \text{ di Jacobi)} \end{aligned} \tag{5.8}$$

per ogni $x, y, z \in \mathfrak{L}$. Tali assiomi implicano l'anticommutatività $[xy] = -[yx]$; infatti,

$$0 = [(x + y)(x + y)] = [xx] + [xy] + [yx] + [yy] = [xy] + [yx].$$

per ogni $x, y \in \mathfrak{L}$. Mentre (tranne il caso in cui $[[xy]z] = 0$ per ogni $x, y, z \in L$) l'associatività non sussiste; infatti, utilizzando l'identità di Jacobi e l'anticommutatività,

$$[[xy]z] - [x[yz]] = [[xy]z] + [[yz]x] = -[[zx]y].$$

ESEMPIO 5.6. Sia R un anello nel senso usuale (cioè, associativo). Ponendo, per ogni $x, y \in R$,

$$[xy] = xy - yx$$

si definisce un prodotto che soddisfa (5.7) e (5.8) (fare le verifiche per esercizio), e quindi rende $(R, +, [\,])$ un anello di Lie, che di solito si denota con R^-. Una conseguenza del Teorema di Poincaré–Birkhoff–Witt è che ogni anello di Lie si può rappresentare come sottoanallo di un anello di Lie R^-, dove R è un anello associativo. □

Algebre di Lie. Sia $\mathbb{F}$ un campo. Una $\mathbb{F}$-*algebra di Lie* è un anello di Lie A che sia anche uno spazio vettoriale su $\mathbb{F}$ (con la somma quella dell'anello) e tale che

$$[(\lambda x)y] = [x(\lambda y)] = \lambda[xy]$$

per ogni $x, y \in A$, $\lambda \in \mathbb{F}$.

ESEMPIO 5.7. Un esempio importante è quello che si ricava dalla procedura descritta nell'esempio 5.6, applicata all'anello associativo di matrici $M_n(\mathbb{F})$. L'anello di Lie $M_n(\mathbb{F})^-$ è un algebra di Lie sul campo $\mathbb{F}$ (si osservi, in questo esempio, che $\det[xy] = 0$ per ogni $x, y \in M_n(\mathbb{F})$). □

Sia $\mathfrak{L}$ un anello (o un algebra) di Lie; le definizioni di sottoanello (sottoalgebra) di Lie, di ideale e di omomorfismo (di Lie) sono quelle naturali. Un sottogruppo M del gruppo additivo di L 'è un sottoanello (di Lie) se $[xy] \in M$ per ogni $x, y \in M$, ed è un ideale se $[xg] \in M$ per ogni $x \in M$, $g \in L$ (si noti che, per l'anticommutatività, gli ideali di Lie sono per natura bilateri); infine un'applicazione $L \to S$ tra anelli di Lie è un omomorfismo di Lie se è un omomorfismo dei gruppo additivi e $[xy]\phi = [(x\phi)(y\phi)]$ per ogni $x, y \in L$ (per le algebre di Lie sul campo $\mathbb{F}$, si richiede che M sia un $\mathbb{F}$-sottospazio e che ϕ sia una applicazione $\mathbb{F}$-lineare).

Per A, B sottoinsiemi di un anello di Lie $\mathfrak{L}$, si definisce $[AB]$ come il sottogruppo additivo (o, nel caso delle algebre su $\mathbb{F}$, il sottospazio) generato da tutti i prodotti $[ab]$ con $a \in A$, $b \in B$. Dagli assiomi (5.7) (5.8) segue facilmente che $[AB] = [BA]$ e che, se A, B sono ideali, anche $[AB]$ è un ideale. Si pone poi

$$\mathfrak{L}^1 = \mathfrak{L},\ \mathfrak{L}^2 = [\mathfrak{L}\mathfrak{L}],\ \text{e per } n \geq 2,\ \mathfrak{L}^n = [\mathfrak{L}^{n-1}\mathfrak{L}].$$

Per ogni $n \geq 1$, $\mathfrak{L}^n$ è un ideale di $\mathfrak{L}$, e l'anello di Lie $\mathfrak{L}$ si dice *nilpotente* se esiste $c \geq 1$ tale che $\mathfrak{L}^{c+1} = 0$. Se $\mathfrak{L}$ è nilpotente, la sua *classe* è il minimo c tale che $\mathfrak{L}^{c+1} = 0$ (il che equivale a dire che c è minimo tale che $[a_1 a_2 \cdots a_{c+1}] = 0$ per ogni $a_1, \ldots, a_{c+1} \in \mathfrak{L}$).

ESEMPIO 5.8. Fissato un campo $\mathbb{F}$, per $d, c \geq 1$, sia $\mathcal{A}$ l'algebra nilpotente libera di classe c su $\mathbb{F}$ nei generatori $x_1, \ldots, x_d$, definita alla fine della sezione 5.4. Ad essa è associata un'algebra di Lie $\mathcal{A}^-$ secondo la definizione dell'esempio 5.6. In questa algebra di Lie si considera la sottoalgebra $\mathcal{L}$ generata (come algebra di Lie) dagli elementi $x_1, \ldots, x_n$ (non coincide con $\mathcal{A}^-$, ad esempio $x_1 x_2 \in \mathcal{A}^- \setminus \mathcal{L}$). $\mathcal{L}$ si chiama $\mathbb{F}$-algebra di Lie nilpotente libera (di classe c nei generatori $x_1, \ldots, x_d$). □

Anello di Lie associato alla serie centrale. Sia G un gruppo, e per ogni $n \geq 1$, denotiamo con Γ_n l'n-esimo fattore $\gamma_n(G)/\gamma_{n+1}(G)$ della serie centrale termine della serie centrale discendente di G, in notazione additiva (cioè $a\gamma_{n+1}(G) + b\gamma_{n+1}(G) = ab\gamma_{n+1}(G)$, per ogni $a, b \in \gamma_n(G)$). Dal Lemma 5.13 segue che, per ogni $a \in \gamma_n(G)$ e $b \in \gamma_m(G)$, $[a, b] \in \gamma_{n+m}(G)$. Questo consente di definire, sul gruppo additivo

$$\mathcal{L}(G) = \Gamma_1 \oplus \Gamma_2 \oplus \cdots = Dir_{n\geq 1}\Gamma_n \tag{5.9}$$

un prodotto di Lie, ponendo, per $\bar{a} = a\gamma_{n+1}(G) \in \Gamma_n$, $\bar{b} = b\gamma_{m+1}(G) \in \Gamma_m$,

$$[\bar{a}\,\bar{b}] = [a, b]\gamma_{n+m+1}(G) \in \Gamma_{n+m} \tag{5.10}$$

ed estendendolo quindi per distributività. Naturalmente, occorre verificare che ciò definisce in modo corretto un prodotto di Lie, cosa che lasciamo come esercizio. Oltre al citato Lemma 5.13, la ragione della correttezza viene dalle formule per i commutatori 2.20; in particolare, le prime tre assicurano la buona definizione e la distributività rispetto alla somma, mentre dall'identità di Hall-Witt deriva in $\mathfrak{L}(G)$ quella di Jacobi. Quindi

Teorema 5.32. *Con le operazioni descritte, $\mathfrak{L}(G)$ è un anello di Lie.*

Esempio 5.9. Sia $D_8 = \langle x, y \mid x^2 = y^2 = (xy)^4\rangle$, il gruppo diedrale di ordine 8. Allora $\Gamma_1 = G/G' \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ e $\Gamma_3 \simeq \mathbb{Z}/2\mathbb{Z}$; $\mathfrak{L}(D_8)$ è un algebra di Lie su $GF(2)$ con base (come spazio vettoriale) $e_1 = xG', e_2 = yG', e_3 = [x, y]$, e conprodotto di Lie descritto da $[e_1e_2] = e_3$ e $[e_1e_3] = [e_2e_3] = 0$. È molto facile verificare poi che $\mathfrak{L}(D_8)$ è isomorfa, come $GF(2)$-algebra di Lie a $\mathfrak{L}(Q_8)$. □

Si constata immediatamente che se G è generato (come gruppo) da X, allora $\mathfrak{L}(G)$ è generato (come anello di Lie) dagli elementi $\overline{x} = x\gamma_2(G)$ con $x \in X$. Inoltre, dalla Proposizione 5.23, segue che, per $n \geq 2$, l'addendo diretto $\gamma_n(G)/\gamma_{n+1}(G)$ è generato dagli elementi $[\overline{x}_1, \ldots, \overline{x}_n]$ con $x_1, \ldots, x_n \in X$. L'anello $\mathfrak{L}(G)$ si può definire per ogni gruppo G, ma è abbastanza naturale che possa codificare significative informazioni su G soprattutto nel caso in cui G è nilpotente (o, almeno, residualmente nilpotente - vedi prossima sezione). La dimostrazione del seguente Lemma è lasciata per esercizio

Lemma 5.33. *Sia $\mathfrak{L}(G)$ l'anello di Lie associato al gruppo $G = \langle X\rangle$. Allora, per ogni $n \geq 1$,*

$$\mathfrak{L}(G)^n = \bigoplus_{i\geq n} \gamma_i(G)/\gamma_{i+1}(G).$$

In particolare, $\mathfrak{L}(G)$ è nilpotente (di classe c) se e solo se G è nilpotente (di classe c).

Esempio 5.10. Sia p un numero primo, e sia $G = \langle X\rangle$ un gruppo nilpotente tale che $x^p \in \gamma_2(G)$ per ogni $x \in G$. Questa condizione, nell'anello di Lie $\mathfrak{L}(G)$, si legge $p\overline{x} = 0$ per ogni $\overline{x} = x\gamma_2(G)$ con $x \in X$; ovvero $p(G/\gamma_2(G)) = 0$. Sia $n \geq 2$, e $x_1, \ldots, x_n \in X$; allora $p[\overline{x}_1, \ldots \overline{x}_n] = [p\overline{x}_1, \ldots, x_n] = 0$; qundii, per quanto osservato sopra, $p(\gamma_n(G)/\gamma_{n+1}(G)) = 0$, per ogni $n \geq 2$. Questo comporta che l'anello $\mathfrak{L}(G)$ è di fatto un'*algebra* di Lie sul campo $GF(p)$. □

Questa, la cui descrizione abbiamo appena accennato, è una delle maniere (la più immediata) per associare ad un gruppo un algebra di Lie; può facilmente essere adattata, secondo l'opportunità, usando per la definizione altre serie centrali $G = G_1 \geq G_2 \geq \dots$ che soddisfano la condizione $[G_1, G_j] \leq G_{i+j}$. Ma esistono altre maniere, che si applicano a specifiche classi di gruppi nilpotenti, e che forniscono corrispondenze anche più complete tra gruppi e algebre di Lie. Accenniamo all'importante *corrispondenza di Mal'cev*. Ricordo che un gruppo G è radicabile se per ogni $x \in G,\ 1 \leq n \in \mathbb{N}$, esiste $y \in G$ tale che $y^n = x$; se, inoltre, G è nilpotente e senza torsione, allora (esercizio 5.33) dati x e $n \geq 1$ un tale $y \in G$ è unico, e può essere quindi denoitato con $x^{\frac{1}{n}}$. Un gruppo radicabile con unicità di radice è detto $\mathbb{Q}$-potente; è evidente che un gruppo $\mathbb{Q}$-potente è senza torsione. La corrispondenza di Mal'cev descrive una procedura canonica per associare ad ogni gruppo nilpotente $\mathbb{Q}$-potente una $\mathbb{Q}$-algebra di Lie nilpotente sullo stesso insieme, e viceversa per definire, su ogni $\mathbb{Q}$-algebra di Lie nilpotente un'operazione che la rende un gruppo nilpotente $\mathbb{Q}$-potente. La corrispondenza che viene così determinata tra $\mathbb{Q}$-algebre di Lie nilpotenti e gruppi nilpotenti rradicabili e senza torsione è quello che si chiama un *isomorfismo di categorie*; senza entrare nel dettaglio, significa che le due teorie sono equivalenti: ogni enunciato riguardante $\mathbb{Q}$-algebre di Lie nilpotenti si traduce in uno riguardante i gruppi nilpotenti radicabili senza torsione, e viceversa. La cosa viene conchiusa da Mal'cev provando che per ogni gruppo nilpotente senza torsione G è definito in modo canonico un gruppo nilpotente $\mathbb{Q}$-potente $\widehat{G}$, detto *completamento di Mal'cev*, con $G \leq \widehat{G}$, minimo nel senso che per ogni $y \in \widehat{G}$ esiste $n \geq 1$ tale che $y^n \in G$. Sarebbe interessante poter descrivere più esplicitamente corrispondenza e completamento di Mal'cev, cosa che coinvolge algebre associative libere, logaritmi formali, etc., ma non ne abbiamo lo spazio: il caso di classe 2 è oggetto dell'esercizo 5.37

5.7 Gruppi residualmente nilpotenti

Un gruppo G si dice *residualmente nilpotente* se l'intersezione dei sottogruppi $N \trianglelefteq G$ tali che G/N è nilpotente è banale. Quindi, il gruppo diedrale infinito è residualmente nilpotente; ed è chiaro che un gruppo G è residualmente nilpotente se e soltanto se

$$\bigcap_{n \geq 1} \gamma_n(G) = 1. \tag{5.11}$$

Un'altra definizione equivalente è che per ogni $1 \neq g \in G$ esiste un gruppo nilpotente P ed un omomorfismo $\phi : G \to P$ tale che $g\phi \neq 1$.

Un altro esempio di gruppo residualmente nilpotente ma non nilpotente è il 5.5 (vedi esercizio 5.21), ma di fatto la classe dei gruppi residualmente nilpotenti è davvero molto ampia, come dichiarato dal seguente fondamentale risultato.

Teorema 5.34. (Magnus) *Ogni gruppo libero è residualmente nilpotente.*

(Quindi, ogni gruppo è immagine omomorfa di un gruppo residualmente nilpotente.) Di fatto, dimostreremo un risultato ancora più forte.

Teorema 5.35. (Iwasawa) *Sia F un gruppo libero. Allora per ogni numero primo p, F è residualmente un p-gruppo finito.*

DIMOSTRAZIONE. Sia p un numero primo e F un gruppo libero con sistema di generatori X. Sia $1 \neq g \in F$. Vogliamo mostrare che esiste un *p-gruppo finito* P ed un omomorfismo $\phi : F \to P$ tale che $g\phi \neq 1$. L'elemento g si scrive in modo unico nella forma

$$g = x_1^{\beta_1} \dots x_n^{\beta_n} \tag{5.12}$$

con $x_i \in X$, $x_{i+1} \neq x_1$ e $\beta_i \in \mathbb{Z} \setminus \{0\}$. Sia $m \geq 1$ tale che $p^m > |\beta_1 \cdots \beta_n|$. Per ogni $1 \leq i, j \leq n+1$ consideriamo la matrice $e_{ij} \in M_{n+1}(\mathbb{Z}/p^m\mathbb{Z})$ nel solito modo (i suoi elementi sono tutti 0 tranne quello di posto (i, j) che è 1), e $P = UT(n+1, \mathbb{Z}/p^m\mathbb{Z})$ il gruppo delle matrici unitriangolari superiori a coefficienti in $\mathbb{Z}/p^m\mathbb{Z}$, che è un p-gruppo finito (il suo ordine è $(p^m)^{\frac{n(n-1)}{2}}$) e contiene $1 + e_{i,i+1}$ per ogni $1 \leq i \leq n$.
Per ciascun $x \in X$ poniamo:

$$xf = \begin{cases} 1 & \text{se} \quad x \notin \{x_1, \dots, x_n\} \\ \prod_{x_i = x}(1 + e_{i,i+1}) & \text{se} \quad x \in \{x_1, \dots, x_n\}. \end{cases} \tag{5.13}$$

Per la proprietà universale del gruppo libero l'applicazione $f : X \to P$ appena definita si estende ad un unico omomorfismo $\phi : F \to P$. A questo punto, con alcune considerazioni sul prodotto di matrici e per le scelte fatte si verifica (ma noi ci risparmiamo la fatica di fare i conti) che $g\phi \neq 1$, così completando la dimostrazione. ∎

Serie centrale discendente dei gruppi liberi. In quest'ultimo paragrafo descriveremo i fattori $\gamma_r(F)/\gamma_{r+1}(F)$ della serie centrale discendente di un gruppo libero di rango finito. Abbiamo già provato (Proposizione 4.14) che il primo di essi, $F/\gamma_2(F)$, è un gruppo abeliano libero (di rango uguale a quello di F); ed è un fatto notevole che una proprietà analoga valga per ogni fattore successivo. Non produrremo però una dimostrazione completa poiché ci pare sufficiente descrivere il metodo ed il risultato. Questi si basano sulla selezione in F di opportuni commutatori (detti basici), che può essere effettuata in vari modi: noi seguiremo quello proposto dal matematico russo Shirshov.

Sia F_n il gruppo libero su $X = \{x_1, \dots, x_n\}$. Definiamo ricorsivamente i *commutatori semplici* di peso k, per $k \geq 1$, nel modo seguente:

- $x_1, x_2, \dots, x_n$ sono i commutatori semplici di peso 1;
- per $k \geq 2$, i commutatori semplici di peso k sono gli elementi $[u_1, u_2]$, dove u_1 u_2 sono commutatori semplici di peso k_1, k_2 e $k = k_1 + k_2$.

Sia W l'insieme delle *parole positive* di F_n, ovvero l'insieme degli elementi $\neq 1$ di F_n la cui scrittura come parola ridotta nell'alfabeto $X \cup X^{-1}$ non contiene alcun elemento in X^{-1} (W è un semigruppo ed è il *semigruppo libero* di rango n); osserviamo che c'è corrispondenza biunivoca tra W e l'insieme delle parole non vuote in X; ad ogni elemento $v \in W$ associamo poi come al solito la lunghezza $\ell(v)$ come lunghezza della parola stessa.

Fissato un ordinamento totale su X, diciamo $x_1 < x_2 < \cdots < x_n$, questo si estende ad un ordinamento totale di W ponendo, per ogni $u, v \in W$, $u < v$ se $\ell(v) < \ell(v)$ e ordinando lessicograficamente se $\ell(u) = \ell(v)$. Diciamo che una parole $v \in W$ è *regolare* se $v \in X$ oppure, per ogni $v_1, v_2 \in W$, da $v = v_1 v_2$ segue $v > v_2 v_1$. La cosa si chiarisce introducendo su W

una relazione d'equivalenza $\sim$ ponendo, per $u, w \in W$, $u \sim w$ se esistono $u_1, u_2 \in W$ tali che $u = u_1u_2$ e $w = u_2u_1$. Si osserva subito che ogni classe di equivalenza $[u]$ con $u \in W$ contiene al più $\ell(u)$ elementi (si osservi anche che gli elementi di $[u]$ si ottengono da u spostando una lettera alla volta dalla fine all'inizio della parola: per questa ragione la classi di equivalenza $[u]$ sono talvolta dette *parole circolari*). Diciamo che $u \in W$ è una potenza se $u = v^d = vv \dots v$ per qualche $v \in W$ e $d \geq 2$. Non è difficile constatare che $u \in W$ è una potenza se e soltanto se esistono $u_1, u_2 \in W$ tali che $u_1u_2 = u = u_2u_1$. Da ciò segue che, per $u \in W$, $|[u]| = \ell(u)$ se e soltanto se u non è una potenza. Per definizione, una potenza non può essere una parola regolare; e se u non è una potenza, la sua classe d'equivalenza $[u]$ contiene un'unica parola regolare che è il suo massimo nell'ordinamento assegnato a W.
Quindi, dato $r \geq 1$, il numero di parole regolari di lunghezza r in W coincide col numero di classi di equivalenza di non-potenze. Tale numero è, per quanto osservato, $R_n(r) = K_n(r)/r$, dove $K_n(r)$ è il numero di parole di lunghezza r (su un alfabeto di n lettere) che non sono potenze. Ora

$$\sum_{d|r} K_n(d) = |\{v \in W \mid \ell(v) = r\}| = n^r.$$

Quindi, per la formula di inversione di Möbius (vedi dispense di Algebra I sez.4.3),

$$R_n(r) = \frac{1}{r} \sum_{d|r} \mu(r/d) n^d. \tag{5.14}$$

Per ogni commutatore semplice c denotiamo con $\bar{c}$ l'elemento di W ottenendo cancellando formalmente le parentesi; ad esempio

$$\overline{[x_4, [x_3, x_2], [x_1, x_2]]} = x_4x_3x_2x_1x_2.$$

(è chiaro che il peso di c coincide con la lunghezza di $\bar{c}$). Denotiamo con R l'insieme della parole regolari in W, e diciamo che un commutatore semplice $c \in F_n$ è *basico* (secondo Shirshov) se $\bar{c} \in R$ e

- se $c = [u, v]$ allora $\bar{u}, \bar{v} \in R$;
- se $c = [[u_1, u_2], v]$ allora $\bar{u}_2 \leq \bar{v}$.

A questo punto si dimostra, procedendo per induzione sulla lunghezza della parola (ma noi non lo faremo), che ad ogni parola regolare $w \in R$ corrisponde uno ed un solo commutatore basico c tale che $\bar{c} = w$. Ad esempio, se $X = \{a, b, c\}$ con $a < b < c$, le parole regolari di lunghezza 3 sono

$$ccb,\ cca,\ cbb,\ cba,\ cab,\ caa,\ bba,\ baa,$$

e i corrispondenti commutatori basici sono::

$$[c,[c,b]],\ [c,[c,a]],\ [c,b,b],\ [c,[b,a]],\ [c,a,b],\ [c,a,a],\ [b,[b,a]],\ [b,a,a].$$

Ci fermiamo qui nella descrizione del metodo, ed enunciamo il fondamentale risultato sui fattori della serie centrale discendente di un gruppo libero.

Teorema 5.36. *Sia F il gruppo libero con generatori $x_1, \ldots, x_n$. Allora, per ogni $r \geq 1$,*

$$\gamma_r(F)/\gamma_{r+1}(F)$$

è un gruppo abeliano libero in cui un sistema libero di generatori è costituito dall'insieme delle immagini modulo $\gamma_{r+1}(F)$ dei commutatori basici di peso r. In particolare, il rango è uguale a $R_n(r)$ dato in (5.14).

Osserviamo, in particolare, che, per $c \geq 1$, il gruppo additivo dell'anello di Lie $\mathfrak{L}(F/\gamma_{c+1}(F))$ è quindi un gruppo abeliano libero, il cui rango è la somma $d = d(n,c) = \sum_{1 \leq r \ c} R_n(r)$. Da ciò (per chi conosce il prodotto tensoriale) deriva che

$$\widehat{\mathfrak{L}} = \mathfrak{L}(F/\gamma_{c+1}(F)) \otimes_{\mathbb{Z}} \mathbb{Q}$$

è una $\mathbb{Q}$-algebra di Lie di dimensione d; si dimostra che è proprio la $\mathbb{Q}$-l'algebra di Lie libera n-generata e nilpotente di classe c (vedi fine sezione 5.4 e l'esempio 5.8).

5.8 Esercizi V

Sezione 5.1

Esercizio 5.1. Un gruppo abeliano A si dice *proiettivo* se che soddisfa alla seguente proprietà universale: per ogni omomorfismo $\alpha : A \to G$ e ogni omomorfismo suriettivo $f : H \to G$, con G, H gruppi abeliani, esiste un omomorfismo $\beta : A \to H$ tale che $\beta f = \alpha$. Si provi che ogni gruppo abeliano libero è proiettivo. Si provi quindi che un gruppo abeliano finitamente generato proiettivo è libero (questo vale anche se il gruppo non è finitamente generato).

Esercizio 5.2. Sia A un gruppo abeliano finitamente generato. Si provi che ogni sottogruppo B di A è finitamente generato, e che $d(B) \leq d(A)$. Si deduca che un gruppo abeliano soddisfa la *condizione di massimo* per sottogruppi (ovvero ogni catena di sottogruppi $H_1 \leq H_2 \leq H_3 \leq \ldots$ è finita, cioè esiste n tale che $H_i = H_n$ per ogni $i \geq n$) se e soltanto se è finitamente generato.

Esercizio 5.3. Sia A un gruppo abeliano finitamente generato. Si provi che sono equivalenti:

(i) Esiste una catena di sottogruppi $A \geq H_1 \geq H_2 \geq \ldots$ tale che A/H_n è ciclico per ogni $n \geq 1$ e $\bigcap_{n \geq 1} H_n = 1$;

(ii) $A \simeq \mathbb{Z}^d \times C$ con $d \in \mathbb{N}$ e C un gruppo ciclico finito.

Esercizio 5.4. Un gruppo G soddisfa la *condizione di minimo* sui sottogruppi (abbreviato, *Min*) se ogni catena $H_0 \geq H_1 \geq H_2 \geq \ldots$ di sottogruppi di G è finita (cioè esiste $n \geq 0$ tale che $H_i = H_n$ per ogni $i \geq n$). Si provi che sono equivalenti:.

(i) Si provi che un gruppo che G soddisfa *Min* è periodico;

(ii) Un gruppo abeliano f.g. soddisfa *Min* se e soltanto se è finito; più in generale si provi che un gruppo abeliano privo di sottogruppi divisibili non-banali soddisfa *Min* se e soltanto se è finito.

Sezione 5.2

Esercizio 5.5. Siano H, K gruppi; si provi che per ogni $n \geq 1$ $\gamma_n(H \times K) = \gamma_n(H) \times \gamma_n(K)$ e $\zeta_n(H \times K) = \zeta_n(H) \times \zeta_n(K)$. Si deduca che se H, K sono nilpotenti di classe, rispettivamente, c_H e c_K, $H \times K$ è nilpotente e di classe $\max\{c_H, c_K\}$.
Sia quindi $(H_i)_{i \in I}$ una famiglia di gruppi nilpotenti, e per ogni $i \in I$ sia c_i la classe di nilpotenza di H_i. Si provi che $Dir_{i \in I} H_i$ è nilpotente se e soltanto se $sup_{i \in I} c_i < \infty$.

Esercizio 5.6. Sia A un gruppo abeliano (additivo); si provi che $\alpha : (a, b) \mapsto (a, a+b)$ definisce un automorfismo del prodotto diretto $A \times A$; si dimostri quindi che il prodotto semidiretto $(A \times A) \rtimes \langle \alpha \rangle$ è nilpotente, determinando le sua serie centrale discendente. Infine, si provi che , con le definizioni di sopra, $\mathbb{Z} \times \mathbb{Z}) \rtimes \langle \alpha \rangle$ è isomorfo al gruppo $UT(3, \mathbb{Z})$.

Esercizio 5.7. Sia A un gruppo abeliano e x l'automorfismo di inversione su A (cioè $a \mapsto a^{-1}$ per ogni $a \in A$). Si provi che il prodotto semidiretto $A \rtimes \langle x \rangle$ è nilpotente se e soltanto se A è un 2-gruppo di esponente finito.

Esercizio 5.8. Sia $H = C_{2^\infty}$ il 2-gruppo di Prüfer e x l'automorfismo di inversione su A. Si descrivano le serie centrali ascendenti e discendenti di $G = H \rtimes \langle x \rangle$; si provi che ogni fattore centrale di G ha ordine 2.

Esercizio 5.9. Sia G un gruppo tale che $\zeta_1(G) < \zeta_2(G)$. Provare che $G' < G$. [sugg.: preso $g \in \zeta_2(G) \setminus \zeta_1(G)$ considerare l'applicazione da G in $\zeta_1(G)$ definita da $x \mapsto [x, g]$]

Esercizio 5.10. Sia G un gruppo nilpotente e A un sottogruppo normale abeliano massimale di G. Si provi che $A = C_G(A)$.

Esercizio 5.11. Si provi il *Teorema di Fitting*: Siano M, N sottogruppi normali e nilpotenti del gruppo G; allora MN è un sottogruppo nilpotente di G. [se c è la classe di nilpotenza di M, provare che $\zeta_1(N) \leq \zeta_c(MN)$; quindi fare induzione sulla classe di N].

Esercizio 5.12. Siano $N_1, N_2, \ldots N_s$ sottogruppi normali e abeliani del gruppo G, tali che $G = N_1 \ldots N_s$. Si provi che G è nilpotente.

Sezione 5.3

Esercizio 5.13. Siano p un numero primo e G un gruppo finito. Si provi che se $G/\Phi(G)$ è un p-gruppo, allora G è un p-gruppo.

Esercizio 5.14. Sia G un gruppo finito. Usando il teorema di Fitting (esercizio 5.7) si dimostri che G ha un massimo sottogruppo normale nilpotente $Fit(G)$ (cioè $Fit(G)$ è nilpotente e normale e ogni sottogruppo normale e nilpotente di G è contenuto in $Fit(G)$). $Fit(G)$ si chiama il *sottogruppo di Fitting* di G.

Esercizio 5.15. Fissato un primo p ed un $n \geq 1$, siano $A = \langle g \rangle$ un gruppo ciclico di ordine p^n e α l'automorfismo di A definito da $g \mapsto g^{p+1}$. Si determini la classe di nilpotenza del p-gruppo $A \rtimes \langle \alpha \rangle$.

Esercizio 5.16. Sia G un gruppo finito. Si provi che G è nilpotente se e solo se $[G, N] < N$ per ogni $1 \neq N \trianglelefteq G$.

Esercizio 5.17. Sia G un gruppo; per $H \leq G$, si definisce $[G,_0 H] = G$ e, per ogni $n \geq 1$, $[G,_n H] = [[G,_{n-1} H], H]$ $(= [G, H, \ldots, H]$ dove H è ripetuto n volte). Si provi che, per ogni $H \leq G$, $H^G = [G, H]H$ e che $H \triangleleft\triangleleft G$ se e solo se esiste $n \geq 1$ tale che $[G,_n H] \leq H$.

Esercizio 5.18. Sia G un gruppo finito tale che per ogni $x, y \in G$, se $(|x|, |y|) = 1$ allora $xy = yx$. Si provi che G è nilpotente.

Esercizio 5.19. Sia G un gruppo finito tale che $\langle g \rangle \triangleleft\triangleleft G$ per ogni $g \in G$. Si provi che G è nilpotente.

Esercizio 5.20. Siano G un gruppo finito, p un divisore primo di $|G|$ e P un p-sottogruppo di Sylow di G. Assumendo inoltre che $P \not\trianglelefteq G$, sia P_1 un p-sottogruppo di Sylow di G tale che $P_1 \neq P$ e $|P \cap P_1|$ è massimo possibile. Si provi che esiste $x \in \mathcal{N}_G(P \cap P_1)$ tale che $P_1 = P^x$.

Sezione 5.4

Esercizio 5.21. Sia G il gruppo dell'esempio 5.5; si provi che $\bigcap_{n\geq 1} \gamma_n(G) = 1$.

Esercizio 5.22. Sia $G = UT(3, \mathbb{Q})$. Si provi che per ogni $x \in G$ e $n \geq 1$ esiste $y \in G$ tale che $y^n = x$.

Esercizio 5.23. Sia p un numero primo. Quanti elementi contiene il gruppo $G = SL(2, \mathbb{Z}/p^2\mathbb{Z})$? Si provi che $UT(n, \mathbb{Z}/p^2\mathbb{Z})$ non è un p-sottogruppo di Sylow di G; si descriva quindi un p-sottogruppo di Sylow P di G tale che $UT(2, \mathbb{Z}/p^2\mathbb{Z}) \leq P$.

Esercizio 5.24. Sa R una anello commutativo. Per ogni $n \geq 1$ sia ϕ_n l'omomorfismo inetttivo $UT(n, R) \to UT(n + 1, R)$ che manda ogni matrice del primo gruppo nell'angolo superiore sinistro di una matrice di rango $n + 1$ che ha poi 1 a completare la diagonale. Sia G il limite diretto (per $n \in \mathbb{N}^*$) di tale sistema di omomorfismi. Si provi che ogni sottogruppo finitamente generato di G è nilpotente (un gruppo con questa proprietà si dice *localmente nilpotente*), ma che G non lo è.

Esercizio 5.25. Sia $\mathbb{F}$ un campo, $n \geq 1$ e $U = UT(n, \mathbb{F})$ Si provi che per ogni $1 \leq i < j \leq n$ e $a \in \mathbb{F}$, $\langle t_{ij}(a) \rangle^U$ è un gruppo abeliano. Si deduca che U è generato da sottogruppi normali abeliani.

Esercizio 5.26. SIa $G = UT(\mathbb{F})$ il limite diretto dei gruppi $UT(n, \mathbb{F})$ come definito nell'esercizio 5.24. Si provi che G è generato da sottogruppi normali abeliani. Si provi quindi che per ogni $g \in G$, $\langle g \rangle \triangleleft\triangleleft G$ (un gruppo con questa proprietà si dice *gruppo di Baer*; questo esercizio mostra che esistono gruppi di Baer non nilpotenti). [sugg. usare l'esercizio 5.12]

Sezione 5.5

Esercizio 5.27. Sia π un insieme di primi, e sia G un gruppo nilpotente. Si provi che se $G/\gamma_2(G)$ è un π-gruppo (cioè ogni suo elemento ha ordine finito i cui divisori primi appartengono a π). Si provi che G è un π-gruppo.

Esercizio 5.28. Sia G un gruppo nilpotente. Si provi che se $Z(G)$ ha esponente finito (cioè esiste $n \geq 1$ tale che $a^n = 1$ per ogni $a \in \mathbb{Z}(G)$), allora G ha esponente finito.
Sia G un gruppo nilpotente finitamente generato tale che $Z(G)$ è un π-gruppo per un insieme π di primi; si provi che G è un π-gruppo finito.

Esercizio 5.29. Sia π un insieme infinito di numeri primi, e per ogni $p \in \pi$ sia $A_p = \langle g_p \rangle$ un gruppo ciclico di ordine p^2. Sia $A = Dir_{p\in\pi} A_p$ e sia α l'automorfismo di A tale che, per ogni primo $p \in \pi$, $g_p\alpha = g_p^{p+1}$ (cfr. esercizio 5.14); poniamo infine $G = A \rtimes \langle\alpha\rangle$. Si provi che G è nilpotente e non periodico, ma che il suo centro è periodico.

Esercizio 5.30. Sia G un gruppo nilpotente finitamente generato; si provi che ogni serie centrale di G a fattori ciclici ha lo stesso numero di fattori infiniti.

Esercizio 5.31. Sia p un numero primo e sia G un p-gruppo nilpotente tale che $G/\gamma_2(G)$ è divisibile. Si provi che $\gamma_2(G) = 1$ (non vale nel caso non periodico, vedi esercizio 5.22).

Esercizio 5.32. SI provi che esistono gruppi nilpotenti senza torsione G tali che $G/\gamma_2(G)$ contiene elementi periodici non banali. [sugg. Si cerchi tra i sottogruppi del gruppo unitriangolare $UT(3, \mathbb{Z})$]

Esercizio 5.33. Sia G un gruppo nilpotente senza torsione. Si provi che per ogni $g, h \in G$, e ogni $n \geq 1$, $g^n = h^n \Rightarrow g = h$.

Sezione 5.6

Esercizio 5.34. Sia $\mathfrak{L}$ un anello di Lie. Si provi che, per ogni $n, m \geq 1$, $[\mathfrak{L}^n\mathfrak{L}^m]$ è contenuto in $\mathfrak{L}^{n+m}$.

Esercizio 5.35. Sia G un gruppo e $\phi \in Aut(G)$. Allora ϕ induce nella maniera naturale un automorfismo ϕ_n su ognuno dei gruppi abeliani $\gamma_n(G)/\gamma_{n+1}(G)$; si provi che questi automorfismi, interpreteti come blocchi diagonali, a loro volta determinano un unico automorfismo ϕ^L dell'anello di Lie $\mathfrak{L}(G)$. Si osservi che ϕ^L può essere banale anche se ϕ non lo è [si pensi agli automorfismi interni]. Si provi tuttavia che se G è un p-gruppo finito e $(|\phi|, p) = 1$, allora ϕ^L non è banale. [sugg. usare l'esercizio 3.5]

Esercizio 5.36. Siano p un primo, P un p-gruppo finito e $\phi \in Aut(G)$ con $(|\phi|, p) = 1$. Si provi che se ϕ induce l'identità su $P/\gamma_2(P)$ allora $\phi = 1$.

Esercizio 5.37. Sia G un gruppo senza torsione, nilpotente di classe 2 e radicabile. Per l'esercizio 5.33, per ogni $x \in G$ esiste un unico $y \in G$ tale che $y^2 = x$ (scriviamo $y = x^{\frac{1}{2}}$). Si definisca un'operazione di addizione in G ponendo, per ogni $x, y \in G$,

$$x + y = xy[x, y]^{\frac{1}{2}},$$

e si provi che, con rispetto alla somma appena definita ed alla moltiplicazione data dal commutatore, G è un anello di Lie, ponendo poi, per $q \in \mathbb{Q}$ e $x \in G$, $(q, x) \mapsto x^q$, si ha una $\mathbb{Q}$-algebra di Lie che denotiamo con $\mathcal{L}_G$. Si dimostri quindi che $\mathcal{L}_G$ è nilpotente e di classe 2, e che gli automorfismi del gruppo G sono esattamente gli automorfismi dell'algebra $\mathcal{L}_G$. Viceversa, sia $\mathcal{L}$ una $\mathbb{Q}$-algebra di Lie nilpotente di classe 2. Per $a, b \in \mathcal{L}$ si pone

$$a \cdot b = a + b + \frac{1}{2}[ab].$$

Si provi che, con tale operazione, l'insieme $\mathcal{L}$ è un gruppo (nilpotente di classe 2, senza torsione e radicabile).

Sezione 5.7

Esercizio 5.38. Si provi che il gruppo G dell'esercizio 5.24 è residualmente nilpotente.

Esercizio 5.39. Sia p un numero primo. Per ogni $n \geq 1$ la riduzione modulo p^n degli elementi di una matrice definisce un omomorfismo suriettivo $\phi_n : SL(2,\mathbb{Z}) \to SL(2,\mathbb{Z}/p^n\mathbb{Z})$. Sia $\Gamma(p) = \ker \phi_1$; si provi che $\Gamma(p)$ è residualmente un p-gruppo finito.

I prossimi tre esercizi guidano (spero) alla dimostrazione di un altro interessante risultato che garantisce che certi gruppi sono residualmente p-gruppi finiti per ogni primo p.

Esercizio 5.40. Sia G un gruppo nilpotente finitamente generato. Si provi che esiste $N \trianglelefteq G$ tale che $|G/N|$ è finito e $T(G) \cap N = 1$.

Esercizio 5.41. Sia G un gruppo nilpotente finitamente generato e senza torsione. Siano A un sottogruppo di $Z(G)$ con $|Z(G) : N|$ finito e N un sottogruppo normale di G tale che sia massimale per $Z(G) \cap N = A$. Si provi che G/N è finito.

Esercizio 5.42. (Gruenberg) Un gruppo nilpotente senza torsione e finitamente generato è residualmente un p-gruppo finito per ogni primo p. [fare induzione sulla classe]

Capitolo 6

Gruppi finitamente generati

6.1 Sottogruppi di gruppi finitamente generati

Sia G un gruppo, scriviamo che G è f.g. se ammette un sistema finito di generatori. Quando sarà necessario essere più precisi, diremo che un gruppo è n-generato se ammette un sistema di generatori X con $|X| = n$; in particolare, un gruppo è 1-generato se e soltanto se è ciclico.

Sottogruppi di gruppi f.g. È chiaro che ogni quoziente (quindi, ogni immagine omomorfa) di un gruppo f.g. G è finitamente generato: se $G = \langle g_1, \ldots, g_r \rangle$ e $N \trianglelefteq G$ allora $G/N = \langle Ng_1, \ldots, Ng_r \rangle$ (dunque $d(G/A) \leq d(A)$). Diversamente, come mostrano i seguente esempi, sottogruppi di gruppi finitamente generati possono non essere tali.

Esempio 6.1. Sia $H = \{n/2^i \mid n \in \mathbb{Z},\ i \geq 0\}$ (H è un sottogruppo del gruppo additivo dei razionali - vedi esercizio 6.2) e sia α l'automorfismo di H definito da $q\alpha = 2q$ per ogni $q \in H$. Allora il prodotto semidiretto $G = H \rtimes \langle \alpha \rangle$ è 2-generato (infatti $G = \langle 1, \alpha \rangle$) ma il suo sottogruppo H non è finitamente generato (esercizio 6.7). □

Esempio 6.2. Come altro esempio si può considerare il gruppo del lampionaio (sezione 2.5) $G = (\mathbb{Z}/2\mathbb{Z}) wr \mathbb{Z}$. Possiamo scrivere $G = B \rtimes \mathbb{Z}$, la base B essendo l'insieme delle applicazioni $f : \mathbb{Z} \to \{0, 1\}$ a supporto finito. Si verifica allora che $G = \langle \{(a, 0), (0, , 1)\} \rangle$ dove $a \in B$ è definita da $a(z) = 1 \Leftrightarrow z = 0$, e 1 è generatore di $\mathbb{Z}$. Quindi G è 2-generato, mentre il suo sottogruppo normale B è un prodotto diretto di infinite copie di $\mathbb{Z}/2\mathbb{Z}$ e non è finitamente generato. □

In effetti, la non-chiusura per sottogruppi della classe dei gruppi finitamente generati si manifesta in modo radicale. Ogni gruppo finitamente generato (e di conseguenza ogni suo sottogruppo) è numerabile; e, come vedremo più avanti (Teorema 6.21) ogni gruppo numerabile è isomorfo ad un sottogruppo di un gruppo 2-generato..

Tuttavia, vi sono dei casi in cui è possibile affermare la finita generabilità di (certi) sottogruppi. Abbiamo visto, ad esempio, che ogni sottogruppo di un gruppo nilpotente finitamente generato è finitamente generato (Lemma 5.25). Ma, senza dover restringersi a particolari classi di gruppi, vi è anche un importante caso che sussiste in generale, che è quello dei sottogruppi di indice finito.

Teorema 6.1. *Un sottogruppo di indice finito di un gruppo finitamente generato è finitamente generato.*

Questo risultato discende immediatamente dal seguente,

Lemma 6.2. *Sia H un sottogruppo di G, $\mathcal{T}$ un sistema di rappresentanti delle classi laterali destre di G modulo H tale che $1 \in T$, e $\tau : G \to \mathcal{T}$ la proiezione associata a $\mathcal{T}$ (cioè $H(g\tau) = Hg$, per ogni $g \in G$). Sia X un sistema di generatori del gruppo G; allora l'insieme degli elementi*

$$Y = \{(tx)[(tx)\tau]^{-1} \mid t \in \mathcal{T},\ x \in X \cup X^{-1}\}$$

costituisce un sistema di generatori di H.

Dimostrazione. Che per ogni $t \in \mathcal{T}$ e $x \in X \cup X^{-1}$ si abbia $(tx)[(tx)\tau]^{-1} \in H$ viene immediatamente dalla definizione di τ. Sia $h = x_1 x_2 \dots x_n$ un elemento di H, con $x_1, \dots, x_n \in X \cup X^{-1}$. Poniamo $t_1 = x_1\tau = (1x_1)\tau$ e, per $2 \leq i \leq n$, $t_i = (t_{i-1}x_i)\tau$. Quindi $x_1 t_1^{-1} \in M$ e $t_{i-1}x_i t_i^{-1} \in M$ per ogni $i = 2, \dots, n$. Allora

$$h = (x_1 t_1^{-1})t_1 x_2 \dots x_n = (x_1 t_1^{-1})(t_1 x_2 t_2^{-1})t_2 x_3 \dots x_n = (x_1 t_1^{-1})(t_1 x_2 t_2^{-1}) \dots (t_{n-1}x_n t_n^{-1})t_n$$

e poiché $(x_1 t_1^{-1})(t_1 x_2 t_2^{-1}) \dots (t_{n-1}x_n t_n^{-1})$ appartiene ad H, si ha $t_n \in H$ e dunque $t_n = 1$. Quindi

$$h = (x_1 t_1^{-1})(t_1 x_2 t_2^{-1}) \dots (t_{n-1}x_n t_n^{-1})$$

è un prodotto di elementi di M, e ciò completa la dimostrazione. ■ Un altra considerazione fondamentale riguardante i sottogruppi di indice finito di un gruppo f.g. è la seguente.

Proposizione 6.3. *Sia G un gruppo finitamente generato. Allora per ogni intero $n \geq 1$ il numero di sottogruppi di G il cui indice è al più n è finito.*

Dimostrazione. Sia G un gruppo finitamente generato e $X = \{x_1, \dots, x_d\}$ un suo sistema finito di generatori. Sia H un sottogruppo di indice al più n di G; per quanto osservato nella sezione 3.1, H contiene un sottogruppo normale H_G il cui indice è al più $n!$. È dunque sufficiente provare che per ogni $n \geq 1$ è finito il numero di sottogruppi normali di G il cui indice è al più n.
Sia F un qualsiasi gruppo; dalla (4.3) segue che ogni omomorfismo $\phi : G \to F$ è determinato dalla d-upla delle immagini degli elementi di X. Se F è finito, per ogni x_i c'è un numero finito di possibili $\phi(x_i)$, e dunque c'è un numero finito di omomorfismi $G \to F$. Ora, per ogni $1 \leq \in \mathbb{N}$, il numero (a meno di isomorfismo) di gruppi finiti di ordine al più n è finito; si deduce che i possibili omomorfismi da G il cui nucleo ha indice al più n sono in numero finito. Picoé ogni sottogruppo normale di G di indice al più n è il nucleo di qualche omomorfsimo da G in un gruppo di ordine al più n, la dimostrazione è finita. ■

Sottogruppo di Frattini. Ricordiamo che il sottogruppo di Frattini $\Phi(G)$ di un gruppo G è l'intersezione di tutti i sottogruppi massimali di G, nel caso ce ne siano, mentre $\Phi(G) = G$ se G non ha sottogruppi massimali (vedi Sezione 5.3).

Un elemento g del gruppo G si dice un *non-generatore* se, per ogni $X \subseteq G$, $G = \langle X, g\rangle$ implica $G = \langle X\rangle$.

Proposizione 6.4. *In ogni gruppo G il sottogruppo di Frattini $\Phi(G)$ coincide con l'insieme dei non-generatori di G.*

DIMOSTRAZIONE. Denotiamo con S l'insieme di tutti i non-generatori di G.
Sia $g \in \Phi(G)$, e supponiamo esista un $X \subseteq G$ tale che $\langle X, g\rangle = G$ ma $\langle X\rangle \neq G$. Sia $\mathcal{L}$ l'insieme di tutti i sottogruppi T di G tale che $\langle X\rangle \leq T$ e $g \notin T$, ordinato per inclusione. $\mathcal{L}$ non è vuoto dato che $\langle X\rangle \in \mathcal{L}$, e l'unione di ogni catena di elementi di $\mathcal{L}$ è ancora un elemento di $\mathcal{L}$. Per il Lemma di Zorn, $\mathcal{L}$ ha elementi massimali; sia M uno di questi. M è massimale in G: infatti se $M < K \leq G$, allora $K \notin \mathcal{L}$ e dunque $g \notin K$, e pertanto $K \geq \langle M, g\rangle \geq \langle x, g\rangle = G$. Poiché $g \notin M$ segue che $g \notin \Phi(G)$, una contraddizione. Questo dimostra che $\Phi(G) \leq S$.
Se $G = \Phi(G)$ abbiamo finito. Altrimenti sia M un sottogruppo massimale di G e sia g un non-generatore. Allora $\langle M, x\rangle \neq G$ e quindi, essendo M massimale, deve essere $\langle M, x\rangle = M$, cioè $x \in M$. Quindi $S \leq \Phi(G)$ e la dimostrazione è completa. ∎

Corollario 6.5. *Sia G un gruppo finitamente generato; se H un sottogruppo proprio di G, allora esiste un sottogruppo massimale di G che contiene H. In particolare $\Phi(G) \neq G$.*

Così, in particolare, si estende il Lemma al caso di gruppi f.g.

La condizione di massimo. Un gruppo G soddisfa la *condizione di massimo* sui sottogruppi (abbreviato: *Max*) se ogni catena $H_0 \leq H_1 \leq H_2 \leq \dots$ di sottogruppi di G è finita (cioè esiste $n \geq 0$ tale che $H_i = H_n$ per ogni $i \geq n$).

Proposizione 6.6. *Un gruppo G soddisfa Max se e solo se ogni sottogruppo di G è finitamente generato.*

DIMOSTRAZIONE. Sia H un gruppo non finitamente generato, allora per ogni sottoinsieme finito U di H esiste $x \in H$ tale che $\langle U\rangle < \langle U, x\rangle$; dunque esiste una successione infinita $x_1, x_2, \dots$ di elementi di H tale che, posto, er ogni $n \geq 1$, $X_n = \langle x_1, x_2, \dots, x_n\rangle$ la catena ascendente $X_1 < X_2 < X_3 \dots$ di sottogruppi di H non ha un massimo elemento. Da questo segue che, poiché ovviamente la prorpietà *Max* si eredita ai sottogruppi, i sottogruppi di un gruppo che la soddisfa sono f.g.

Viceversa, sia G un gruppo ogni cui sottogruppo è f.g., e sia $H_0 \leq H_1 \leq H_2 \leq \dots$ una catena ascendente di sottogruppi di G. Posto $H = \bigcup_{n\in\mathbb{N}} H_n$, si ha che H è un sottogruppo di G, dunque finitamente generato. Sia $H = \langle x_1, \dots, x_n\rangle$; allora per ogni $i = 1, \dots, n$, $x_i \in H_{n(i)}$ per qualche $n(i) \in \mathbb{N}$, e dunque $H = H_n$ dove $n = \max\{n(i) \mid i = 1, \dots, n\}$. ∎

Un gruppo nilpotente soddisfa *Max* se e solo se è finitamente generato (Lemma 5.25), mentre il caso dei gruppi risolubili lo tratteremo nella prossima sezione. Ciò non deve far pensare che la classe dei gruppi con *Max* sia, in generale, trattabile: una notevole e complessa costruzione di Ol'shanskii porta al seguente e sorprendente risultato:

Teorema 6.7. *Per ogni primo p sufficientemente grande, esiste un gruppo infinito in cui ogni sottogruppo proprio non-banale è ciclico di ordine p.*

Gruppi come questi (oltre ad essere familiarmente chiamati "mostri di Tarski") sono chiaramente 2-generati e soddisfano *Max*.

6.2 Gruppi policiclici

Un gruppo G si dice *policiclico* se ammette una serie finita a fattori ciclici. Ogni gruppo policiclico è (per definizione) risolubile, ed è piuttosto ovviamente finitamente generato; infatti se G è un gruppo policiclico e

$$1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$$

è una serie a fattori ciclici, allora per ogni $i = 1, \dots n$ esiste un $x_i \in G_i$ tale che $G_{i-1}x_i$ è un generatore del gruppo ciclico G_i/G_{i-1}; si riconosce allora che $\{x_1, \dots, x_n\}$ è un sistema di generatori di G.

Ogni gruppo risolubile finito è policiclico, mentre l'esempio più immediato di un gruppo policiclico infinito e non abeliano è il gruppo diedrale infinito, che ha una serie i cui due fattori sono un ciclico infinito ed uno di ordine 2; la Proposizione 5.31 dice poi, in particolare, che ogni gruppo nilpotente finitamente generato è policiclico. Un gruppo periodico è policiclico se e solo se è risolubile e finito.

Alcuni aspetti di base riguardanti la classe dei gruppi policiclici si possono dimostrare molto facilmente, come il fatto che *quozienti e sottogruppi di un gruppo policiclico sono policiclici*, e che *se $N \trianglelefteq G$ e sia N che G/N sono policiclici allora G è policiclico*, in particolare il prodotto diretto di un numero finito di gruppi policiclici è policiclico.

Esempio 6.3. Per $n \geq 1$ il gruppo delle matrici triangolari $G = T(n, \mathbb{Z})$ è policiclico. Infatti, G è il prodotto semidiretto del gruppo delle matrici unitriangolari $U = UT(n, \mathbb{Z})$ per il gruppo H delle matrici diagonali i cui elementi diagonali sono ± 1. U è policiclico perché nilpotente e finitamente generato (vedi sezione 5.4), mentre H è chiaramente isomorfo al prodotto diretto di n copie del gruppo ciclico di ordine 2, quindi è finito. □

Dal fatto che ogni sottogruppo di un gruppo policiclico è policiclico segue subito l'osservazione

Proposizione 6.8. *Sia G un gruppo policiclico. Allora ogni sottogruppo di G è finitamente generato.*

Quindi, un gruppo abeliano (o, meglio, nilpotente) è policiclico se e soltanto se è finitamente generato; mentre il gruppo del Lampionaio, che ammette sottogruppi non finitamente generati, è, ci fossero stati dei dubbi, un gruppo risolubile f.g. ma non policiclico. Dalla Proposizione 6.8, assieme alla Proposizione 6.6, si deduce agevolmente la seguente caratterizzazione dei gruppi policiclici.

Proposizione 6.9. *Sia G un gruppo risolubile. Sono equivalenti*

1. *G è policiclico;*
2. *ogni sottogruppo di G è finitamente generato;*
3. *G soddisfa la condizione di massimo per sottogruppi.*

Dimostrazione. Modulo quanto già dimostrato, basta ora provare che un gruppo risolubile G in cui ogni sottogruppo è finitamente generato è policiclico; cosa che facciamo Procedendo per induzione sulla lunghezza derivata d di G. Se $d = 1$, G è abeliano finitamente generato, e dunque è policiclico. Sia quindi $d > 1$ e poniamo $N = G'$. N è finitamente generato e tali

sono tutti i suoi sottogruppi; poiché ha lunghezza derivata $d-1$ si ha, per ipotesi induttiva, che N è policiclico. Inoltre G/N è policiclico in quanto finitamente generato e abeliano. Per un osservazione fatta sopra, si conclude che G è policiclico. ∎

Ovviamente, il numero di termini in una serie a fattori ciclici di un gruppo policiclico G non è invariante; tuttavia è invariante quello dei termini infiniti.

Lemma 6.10. *Sia G un gruppo policiclico:*

(i) *il numero di fattori infiniti (cioè isomorfi a $\mathbb{Z}$) in una serie a fattori ciclici di G è un invariante $h(G)$ di G;*

(ii) *se G è infinito, G ammette un sottogruppo normale infinito A che è abeliano libero (di rengo al più $h(G)$);*

(iii) *G ammette un sottogruppo normale H privo di torsione di indice finito;*

Dimostrazione. (i) Sia $\mathcal{C}$ una serie a fattori ciclici di G e sia h il numero di fattori infiniti in $\mathcal{C}$; è chiaro che ogni serie che raffina $\mathcal{C}$ ha esattamente lo stesso numero di fattori infiniti. Se $\mathcal{C}'$ è un'altra serie a fattori ciclici di G allora, per il Teorema di raffinamento 2.9, $\mathcal{C}$ e $\mathcal{C}'$ ammettono raffinamenti concordanti, dunque con lo stesso numero di fattori ciclici; per quanto osservato, tale numero deve essere h.

(ii) Induzione sulla lunghezza derivata d di G. Se $d=1$, G è abeliano finitamente generato e l'asserto viene immediatamente dal Teorema 5.6. Sia $d \geq 2$ e $A = G^{(d-1)}$; A è un gruppo abeliano f.g.; se A è infinito, segue dal Teorema 5.6 che esiste $n \geq 1$ tale che A^n è abeliano libero infinito; siccome $A^n charA \trianglelefteq G$ si ha $A^n \trianglelefteq G$. Supponiamo A finito; allora G/A è infinito e per ipotesi induttiva ammette un sottogruppo normale H/A abeliano libero infinito Ora, $B = C_H(A)$ ha indice finito in H, è normale in G, inoltre è nilpotente e finitamente generato, quindi (esercizio 5.28), $Z(B)$ è infinito (e f.g.); come prima, esiste allora $n \geq 1$ tale che $N = Z(B)^n$ è abeliano libero infinito; infine $N charZ(B) charB \trianglelefteq G$ e dunque $N \trianglelefteq G$.

(iii) Poiché G soddisfa la condizione di massimo sui sottogruppi, esiste un sottogruppo N di G massimale per essere normale e privo di torsione. Se G/N è infinito ammette, per il punto precedente, un sottogruppo normale abeliano infinito e privo di torsione M/N; ma allora M è normale e privo di torsione, contro la scelta di N. Dunque G/N è finito. ∎

L'invariante $h(G)$ del punto (i) è detto *lunghezza di Hirsch* del gruppo policiclico G.

Esempio 6.4. Oltre agli esempi più o meno banali già citati, una maniera per costruire gruppi policiclici è la seguente. Fissato un intero $n \geq 1$ sia $A \in GL(n,\mathbb{Z})$; allora ad A è naturalmente associato un automorfismo del gruppo additivo $\mathbb{Z}^n$; il conseguente prodotto semidiretto $\mathbb{Z}^n \rtimes \langle A \rangle$ è un gruppo policiclico, la cui lunghezza di Hirsch è n o $n+1$ a seconda che $|A|$ sia finito o infinito. □

Teorema 6.11. (Mal'cev) *Ogni sottogruppo H di un gruppo policiclico G è l'intersezione dei sottogruppi di indice finito di G che contengono H.*

Dimostrazione. Procediamo per induzione sulla lunghezza di Hirsch $h = h(G)$. Se $h=0$, G è finito e non c'è nulla da provare. Sia quindi $h \geq 1$. In particolare G è infinito e dunque per il punto (ii) del Lemma 6.10 esiste un sottogruppo normale A di G abeliano

libero infinito (quindi $A \simeq \mathbb{Z}^d$ per qualche $1 \leq d \leq h$). Supponiamo, per assurdo, che G non soddisfi la proprietà enunciata e per ogni $K \leq G$ denotiamo con $\overline{K}$ l'intersezione di tutti i sottogruppi di indice finito in G che contengono K; allora, per la condizione di massimo, esiste un sottogruppo H di G massimale tale che $H \neq \overline{H}$. Per ipotesi induttiva (applicata al quoziente G/A, $\overline{AH} = AH$; in particolare $\overline{H} \leq AH$; inoltre, per la massimalità di H, $K\overline{K} \geq overline H$ per ogni $H < K \leq G$. Supponiamo $A_0 = A/A \cap H$ sia infinito; allora (per il teorema di struttura dei gruppi abeliani finitamente generati) esiste un primo p tale che $\bigcap_{n\geq 1} A_0^{p^n} = 1$; poniamo, per ogni $n \geq 1$, $B_n = A^{p^n}(A \cap H)$ (quindi $A_0^{p^n} = B_n/A \cap H$ e $[A : B_n] \leq (p^n)^d)$). Siccome H normalizza $A \cap H$, H normalizza B_n per ogni n, $B_n H \leq G$ e $B_n H > H$ (altrimenti $B_n \leq A \cap H$ contro l'assunzione che $A/A \cap H$ sia infinito). Dunque per quanto osservato sopra $\overline{H} \leq B_n H$ per ogni $n \geq 1$. Quindi

$$\overline{H} \leq \bigcap_{n\geq 1} B_n H = H\big(\bigcap_{n\geq 1} B_n\big) = H(H \cap A) = H$$

contro la scelta di H.

Dunque $A/A \cap H$ è finito, e quindi esiste $n \geq 1$ tale che $M := A^n \leq A \cap H$. Ora, M è normale in G ed è infinito; quindi (considerando una serie a fattori ciclici in cui uno dei termini e M) $h(G/M) \leq h(G) - 1$. Poiché $M \leq H$, per ipotesi induttiva H/M è l'intersezione dei sottogruppi di indice finito di G/M contenenti H/M e dunque (per il Teorema di Corrispondenza) $\overline{H} = H$. Contraddizione che conclude l'argomento. ∎

Specializzando al caso $H = 1$ si ha

Corollario 6.12. *Ogni gruppo policiclico è residualmente finito.*

Un gruppo G è *policiclico per finito* se ammette un sottogruppo H policiclico e di indice finito.

Esempio 6.5. Sia H un gruppo finito e F_n un gruppo libero di rango finito tale che $H \simeq F_n/N$ per $N \trianglelefteq F_n$. Per l Teorema di Nielsen–Schreier, che vedremo più avanti (Teorema 7.8), N è libero di rango finito; quindi, per $c \geq 2$, $N/\gamma_c(N)$ è un gruppo nilpotente finitamente generato (e privo di torsione: vedi sezione 5.7) quindi policiclico. Poiché $\gamma_c(N)$ è caratteristico in N, è normale in F_n e il gruppo $F_n/\gamma_c(N)$ è un gruppo policiclico per finito. □

Citiamo quindi, senza dimostrazione, un importante risultato di Mal'cev.

Teorema 6.13. (Mal'cev) *Sia G un gruppo policiclico per finito; ogni sottogruppo risolubile di $Aut(G)$ è policiclico. In particolare, per ogni $n \geq 1$, ogni sottogruppo risolubile di $GL(n, \mathbb{Z})$ è policiclico.*

E l'altrettanto importante enunciato inverso: il quale assicura la rappresentabilità di ogni gruppo policiclico come un gruppo di matrici invertibili a coefficienti interi.

Teorema 6.14. (Auslander) *Ogni gruppo policiclico-per-fimito è isomorfo ad un sottogruppo di qualche $GL(n, \mathbb{Z})$.*

6.3 Gruppi finitamente presentati

Per diverse regioni, un caso particolarmente importante di presentazioni è costituito da quelle finite; dove una presentazione $G = \langle X \mid R \rangle$ si dice finita se sia X che R sono finiti Un gruppo che ammette una presentazione finita si dice *finitamente presentato*. Per dire una delle ragioni di cui sopra, il gruppo fondamentale di ogni varietà topologica compatta è finitamente presentato.
Ogni gruppo finito è (ovviamente) finitamente presentato: la tavola di moltiplicazione di un gruppo finito fornisce infatti relazioni sufficienti a presentarlo (un'altra dimostrazione viene applicando il Teorema 6.1); ed è finitamente presentato ogni gruppo libero finitamente generato. In effetti, tutti gli esempi di presentazione che abbiamo esaminato sin qui hanno riguardato presentazioni finite; in particolare l'esempio 4.3 mostra come sottogruppi normali di gruppi finitamente presentati non siano necessariamente finitamente generati. Un esempio di gruppo finitamente generato ma non finitamente presentato è il gruppo del Lampionaio; questo proveremo tra poco; prima diciamo solo che il punto di partenza per provare affermazioni del genere è la seguente osservazione:

Proposizione 6.15. *Sia G un gruppo finitamente presentato. Per ogni sistema di generatori X di G esiste un sottoinsieme finito $Y \subseteq X$ tale che G ha un presentazione finita nei generatori Y.*

Dimostrazione. La dimostrazione non è difficile ma non ho voglia di scriverla. ∎

Gruppi f.g. non finitamente presentati. Sia $L = \mathbb{Z}_2 \wr \mathbb{Z}$, il gruppo del Lampionaio (sezione 3.5). Non è complicato provare che L ammette la seguente presentazione

$$L = \langle a, x \mid a^2 = 1,\ [a^{x^i}, a] = 1, i \in \mathbb{Z} \rangle \tag{6.1}$$

dovd $\langle x \rangle = \mathbb{Z}$ è il complemento e $a \neq 1$ un elemento della base. Supponiamo, per assurdo, che L sia finitamente presentato. Esisterebbe allora, per la Proposizione 6.15, una presentazione finita di L negli stessi generatori a, x con relazioni $r_1, \ldots, r_n$. Detta in maniera scorrevole, ogni relazione r_j è una conseguenza delle relazioni in (6.1), cioè un prodotto di un numero finito di tali relazioni o loro coniugati; poiché il numero delle r_j è finito, è possibile selezionare un insieme finito S di relazioni in (6.1) tale che ogni r_j è conseguenza di relazioni in S. Allora, esiste $t \in \mathbb{N}$, tale che $S \subseteq \{a^2, [a^{x^i}, a], -t \leq i \leq t\}$. Per il Lemma di von Dyck, L ammette un quoziente isomorfo al gruppo

$$\langle a, x \mid a^2 = 1,\ [a^{x^i}, a] = 1, -t \leq i \leq t \rangle. \tag{6.2}$$

Deriveremo un assurdo, provando che L non può avere un tale quoziente.
Sia $n = 2t + 3$ e, nel gruppo $SL(n, 2)$ consideriamo le trasvezioni $1 + e_{ij}$ $(1 \leq i \neq j \leq n)$; queste sono elementi di ordine 2 in $SL(n, 2)$; poniamo $a = 1 + e_{12}$. Quindi, sia x la matrice associata all'endomorfismo dello spazio $GF(2)^n$ che permuta i vettori della base (la base è qualla canonica e l'azione delle matrici sulla destra) come il ciclo

$$\sigma = (1\ 3 \ldots n-2\ n\ 2\ 4 \ldots n-1).$$

Si vede immediatamente che, per ogni $i \neq j$, $(1 + e_{ij})^x = 1 + e_{i^\sigma j^\sigma}$. Dalle formule di composizione di trasposizioni (3.13) segue che

$$[1 + e_{ij}, 1 + e_{rs}] = 1 \quad \Leftrightarrow \quad i \neq s,\ j \neq r. \tag{6.3}$$

Ora, per $0 \leq m \leq 2t$, $2m+2 \leq n$, e quindi si vede che $a^{x^t} = 1 + e_{1+2m,2+2m}$ commuta con a ovvero $[a, a^{x^t}] = 1$ per ogni $0 \leq t \leq 2m$, il che equivale a

$$[a, a^{x^t}] = 1 \quad \text{per ogni } -m \leq t \leq m.$$

Dunque il sottogruppo H di $SL(n,2)$ generato da $\{a, x\}$ soddisfa alle relazioni
D'altra parte, in H, $a^{x^{m+1}} = 1 + e_{n2}$ non commuta con a; quindi H non può essere un quoziente di L (si può anzi provare che $H = SL(n,2)$); una contraddizione.

Osserviamo che, poiché il gruppo libero generato da a e x è finitamente presentato, questo esempio mostra che quozienti di gruppi finitamente presentati non sono necessariamente finitamente presentati.

Per contro, il seguente risultato (dovuto a P. Hall) può servire per fornire esempi di gruppi finitamente presentati.

Teorema 6.16. *Sia G un gruppo; se esiste un sottogruppo $N \trianglelefteq G$ tale che N e G/N sono finitamente presentati allora G è finitamente presentato.*

Dimostrazione. Siano G ed N come nelle ipotesi. Siano $y_1, \ldots, y_n \in G$ tali che gli elementi $Ny_1, \ldots, Ny_m$ costituiscono un sistema di generatori di G/N associato ad una presentazione finita $G/N = \langle u_1, \ldots, u_m \mid r_1, \ldots, r_s \rangle$, e sia $N = \langle x_1, \ldots, x_n \mid s_1, \ldots, s_t \rangle$ una presentazione finita di N. Allora $G = \langle y_1, \ldots, y_m, x_1, \ldots, x_n \rangle$. sia $X = \{x_1, \ldots, x_n\}$ un suo sistema di generatori. Poiché G/N è finitamente presentato, applicando la Proposizione 6.15 si deduce che esiste un insieme finito $s_1, \ldots, s_t$ di parole nelle variabili $X \cup X^{-1}$ tale che, in G, $g_i = s_i(x_1, \ldots, x_n) \in N$ per ogni $i = 1, \ldots n$ e N è generato dall'insieme $\mathcal{R}$ di tutti i coniugati in G degli elementi g_i. Poiché N è finitamente generato, dalla Proposizione 6.15 segue che esiste un sottoinsieme finito $Y = \{y_1, \ldots, y_t\}$ di $\mathcal{R}$ ed un insieme finito $r_1, \ldots, r_m$ di parole in $Y \cup Y^{-1}$ tali che

$$N = \langle Y \mid r_1, \ldots, r_m \rangle.$$

Ora, ogni elemento $y_j \in Y$ può essere espresso come una parola $\omega_j(x_1, \ldots, x_n)$ in $X \cup X^{-1}$, e quindi ogni r_i è una parola $\bar{r}_i = r_i(\omega_1, \ldots, \omega_t)$. Osserviamo che per ogni x nel gruppo libero $F(X)$ ed ogni $i = 1, \ldots, m$, $\bar{r}_i^x = r_i(\omega_1^x, \ldots, \omega_t^x) = r_i^x \in N$. Poniamo

$$W = \langle x_1, \ldots, x_n \mid \bar{r}_1, \ldots, \bar{r}_m \rangle.$$

Per costruzione, il nucleo dell'omomorfismo $\phi : F(X) \to G$ (quello dato da, con abuso di notazione, $x_i \mapsto x_i$) contiene $\bar{r}_i$ per ogni $i = 1, \ldots, n$, e quindi induce un omomorfismo suriettivo $\overline{\phi} : W \to G$. Sia $\omega \in \ker \phi$, allora, in G, $\omega(x_1, \ldots, x_n) = 1 \in N$, quindi, in prima battuta, $\omega \in \langle \mathcal{R} \rangle$, e poi ancora $\omega \in \langle r_1, \ldots, r_m \rangle^Y \langle \mathcal{R} \setminus Y \rangle^{F(X)} \leq \langle \mathcal{R} \rangle^{F(X)}$ ∎

Gruppi hopfiani. Un gruppo G si dice *hopfiano* se non è isomorfo ad alcun suo quoziente proprio (cioè $G \not\cong G/N$ per ogni $1 \neq N \trianglelefteq G$). Sono ad esempio hopfiani tutti i gruppi finiti, i gruppi semplici e i gruppi liberi di rango finito (vedi esercizio 4.18 oppure la prossima proposizione), anche il gruppo additivo $\mathbb{Q}$ dei razionali. Di contro, non è difficile trovare gruppi non-hopfiani tra quelli non finitamente generati: ad esempio sono non-hopfiani, i gruppi di Prüfer C_∞, i gruppi liberi di rango infinito cos come i gruppi abeliani liberi di rango infinito. Più difficile è reperire gruppi finitamente generati non-hopfiani (questa era la domanda originalmente posta da H. Hopf (1894–1971)). Ad esempio, vale il seguente risultato

Proposizione 6.17. *Ogni gruppo finitamente generato e residualmente finito è hopfiano.*

DIMOSTRAZIONE. Sia G un gruppo f.g. residualmente finito e sia $\phi : G \to G$ un omomorfismo suriettivo. Supponiamo per assurdo che esista $1 \neq x \in K = \ker \phi$. Poiché G è residualmente finito esiste un sottogruppo normale N di indice finito in G tale che $x \notin N$. Poiché G è finitamente generato il numero di sottogruppi normali di G il cui indice è al più $k = |G/N|$ è finito; siano $M_1, \ldots, M_n$ tali sottogruppi. Allora le retroimmagini $\phi^{-1}(M_1), \ldots, \phi^{-1}(M_n)$ sono n sottogruppi normali e distinti di G di indice al più k, qundi tra di loro c'è anche il sottogruppo N, il che è una contraddizione dato che $N \not\geq K$. ∎

Ma gruppi f.g. non hopfiani esistono: un caso risolubile è descritto nell'esercizio 6.18, qui vediamo che nemmeno i gruppi finitamente presentati sono necessariamente hopfiani.

Dati due interi non nulli $m, n \in \mathbb{Z} \setminus \{0\}$, il gruppo con presentazione

$$BS(n, m) = \langle a, b \mid a^{-1}b^n a = b^m \rangle$$

è detto un gruppo di Baumslag–Solitar.

Proposizione 6.18. *IL gruppo di Baumslag–Solitar $BS(2, 3)$ è non-hopfiano. Quindi esistono gruppi finitamente presentati non-hopfiani.*

DIMOSTRAZIONE. Sia $G = BS(2, 3) = \langle a, b \mid a^{-1}b^2a = b^3 \rangle$, e sia $H = \langle a, b^2 \rangle$. Ora $a^{-1}(b^2)^2a = (a^{-1}b^2a^2 = b^6 = (b^2)^3$; quindi per il teorema di van Dyck, esiste un omomorfismo $\phi : G \to H$ tale che $a\phi = a$ e $b^2 = b\phi$. Ma, poichè $[b^2, a] = b^{-2}b^3 = b$, si ha $H = G$. Proviamo che ϕ non è iniettivo. Sia $u = [b, a]^2b^{-1}$: per la definizione di ϕ e quanto appena osservato,

$$u\phi = [b^2, a]^2b^{-2} = b^2b^{-2} = 1$$

quindi $u \in \ker \phi$. Consideriamo ora il gruppo $K = \langle x, y \mid x^7 = y^6 = 1,\ x^y = x^5 \rangle$ (che è - lo si dimostri - il prodotto semidiretto di un gruppo ciclico $\langle x \rangle$ di ordine 7 per un gruppo ciclico $\langle y \rangle$ di ordine 6) ed osserviamo che $(x^2)^y = x^{10} = x^3$; dunque K è un immagine omomorfa di G, mediante un omomorfismo η che manda b in x ed a in y; valutato nell'elemento u,

$$u\eta = [x, y]^2x^{-1} = (x^{-1}x^y)^2x = x^9 = x^2 \neq 1.$$

Dunque $u \neq 1$ e pertanto $N = \ker \phi \neq 1$, il che mostra che G è non-hopfiano. ∎

6.4 Estensioni HNN

Prodotti liberi amalgamati. Siano G_1, G_2, H gruppi e $\phi_i : H \to G_i$ $(i = 1, 2)$ omomorfismi iniettivi; il *prodotto amalgamato* $G_1 *_H G_2$ è il massimo quoziente del prodotto libero $G_1 * G_2$ nel quale i sottogruppi $H\phi_1, H\phi_2$ sono identificati (elemento per elemento). Quindi

$$G_1 *_H G_2 = \frac{G_1 * G_2}{N} \tag{6.4}$$

dove N è il sottogruppo normale di $G_1 * G_2$ generato da tutti i coniugati degli elementi del tipo $(x\phi_1)(x\phi_2)^{-1}$ $(x \in H)$.

Se $\langle X \mid R\rangle$, $\langle Y \mid S\rangle$ sono presentazioni, rispettivamente di G_1 e di G_2, allora

$$G_1 *_H G_2 = \langle X \cup Y \mid R, S, (x\phi_1)(x\phi_2)^{-1}\ (x \in H)\rangle. \tag{6.5}$$

Il prodotto amalgamato svolge un ruolo naturale in topologia: il Teorema di Seifert–Van Kampen dice il gruppo fondamentale dell'unione di due spazi topologici lungo un sottospazio (dove tutto quanto è connesso per archi) è il prodotto amalgamato dei gruppi fondamentali dei due spazi rispetto al gruppo fondamentale dell'intersezione.

Esempio 6.6. Siano $G_1 = \langle a\rangle$, $G_2 = \langle b\rangle$ gruppi ciclici e $H = \mathbb{Z}$; fissiamo gli omomorfismi $\phi_1 : \mathbb{Z} \to G_1$, $\phi_2 : \mathbb{Z} \to G_2$ ponendo $z\phi_1 = a^{2z}$, $z\phi_2 = b^3 z$ (per ogni $z \in \mathbb{Z}$) □

Esempio 6.7. Non è sempre così agevole determinare la forma di un prodotto amalgamato; consideriamo ad esempio il prodotto $PSL(2,\mathbb{Q}) *_{\mathbb{Z}} \mathbb{Z}$ dove ϕ_1 e ϕ_2 è una qualsiasi coppia di omomorfismi iniettivi da $\mathbb{Z}$ in $PSL(2,\mathbb{Q})$ e in $\mathbb{Z}$, rispettivamente. Osserviamo che le immagini $x = 1\phi_1$ e $y = 1\phi_2$ sono elementi di ordine infinito. Se N è il sottogruppo normale del prodotto amalgamato $PSL(2,\mathbb{Q})*\mathbb{Z}$ come in (6.4) allora per ogni $z \in \mathbb{Z}$ (come sottogruppo del prodotto) si ha

$$N \ni (y^{-1}x)^{-1}(y^{-1}x)^z = x^{-1}x^z$$

(questo esempio è tratto da un esercizio nel libro *Trees* di J.P. Serre). □

Anche il prodotto amalgamato, come è facile prevedere, soddisfa una proprietà universale, la cui dimostrazione omettiamo.

Proposizione 6.19. *Siano H e K sottogruppi isomorfi dei gruppi G_1, G_2, e $f : H \to K$ un fissato isomorfismo. Allora per ogni gruppo G ed omomorfismi $\alpha_i : G_i \to G$ $(i = 1, 2)$ tali che $xf\alpha_2 = x\alpha_1$ per ogni $x \in H$, esiste un'unico omomorfismo $\phi : G_1 *_H G_2 \to G$ tale che ristretto a G_1 coincide con α_i (per $i = 1, 2$).*

Dove, per non sovraccaricare di notazione l'enunciato, i gruppi G_i sono visti nel modo ovvio come sottogruppi del prodotto $G_1 *_H G_2$.

Estensioni HNN. Le estensioni HNN (acronimo dei nomi degli scopritori: Graham Higman, Bernhard Neumann e Hanna Neumann) sono uno strumento fondamentale, e per così dire idiomatico, nella teoria dei gruppi infiniti. Sono quelle che comp[aiono nel seguente e un poco sorprendente risultato.

Teorema 6.20. (G. Higman, B. Neumann, H. Neumann) *Siano H, K sottogruppi isomorfi di uno stesso gruppo G, e $\alpha : H \to K$ un fissato isomorfismo. Allora G può essere immerso in un gruppo $\overline{G}$ nel quale α è indotto da un automorfismo interno.*

Dimostrazione. Siano G, H, K e α come nelle ipotesi. Poniamo $U = G * \langle u\rangle$, $V = G * \langle v\rangle$, con $\langle u\rangle$ e $\langle v\rangle$ gruppi ciclici infiniti. Nel gruppo U si vede che $R = \langle G, H^u\rangle = G * H^u$, similmente in V, $S = \langle G, H^u\rangle = G * K^v$. Ora, esiste un omomorfismo $\phi : R \to S$ tale che $g\phi = g$ per ogni $g \in G$ e $(h^u)\phi = (h\alpha)^v$ per ogni $h \in H$. È immediato verificare che ϕ è un isomorfismo. A questo punto, si considera il prodotto libero amalgamato $\overline{G} = U *_\phi V$ in cui R è amalgamato a S tramite ϕ. Sia ha $G \leq \overline{G}$, e per ogni $h \in H \leq G$,

$$h^u = (h^u)\phi = (h\alpha)^v,$$

quindi $h\alpha = h^{uv^{-1}}$, e questo mostra che α è indotto dal coniugio per uv^{-1}. ∎

Osservazione. Se il gruppo G è senza torsione, allora, per l'esercizio 4.22, anche U e V lo sono, e per ragioni simili anche $\overline{G}$ è senza torsione.

Se, con le notazioni della dimostrazione precedente, poniamo $t = uv^{-1}$, il gruppo (sottogruppo di $\overline{G}$) $\langle G, t\rangle$ è detto una *HNN-estensione* di G.

Teorema 6.21. (H.N.N.) *Ogni gruppo numerabile è isomorfo ad un sottogruppo di un gruppo* 2*-generato.*

Dimostrazione. Sia $H = \{1 = x_0, x_1, x_2, \dots\}$ un gruppo numerabile e $F = F_2$ il gruppo libero generato da $\{a, b\}$. Si considerino i due sottogruppo del prodotto libero $G = H * F$,

$$A = \langle a, a^b, a^{b^2}, \dots\rangle \qquad \text{e} \qquad B = \langle bx_0, b^a x_1, b^{a^2} x_2, \dots\rangle$$

Allora (esercizio) $\{a, a^b, a^{b^2}, \dots\}$ è un sistema libero di generatori per A, e $\{bx_0, b^a x_1, b^{a^2} x_2, \dots\}$ un sistema libero di generatori per B. Dunque porre, per ogni $i \in \mathbb{N}$, $a^{b^i} \mapsto b^{a^i} x_i$, definisce un isomorfismo $\alpha : A \to B$. Un'applicazione del Teorema 6.20 assicura l'esistenza di una HNN-estensione $\overline{G} = \langle G, t\rangle$ in cui $(a^{b^i})^t = b^{a^i} x_i$, per ogni $i \in \mathbb{N}$. Ora, il sottogruppo $\langle a, t\rangle$ contiene $a^t = b$ e quindi contiene $(a^{b^i})^t = b^{a^i} x_i$. Dunque $\langle a, t\rangle$ contiene x_i, per ogni $i \in \mathbb{N}$, e pertanto $H \leq \langle a, t\rangle$. ∎

6.5 Crescita

Sia G un gruppo finitamente generato e sia X un suo sistema finito di generatori. Per ogni elemento $g \in G$ denotiamo con $\ell(g) = \ell_X(g)$ la *lunghezza* di g in X; ovvero $\ell(1) = 0$ e, se $g \neq 1$, $\ell(g)$ è il minimo intero $n \geq 1$ tale che $g = x_1 \dots x_n$ con $x_1, \dots, x_n \in X \cup X^{-1}$. In altri termini, $\ell(g)$ è la distanza del vertice g dal vertice 1 nel grafo di Cayley $\Gamma[G, X]$. In generale, per ogni $g, h \in G$, si avrà

$$d_{\Gamma[G,X]}(g, h) = \ell_X(g^{-1}h). \tag{6.6}$$

[Questo definisce una metrica sull'insieme dei vertici del grafo $\Gamma[G; X]$ e quindi sul gruppo stesso, la cui ovvia dipendenza dal sistema di generatori si può confinare mediante un'appropriata forma di equivalenza - vedi esercizio 6.33. Ciò consente di guardare al gruppo G come ad un oggetto geometrico; ed è infatti uno dei concetti fondanti di quella che si chiama "teoria geometrica dei gruppi"].

In maniera naturale si definiscono poi le palle (centrate in 1) ponendo, per ogni $n \in \mathbb{N}$,

$$B_G^X(n) = B^X(1, n) = \{g \in G \mid \ell_X(g) \leq n\}. \tag{6.7}$$

La *funzione di crescita.* γ_G^X del gruppo G rispetto al sistema di generatori X associa ad ogni $n \in \mathbb{N}$ il numero di elementi di G la cui X-lunghezza non supera n; ovvero

$$\gamma_G^X(n) = |B_G^X(n)|. \tag{6.8}$$

È chiaro che, fissato il gruppo G, la funzione di crescita γ_G^X dipende dal sistema di generatori X. Tuttavia funzioni di crescita in uno stesso gruppo, definite da sistemi diversi (finiti) di generatori, sono correlate in un senso molto preciso.

Date due funzioni $\gamma, \mu : \mathbb{N} \to \mathbb{R}$, poniamo $\gamma \preccurlyeq \mu$, se esiste una costante $1 \leq C \in \mathbb{N}$ tale che

$$\gamma(n) \leq \mu(Cn) \text{ per ogni } n \in \mathbb{N}.$$

Diciamo quindi che γ e μ sono *equivalenti*, scrivendo $\gamma \sim \mu$, se $\gamma \preccurlyeq \mu$ e $\mu \preccurlyeq \gamma$. È immediato verificare che $\preccurlyeq$ definisce un pre-ordine sull'insieme delle funzioni $\mathbb{N} \to \mathbb{R}$; quindi, $\sim$ è un'equivalenza e $\preccurlyeq$ induce una relazione d'ordine sulle classi ($[\gamma]_\sim \leq [\mu]_\sim$ se $\gamma \preccurlyeq \mu$).
Siano ora X e Y due sistemi finiti di generatori dello stesso gruppo G; allora esistono due interi positivi N e M tali che $X \subseteq B_G^Y(N)$ e $Y \subseteq B_G^X(M)$. Da ciò segue che ogni elemento di g che ha lunghezza ℓ in X ha lunghezza al più $N\ell$ in Y (si osservi che, per ogni elemento $g \in G$ ed ogni sistema finito di generatori U, $\ell_U(g^{-1}) = \ell_U(g)$, quindi nell nostro caso, $X \cup X^{-1} \subseteq B_G^Y(N)$); dunque $B_G^X(n) \leq B_G^Y(Nn)$ per ogni $n \geq 1$; similmente, $B_G^Y(n) \leq B_G^X(Mn)$. Ponendo $C = \max\{N, M\}$ si ottiene che $\gamma_G^X(n) \leq \gamma_G^Y(Cn)$ e $\gamma_G^Y(n) \leq \gamma_G^X(Cn)$, per ogni $n \in \mathbb{N}$. Abbiamo quindi provato il seguente elementare ma fondamentale fatto.

Proposizione 6.22. *Siano X e Y sistemi finiti di generatori del gruppo G. Allora le funzioni di crescita γ_G^X e γ_G^Y sono equivalenti.*

Quindi, se X è un sistema di generatori finito del gruppo G, la classe d'equivalenza $[\gamma_G^X]_\sim$ si chiama semplicemente *crescita* del gruppo G. È evidente che la crescita è invariante per isomorfismo; l'esercizio 6.32 stabilisce l'importante fatto che la crescita è invariante per sottogruppi di indice finito.

Esempio 6.8. Sia $r \geq 1$ e sia X un sistema libero di generatori del gruppo libero F_r. Denotiamo con $\sigma_r(n)$ il numero di elementi di F_r la cui X-lunghezza è esattamente n; poiché il grafo di Cayley di F_n rispetto a X è un albero regolare di grado $2r$ (Proposizione 7.4), si vede che $\sigma_r(0) = 1$, $\sigma_r(1) = 2r$ e, per $n \geq 2$, $\sigma_r(n) = (2r-1)\sigma_r(n-1) = 2r(2r-1)^{n-1}$; quindi per $n \geq 1$,

$$\gamma_{F_r}^X(n) = \sum_{i=o}^{n} \sigma_r(i) = 1 + 2r \sum_{j=0}^{n-1} (2r-1)^j = 1 + 2r \frac{(2r-1)^n - 1}{(2r-1) - 1} \geq (2r-1)^n.$$

In particolare, per $r = 2$ si ha $\gamma_{F_2}(n) = 2 \cdot 3^n - 1$. A questo punto, non è difficile provare (lo si faccia per esercizio) che, per ogni r, $\gamma_{F_r}(n) \sim 2^n$. □

Tutte le funzioni esponenziali, cioè del tipo a^n, con $a > 1$, sono equivalenti; dunque equivalenti alla funzione 2^n. Si dice che un gruppo finitamente generato G ha *crescita esponenziale* se $\gamma_G(n) \sim 2^n$. L'esempio di sopra mostra quindi che ogni gruppo libero di rango finito $r \geq 2$ ha crescita esponenziale. È chiaro che, rispetto alla relazione d'ordine definita prima, quella esponenziale è la massima crescita possibile per gruppi finitamente generati. La crescita esponenziale non implica tuttavia, come forse si sarebbe portati a credere, che il sistema di generatori in questione sia prossimo ad essere libero. Ad esempio, vediamo come il gruppo del Lampionaio, che è abeliano per ciclico, abbia crescita esponenziale.

Esempio 6.9. Il gruppo del lampionaio è il prodotto intrecciato $C_2 \wr \mathbb{Z}$; che a sua volta vediamo come il prodotto demidiretto $L = B \rtimes \langle x \rangle$ dove B è l'insieme delle funzioni $\mathbb{Z} \to \{0, 1\}$ a supporto finito e x la traslazione $z \mapsto z + 1$. Detta b la funzione $b(0) = 1$ e $b(z) = 0$ per $0 \neq z \in \mathbb{Z}$, allora per ogni $z \in \mathbb{Z}$, b^z è la funzione che vale 1 in z e 0 altrove; perciò, $X = \{b, x\}$

è un sistema di generatori di L. Sia $n \geq 1$ e sia $g \in B$ tale che il supporto di g è contenuto in $[1, n]$; allora esistono $0 \leq k \leq n$ e interi $1 \leq n_1 < n_2 < \cdots < n_k \leq n$ tali che

$$g = b^{x^{n_1}} b^{x^{n_2}} \cdots b^{x^{n_k}} = x^{-n_1} b x^{n_1 - n_2} \ldots b x^{n_{k-1} - n_k} b x^{n_k}.$$

Dunque

$$\ell_X(g) \leq n_1 + n_k + k + \sum_{j=1}^{k+1} |n_j - n_{j+1}| = 2n_k + k \leq 3n. \tag{6.9}$$

Ora, il numero di funzioni $\mathbb{Z} \to \{0, 1\}$ il cui supporto è contenuto in $[1, n]$ è chiaramente 2^n. Ad (6.9) segue pertanto che $\gamma_L^X(3n) \geq 2^n$; quindi $2^n \preccurlyeq \gamma_L^X$ e dunque $\gamma_L^X \sim 2^n$. □

A questo punto è opportuno mostrare che esistono tipi di crescita non esponenziali.

Esempio 6.10. Sia $A \simeq \mathbb{Z}^r$ il gruppo abeliano libero di rango r e $\mathcal{X} = \{x_1, \ldots, x_r\}$ un suo sistema libero di generatori. Allora ogni elemento $a \in A$ si scrive in modo unico come $a = x_1^{\beta_1(g)} \cdots x_r^{\beta_r(g)}$ con $(\beta_1(g), \ldots, \beta_r(g)) \in \mathbb{Z}^r$. Quindi $\ell_{\mathcal{X}}(a) = \sum_{i=1}^r |\beta_i(g)|$ e, per ogni $n \geq 1$,

$$\gamma_A^{\mathcal{X}}(n) = |\{(\beta_1, \ldots, \beta_r) \in \mathbb{Z}^r \mid |\beta_1| + \cdots + |\beta_r| \leq n\}|.$$

Per ragioni che vedremo tra poco, in questo caso ci basta notare che, per ogni $n \geq 1$,

$$\gamma_A^{\mathcal{X}} \leq (2n + 1)^r.$$

Per $r = 2$, e facendo i conti esatti, si trova $\gamma_{\mathbb{Z}^2}(n) = n^2 + (n + 1)^2$ (per il valore esatto in generale, vedi esercizio 6.28). □

Se f e g sono polinomi reali, allora le funzioni $f(n)$ e $g(n)$ sono equivalenti se e soltanto se $\deg f = \deg g$; quindi, al variare di $1 \leq d \in \mathbb{N}$, le funzioni $n \mapsto n^d$ costituiscono un sistema di rappresentanti modulo $\sim$ per le funzioni polinomiali. Più in generale, per ogni $0 < \alpha, \beta \in \mathbb{R}$, $n^\alpha \sim n^\beta$ se e solo se $\alpha = \beta$.
Si dice che un gruppo finitamente generato G ha *crescita polinomiale* se esistono $C, d > 0$ tali che $\gamma_G(n) \leq C n^d$ per ogni $n \in \mathbb{N}$.

L'esempio 6.10 mostra che ogni gruppo abeliano libero di rango finito (e quindi ogni gruppo abeliano finitamente generato) ha crescita polinomiale. Nel 1968, Milnor e Wolf (e Hartley), provarono che ogni gruppo nilpotente ha crescita polinomiale. Quindi ogni gruppo *virtualmente nilpotente*, cioè tale che ammette un sottogruppo nilpotente di indice finito, ha crescita polinomiale. Inoltre, i contributi combinati dei due autori stabilirono che un gruppo risolubile la cui crescita non è esponenziale è virtualmente nilpotente. Ciò suggerì a Milnor di congetturare che la classe dei gruppi virtualmente nilpotenti coincide con quella dei gruppi a crescita polinomiale. La dimostrazione di questa congettura, dovuta a Gromov, è uno dei risultati più importanti e fondamentali in teoria geometrica dei gruppi.

Teorema 6.23. (Gromov 1981) *Un gruppo finitamente generato ha crescita polinomiale se e soltanto se è virtualmente nilpotente.*

La dimostrazione è al di fuori delle intenzioni (e possibilità) di questo corso. Concludiamo accennando ad una questione di base riguardante la crescita: naturalmente, esistono numerose

funzioni crescenti $\mathbb{N} \to \mathbb{R}$ - che a priori non si può escludere rappresentino funzioni di crescita di qualche gruppo - che sono "intermedie" tra quelle polinomiali e quelle esponenziali. Tali, ad esempio, sono tali le funzioni $n \to 2^{\sqrt{n}}$, oppure $n \to 2^{\frac{n}{\log n}}$. Tuttavia, nel 1968 Milnor e Wolf provarono, appunto, che in ogni gruppo finitamente generato risolubile la crescita è polinomiale oppure esponenziale. Milnor pose quindi il problema se esistano gruppi finitamente generati "a crescita intermedia". Torneremo su questo argomento fra qualche pagina; prima occorre introdurre uno strumento generale che si è rivelato estremamente fruttuoso nello studio dei gruppi finitamente generati, che è la rappresentazione di gruppi come gruppi di automorfismi di alberi con radice.

6.6 Esercizi VI

Sezione 6.1

Esercizio 6.1. Sia G un gruppo finitamente generato. Si provi che per ogni sistema di generatori X di G esiste un sottoinsieme finito di $Y \subseteq X$ tale che $\langle Y \rangle = G$.

Esercizio 6.2. Fissato un primo p, sia $G = \{m/p^n \mid m \in Z,\ n \in \mathbb{N}\}$. Si provi che G è sottogruppo di $\mathbb{Q}$, che non è finitamente generato, e che $\Phi(G) = \{0\}$.

Esercizio 6.3. Sia $G = H \rtimes \langle \alpha \rangle$ il gruppo dell'esempio 6.1. In $Aut(\mathbb{R}, \leq)$ si considerino gli elementi f, g definiti da $f(x) = 2x$ e $g(x) = x + 1$, per ogni $x \in \mathbb{R}$. Si provi che $G \simeq \langle f, g \rangle$.

Esercizio 6.4. Si provi che per ogni $n \geq 1$ il gruppo $SL(n, \mathbb{Z})$ è finitamente generato.

Esercizio 6.5. Sia G un gruppo e $N \trianglelefteq G$. Si provi che G soddisfa *Max* se e soltanto se N e G/N soddisfano *Max*.

Esercizio 6.6. Si dice che un gruppo G ha *rango di Prüfer finito* se esiste $n \in \mathbb{N}$ tale per ogni sottogruppo finitamente generato H di G si ha $d(H) \leq n$.

1. Si provi che sottogruppi e quozienti di gruppi con rango di Prüfer finito hanno rango di Prüfer finito.
2. Sia G un gruppo e $N \trianglelefteq G$; si provi che se N e G/N hanno ranfgo di Prüfer finito, allora G ha rango di Prüfer finito.

Esercizio 6.7. Si provi che $\mathbb{Q}$ e C_{p^∞} sono gruppi con rango di Prüfer finito (meglio: che ogni loro sottogruppo f.g. è ciclico).

Sezione 6.2

Esercizio 6.8. Si provi, a partire dalla definizione, che sottogruppi e quozienti di gruppi policiclici sono policiclici.

Esercizio 6.9. Sia G un gruppo policiclico e $H \leq G$; si provi che $h(H) \leq h(G)$ e che $h(H) = h(G)$ se e solo se $[G : H]$ è finito.

Esercizio 6.10. Sia G un gruppo policiclico; si provi che il sottogruppo di Frattini $\Phi(G)$ è nilpotente.

Esercizio 6.11. Sia G un gruppo risolubile si provi che G è policiclico se e solo se ha una serie normale i cui fattori sono finiti oppure abeliani liberi.

Esercizio 6.12. Si dimostri che un gruppo è policiclico per finito se e solo se ammette una serie (finita) a fattori finiti o ciclici.

Esercizio 6.13. Sia G un gruppo policiclico; si dimostri che G è nilpotente se e solo se ogni suo quoziente finito è nilpotente.

Sezione 6.3

Esercizio 6.14. Si provi che un gruppo nilpotente è finitamente presentato se e solo se è finitamente generato.

Esercizio 6.15. Sia G un gruppo e H un sottogruppo di indice finito di G. Si provi che G è finitamente presentato se e solo se H è finitamente presentato.

Esercizio 6.16. Si provi che il gruppo del Lampionaio ha la presentazione descritta in (6.1).

Esercizio 6.17. Siano G un gruppo finitamente presentato e $N \trianglelefteq G$; si provi che se N è finitamente generato allora G/N è finitamente generato.

Esercizio 6.18. (P. Hall: un gruppo risolubile f.g. non hopfiano). Sia $\mathbb{Q}_2$ l'anello dei razionali della forma $m2^z$ con $m, z \in \mathbb{Z}$, e sia $U = UT(3, \mathbb{Q}_2)$ il gruppo delle matrici unitriangolari di ordine 3 su $\mathbb{Q}_2$ (vedi sezione 5.4); siano

$$g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \zeta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

e $G = \langle U, g \rangle$. Poiché g normalizza U sia ha $G = U \rtimes \langle g \rangle$ (con $\langle g \rangle$ gruppo ciclico infinito); inoltre $\zeta \in Z(G)$. Si provi che G è finitamente generato, e che porre, $g \mapsto g$ e, per $a, b, c \in \mathbb{Q}_2$,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & a & 2b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

definisce un automorfismo di G. A questo punto si provi che $H = G/\langle \zeta \rangle$ è hopfiano

Esercizio 6.19. Si provi che il gruppo del Lampionaio è hopfiano.

Esercizio 6.20. È vero che ogni quoziente di un gruppo hopfiano è hopfiano?

Esercizio 6.21. Diciamo che un gruppo G soddisfa la condizione di massimo sui sottogruppi normali (*Max*-n) se ogni catena $N_1 \leq N_2 \leq \dots$ di sottogruppi normali N_1 di G è finita. Si provi che *Max*-n implica hopfiano.

Esercizio 6.22. Sia $0 \neq m \in \mathbb{Z}$; si provi che il gruppo $BS(1, m)$ è prodotto semidiretto di un gruppo abeliano A per un gruppo ciclico infinito. Si descriva quindi A in relazione ad m.

Sezione 6.4

Esercizio 6.23. Si provi che $SL((2,\mathbb{Z}) = C_4 *_{C_2} C_6$.

Esercizio 6.24. Il gruppo fondamentale $G = \pi_1(X)$ di una superficie compatta X di genere 2 ha presentazione

$$G = \langle x, x_1, y, y_1 \mid [x,y] = [x_1, y_1] \rangle$$

si provi che $G = F_2 *_{\mathbb{Z}} F_2$ (dove F_2 è il gruppo libero di rango 2).

Esercizio 6.25. Si provi che il gruppo $\langle x, y \mid xyx = yxy \rangle$ è un prodotto amalgamato di due gruppi ciclici infiniti.

Esercizio 6.26. Si provi che esiste un gruppo 2-generato che contiene come sottogruppo una copia isomorfa di qualsisa gruppo abeliano numerabile.

Sezione 6.5

Esercizio 6.27. Si determini la funzione di crescita, rispetto al sistema di generatori $\{x, y\}$, del gruppo diedrale infinito $D = \langle x, y \mid x^2 = y^2 = 1 \rangle$.

Esercizio 6.28. Dato $r \geq 1$, sia A il gruppo abeliano libero di rango r e $X = \{x_1, \ldots, x_r\}$ un suo sistema libero di generatori. Si provi che, per ogni $n \geq 1$,

$$\gamma_A^X(n) = \sum_{i=0}^{r} 2^i \binom{r}{i} \binom{n}{i}.$$

Esercizio 6.29. Siano G, H gruppi finitamente generati e X, Y sistemi di generatori finiti, rispettivamente, di G e di H. Posto $D = (X \cup \{1\}) \times (Y \cup \{1\})$, si provi che

$$\gamma_{G\times H}^D \sim \gamma_G^X \cdot \gamma_H^Y.$$

Esercizio 6.30. Sia $G = F_2/\gamma_3(F_2)$, dove F_2 è il gruppo libero di rango 2, e sia X un suo sistema finito di generatori. Si provi che $\gamma_G^X \sim n^4$.

Esercizio 6.31. Sia G un gruppo f.g. a crescita polinomiale. Si provi che ogni sottogruppo finitamente generato ed ogni quoziente di G hanno crescita polinomiale.

Esercizio 6.32. Sia G un gruppo finitamente generato e sia $H \leq G$ di indice finito: si provi che se X e Y sono sistemi finiti di generatori, rispettivamente, di G e di H, allora $\gamma_G^X \sim \gamma_H^Y$ (in particolare, se H ha crescita polinomiale, allora anche la crescita di G è ;polinomiale).

Esercizio 6.33. Seguendo Gromov, diciamo che un'applicazione $\phi : X \to Y$ fra due spazi metrici $(X, d_x), (Y, d_Y)$ è una *quasi-isometria* se esistono costanti $C \geq 1, D \geq 0$ e $m > 0$ tali che

- $C^{-1} d_X(x_!, x_2) - D \leq d_Y(\phi(x_1), \phi(x_2)) \leq C d_X(x_1, x_2) + D$, per ogni $x_1, x_2 \in X$;
- per ogni $y \in Y$ esiste $x \in X$ tale che $d_Y(y, \phi(x)) \leq m$.

In tal caso, si dice che gli spazi X e Y sono quasi-isometrici. Si può provare che questa proprietà stabilisce una relazione di equivalenza tra spazi metrici

(a) Sia G un gruppo finitamente generato e siano A, B due sistemi finiti di generatori di G; si provi che i grafi di Cayley $\Gamma[G; A]$ e $\Gamma[G; B]$ sono quasi isometrici. (rispetto alle distanza definite in (6.6)). Questo fatto permette di definire la classe di quasi-isometria di un gruppo G, e di definire due gruppi fin.gen. G e H *quasi isometrici* se per sistemi di generatori A e B, di G e H rispettivamente, i grafi $\Gamma[G; A]$ e $\Gamma[H; B]$ sono quasi-isometrici.

(b) Si provi che se H è un sottogruppo di indice finito del gruppo G, allora H è quasi isometrico a G.

Esercizio 6.34. Sia G un gruppo finitamente generato. Si provi che se G è quasi isometrico a $G \times G$ allora G non può avere una crescita polinomiale.

Capitolo 7

Gruppi e grafi

7.1 Grafi di Cayley

Grafi. Un *grafo* (semplice) è una coppia $\Gamma = (V(\Gamma), E(\Gamma))$, dove $V(\Gamma)$ è un insieme non vuoto i cui elementi sono i *vertici* del grafo, ed $E(\Gamma)$ è un sottoinsieme (che può anche essere vuoto) dell'insieme dei sottoinsiemi di ordine 2 di $V(\Gamma)$, i cui elementi sono gli *archi* del grafo[1].
Se $e = \{x, y\} \in E(\Gamma)$, si dice che x e y sono vertici *adiacenti* e scriviamo $x \sim y$ (o, se è necessario specificare a quale grafo ci riferiamo, $x \sim_\Gamma y$) e che il vertice x e l'arco e sono *incidenti*. Il grafo si dice finito se tale è l'insieme dei suoi vertici[2]. Nel nostro contesto sarà importante considerare anche grafi infiniti ma localmente finiti: intendendo con ciò grafi in cui ciascun vertice è incidente ad un numero finito di archi. Se v è un vertice del grafo localmente finito Γ, il *grado* $d_\Gamma(v)$ di v è appunto il numero di archi incidenti a v; in altri termini, $d_\Gamma(v)$ è il il numero di vertici di Γ che sono adiacenti a v. Poiché ogni arco contiene due vertici distinti, nel caso in cui Γ sia un grafo in cui il numero di archi è finito, si ricava la seguente utile formula:

$$2|E(\Gamma)| = \sum_{v \in V(\Gamma)} d_\Gamma(v). \tag{7.1}$$

Un grafo Γ si dice *regolare* se esiste $d \in \mathbb{N}$ tale che $d_\Gamma(v) = d$ per ogni vertice v di Γ (in modo più preciso, si dice in tal caso che Γ è d-regolare)

Connessione. Un *cammino* nel grafo $\Gamma = (V(\Gamma).E(\Gamma))$ è una sequenza finita di vertici $v_0,\ v_1, \ldots,\ v_n$, tale che per ogni $i = 0, \ldots, n-1$,

$$v_i \sim v_{i+1} \qquad \text{e} \qquad \mathrm{v_i} \neq \mathrm{v_{i+2}} \ \ (\mathrm{v_{i-1}} \neq \mathrm{v_0}).$$

Il numero intero $n \geq 0$ è detto *lunghezza* del cammino. Un *circuito* in Γ è un cammino in cui il vertice iniziale e quello finale coincidono; si osservi che un circuito non banale (che, cioè,

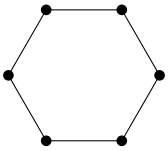
[1] Se V un insieme e $1 \leq n \in \mathbb{N}$, si denota con $V^{[n]}$ l'insieme di tutti i sottoinsiemi di V di cardinalità n. Dunque, nella nostra definizione di grafo, $E(\Gamma) \subseteq V(\Gamma)^{[2]}$.

[2] In accezioni più ampie del concetto di grafo, in cui sono ammessi diversi archi tra gli stessa coppia di estremi, dovrà essere finito anche il numero di archi.

non consiste di un unico vertice) ha lunghezza almeno 3. Un *ciclo* è un circuito in cui tutti i vertici (tranne ovviamente il primo e l'ultimo) sono distinti.
Un grafo Γ si dice *connesso* se per ogni coppia di vertici distinti x e y esiste un cammino

$$x = v_0,\ v_1,\ \ldots,\ v_n = y.$$

Ad esempio (lo si domostri per esercizio), un grafo connesso e 2-regolare è un singolo ciclo finito (come il 6-ciclo della figura seguente),



oppure un cammino infinito:

Alberi. Un *albero* è un grafo connesso e privo di circuiti non banali. La seguente proposizione è semplice ma importante.

Proposizione 7.1. *Sia Γ un grafo. Sono equivalenti*

1. *Γ è un albero;*
2. *per ogni coppia di vertici distinti x, y di Γ esiste uno ed un solo cammino in Γ che inizia in x e termina in y.*

Dimostrazione. 1. $\Rightarrow$ 2. Sia Γ un albero, e siano u, v vertici distinti di Γ. Siccome Γ è connesso, esiste un cammino $\mathcal{C} : u = v_0\, v_1 \ldots v_{d-1}\, v_d = v$. Osserviamo che, poiché Γ è privo di circuit non banali, i vertici di $\mathcal{C}$ sono tutti distinti. Supponiamo, per assurdo, che $\mathcal{C}' : u = w_0\, w_1\, w_2 \ldots$ sia un altro cammino da u a v, distinto da $\mathcal{C}$. Allora esiste un minimo indice $i = 1, \ldots, d$ tale che $v_i \neq w_i$, ed un minimo $j > i$ tale che $v_j \in \{w_{i+1}, w_{i+2}, \ldots\}$. Ma allora G conterrebbe un ciclo non banale che inizia e termina in v_{i-1}, il che è contro l'ipotesi.
2. $\Rightarrow$ 1. Esercizio. ∎

Sottografi. Sia X un sottoinsieme dell'insieme dei vertici di un grafo Γ. Il *sottografo indotto* da X è il grafo Γ_X il cui insieme dei vertici è X e quello degli archi è $E(\Gamma) \cap X^{[2]}$; cioè, per ogni $x, y \in X$, $\{x, y\} \in E(\Gamma_X)$ se e soltanto se $\{x, y\} \in E(\Gamma_1)$. In maniera discorsiva, un sottografo indotto di un grafo Γ è un sottoinsieme di vertici di Γ assieme a tutti gli archi di Γ i cui estremi appartengono a tale insieme.

Automorfismi di un grafo. Siano Γ e Δ grafi; un isomorfismo da Γ in Δ è un'applicazione biettiva $\phi : V(\Gamma) \to V(\Delta)$ tale che, per ogni $x, y \in V(\Gamma)$,

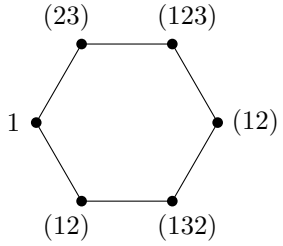
$$\{x, y\} \in E(\Gamma) \quad \Leftrightarrow \quad \{x\phi, y\phi\} \in E(\Delta).$$

Ovviamente, un automorfismo di Γ è un isomorfismo di Γ in se stesso, e l'insieme $Aut(\Gamma)$ degli automorfiami di un grafo Γ costituisce un gruppo.

Un grafo Γ si dice *vertex–transitivo* se il suo gruppo degli automorfismi opera transitivamente sull'insieme dei suoi vertici.

Grafi di Cayley. Sia G un gruppo, e sia S un sottoinsieme di G tale che $1 \notin S$. Il *Grafo di Cayley* $\Gamma[G, S]$ è il grafo il cui insieme dei vertici è G, e gli archi sono tutti i sottoinsiemi $\{g, gs\}$, al variare di $g \in G$ ed $s \in S \cup S^{-1}$.

ESEMPIO 7.1. Sia $G = S_3$ il gruppo simmetrico su 3 punti, e $S = \{(12), (23)\}$; allora il grafo di Cayley $\Gamma[G, S]$ è un 6-ciclo:



Lo stesso grafo che si ottiene come grafo di Cayley $\Gamma[C; X]$ con $C = \langle x \rangle$ un gruppo ciclico di ordine 6 e $X = \{x\}$. In generale, si vede facilmente che se x, y sono due involuzioni (cioè elementi di ordine 2) e $G = \langle x, y \rangle$, allora $\Gamma[G, \{x, y\}]$ è un ciclo di lunghezza $|G|$ se G è finito, mentre se G è infinito è una catena infinita

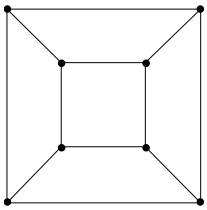
che, a sua volta, è il grafo di Cayley $\Gamma[\mathbb{Z}, \{1\}]$. □

Sia $\Gamma = \Gamma[G, S]$ un grafo di Cayley nel gruppo G, e supponiamo che S sia finito; allora, risulta dalla costruzione che Γ è un grafo d-regolare, dove $d = |S \cup S^{-1}|$. Un'altra semplice ma importante e proprietà dei grafi di Cayley è descritte nel seguente enunciato.

Lemma 7.2. *Un grafo di Cayley $\Gamma[G; S]$ è connesso se e soltanto se S è un sistema di generatori di G.*

DIMOSTRAZIONE. Supponiamo che $\Gamma = \Gamma[G; S]$ sia connesso, e sia $y \in G$. Allora esiste un cammino $1 = g_0\ g_1\ g_2 \ldots\ g_n = y$ in Γ. Dunque, esistono $s_1, s_2, \ldots, s_n \in S \cup S^{-1}$ tali che $g_1 = 1s_1$, $g_2 = g_1 s_2 = 1s_1 s_2$, e così via, sino a $y = g_n = 1s_1 \cdots s_n$. Quindi $y \in \langle S \rangle$. Viceversa, sia $\langle S \rangle = G$, e siano $x, y \in G$ con $x \neq y$. Allora, esistono $s_1, \ldots, s_n \in S \cup S^{-1}$ (con $s_{i+1} \neq s_i^{-1}$) tali che $x^{-1}y = s_1 \cdots s_n$. Ponendo $g_0 = x$ e, per ogni $i = 1, \ldots, n$, $g_i = x s_1 \cdots s_{i-1}$, si descrive un cammino $x = g_0\ g_1\ \ldots\ g_n = y$ in Γ. Pertanto, il grafo Γ è connesso. ■

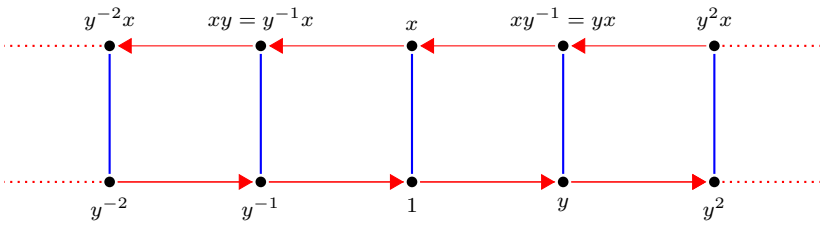
ESEMPIO 7.2. Sia G il gruppo delle simmetrie di un quadrato; allora $|G| = 8$ e $G = \langle \rho, \tau \rangle$, dove ρ è una rotazione di un angolo $\pi/2$ e τ la riflessione con asse una delle diagonali; si ha $|\rho| = 4$, $|\tau| = 2$ e, come si verifica subito, $\tau\rho\tau = \rho^{-1}$ (di fatto, G è isomorfo al gruppo diedrale di ordine 8). Posto $S = \{\rho, \tau\}$, si trova che il grafo di Cayley $\Gamma[G, S]$ è isomorfo al grafo del cubo □



Azione del gruppo sul grafo di Cayley. Siano G un gruppo e $\Gamma = \Gamma[G, S]$ un grafo di Cayley su G. Allora, per ogni $g \in G$, la moltiplicazione a sinistra $\lambda_g : G \to G$, definita da $x \mapsto gx$ (per ogni $x \in G$), è una biezione sull'insieme dei vertici di Γ che conserva la relazione di adiacenza (infatti, per ogni $x \in G$ e ogni $s \in S$, si ha $\lambda_g(\{x, xs\}) = \{gx, (gx)s\}$). Quindi λ_g induce un automorfismo del grafo Γ. Inoltre, la posizione $g \mapsto \lambda_{g^{-1}}$ definisce un omomorfismo iniettivo del gruppo G nel gruppo $Aut(\Gamma)$. Quindi, G è isomorfo ad un sottogruppo del gruppo $Aut(\Gamma)$. Inoltre, G opera transitivamente sui vertici di Γ, infatti per ogni coppia (x, y) di vertici di Γ, ponendo $g = yx^{-1}$, si ha $\lambda_g(x) = y$. In particolare, quindi, i grafi di Cayley sono vertex–transitivi. Questa è un'importante osservazione che fissiamo nella seguente proposizione.

Proposizione 7.3. *Sia $\Gamma = \Gamma[G, S]$ un grafo di Cayley sul gruppo G. Allora, per ogni $g \in G$, la moltiplicazione a sinistra per g induce un automorfismo di Γ. Ne segue che G è isomorfo ad un sottogruppo di $Aut(\Gamma)$ che è transitivo sull'insieme dei vertici.*

Esempio 7.3. Sia $D = \langle x, y \mid x^2 = 1,\ y^x = y^{-1} \rangle$, il gruppo diedrale infinito; allora il grafo di Cayley $\Gamma = \Gamma[D, \{x, y\}]$ ha il seguente aspetto:



dove gli archi in rosso corrispondono al generatore y (con la freccia nel verso $g \mapsto gy$) e in blu gli archi corrispondenti al generatore x. Il gruppo D è identificabile, per moltiplicazione a sinistra, con un sottogruppo di $Aut(\Gamma)$: l'elemento y opera come l'automorfismo che trasla orizzontalmente tutto il diagramma di un passo (verso destra), mentre l'involuzione x opera come una rotazione del diagramma di 180^o intorno al centro dell'arco $\{1, x\}$. Ci sono automorfismi di Γ che non sono indotti da elementi di D, come - ad esempio - la riflessione che scambia i due binari del diagramma (vedi esercizio 7.7). □

7.2 Sottogruppi di un gruppo libero

In questa sezione, utilizzeremo le azioni di un gruppo su oppurtuni grafi (in questo caso alberi) per provare l'importante fatto per cui ogni sottogruppo di un gruppo libero è a un

gruppo libero. Cominciamo con un'osservazione piuttosto semplice, ma che fornisce lo spunto iniziale.

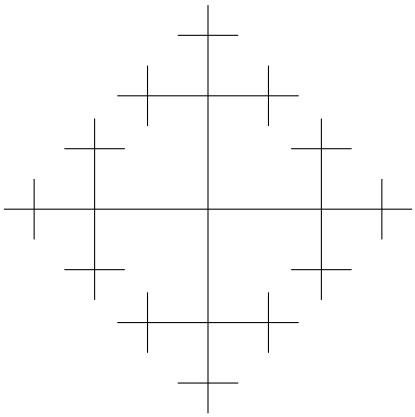
Proposizione 7.4. *Sia G è un gruppo libero su X, allora il grafo di Cayley $\Gamma[G;X]$ è un albero.*

DIMOSTRAZIONE. Sia G libero su X (che identifichiamo con un insieme di generatori di G) e $\Gamma = \Gamma[G;X]$. Poiché $G = \langle X \rangle$, Γ è connesso per il Lemma 7.2. Supponiamo, per assurdo, che Γ non sia un albero, e siano $g_1, g_2, \ldots, g_{n-1}, g_n = g_1$ i vertici di un circuito non banale $\mathcal{C}$ di Γ . Scegliendo $\mathcal{C}$ di lunghezza minima possiamo assumere $x_i \neq x_j$ per ogni $i \neq j$, $i, j \in \{1, \ldots, n-1\}$. Per ogni tale indice i, esiste $x_i \in X \cup X^{-1}$ tale che $g_{i+1} = g_i x_i$. Allora

$$g_1 = g_n = g_1 x_1 x_2 \ldots x_{n-1}$$

q quindi $x_1 x_2 \ldots x_{n-1} = 1$. Poiché X è un sistema libero di generatori deve esistere $i = 1, \ldots, n-2$ tale che $x_{i+1} = x_i^{-1}$. Ma allora $g_{i+1} = g_{i-1}$, che è una contraddizione. ∎

Con qualche specifica su X questa proposizione si può invertire (vedi esercizio 7.9).



un pezzo del grafo di Cayley di F_2

Un'azione $G \to Aut(\Gamma)$ di un gruppo G su un grafo Γ si dice *libera* se

- è priva di vertici fissi, ovvero per ogni $v \in V(\Gamma)$ ed ogni $1 \neq g \in G$, $v \neq v^g$;
- è priva di inversioni, cioè di archi fissi: per ogni $e = \{x, y\} \in E(\Gamma)$ ed ogni $1 \neq g \in G$, $e^g = \{x^g, y^g\} \neq e$.

Azioni libere su grafi in generale non sono inusitate: ad esempio il gruppo ciclico di ordine n opera naturalmente in modo libero sul grafo n-ciclo (di fatto, se il sistema di generatori S del gruppo G non contiene involuzioni allora l'azione di G su $\Gamma[G:S]$ descritta nella sezione precedente è libera). Tuttavia, se ci si restringe agli alberi la situazione cambia. Cominciamo con una semplice osservazione.

Lemma 7.5. *Sia G un gruppo che opera liberamente su un albero Γ. Allora, per ogni $y \in G$, $y^2 = 1 \;\Rightarrow\; y = 1$.*

DIMOSTRAZIONE. Sia $y \in G$ con $y^2 = 1$ e supponiamo per assurdo $y \neq 1$. Allora, fissato un vertice v di Γ, $v \neq v^y$, ed esiste un unico cammino in Γ che congiunge v a v^y, i cui vertici denotiamo con $v = v_0\ v_1\ \ldots\ v_n = v^y$. Applicando y e poiché $y^2 = 1$, si ha che $v^y\ v_1^y \ldots\ v_n^y = v^{y^2} = v$ è lo stesso (unico) cammino letto viceversa. Quindi $v_1^y = v_{n-1}^y$ e così via. Si riconosce dunque che y fissa il vertice o l'arco centrale del cammino a seconda che n sia pari o dispari, ma in ogni caso si ha contraddizione con l'ipotesi che l'azione sia libera. ∎

Teorema 7.6. (Serre) *Sia G un gruppo. Sono equivalenti*

1. *G è un gruppo libero:*
2. *G opera liberamente su un albero.*

DIMOSTRAZIONE. [1 ⇒ 2]. Sia G gruppo libero sul sistema libero di generatori X. Allora, per la Proposizione 7.4, il grafo di Cayley $\Gamma = \Gamma[G; x]$ è un albero. Per la Proposizione 7.3 la moltiplicazione a sinistra descrive un'azione di G su Γ, che chiaramente non ha vertici fissi. Sia $e = \{u, v\}$ un arco di Γ, allora $v = ux$ con $x \in X \cup X^{-1}$. Supponiamo, per assurdo, che esista $1 \neq g \in G$ tale che $e = e^g$; allora $gu = ux$ e $gux = u$, da cui $u = gux = ux^2$ da cui l'assurdo $x^2 = 1$. Quindi G opera liberamente su Γ.

[2 ⇒ 1]. Supponiamo che il gruppo G operi liberamente sull'albero Γ. Il passo fondamentale è ricavare da tale azione un'azione transitiva (e libera) su un altro albero.
Sia τ un sottoalbero (cioè un sottografo indotto e connesso di Γ) di Γ che sia massimale con la proprietà che i suoi vertici appartengono a orbite diverse per l'azione di G su $V(\Gamma)$ (un tale τ esiste per il Lemma di Zorn, e si riduce ad un unico vertice se G è transitivo su $V(\Gamma)$). Se $T = V(\tau)$ è l'insieme dei vertici di τ. Se $1 \neq g \in G$, allora l'assenza di punti fissi per g su $V(\Gamma)$ implica $T^g \cap T = \emptyset$; infatti, se $x, y \in T$ sono tali che $x^g = y$ allora, per la scelta di τ, $x = y$ e quindi $g = 1$. Da ciò segue che per ogni $g, h \in G$ se $g \neq h$, allora

$$T^g \cap T^h = \emptyset. \tag{7.2}$$

Osserviamo anche che

$$\bigcup_{g \in G} T^g = V(\Gamma). \tag{7.3}$$

Infatti, sia per assurdo, $v \in V(\Gamma)$, tale che v non appartiene ad alcun T^g. Poiché Γ è connesso, possiamo assumere che v sia adiacente a qualche vertice x^g per qualche $x \in T$ e $g \in G$; ma allora il sottografo di Γ ottenuto da τ aggiungendo il vertice $v^{g^{-1}}$ e l'arco $\{x, v^{g^{-1}}\}$ è ancora un sottoalbero i cui vertici appartengono a G-orbite diverse, il che contraddice la massimalità di τ.

Definiamo ora un grafo Δ ponendo $V(\Delta) = \{T^g \mid g \in G\}$ (per quanto osservato in (7.2), $g \mapsto T^g$ definisce una biezione tra G e $V(\Delta)$), e, per ogni $g, h \in G$ con $g \neq h$, $\{T^g, T^h\} \in E(\Delta)$ se e solo se esistono $x \in T^g$, $y \in T^h$ tale che $\{x, y\} \in E(\Gamma)$.

- Δ è connesso. Questo discende dal fatto che Γ è connesso e da (7.3).

- Δ è un albero. Siano, per assurdo, $T^{g_0}\ T^{g_1} \ldots\ T^{g_n} = T^{g_0}$ i vertici di un circuito non banale in Δ. Scegliendolo di lunghezza minima possiamo supporre $g_i \neq g_j$ per ogni $i, j = 1, \ldots, n-1$ e $i \neq j$. Per ogni $i = 0, \ldots, n-1$, siano $u_i, v_i \in T^{g_i}$ (non necessariamente

distinti) tali che v_i è adiacente a u_{i+1} in Γ (e dove $u_n = u_0$). allora, per (7.2), Ora, per ogni i, u_i e v_i sono vertici dell'albero τ^{g_i} e dunque esiste un unico cammino (eventualmente banale) in Γ, tra u_i e v_i e questo giace interamente in τ^{g_i}. Poiché $T^{g_0}, \dots, T^{g_{n-1}}$ sono a due a due disgiunti, alternando gli archi $\{v_i, u_{i+1}\}$ con il cammini $u_{i+1} - v_{i+1}$ si ottiene un cammino in Γ

$$v_0 \; u_1 - v_1 \; u_2 - v_2 \; \dots \; u_{n-1} - v_{n-1} \; u_n = u_0$$

i cui archi sono tutti diversi. Aggiungendo il cammino (che giace tutto in τ^{g_0}) tra u_0 e v_0 si finisce con un circuito non banale in Γ e dunque una contraddizione.

A questo punto, si riconosce che l'azione di G su Γ induce un'azione su Δ: per ogni $T^g \in V(\Delta)$ ed ogni $y \in G$, $(T^g)^y = T^{gy}$. Sia $1 \neq y \in G$: (7.2) assicura che y agisce senza punti fissi si $V(\Delta)$. Supponiamo che per qualche $\{T^g, T^h\} \in E(\Delta)$, $T^{gy} = T^h$ e $T^{hy} = T^g$, allora $T^{gy^2} = T^{hy} = T^g$ e dunque $y^2 = 1$ che, per il Lemma 7.5, implica la contraddizione $y = 1$. In conclusione, G opera liberamente su Δ, e regolarmente sull'insieme dei suoi vertici. Sia

$$Y = \{x \in G \mid \{T, t^x\} \in E(\Delta)\}.$$

Osserviamo che $x \in Y \Rightarrow x^{-1} \in Y$, e che, per il Lemma 7.5, $x \neq x^{-1}$. Possiamo quindi selezionare un sottoinsieme X di Y in modo che $Y = X \cup X^{-1}$ e $X \cap X^{-1} = \emptyset$. Proviamo che G è libero su X. Sia $g = x_1 \dots x_n$ con $n \geq 2$, $x_i \in Y$ e $x_{i+1} \neq x_i^{-1}$, per $i = 1, \dots, n-1$. Posto $x_0 = 1$, osserviamo che, per ogni $i = 1, \dots, n-1$, $\{T, T^{x_i}\} \in E(\Delta)$, e dunque

$$\{T^{x_{i+1} \dots x_n}, T^{x_i x_{i+1} \dots x_n}\} \in E(\Delta).$$

Inoltre, per ogni $i = 1, \dots, n-2$, $T^{x_i \dots x_n} \neq T^{x_{i+2} \dots x_n}$, perché se valesse l'uguaglianza, la libertà dell'azione di G su Δ darebbe $T = T^{x_i x_{i+1}}$ e, a sua volta, $x_i x_{i+1} = 1$ che va contro la scelta fatta. Concludiamo che se $g = 1$, allora

$$T = T^{x_1 \dots x_n}, \; T^{x_2 \dots x_n}, \; \dots, T^{x_n}, \; T$$

è la successione dei vertici di un circuito non banale in Δ, il che è ancora una contraddizione. Pertanto $g = 1$, e questo completa la dimostrazione. ∎

Sia F un gruppo libero. Allora, per il Teorema 7.6, F opera liberamente su un albero Γ; ne segue che ogni sottogruppo di F opera liberamente su Γ e dunque è libero. Si ha quindi il seguente importante risultato.

Teorema 7.7. *Ogni sottogruppo di un gruppo libero è libero.*

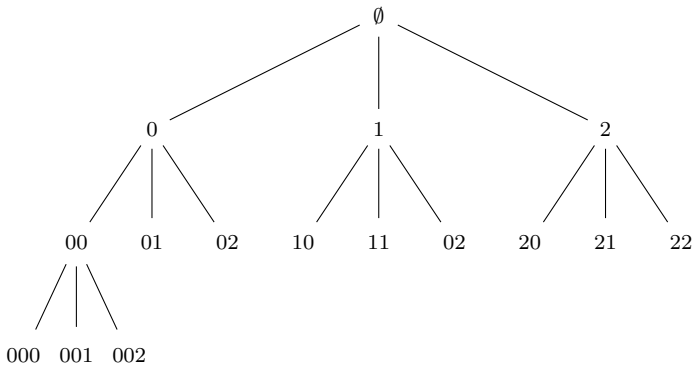
Di fatto, è possibile provare (anche se con un metodo diverso) dei risultati quantitativamente più accurati, come il giustamente celebre Teorema di Nielsen–Scrheier:

Teorema 7.8. (Nielsen–Schreier) *Sia F un gruppo libero di rango finito n, e sia $H \leq F$ un sottogruppo di indice finito $|F : H| = m$. Allora H è un gruppo libero ed il suo rango è $nm + 1 - m$.*

7.3 Automorfismi di alberi con radice

Un *albero con radice* è un albero in cui è stato fissato un vertice (detto appunto *radice*). Per i nostri scopi ci interessano principalmente degli alberi con radice n-regolari, che definiamo qui di seguito.

Fissato $n \geq 1$, sia I un insieme di cardinalità n, per fissare le notazioni faremo riferimento a $I = I_n = \{0, \ldots, n-1\}$. Allora, *l'albero n-regolare* T_n è il grafo i cui vertici sono le parole di lunghezza finita nell'alfabeto I (questo insieme lo denotiamo con $W(I)$) in cui la parola vuota sarà la radice, e due parole sono adiacenti se differiscono per l'aggiunta di una lettera a destra. Quindi, la radice (la parola vuota) è adiacente a tutte le parole di lunghezza 1 (che non sono altro che gli elementi dell'alfabeto I), mentre una parola w di lunghezza ≥ 1 è adiacente a wx per ogni $x \in I$ e alla parola che si ottiene da w togliendo l'ultima lettera a destra. Una maniera conveniente per lavorare con T_n è quella di definirlo come l'insieme delle parole $W(I_n)$ ordinato ponendo, per ogni due parole $v, w \in W(I_n)$, $v \leq w$ se v è un prefisso in w (cioè se esiste una parola u tale che $w = vu$).
Secondo questo punto di vista, la parola vuota $\emptyset$ è il minimo dell'insieme parzialmente ordinato: nei disegni di solito si mette però in alto. Ad esempio, si usa disegnare la parte "bassa" dell'albero T_3 nel modo seguente:



Livelli. Ad ogni vertice v di un albero con radice è assegnato il *livello* $\ell(v)$, che è la distanza nel senso dei grafi del vertice v dalla radice dell'albero.
Nel caso degli alberi regolari T_n, il livello del vertice v non è altro che la lunghezza di v come parola nell'alfabeto I_n. In questo caso, denotiamo con E_n^k l'insieme dei vertici di livello k di T_n; ad esempio, il secondo livello di T_3 è $E_3^2 = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}$. È chiaro che, per ogni $n, k \geq 1$, il numero di vertici del k-esimo livello dell'albero T_n è n^k.

Automorfismi. Un *automorfismo* di un albero con radice è una permutazione dei vertici dell'albero che conserva l'adiacenza e fissa la radice. In particolare, per un albero del tipo T_n gli automorfismi non sono altro che gli automorfismi dell'insieme parzialmente ordinato delle parole $W(I_n)$ con l'ordine naturale descritto sopra.
Osserviamo, in particolare, che un automorfismo α di un albero T_n permuta i vertici su uno stesso livello, e che se fissa un vertice v, allora fissa tutti i vertici dell'unico cammino che congiunge v alla radice.

Da quanto appena detto, segue che, posto A il gruppo degli automorfismi dell'albero T_n, allora per ogni $k \geq 1$ è definita una applicazione $\pi_k : A \to S_{n^k}$ che ad ogni $\alpha \in A$ associa la permutazione indotta da α sull'insieme E_n^k dei vertici al livello k. Di fatto, è evidente che π_k è un omomorfismo di gruppi per ogni $k \geq 1$. Denotiamo con A_k il nucleo $\ker \pi_k$; quindi A_k è l'insieme degli automorfismi di T_n che operano come l'identità sul k-esimo livello e dunque, per quanto osservato sopra, fissano ogni vertice di lunghezza minore o uguale a k. Allora, per ogni $k \geq 1$,

$$A/A_k \simeq Im(\pi_k)$$

è un sottogruppo di S_{n^k}; in particolare, A/A_k è finito. Inoltre, poiché ogni vertice di T_n appartiene ad un qualche livello finito:, si avrà

$$\bigcap_{k \geq 1} A_k = 1. \tag{7.4}$$

Quindi (vedi sezione 2.6 per la definizione di gruppo resifualmente finito),

Proposizione 7.9. *$Aut(T_n)$ è un gruppo residualmente finito.*

Vediamo nel dettaglio cosa avviene al primo livello; osservando innanzi tutto come ad ogni permutazione $\sigma \in S_n = Sym(I_n)$ sia possibile associare in modo canonico un automorfismo di T_n, che denotiamo ancora con σ, ponendo, per ogni vertice $v = x_1 \dots x_k$ di T_n (dove $x_1, \dots, x_k \in I_n$).

$$v\sigma = (x_1\sigma)x_2 \dots x_k. \tag{7.5}$$

In questo modo, al variare di $\sigma \in S_n$ si ottiene un sottogruppo $H_1 \simeq S_n$ di A. Chiaramente, $A_1 \cap H_1 = 1$, quindi (poiché, come abbiamo visto, $|A/A_1| \leq n!$) $A = A_1H_1$ e pertanto

$$A = A_1 \rtimes H_1 \simeq A_1 \rtimes S_n. \tag{7.6}$$

In particolare, questo comporta che $A/A_1 \simeq S_n$, come era facilmente intuibile. Questo per il primo livello; per $k \geq 2$, il gruppo A/A_k non è l'intero gruppo simmetrico S_{n^k}. Infatti, se è facile capire che l'azione di A sull'insieme E_n^k dei vertici del k-esimo livello è transitiva, essa non è primitiva (tranne che per $k = 1$): se v è un vertice di livello $k-1$, allora l'insieme dei vertici in E_n^k che giacciono sotto v (cioè $\{w \in E_n^k \mid v \leq w\}$) è un blocco per l'azione di A su E_n^k, la cui cardinalità è n. Quindi, se $k \geq 2$, E_n^k ammette, per l'azione di A, una decomposizione di imprimitività in $n^{k-1} = |E_n^{k-1}|$ blocchi di cardinalità n. Considerando che l'azione dello stabilizzatore di un vertice di livello $k-1$ sul blocco ad esso corrispondente è simile a quella di tutto A sul primo livello si ricava $A/A_k \simeq S_n \wr (A/A_{k-1})$. Tenendo conto che l'azione di A sui blocchi è quella sui vertici del livello $k-1$, con un semplice argomento induttivo si perviene allora a

$$A/A_k \simeq S_n \wr S_n \wr \cdots \wr S_n. \tag{7.7}$$

dove il prodotto intrecciato è permutazionale e iterato k volte.

Auto-similarità. Nell'ultimo ragionamento, abbiamo implicitamente fatto ricorso ad un aspetto molto importante che è bene rendere esplicito (introducendo tra l'altro particolari notazioni che continueremo a usare anche nella prossima sezione). Come sopra, sia $n \geq 2$, $T = T_n$ l'albero con radice n-regolare (e anche l'insieme dei suoi vertici) e A il suo gruppo degli

automorfismi. Se v è un vertice di T denotiamo con $T(v)$ il sottografo indotto dall'insieme di tutti i vertici u di T con $u \leq v$. Quindi, $T(v)$ è un albero con radice v ed è chiaro che $T(v) \simeq T$; esplicitamente, c'è un isomorfismo canonico $T \to T(v)$ definito da

$$w \mapsto vw \quad \text{per ogni } w \in T.$$

Questo isomorfismo induce in modo naturale un isomorfismo $A \to Aut(T(v))$, che si ottiene associando ad ogni $\phi \in A$, l'automorfismo $\phi(v)$ di $T(v)$ (attenzione: $\phi(v)$ *non* è l'immagine di v mediante ϕ) definito da, per ogni $w \in T$,

$$(vw)\phi(v) = v(w\phi).$$

Viceversa, ogni automorfismo α di $T(v)$ si solleva in modo naturale ad un automorfismo α^T di T, ponendo, per ogni $u \in T$,

$$u\alpha^T = \begin{cases} u\alpha & \text{se} \quad u \in T(v) \\ u & \text{se} \quad u \notin T(v) \end{cases} \tag{7.8}$$

È chiaro che la posizione $\alpha \mapsto \alpha^T$ definisce un omomorfismo iniettivo di $Aut(T(v))$ in A, la cui immagine, che denotiamo con $A(v)$ è contenuta nello stabilizzatore A_k del livello $k = \ell(v)$. Si vede poi immediatamente che se u, v sono vertici *non confrontabili* di T allora $A(u) \cap A(v) = 1$ e $\langle A(u), A(v) \rangle = A(u) \times A(v)$. Ne segue che se $v_1, \ldots, v_{n^k}$ sono i vertici di T che costituiscono il livello E_n^k allora

$$A_k = \langle A(v_1), \ldots, A(v_{n^k}) \rangle = A(v_1) \times \cdots \times A(v_{n^k}) \tag{7.9}$$

Poiché $A(v) \simeq A$ per ogni $v \in T$, se ne deduce che $A_k \simeq A \times \cdots \times A$ (n^k volte).

Soffermiamoci anche in questo caso ad esaminare quel che accade al primo livello, i cui elementi sono le singole lettere $0, 1, \ldots, n-1$. Abbiamo $A_1 = A(0) \times \cdots \times A(n-1)$, e qundi, per la (7.6),

$$A = (A(0) \times \ldots A(n-1)) \rtimes H_1 \simeq A^n \rtimes S_n. \tag{7.10}$$

Osservando che l'effetto su T di ogni $\sigma \in H_1$ come definita in (7.5) è quello di permutare i sottoalberi $T(0), \ldots, T(n-1)$ così come la permutazione σ permuta I_n (esplicitamente, $T(i)\sigma = T(i\sigma)$), non è troppo difficile (lo si tenti per esercizio) provare che

$$Aut(T) \simeq Aut(T) \wr S_n. \tag{7.11}$$

7.4 Esempi (gruppi di Grigorchuk e Gupta-Sidki)

Gruppi come gruppi di automorfismi di un albero. Poiché, per ogni $n \geq 1$, $Aut(T_n)$ è residualmente finito, ogni suo sottogruppo è tale. Quindi, condizione necessaria perché un gruppo sia rappresentabile come un gruppo di automorfismi di un albero regolare è la residuale finitezza. Come poi risulta chiaro dalla sezione precedente, ogni gruppo finito si può rappresentare come un gruppo di automorfismi di un albero regolare; questo è vero per molti altri gruppi conosciuti, anche se non sempre è facile trovare esplicitamente una rappresentazione: un caso relativamente facile è quello del gruppo diedrale infinito D_∞.

ESEMPIO 7.4. Consideriamo i seguenti automorfismi α, τ dell'albero binario T_2 (sono le parole nell'alfabeto $\{0,1\}$) definiti nel modo seguente:

– τ è la trasposizione $(0\ 1)$ applicata alla prima lettera come in (7.5);
– per quanto riguarda α, dato un vertice di T_2, lo scorre da sinistra a destra fino a quando trova degli zeri, quando incontra un 1 allora permuta la lettera successiva ancora come la trasposizione $(0\,1)$; per esempio $(11010)\alpha = 10010,\ (00101)\alpha = 00111$.

È chiaro che α e τ sono automorfismi di T_2 di periodo 2; quindi il sottogruppo di $A = Aut(T_2)$ da essi generato, $G = \langle \alpha, \tau \rangle$, è un gruppo diedrale (Proposizione 2.4). Per provare che G è infinito, utilizziamo una tecnica che applicheremo anche più sotto.
Con le notazioni introdotte nella sezione precedente, sia $A_1 = A(0) \times A(1)$ il nucleo dell'azione di A sull'insieme dei vertici $\{0,1\}$ del primo livello. Allora, $G \not\leq A_1$ (dato che $\tau \notin A_1$), quindi $G \cap A_1$ è un sottogruppo normale e proprio di G. D'altra parte, α fissa entrambi tali vertici, quindi $\alpha \in A(0) \times A(1)$, dunque $\langle \alpha, \alpha^\tau \rangle \leq G \cap A_1$. Ora, segue dalla definizione che $\alpha = (\alpha(0), \tau(1))$ mentre, facendo un minimo di conti, si trova $\alpha^\tau = (\tau(0), \alpha(1))$. Dunque se H è la proiezione di $G \cap A_1$ sulla ptrima componente $A(0)$ si ha $H = \langle \alpha(0), \tau(0) \rangle$. Ma allora $H \simeq G$. Poiché H è isomorfa ad un quoziente di $G \cap A_1$ che a sua volta è un sottogruppo proprio di G, si conclude che G deve essere un gruppo infinito. (questo esempio viene ripreso nel'esercizio 7.25, mentre con gli esercizi seguenti si mostra che il gruppo libero F_2 è un sottogruppo di $Aut(T_2)$). □

Definizioni ricorsive. La definizione diretta dell'automorfismo α nell'esempio 7.4 è (spero) convincente ma non quella più conveniente. Per definire automorfismi di un albero regolare T_n di tal genere, si ricorre piuttosto ad una definizione ricorsiva; metodo che consente molta maggiore disinvoltura nel trattamento. Ci limitiamo a darne la nozione più semplice, perché questa è sufficiente per l'uso che ne faremo, avvertendo che è possibile formularne di più generali e potenti. Sia dunque fissato $n \geq 1$ e l'immersione di S_n in $Aut(T_n)$ che abbiamo già descritto; se a è un simbolo, allora l'uguaglianza

$$a = (f_0, \ldots, f_{n-1}) \tag{7.12}$$

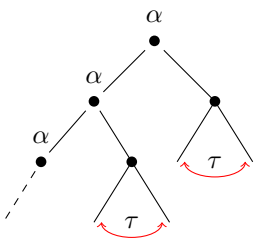
con $f_i \in \{a\} \cup S_n$ (più in generale si possono prendere gli f_i tra gli automorfismi finitari dell'albero - vedi esercizio 7.20), definisce ricorsivamente un unico automorfismo a di T_n, nel senso che a è l'automorfismo che fissa tutti gli elementi del primo livello $\{0, \ldots, n-1\}$) e opera su ogni sottografo $T(i)$ $(i = 1, \ldots, n-1$ come $f_i(i)$ se $f_i \in S_n$ e come $a(i)$ se $f_i = a$. Invece della (7.12), si usa anche scrivere, come faremo,

$$a = f_0(0) f_1(1) \ldots f_{n-1}(n-1).$$

Ci si convince che ciò effettivamente definisce un automorfismo osservando che esso (o più esttamente il suo ritratto - vedi esercizio 7.19) è direttamente definito per vertici di livello 1 e induttivamente per quelli di livello inferiore. Così, l'automorfismo α dell'esempio 7.4 si può definire ricorsivamente nella maniera seguente:

$$\alpha = (\alpha, \tau)$$

con $\tau = (0\ 1)$. La figura che segue cerca, appunto, di dar conto dell'automorfismo α.



Come detto, questa è la forma più semplice di definizione ricorsiva di automorfismi di alberi: si veda ad esempio l'esercizio 7.24, dove viene utilizzata una definizione ricorsiva multipla.

Il gruppo di Gupta–Sidki. Come già accennato, l'interesse principale dei gruppi di automorfismi di alberi con radice non sta tanto nel problema (comunque interessante) di quali gruppi, più o meno già noti, si possano così rappresentare, bensì nella possibilità di trovare nuovi gruppi, prima sconosciuti, con proprietà spesso inattese. In questo senso, l'esempio principale, che ha di fatto ha segnato l'inizio del crescente interesse per lo studio gruppi di automorfismi di alberi con radice, è costituito dai gruppi di Grigorchuk, la cui prima apparizione è del 1980. Si tratta di gruppi finitamente generati, periodici e infiniti, la cui basilare importanza discuteremo nella prossima sezione. Fra questi primi esempi, il più studiato è il cosiddetto primo gruppo di Grigorchuk, che è un 2-sottogruppo infinito dell'albero T_2 generato da tre involuzioni e che definiremo nell'esercizio 7.24. Qui, tratteremo più in dettaglio una variante, dovuta a Gupta e Sidki (1983), che fornisce, per ogni primo $p \geq 3$, un p-sottogruppo infinito di $Aut(T_p)$ generato da 2 elementi di ordine p.

Per semplicità, descriviamo il caso $p = 3$, ma la costruzione si applica ad ogni primo p dispari. Sia dunque $T = T_3$ l'albero con radice regolare di grado 3, e $A = Aut(T)$. Per quanto riguarda gli elementi e i sottogruppi di A adotteremo (senza rispiegarle) le notazioni introdotte nella sezione precedente. È conveniente rappresentare i vertici di T come le parole $x_1x_2\dots x_n$ con $x_i \in \{0,1,2\}$. Definiamo due automorfismi σ, α di T nel modo seguente:

- σ è l'automorfismo che opera come il ciclo $\sigma = (012)$ sulla prima lettera; pertanto, se $x = x_1x_2\dots x_n$ è un vertice di T:

$$x\sigma = (x_1\sigma)x_2\dots x_n.$$

- α è definito ricorsivamente dall'uguaglianza:

$$\alpha = (\alpha, \sigma, \sigma^{-1}).$$

L'effetto dell'automorfismo σ è quello di permutare ciclicamente e rigidamente i tre rami iniziali dell'albero. Mentre per α, dato un vertice di T come parola in $\{0,1,2\}$, lo scorre da sinistra a destra fino a quando trova degli zeri, e quando incontra una lettera $x_i \neq 0$, allora permuta la lettera successiva x_{i+1} così come il ciclo σ^{x_i} (cioè come σ se $x_i = 1$ e come $\sigma^2 = \sigma^{-1} = (021)$ se $x_i = 2$); per esempio:

$$(120)\alpha = 1(2\sigma)0 = 100, \quad (00201)\alpha = 002(0\sigma^{-1})1 = 00221.$$

Seguendo Gupta e Sidki, risulterà più comodo, esprimere α nella forma più esplicita:

$$\alpha = \alpha(0)\sigma(1)\sigma^{-1}(2) \tag{7.13}$$

È facile vedere che σ e α automorfismi di T tali che

$$|\sigma| = 3 = |\alpha|. \tag{7.14}$$

Sia $G = \langle \sigma, \alpha \rangle \leq A$. Dimostreremo che G è un 3-gruppo infinito.

Iniziamo con il sottogruppo $N = \langle \alpha \rangle^G$. Poiché $\alpha \in A_1 \cap G \trianglelefteq G$ e G è generato da α e σ con $|\sigma| = 3$, si ha $N \leq A_1 \cap G$ e

$$N = \langle \alpha, \alpha^\sigma, \alpha^{\sigma^2} \rangle. \tag{7.15}$$

È quindi essenziale descrivere i tre coniugati di α nella forma analoga a (7.13): si verifica direttamente che

$$\begin{aligned} \alpha &= \alpha(0)\sigma(1)\sigma^{-1}(2) \\ \alpha^\sigma &= \sigma^{-1}(0)\alpha(1)\sigma(2) \\ \alpha^{\sigma^2} &= \sigma(0)\sigma^{-1}(1)\alpha(2) \end{aligned} \tag{7.16}$$

Osserviamo inoltre che $G = N\langle\sigma\rangle$; poiché $\sigma \notin N$ (dato che $\sigma \notin A_1$) $G = N \rtimes \langle\sigma\rangle$ e, particolare, $|G/N| = 3$

G è infinito. Abbiamo $N \leq A_1 = A(0) \times A(1) \times A(2)$ (vedi (7.9)). Per $i = 0, 1, 2$, denotiamo con $G(i)$ la proiezione di N su $A(i)$; dalle identità (7.16) segue che, per $i = 0, 1, 2$,

$$G(i) = \langle \alpha(i), \sigma(i) \rangle, \tag{7.17}$$

e dunque $G(i) \simeq G$, e

$$N \leq G(0) \times G(1) \times G(2) \tag{7.18}$$

Ora, la proiezione $N \to G(0)$ è un omomorfismo suriettivo, quindi N contiene un quoziente isomorfo a $G(0) \simeq G$; poiché $|G/N| = 3$ si conclude che G è necessariamente di ordine infinito.

G è un 3-gruppo. Poniamo $a_0 = \alpha$, $a_1 = \alpha^\sigma$, $a_2 = \alpha^{\sigma^2}$. Quindi $N = \langle a_0, a_1, a_2 \rangle$. Ogni elemento di G si scrive nella forma

$$g = h\sigma^j, \text{ con } h \in N \text{ e } j \in \{0, 1, 2\}. \tag{7.19}$$

Poiché $h \in N$, h è un prodotto finito degli elementi a_0, a_1, a_2 (osserviamo infatti che, per ogni $i \in \{0, 1, 2\}$, $a_i^{-1} = a_i a_i$); scriviamo $h(a_0, a_1, a_2)$ per intendere formalmente la parola nell'alfabeto $\{a_0, a_1, a_2\}$ che rappresenta h. posto $\ell(h)$ la lunghezza della parola $h(a_0, a_1, a_2)$, definiamo la lunghezza di $g = h\sigma^j$ ponendo

$$\ell(h\sigma^j) = \begin{cases} \ell(h) \text{ se } j = 0 \\ \ell(h) + 1 \text{ se } j = 1, 2 \end{cases} \tag{7.20}$$

Facciamo una osservazione che ci sarà utile; siano $g = h\sigma^j, g_1 = h_1\sigma^t$, allora quando si rinormalizza il prodotto gg_1 per portarlo nella forma (7.19), si ha

$$gg_1 = h\sigma^j h_1 \sigma^t = h h_1^{\sigma^{-j}} \sigma^{j+t} = h(a_0, a_1, a_2) h_1(a_0^{\sigma^{-j}}, a_1^{\sigma^{-j}}, a_2^{\sigma^{-j}}) \sigma^{j+t} \tag{7.21}$$

dunque

$$\ell(gg_1) \leq \ell(g) + \ell(g_1) \quad \text{e} \quad \ell(gg_1) = \ell(g) + \ell(g_1) \Rightarrow g \in N. \tag{7.22}$$

Proviamo che l'ordine di $g = h\sigma^j$ è una potenza di 3 procedendo per induzione su $\ell(g)$. Se $\ell(g) = 1$, allora $g \in \{a_0, a_1, a_2, \sigma, \sigma^2\}$ e dunque, per quanto già noto $|g| = 3$.

Sia quindi $n \geq 1$, ed assumiamo che tutti gli elementi di lunghezza al più n abbiano ordine una potenza di 3. Sia $g = h\sigma^j$ di lunghezza $n+1$; per $i = 0, 1, 2$ denotiamo con r_i il numero di occorrenze della lettera a_i nella parola $h = h(a_0, a_1, a_2)$; quindi $r_0 + r_1 + r_2 = \ell(h)$. Distinguiamo due casi.

[**caso 1.** $j \neq 0$] Per comodità, assumiamo $j = 1$ (il caso $j = 2$ è analogo). Allora

$$g^3 = h\sigma h\sigma h\sigma = hh^{\sigma^2}h^\sigma\sigma^3 = hh^{\sigma^2}h^\sigma$$

e quindi $b = g^3$ coincide con

$$h(a_0, a_1, a_2)h(a_0, a_1, a_2)^{\sigma^2}h(a_0, a_1, a_2)^\sigma = h(a_0, a_1, a_2)h(a_2, a_0, a_1)h(a_1, a_2, a_0). \tag{7.23}$$

Ora, $b \in N$ e dunque, per (7.18), $b = (b_0, b_1, b_2)$ dove b_i è la proiezione di b su $G(i)$. Tenendo conto di (7.23) e delle identità (7.16) si ricava:

$$b_0 = h(a_0(0), \sigma^2(0), \sigma(0))h(\sigma(0), a_0(0), \sigma^2(0))h(\sigma^2(0), \sigma(0), a_0(0))$$

(ricordo che $a_0(0) = \alpha(0)$). In questa scrittura, ognuno di $\alpha(0), \sigma(0), \sigma^2(0)$ compare $r_0 + r_1 + r_2 = \ell(h) = n$ volte. Da (7.21) si conclude che

$$b_0 = y_0\sigma(0)^{n-n} = y_0(a_0(0), a_1(0), a_2(0)) \in G(0) \cap N = N(0) \tag{7.24}$$

con $\ell(b_0) = \ell(y_0) = n$. Per l'iptesi induttiva (applicata al gruppo $G(0) = \langle \alpha(0), \sigma(0) \rangle \simeq G$, si conclude che $|b_0|$ è una potenza di 3. La stessa cosa si prova per $|b_1|$ e $|b_2|$, e poiché gli elementi b_i commutano tra loro, si conclude che

$$|g^3| = |b| = m.c.m\{|b_0|, |b_1|, |b_2|\}$$

è una potenza di 3.

[**caso 2.** $j = 0$] In questo caso $g = g(a_0, a_1, a_2) \in N$ e $r_0 + r_1 + r_2 = n + 1$. Possiamo assumere che almeno due tra gli r_i siano diversi da 0, perché altrimenti g è una potenza di un a_i e pertanto ha ordine 3. Chiamando g_i la proiezione di g su $G(i)$ e, come prima, utilizzando le identità (7.16) si ha

$$\begin{aligned} g_0 &= g(a_0(0), \sigma^2(0), \sigma(0)) \\ g_1 &= g(\sigma(1), a_0(1), \sigma^2(1)) \\ g_2 &= g(\sigma^2(2), \sigma(2), a_0(2)) \end{aligned} \tag{7.25}$$

Applicando ancora le osservazioni in (7.21) e (7.22), si deduce che

$$g_0 = h_0\sigma(0)^{k_0} \qquad g_1 = h_1\sigma(1)^{k_1} \qquad g_0 = h_2\sigma(2)^{k_2}$$

con $h_i = h_i(a_0(i), a_1(1), a_2(i))$, $\ell(h_0) = r_0,\ \ell(h_1) = r_1,\ \ell(h_2) = r_2$, e

$$k_0 = r_2 - r_1, \quad k_1 = r_0 - r_1, \quad k_2 = r_2 - r_0.$$

poiché, come supposto, almeno due degli r_i sono diversi da 0 (e di conseguenza, $r_i \leq n$ per ciascun $i = 0, 1, 2$) si deduce, per definizionje di lunghezza, che

$$\ell(g_i) = \ell(h_i \sigma(i)^{k_i}) \leq n \quad (\forall i = 0, 1, 2). \tag{7.26}$$

Per ipotesi induttiva (applicata a $G(i)$) ogni g_i ha ordine una potenza di 3 e dunque, come nel primo caso per b, g ha ordine una potenza di 3. Ciò completa la dimostrazione.

7.5 Problemi di Burnside e di Milnor

I problemi di Burnside. Il gruppo diedrale infinito $D_\infty = \langle x, y \mid x^2 = y^2 = 1 \rangle$ è l'esempio più immediato di un gruppo finitamente generato *infinito* con un sistema di generatori (in questo caso $\{x, y\}$) costituito da elementi di ordine finito (altri esempi sono quelli dell'esercizio 4.10, mentre ciò non può accadere per gruppi abeliani, vedi Lemma 5.4). Il gruppo di Gupta-Sidki, così come il gruppo di Grigorchuk dell'esercizio 7.24, presentano l'ulteriore notevole proprietà che, pur essendo infiniti, tutti i loro elementi (e non solo quelli di un particolare sistema di generatori) hanno ordine finito (si tratta, cioè di gruppi periodici). Fu William Burnside, nel 1902, a porre per primo la questione: "è vero che ogni gruppo finitamente generato e periodico è finito?". Nella sezione precedente abbiamo dunque provato (mediante un gruppo di Gupta-Sidki) che la risposta è negativa; anche se la prima dimostrazione di ciò è dovuta a Golod e risale al 1964. Precisamente, impiegando importanti risultati ottenuti in collaborazione con Shafarevic intorno alle algebre polinomiali non commutative, (quindi, con metodi assai diversi Golod dimostrò il seguente,

Teorema 7.10. *Sia p un numero primo e sia $d \geq 2$. Allora esiste un p-gruppo infinito d-generato in cui ogni sottogruppo $(d-1)$-generato è finito.*

L'esponente di un gruppo G è, se esiste, il minimo intero $n \geq 1$ tale che $g^n = 1$ per ogni $g \in G$ (se non esiste G ha esponente infinito). Si può provare che i gruppi finitamente generati costruiti nel Teorema 7.10 sono periodici ma hanno esponente infinito, contengono cioè elementi il cui ordine è una potenza di p arbitrariamente grande.
Sempre nel 1902, W. Burnside pose la questione che divenne nota come *Problema di Burnside*: è vero che ogni gruppo finitamente generato di esponente finito è finito?
Egli stesso provò che la risposta è affermativa per sottogruppi di gruppi di matrici $GL(n, \mathbb{C})$ (vedi Esercizio 7.31). Ma anche in questo caso, la risposta è oggi nota essere negativa.

Per inquadrare meglio il problema, dati interi positivi n, r, il gruppo di Burnside $B(r, n)$ è definito come il quoziente F_r/F_r^n, dove F_r è il gruppo libero di rango r e $F_n^r = \langle w^n \mid w \in F_n \rangle$ è il sottogruppo (normale) generato da tutte le potenze n-esime in F_r.
Il problema di Burnside, enunciato in modo più completo, chiede per quali coppie di interi r, n il gruppo $B(r, n)$ è finito. Oltre al caso $r = 1$ che è banale, dato che $B(1, n)$ non è altro che il gruppo ciclico di ordine n, è noto che $B(r, n)$ è finito per ogni $r \geq 2$ e $n = 2, 3, 4, 6$. Il caso $n = 2$ è facile (un gruppo di esponente 2 è necessariamente abeliano), mentre i casi $3, 4$

e 6 sono dovuti, rispettivamente, a Burnside stesso, a Sanov e a M. Hall. Nel 1968, Novikov e Adjan hanno però dimostrato che, per $r \geq 2$ e n un numero dispari sufficientemente grande, $B(r,n)$ è infinito. In seguito, Adian migliorò il limite inferiore per n, mostrando che $B(r,n)$ è infinito per ogni $r \geq 2$ ed ogni dispari $n \geq 665$. Ol'shanskii provo poi che per ogni primo $p > 10^{40}$ esiste un p-gruppo infinito in cui ogni sottogruppo proprio è ciclico di ordine p (un tale gruppo è chiaramente 2-generato ed ha esponente p). A tutt'oggi, è ancora aperta la questione se i gruppi $B(2,5)$ e $B(2,8)$ siano infiniti.

Problema di Burnside ristretto. Stabilito che $B(r,n)$ non è in generale un gruppo finito, acquisì maggiore rilevanza il cosiddetto *problema di Burnside ristretto*: dati r, n come sopra, esiste un limite all'ordine di un *gruppo finito* r-generato di esponente n?
Indicato con $R(r,n)$ tale limite (eventualmente infinito), nel 1956 P. Hall and G. Higman provarono un risultato che riduce la questione al caso in cui n è la potenza di un primo: $R(r,n)$ è finito se e solo se $R(r,q)$ è finito per ogni q che sia potenza di un primo e divida n. Nel frattempo, Kostrikin dimostrò che $R(r,p)$ è finito per ogni r e p un numero primo. Ci vollero però diversi anni prima che, nel 1991, Zel'manov fosse in grado di provare (cosa che gli valse la Fields Medal) che $R(r,p^k)$ è finito per ogni primo p ed ogni $k \geq 1$, completando così la dimostrazione che $R(r,n)$ è finito per ogni r ed n.

Teorema 7.11. (Zelmanov 1990/91) *Esiste una funzione $R : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tale che per ogni $r, n \geq 1$, ogni gruppo finito r-generato di esponente n ha ordine al più $R(r,n)$.*

Il problema di Milnor. Il problema di Milnor (al quale abbiamo già accennato) riguarda i possibili tipi di crescita dei gruppi finitamente generati.
Nella sezione 6.5 abbiamo dato semplici esempi di gruppi a crescita polinomiale e di gruppi a crescita esponenziale, e riferito di un risultato di Milnor e Wolf che stabilisce che per gruppi risolubili queste sono le sole possibilità. Il *Problema di Milnor*, formulato di lì a poco, chiede se esistano gruppi finitamente generati a crescita "intermedia"; ovvero se esistano gruppi f.g. G tali che la crescita γ_G è

- *superpolinomiale*, nel senso che non esiste alcun intero $k \geq 1$ tale che $\gamma_G(x) \preccurlyeq x^k$;
- *subesponenziale*, ovvero tale che $\gamma_G(x) \not\sim 2^x$.

(Abbiamo già osservato che, comunque, $\gamma_G(x) \preccurlyeq 2^x$). La risposta fu data da Grigorchuk nel 1983, provando che il primo gruppo di Grigorchuk (definito nell'esercizio 7.24) è un gruppo a crescita intermedia. La dimostrazione di ciò richiederebbe alcune altre pagine e la omettiamo (sarà aggiunta forse nelle prossime versioni).
Grigorchuk dimostrò anche che i tipi di funzioni di crescita sono in quantità non numerabile, e che esistono gruppi finitamente generati con funzioni di crescita che non sono confrontabili nel senso della relazione $\preccurlyeq$. Da allora, molte altri risultati intorno alla crescita intermedia sono stati ottenuti, ad esempio è stato provato (Shalom e Tao, 2010) che se $\gamma_G(n) \preccurlyeq n^{(\log\log n)^c}$, per qualche $c > 0$, allora γ_G è polinomiale (quindi esistono degli "intervalli" nella distribuzione dei possibili tipi di crescita; la natura di tali intervalli è oggetto di una congettura), ma molte questioni rimangono aperte, come quella dell'esistenza di gruppi *finitamente presentati* a crescita intermedia.

7.6 Esercizi VII

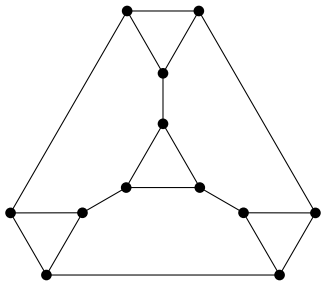
Sezione 7.1

Esercizio 7.1. Si dimostri che un albero finito con almeno due vertici ha (almeno) un vertice di grado 1 (i vertici di grado 1 sono chiamati "foglie" dell'albero)

Esercizio 7.2. Sia Γ un albero finito. Si provi che $|V(\Gamma)| = |E(\Gamma)| + 1$.

Esercizio 7.3. Sia $n \geq 2$, e sia $D_{2n} = \langle x, y \mid y^n = x^2 = 1,\ y^x = y^{-1} \rangle$ il gruppo diedrale di ordine $2n$. Posto $S = \{y, x\}$, si descriva il grafo di Cayley $\Gamma[D_{2n}, S]$.

Esercizio 7.4. Si trovi un gruppo G ed un suo sistema di generatori S tale che il corrispondente grafo di Cayley sia il seguente:

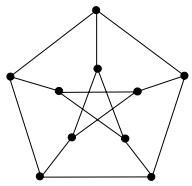


Esercizio 7.5. Si trovi un gruppo G assieme ad un suo sistema di generatori S tali che il grafo di Cayley $\Gamma[G; S]$ è una griglia esagonale (infinita).

Esercizio 7.6. Dato un grafo Γ con insieme di vertici $V = V(\Gamma)$, il *grafo complementare* è il grafo $\overline{\Gamma}$ con $V(\overline{\Gamma}) = V$ e insieme di archi il complementare di quello degli archi di Γ, ovvero $E(\overline{\Gamma}) = V^{[2]} \setminus E(\Gamma)$. Si provi che il grafo complementare di un grafo di Cayley è un grafo di Cayley.

Esercizio 7.7. Sia D il gruppo diedrale infinito, e sia Γ il grafo di Cayley definito nell'esempio 7.3. Sia quindi $A = Aut(\Gamma)$ (quindi $D \leq A$ mediante la rappresentazione per moltiplicazione a sinistra). Sia v un vertice di Γ e $H = \{\alpha \in A \mid v\alpha = v\}$ lo stabilizzatore in A di v; si provi che $|H| = 2$. Si concluda che $DH = A$, e dunque, in particolare, che $D \trianglelefteq A$

Esercizio 7.8. Un celebre grafo 3-regolare è il *grafo di Petersen P*



Si provi che P è vertex–transitivo, ma che P non è un grafo di Cayley.

Sezione 7.2

Esercizio 7.9. Sia G un gruppo e sia $\emptyset \neq X \subseteq G$. Si provi che sono equivalenti:
1) G è un gruppo libero su X;
2) $X \cap X^{-1} = \emptyset$ e $\Gamma[G, X]$ è un albero.

Esercizio 7.10. Siano Γ un grafo e G un gruppo automorfismi di Γ. Si provi che se l'azione di G su $V(\Gamma)$ è regolare, allora esiste $S \subseteq G$ tale che $\Gamma \simeq \Gamma[G; S]$..

Esercizio 7.11. Sia F un gruppo libero e sia $1 \neq a \in F$.
1. Si provi che $C_F(a)$ è ciclico.
2. Si provi che esiste $n \geq 1$ tale che per ogni $m > n$ non esiste alcun $b \in F$ tale che $b^m = a$.

Esercizio 7.12. Sia F un gruppo libero su X, e sia $\alpha \in Aut(F)$ tale che $X^\alpha = X$. Si provi che se $C_F(\alpha) \cap X = \emptyset$, allora $C_F(\alpha) = 1$.

Esercizio 7.13. Si descriva un sottogruppo del gruppo libero F_2 che abbia rango infinito.

Esercizio 7.14. Sia F un gruppo libero di rango almeno 2. Si provi che il sottogruppo derivato F' ha rango infinito.

Sezione 7.4

Esercizio 7.15. Sia $\mathfrak{T}$ un albero localmente finito (cioè tale che il grado di ogni vertice è finito) e sia $A = Aut(\mathfrak{T})$. Fissato un vertice $v \in V(\mathfrak{T})$, sia $S_A(v) = \{\phi \in A \mid v\phi = v\}$. Si provi che $S_A(v)$ è un gruppo residualmente finito.

Esercizio 7.16. Si provi che il gruppo degli automorfismi A dell'albero T_2 è residualmente un 2-gruppo finito.

Esercizio 7.17. Sia $1 \neq g \in Aut(T_n)$. Si provi che esiste $0 < k \in \mathbb{N}$ tale che l'equazione $x^k = g$ non ha soluzioni in $Aut(T_n)$.

Esercizio 7.18. Si dimostri in modo compiuto l'isomorfismo (7.11).

Esercizio 7.19. Sia $n \geq 2$ e $T = T_n$. Sia $g \in Aut(T)$; allora per ogni vertice v di T, g permuta gli n elementi $(vg)0, (vg)1, \ldots, (vg)(n-1)$ del primo livello dell'albero $T(vg)$; denotiamo con $\pi(g, v)$ la permutazione indotta da g su questo insieme di vertici. Quindi $\pi(g, v) \in S_n$. L'insieme $\Pi(g) = \{\pi(g, v) \mid v \in V(T)\}$ è detto *ritratto* di g. Si provi che $g \mapsto \Pi(g)$ definisce una biezione tra $Aut(T)$ e l'insieme di tutte le applicazioni $V(T) \to S_n$. Si concluda che $Aut(T)$ non è numerabile e quindi non è finitamente generato.

Esercizio 7.20. Con le notazioni introdotte nell'esercizio precedente, diciamo che un automorfismo ϕ del grafo regolare T_n è *finitario* se $\pi(\phi, v) \neq 1$ soltanto per un numero finito di vertici v. Si provi che $Aut_f(T_n) = \{\phi \in A \mid \phi \text{ finitario}\}$ è un sottogruppo periodico di $A = Aut(T_n)$.

Sezione 7.5

Esercizio 7.21. Si provi che il gruppo di Gupta–Sidki costruito in questa sezione è residualmente un 3-gruppo finito.

Esercizio 7.22. Si descriva il sottogruppo di $Aut(T_2)$ generato dagli automorfismi ricorsivamente definiti

$$\alpha(\alpha, \tau) \qquad \beta = (\tau, \beta)$$

dove $\tau = (0\ 1)$.

Esercizio 7.23. Con le notazioni utilizzate nella costruzione del gruppo di Gupta–Sidki, si ponga

$$\beta = \beta(0)\sigma(1)\sigma(2).$$

Si provi che $|\beta| = 3$, ma che il sottogruppo $\langle \beta, \sigma \rangle$ di $Aut(T_3)$ non è periodico (Bartholdi e Grigorchuk hanno provato che tale gruppo ha un sottogruppo privo di torsione di indice 3).

Esercizio 7.24. (*Primo gruppo di Grigorchuk*) Sia $T = T_2$ e $\tau = (01)$. Si considerino le seguenti relazioni ricorsive

$$a = (\tau, b) \quad b = (\tau, c) \quad c = (1, a).$$

(i) Si provi che tali relazioni definiscono tre automorfismi a, b e c di T, che $|a| = |b| = |c| = 2$ e $c = ab$ (quindi, $\langle a, b \rangle \simeq C_2 \times C_2$).

(ii) Si provi che $\langle \tau, c \rangle \simeq D_8$, $\langle \tau, b \rangle \simeq D_{16}$ e $\langle \tau, a \rangle \simeq D_{32}$.

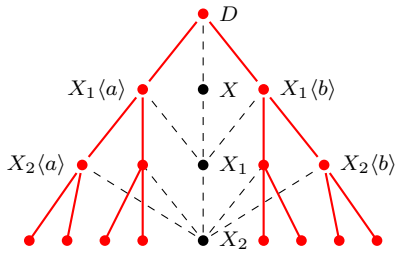
(iii) Sia $G_1 = \langle \tau, a, b \rangle$. Si provi che $H = \langle a, b, a^\tau, b^\tau \rangle$ è un sottogruppo normale di indice 2 di G_1, Si provi che G_1 è infinito (come detto, si può dimostrare poi che ogni suo elemento ha ordine una potenza di 2).

Esercizio 7.25. Sia $D = \langle a, b \mid a^2 = b^2 = 1 \rangle$ il gruppo diedrale infinito. Poniamo $x = ab$, $X = \angle x \rangle$ (quindi X è infinito e $[D : X] = 2$), e per ogni $n \geq 0$ scriviamo $X_n = \langle x^{2^n} \rangle$. Denotiamo quindi con $\mathfrak{D}$ l'insieme di tutti i sottogruppi di D che sono diedrali infiniti; cioè

$$\mathfrak{D} = \{H \leq D \mid H \simeq D\}.$$

1. Si provi che gli elementi di $\mathfrak{D}$, oltre a D stesso, sono tutti e soli i sottogruppi del tipo $X_n\langle a^{x^i} \rangle$, $X_n\langle b^{x^i} \rangle$, con $n \geq 1$ e $0 \leq i < 2^{n-1}$.

2. Si provi che, ordinato per inclusione, l'insieme $\mathfrak{D}$ è isomorfo all'albero regolare T_2 (la figura di sotto mostra - in rosso - la parte superiore di $\mathfrak{D}$, mentre in tratteggio altre inclusioni tra sottogruppi di D) e che l'azione per coniugio di D induce un'azione fedele di D come gruppo di automorfismi di $\mathfrak{D}$.



I prossimi tre esercizi descrivono un metodo per rappresentare i gruppi liberi (di rango al più numerabile) come gruppi di automorfismi dell'albero T_2. Il primo è una osservazione tecnica sui 2-gruppi abeliani finiti.

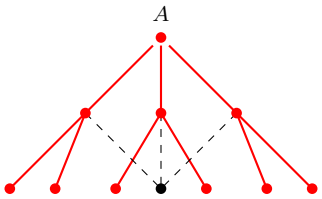
Esercizio 7.26. Sia G gruppo abeliano 2-generato non ciclico di ordine una potenza di 2. Allora $X = \{g \in G \mid g^2 = 1\} \simeq C_2 \times C_2$. Si provi che se G/X è ciclico di ordine 2^n con $n \geq 1$, allora $G = \langle a \rangle \times \langle b \rangle$ con $|a| = 2$, $|b| = 2^{n+1}$; si provi quindi che, in questo caso, esistono esattamente due sottogruppi H di ordine 2 tali che il quoziente G/H è ciclico.

Esercizio 7.27. Sia $A = \mathbb{Z} \times \mathbb{Z}$; si dimostrino i seguenti fatti.

(i) Posto $A^2 = \{a^2 \mid a \in A\}$, si ha $A/A^2 \simeq C_2 \times C_2$.

(ii) Ogni sottogruppo di indice finito di A è isomorfo ad A.

(iii) L'insieme $\mathfrak{U}$ di tutti i sottogruppi $H \leq G$ tali che A/H è ciclico di ordine una potenza di 2, ordinato per inclusione, è un albero con radice G (la figura di sotto ne mostra - in rosso - la parte superiore), e per ogni $G \neq H \in \mathfrak{U}$, $\mathfrak{U}(H)$ è isomorfo all'albero binario T_2.



(iv) Ogni automorfismo di A induce un automorfismo dell'albero $\mathfrak{U}$. Sia $\phi \in Aut(A)$: se esiste $H \in \mathfrak{U}$ tale che ϕ fissa tutti i vertici di $\mathfrak{U}(H)$, allora $\phi = 1$ oppure ϕ è l'inversione su A.

Esercizio 7.28. Con le notazioni dell'esercizio precedente, sia $A = \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z} \times \mathbb{Z}$ e poniamo $H = \langle a, b^2 \rangle$ e $W = Stab_{Aut(A)}(H)$. Allora $W/\{\pm 1\}$ è isomorfo ad un sottogruppo di $Aut(\mathfrak{U}(H))$ e quindi di $Aut(T_2)$. Utilizzando l'esempio 4.4 si dimostri quindi che W contiene un sottogruppo libero di rango 2.

Sezione 7.6

Esercizio 7.29. Si provi che un gruppo risolubile finitamente generato e periodico è finito. [sugg.: fare induzione sulla lunghezza derivata del gruppo]

Esercizio 7.30. Sia G un gruppo di esponente 3.

(i) Si provi che, per ogni $a, b \in G$, a e a^b commutano e $aa^b a^{b^2} = 1$.

(ii) Si provi che, per ogni $a \in G$, $\langle a \rangle^G = \langle a^b \mid b \in G \rangle$ è un gruppo abeliano. Si deduca che se $G = \langle a, b \rangle$ allora $|G| \leq 27$. Si trovi quindi un gruppo 2-generato di esponente 3 ed ordine 27. Pertanto $|B(2,3)| = 27$.

(iii) Si provi che, per ogni $r \geq 1$, $|B(r+1,3)| \leq 3^{|B(r,3)|}|B(r,3)|$.

Esercizio 7.31. Sia $1 \leq m \in \mathbb{N}$, e sia $G \leq GL(m, \mathbb{C})$.

(i) Sia $\mathcal{L}$ il sottospazio del $\mathbb{C}$-spazio vettoriale $M_m(\mathbb{C})$ di tutte la matrici di ordine m su $\mathbb{C}$ generato da G; allora esiste un sottoinsieme finito $\{g_1, \ldots, g_s\}$ di G che genera $\mathcal{L}$. Sia $b \in \mathcal{L}$; si provi che se $tr(g_i b) = 0$ per ogni $i = 1, \ldots, s$, allora $b = 0$. Si concluda che se $b, b_1 \in \mathcal{L}$ e $b \neq b_1$ allora esiste $i = 1, \ldots, s$ tale che $tr(g_i b) \neq tr(g_i b_1)$. [Usare il fatto che se $tr(b^k) = 0$ per ogni $k \geq 0$ allora $b = 0$].

(ii) (*Burnside*) Si assuma ora che il gruppo G abbia esponente finito, cioè che esista $n \geq 1$ tale che $g^n = 1$ per ogni $g \in G$. Si osservi che, per ogni $g \in G$, tutti gli autovalori di g sono

radici dell'unità. Utilizzando il punto (i), si provi quindi che G è un gruppo finito. [Tener conto che la traccia di una matrice complessa è la somma dei suoi autovalori].

Esercizio 7.32. Applicando il Teorema di Zelmanov, si provi che un gruppo di automorfismi di un albero con radice finitamente generato e di esponente finito è finito.

Indice analitico

Bibliografia

[1] M. Artin, Algebra. Prentice–Hall 1991 (ed. italiana: Bollati–Boringhieri 1997).

[2] C. Casolo, Dispense Algebra I e II. *web.math.unifi.it/users/casolo/didattica.html*

[3] D. J. S. Robinson, A Course in the Theory of Groups. Graduate Texts in Mathematics **80**. Springer–Verlag, 1982.

[4] C. D. Bennett, Explicit free subgroups of $Aut(\mathbb{R}, \leq)$. *Proc. Amer. Math. Soc.* **125**, 1305–1308 (1997).