Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

IL GRUPPO DEI QUATERNIONI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Irene Azzali

II Sessione
Anno Accademico 2013/2014

Introduzione

In questa tesi si trattano alcuni problemi interessanti legati al gruppo dei quaternioni.

In teoria dei gruppi è noto che ogni gruppo commutativo ha la proprietà che ogni suo sottogruppo è normale. Sorgono allora spontanee alcune domande: esistono gruppi abeliani in cui tutti i sottogruppi sono normali? Se sì, hanno una struttura simile?

In questo lavoro è stata data una risposta ad entrambi i quesiti. Per prima cosa infatti è presentato il gruppo dei quaternioni; si tratta di un gruppo di ordine 8 i cui elementi sono matrici invertibili 2x2 a coefficienti nel campo complesso. Dalla sua tavola di moltiplicazione si deduce che il gruppo non è commutativo. Tuttavia descrivendo i suoi sottogruppi si trova che essi sono tutti normali. Successivamente si passa a classificare tutti i gruppi con la proprietà di avere tutti i sottogruppi normali. Si scopre così che non si allontanano molto dal gruppo dei quaternioni. La classificazione è determinata dal teorema di Dedekind che afferma che tutti i sottogruppi di un gruppo sono normali se e solo se il gruppo è commutativo oppure prodotto diretto del gruppo dei quaternioni, di un gruppo commutativo i cui elementi hanno ordine al più 2 e di un gruppo commutativo i cui elementi hanno ordine dispari.

L'ultimo capitolo sviluppa un recente risultato del matematico Richard Dean. Un importante problema aperto della teoria di Galois è il seguente: dato un gruppo finito G, è sempre possibile trovare una estensione dei razionali tale che G sia il gruppo di Galois di quella estensione? E' naturale

quindi chiedersi se esista un polinomio a coefficienti razionali il cui gruppo di Galois coincida proprio con il gruppo dei quaternioni. Sfruttando il teorema fondamentale della teoria di Galois e due teoremi sulle estensioni cicliche di grado 4 si trova che il polinomio $q(x) = x^8 - 72x^6 + 180x^4 - 144x^2 + 36$ ha gruppo di Galois uguale al gruppo dei quaternioni.

Indice

Capitolo 1

Nozioni preliminari

In questo capitolo verranno riportati enunciati e dimostrazioni di teoria dei guppi necessari per lo studio delle caratteristiche del gruppo dei quaternioni.

1.1 Commutatori

Tutti i gruppi considerati sono moltiplicativi, salvo diversa indicazione. Notazione: Dato un gruppo G e un suo elemento x denotiamo con $|x|$ l'ordine di x.

Definizione 1.1.1. Sia G un gruppo e siano x_1, x_2 elementi di G. Si dice *commutatore* di x_1 e x_2 l'elemento

$$[x_1, x_2] = {x_1}^{-1}{x_2}^{-2}x_1x_2.$$

Possiamo poi ricorsivamente definire un *commutatore di lunghezza* $n \geq 2$ secondo la regola

$$[x_1, \cdots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$$

dove $[x_1] = x_1$.

Elenchiamo ora una serie di proprietà dei commutatori. Se a, $x \in G$ con la notazione a^x indichiamo l'elemento $a^x = x^{-1}ax$.

Proposizione 1.1.1. *Siano x, y, z elementi di un gruppo G. Allora:*

1. $[x,y]=1$ *se e solo se x e y commutano tra loro;*
2. $[x,y]=[y,x]^{-1}$;
3. $[xy,z]=[x,z]^y[y,z]$ *e* $[x,yz]=[x,z][x,y]^z$;
4. $[x,y^{-1}]=([x,y]^{y^{-1}})^{-1}$ *e* $[x^{-1},y]=([x,y]^{x^{-1}})^{-1}$;
5. $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x=1$.

Dimostrazione. 1. $[x,y]=1 \Leftrightarrow x^{-1}y^{-1}xy=1 \Leftrightarrow xy=yx$.

2. $[y,x]=y^{-1}x^{-1}yx$, quindi si ha $[y,x]^{-1}=(y^{-1}x^{-1}yx)^{-1}=x^{-1}y^{-1}xy=[x,y]$.

3. $[xy,z]=(xy)^{-1}z^{-1}xyz=y^{-1}x^{-1}z^{-1}xyz$
   $[x,z]^y=y^{-1}[x,z]y=y^{-1}x^{-1}z^{-1}xzy$, quindi si ha:
   $[x,z]^y[y,z]=y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz=y^{-1}x^{-1}z^{-1}xzz^{-1}yz=y^{-1}x^{-1}z^{-1}xyz=[xy,z]$.
   analogamente
   $[x,yz]=x^{-1}(yz)^{-1}xyz=x^{-1}z^{-1}y^{-1}xyz$
   $[x,y]^z=z^{-1}[x,y]z=z^{-1}x^{-1}y^{-1}xyz$, quindi si ha:
   $[x,z][x,y]^z=x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz=x^{-1}z^{-1}xx^{-1}y^{-1}xyz=x^{-1}z^{-1}y^{-1}xyz=[x,yz]$.

4. $[x,y^{-1}]=x^{-1}yxy^{-1}$
   $[x,y]^{y^{-1}}=y[x,y]y^{-1}=yx^{-1}y^{-1}xyy^{-1}=yx^{-1}y^{-1}x$, quindi:
   $([x,y]^{y^{-1}})^{-1}=x^{-1}yxy^{-1}=[x,y^{-1}]$.
   analogamente
   $[x^{-1},y]=xy^{-1}x^{-1}y$
   $[x,y]^{x^{-1}}=x[x,y]x^{-1}=xx^{-1}y^{-1}xyx^{-1}=y^{-1}xyx^{-1}$, quindi:
   $([x,y]^{x^{-1}})^{-1}=xy^{-1}x^{-1}y=[x^{-1},y]$.

5. Poniamo $u = xzx^{-1}yx, v = yxy^{-1}zyew = zyz^{-1}xz$ e osserviamo che $[x, y^{-1}, z]^y = u^{-1}v, [y, z^{-1}, x]^z = v^{-1}w$ e $[z, x^{-1}, y]^x = w^{-1}u$; l'identità è così ovvia.

□

Osservazione 1. Si ha che $a^x = a \Leftrightarrow x^{-1}ax = a \Leftrightarrow ax = xa \Leftrightarrow [x, a] = 1$.

Proposizione 1.1.2. *Sia G un gruppo e sia H un sottogruppo di G. Sono equivalenti:*

1. *Per ogni $y \in G$ si ha che $y^{-1}Hy \subseteq H$*

2. *Per ogni $x \in H$ e per ogni $y \in G$ si ha che $[x, y] \in H$*

Se si verifica una di queste due condizioni diciamo che H è un sottogruppo normale di G e utilizziamo la notazione $H \trianglelefteq G$.

Dimostrazione. $1 \Rightarrow 2$ Siano $x \in H, y \in G$, allora $[x, y] = x^{-1}y^{-1}xy \in H$ poiché $x^{-1} \in H$ come pure $y^{-1}xy \in H$.

$2 \Rightarrow 1$ Siano $x \in H, y \in G$, allora $[x, y] \in H$ ossia $x^{-1}y^{-1}xy \in H$. Si ha quindi che $xx^{-1}y^{-1}xy \in H$ cioè $y^{-1}xy \in H$.

□

Per la dimostrazione della seguente proposizione si veda [1].

Proposizione 1.1.3. *Se G è un gruppo e H un sottogruppo di G di indice 2, allora H è un sottogruppo normale in G.*

Se $g_1, \ldots, g_n$ sono elementi di un gruppo G con la notazione $\langle g_1, \ldots, g_n \rangle$ indichiamo il sottogruppo di G da essi generato.

Definizione 1.1.2. Siano X_1, X_2 sottoinsiemi non vuoti di un gruppo G. Si dice *sottogruppo commutatore* di X_1 e X_2

$$[X_1, X_2] = \langle [x_1, x_2] \mid x_1 \in X_1, x_2 \in X_2 \rangle .$$

Osservazione 2. Grazie alla seconda proprietà dei commutatori $[X_1, X_2] = [X_2, X_1]$.

Definizione 1.1.3. Sia G un gruppo. Si dice *sottogruppo derivato*

$$G' = \langle [x_1, x_2] \mid x_1, x_2 \in G \rangle .$$

Definizione 1.1.4. Sia G un gruppo. Si dice *centro di* G l'insieme

$$Z(G) = \{ x \in G \mid ax = xa \quad \text{per ogni} \quad a \in G \} .$$

Proposizione 1.1.4. *Il centro $Z(G)$ di G è un sottogruppo del gruppo G.*

Dimostrazione. Si ha che $1 \in Z(G)$ perchè $a1 = 1a$ per ogni $a \in G$. Occorre poi provare che dati $x, y \in Z(G)$ si ha che $xy^{-1} \in Z(G)$. Sia $a \in G, a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = x(ya^{-1})^{-1} = x(a^{-1}y)^{-1} = xy^{-1}(a^{-1})^{-1} = (xy^{-1})a$.
Si ha quindi che $Z(G)$ è un sottogruppo di G. □

Proposizione 1.1.5. *Dato un gruppo G ogni sottogruppo H del centro $Z(G)$ di G è normale in G. In particolare $Z(G) \trianglelefteq G$.*

Dimostrazione. Siano H un sottogruppo di $Z(G)$, $h \in H$, $g \in G$, allora $[h, g] = 1 \in H$ poiché H è un sottogruppo normale. □

Definizione 1.1.5. Sia G un gruppo. G si dice *nilpotente di classe* 2 se $G' \subseteq Z(G)$.

Lemma 1.1.6. *Sia G un gruppo e siano $x, z \in G$ tali che $[[x, z], x] = 1 = [[x, z], z]$. Allora*

$$[x^n, z] = [x, z]^n = [x, z^n] \quad \textit{per ogni} \quad n \in \mathbb{N}.$$

Dimostrazione. Dimostriamo l'asserto per induzione su n.
Per $n = 1$ è ovvio.
Siano $n = 2$ e $x, z \in G$. Allora $[x^2, z] = [xx, z] = [x, z]^x[x, z] = [x, z][x, z] = [x, z]^2$. Supponiamo che l'asserto valga per $n - 1$ e dimostriamolo per n :

$[x^n, z] = [x^{n-1}x, z] = [x^{n-1}, z]^x[x, z] = ([x, z]^{n-1})^x = [x, z]^{n-1}[x, z] = [x, z]^n$ dove abbiamo usato il fatto che se x commuta con $[x, z]$ allora commuta con ogni sua potenza.
Analogamente dimostriamo che $[x, z^n] = [x, z]^n$ usando la proprietà 2 della Proposizione 1.1.1. Si ha infatti che $[x, z^n] = [z^n, x]^{-1} = ([z, x]^n)^{-1} = ([z, x]^{-1})^n = [x, z]^n$. □

Lemma 1.1.7. *Sia G un gruppo. Se $g_1, g_2 \in G$ e $z_1, z_2 \in Z(G)$ allora*

$$[g_1z_1, g_2z_2] = [g_1, g_2].$$

Dimostrazione. Si ha che $[g_1z_1, g_2z_2] = [g_1, g_2z_2]^{z_1}[z_1, g_2z_2] = [g_1, g_2z_2]^{z_1} = [g_1, g_2z_2] = [g_1, z_2][g_1, g_2]^{z_2} = [g_1, g_2]^{z_2} = [g_1, g_2]$. □

Lemma 1.1.8. *Sia G un gruppo e siano $x, y \in G$ tali che $[[x, y], x] = 1 = [[x, y], y]$. Allora*

$$[x^m, y^n] = [x, y]^{mn} \quad \textit{per ogni} \quad m, n \in \mathbb{Z}.$$

Dimostrazione. Abbiamo che $[x, y^n] = [x, y]^n$ commuta con x^m, y^n, x, y per ipotesi, quindi per il Lemma 1.1.6 otteniamo: $[x^m, y^n] = [x, y^n]^m = ([x, y]^n)^m = [x, y]^{mn}$. □

Lemma 1.1.9. *Sia G un gruppo e siano $x, y \in G$ e tali che $[[x, y], x] = 1 = [[x, y], y]$. Allora*

$$[x^{n_1}y^{m_1}[x, y]^{r_1}, x^{n_2}y^{m_2}[x, y]^{r_2}] = [x, y]^{n_1m_2-n_2m_1} \quad \textit{per ogni} \quad n_i, m_i, r_i \in \mathbb{Z}.$$

Dimostrazione. Ricordiamo che per ipotesi ogni potenza di $[x, y]$ commuta con ogni potenza sia di x che di y.
Si ha che $[x^{n_1}y^{m_1}[x, y]^{r_1}, x^{n_2}y^{m_2}[x, y]^{r_2}] =$
$[x^{n_1}, x^{n_2}y^{m_2}[x, y]^{r_2}]^{y^{m_1}}[y^{m_1}[x, y]^{r_1}, x^{n_2}y^{m_2}[x, y]^{r_2}]$. Ora, $[x^{n_1}, x^{n_2}y^{m_2}[x, y]^{r_2}]^{y^{m_1}} =$
$([x^{n_1}, y^{m_2}[x, y]^{r_2}][x^{n_1}, x^{n_2}]^{y^{m_2}[x,y]^{r_2}})^{y^{m_1}} =$
$[x^{n_1}, [x, y]^{r_2}][x^{n_1}, y^{m_2}]^{[x,y]^{r_2}y^{m_1}} = [x, y]^{n_1m_2}$, dove abbiamo usato il Lemma 1.1.8.
Consideriamo $[y^{m_1}[x, y]^{r_1}, x^{n_2}y^{m_2}[x, y]^{r_2}] =$

$[y^{m_1}, x^{n_2}y^{m_2}[x,y]^{r_2}]^{[x,y]^{r_1}}[[x,y]^{r_1}, x^{n_2}y^{m_2}[x,y]^{r_2}] =$
$([y^{m_1}, y^{m_2}[x,y]^{r_2}][y^{m_1}, x^{n_2}]^{y^{m_2}[x,y]^{r_2}})^{[x,y]^{r_1}}[[x,y]^{r_1}, y^{m_2}[x,y]^{r_2}][[x,y]^{r_1}, x^{n_2}]^{y^{m_2}[x,y]^{r_2}} =$
$[y^{m_1}, [x,y]^{r_2}]([y^{m_1}, y^{m_2}]^{[x,y]^{r_2}})(([y,x]^{m_1n_2})^{y^{m_2}[x,y]^{r_2}})^{[x,y]^{r_1}}[[x,y]^{r_1}, [x,y]^{r_2}][[x,y]^{r_1}, y^{m_2}]^{[x,y]^{r_2}} =$
$[x,y]^{-m_1n_2}$, dove abbiamo usato il Lemma 1.1.8.
Quindi $[x^{n_1}y^{m_1}[x,y]^{r_1}, x^{n_2}y^{m_2}[x,y]^{r_2}] = [x,y]^{n_1m_2-n_2m_1}$. □

Proposizione 1.1.10. *Se G è un gruppo generato da due elementi x e y tali che $[[x,y],x] = 1 = [[x,y],y]$ allora*

$$G = \{\, x^n y^m [x,y]^s \mid \quad m,n,s \in \mathbb{Z} \,\}.$$

Dimostrazione. Indichiamo con S l'insieme $\{\, x^n y^m [x,y]^s, \quad m,n,s \in \mathbb{Z} \,\}$. Si ha che $1 = x^0y^0[x,y]^0 \in S$. Siano poi $g_1 = x^{n_1}y^{m_1}[x,y]^{s_1}$ e $g_2 = x^{n_2}y^{m_2}[x,y]^{s_2}$. Utilizzando il fatto che $yx = xy[y,x] = xy[x,y]^{-1}$, che le potenze di $[x,y]$ commutano con le potenze di x e di y e il Lemma 1.1.8 si ha: $g_1g_2 =$
$x^{n_1}y^{m_1}[x,y]^{s_1}x^{n_2}y^{m_2}[x,y]^{s_2} =$
$x^{n_1}y^{m_1}x^{n_2}[x,y]^{s_1}y^{m_2}[x,y]^{s_2} = x^{n_1}y^{m_1}x^{n_2}y^{m_2}[x,y]^{s_1+s_2} =$
$x^{n_1}x^{n_2}y^{m_1}[x,y]^{-n_2m_1}y^{m_2}[x,y]^{s_1+s_2} =$
$x^{n_1+n_2}y^{m_1+m_2}[x,y]^{s_1+s_2-n_2m_1}$.
Sia $g = x^ny^m[x,y]^s$; allora si ha: $g^{-1} = [x,y]^{-s}y^{-m}x^{-n} = y^{-m}[x,y]^{-s}x^{-n} =$
$y^{-m}x^{-n}[x,y]^{-s} = x^{-n}y^{-m}[x^{-n},y^{-m}]^{-1}[x,y]^{-s} = x^{-n}y^{-m}[x,y]^{-nm-s}$, dove abbiamo usato il fatto che $yx = xy[y,x] = xy[x,y]^{-1}$, e il Lemma 1.1.6. Ne viene che S è chiuso rispetto al prodotto e all'inverso, quindi S è un sottogruppo di G, ma poiché contiene x e y si ha che $S = G$. □

Proposizione 1.1.11. *Se G è un gruppo generato da due elementi x e y tali che $[[x,y],x] = 1 = [[x,y],y]$ allora $G' = \langle [x,y] \rangle$; quindi G è nilpotente di classe* 2.

Dimostrazione. Utilizzando la Proposizione 1.1.10 e il Lemma 1.1.9 abbiamo che il commutatore tra due qualsiasi elementi di G è una potenza di $[x,y]$ e quindi appartiene al centro di G. □

Proposizione 1.1.12. *In un gruppo G nilpotente di classe* 2 *vale*

$$(xy)^m = x^m y^m [y,x]^{\binom{m}{2}}, \quad \textit{per ogni} \quad x,y \in G \quad \textit{e per ogni} \quad m \in \mathbb{N}.$$

Dimostrazione. Dimostriamo l'enunciato per induzione su m.
Per $m = 1$ è ovvio.
Supponiamo che l'asserto valga per m e dimostriamolo per $m + 1$:
$(xy)^{m+1} = (xy)^m(xy) = x^m y^m [y, x]^{\binom{m}{2}} xy = x^m y^m xy [y, x]^{\binom{m}{2}}$ poiché $[y, x]^{\binom{m}{2}} \in G' \subseteq Z(G)$; sappiamo che $[y^m, x] = [y, x]^m = y^{-m} x^{-1} y^m x$; si ha quindi $y^m x = xy^m [y, x]^m$; ne viene che:
$x^m y^m xy [y, x]^{\binom{m}{2}} = x^m xy^m [y, x]^m y [y, x]^{\binom{m}{2}} = x^{m+1} y^{m+1} [y, x]^{m+\binom{m}{2}} =$
$x^{m+1} y^{m+1} [y, x]^{\binom{m+1}{2}}$, dove abbiamo utilizzato $[y, x]^m \in G' \subseteq Z(G)$. □

Definizione 1.1.6. Siano G un gruppo e H un sottogruppo di G. Si dice *centralizzante di H in G* l'insieme

$$C_G(H) = \{\, g \in G \mid [g, h] = 1 \quad \text{per ogni} \quad h \in H \,\}.$$

Proposizione 1.1.13. *Se G è un gruppo e H è un sottogruppo di G, allora $C_G(H)$ è un sottogruppo di G.*

Dimostrazione. Sia $C = C_G(H)$, si ha che C è non vuoto poi contiene 1. Siano $g_1, g_2 \in C, h \in H$ e consideriamo $[g_1 g_2, h] = (g_1 g_2)^{-1} h^{-1} g_1 g_2 h = {g_2}^{-1} {g_1}^{-1} h^{-1} g_1 g_2 h$, poiché g_2 e h commutano tra loro si ha ${g_2}^{-1} {g_1}^{-1} h^{-1} g_1 g_2 h = {g_2}^{-1} {g_1}^{-1} h^{-1} g_1 h g_2$ e poiché ${g_1}^{-1} h^{-1} g_1 h = 1$ per ipotesi segue che:
${g_2}^{-1} {g_1}^{-1} h^{-1} g_1 h g_2 = 1$.
Quindi C è chiuso rispetto al prodotto.
Non resta che provare che l'inverso di ogni elemento in C appartiene ancora a C. Siano quindi $g_1 \in C$ e $h \in H$; $[{g_1}^{-1}, h] = g_1 h^{-1} {g_1}^{-1} h$, poiché g_1 commuta con ogni elemento di H si ha $g_1 h^{-1} {g_1}^{-1} h = h^{-1} g_1 {g_1}^{-1} h = 1$. Abbiamo allora dimostrato che ${g_1}^{-1} \in C$. In conclusione C è sottogruppo di G. □

Proposizione 1.1.14. *Sia G un gruppo e siano C, Q sottogruppi di G. Se $[C, H] = 1$ allora l'insieme*

$$CH = \{\, xy \mid \quad x \in C, \quad y \in H \,\}$$

è sottogruppo di G.

Dimostrazione. CH non è vuoto poiché $1 = 1 \cdot 1 \in CH$.
Siano $z_1, z_2 \in CH$ allora $z_1 = x_1y_1$ e $z_2 = x_2y_2$ con $x_i \in C$ e $y_i \in H$. Si ha che $z_1z_2 = x_1y_1x_2y_2 = x_1x_2y_1y_2$ poiché gli elementi di C commutano con gli elementi di H; allora CH è chiuso rispetto al prodotto.
Sia z in CH, allora z è della forma $z = x_1y_1$ con $x_1 \in C$ e $y_1 \in H$. L'inverso di z è $z^{-1} = x^{-1}y^{-1}$ in quanto gli elementi di C commutano con gli elementi di H. Allora CH è sottogruppo di G. □

Corollario 1.1.15. *Sia G un gruppo e siano $H_1, \ldots, H_n$ sottogruppi di G tali che $[H_i, H_j] = 1$ per ogni $i \neq j$. Allora $H_1 \cdots H_n = \{ h_1 \cdots h_n \mid h_i \in H_i \}$ è un sottogruppo di G.*

Dimostrazione. La dimostrazione è una facile induzione su n utilizzando la Proposizione 1.1.14. □

1.2 Prodotto diretto interno ed esterno

Definizione 1.2.1. Consideriamo i gruppi $G_1, \ldots, G_n$. Si dice *prodotto diretto (esterno)* il gruppo $G_1 \times \ldots \times G_n$ che si ottiene munendo l'insieme

$$G = G_1 \times \ldots \times G_n = \{ (g_1, \ldots, g_n) \mid g_i \in G_i \quad \text{per ogni } i = 1, \ldots, n \}$$

del prodotto "componente per componente", ossia

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

Osservazione 3. Il gruppo $\overline{G_i} = \{ (g_i, 1, \ldots, 1) \mid g_i \in G_i \}$ è un sottogruppo di G isomorfo a G_i per ogni i tale che $1 \leq i \leq n$.

Dato un insieme A, denotiamo con $\langle A \rangle$ il sottogruppo generato da A.

Definizione 1.2.2. Consideriamo un gruppo H e una famiglia di suoi sottogruppi normali $\{ H_\lambda \mid \lambda \in \Lambda \}$ tale che valgano :

$$H = \langle H_\lambda \,|\, \lambda \in \Lambda \rangle \,,$$

$$H_\lambda \cap \langle H_\mu \,|\, \lambda \neq \mu \rangle = 1.$$

H si dice *prodotto diretto interno* degli H_λ.

Osservazione 4. Gli elementi di H che appartengono a diversi H_λ commutano tra loro. Infatti preso $x \in H_\lambda$ e $y \in H_\mu$ si ha che $x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) = (x^{-1}y^{-1}x)y$ quindi $[x, y]$ appartiene a $H_\lambda \cap H_\mu$ e perciò è uguale ad 1. Allora $xy = yx$.

Proposizione 1.2.1. *Sia $G = G_1 \times \ldots \times G_n$; allora G è prodotto diretto interno dei $\overline{G_i} = \{\, (g_i, 1, \ldots, 1) \mid g_i \in G_i \,\}$ per ogni i tale che $1 \leq i \leq n$.*

Dimostrazione. Dobbiamo per prima cosa mostrare che $\overline{G_i}$ è un sottogruppo normale di G.
Siano quindi $(g_1, \ldots, g_n) \in G$ e $(1, \ldots, \overline{g_\lambda}, \ldots, 1) \in \overline{G_\lambda}$; si ha che:
$(g_1, \ldots, g_n)(1, \ldots, \overline{g_\lambda}, \ldots, 1)({g_1}^{-1}, \ldots, {g_n}^{-1}) = (1, \ldots, g_\lambda \overline{g_\lambda} {g_\lambda}^{-1}, \ldots, 1) \in \overline{G_\lambda}$ poichè $g_\lambda \overline{g_\lambda} {g_\lambda}^{-1} \in G_\lambda$.
Ora proviamo che G è generato dall'insieme dei sottogruppi $\overline{G_i}$.
Sia $(g_1, \ldots, g_n)$ un elemento di G, allora
$(g_1, \ldots, g_n) = (g_1, 1, \ldots, 1)(1, g_2, 1, \ldots, 1) \cdots (1, \ldots, 1, g_n)$ quindi
$G = \left\langle \overline{G_i} \,\middle|\, 1 \leq i \leq n \right\rangle$.
Non resta che dimostrare $\overline{G_i} \cap \left\langle \overline{G_j} \,\middle|\, i \neq j \right\rangle = 1$.
Poichè se $i \neq j$ un elemento di $\overline{G_j}$ ha sempre 1 in i-esima posizione e un elemento di $\overline{G_i}$ ha sempre 1 in j-esima posizione l'intersezione tra G_i e $\langle G_j \,|\, i \neq j \rangle$ è $(1, \ldots, 1) = 1$. □

Proposizione 1.2.2. *Sia H prodotto diretto interno degli $\{\, H_i \mid 1 \leq i \leq n \,\}$, allora $H \cong H_1 \times \cdots \times H_n$.*

Dimostrazione. Costruiamo la seguente applicazione:

$$f \colon H_1 \times \cdots \times H_n \longrightarrow H$$

$$(x_1, \dots, x_n) \longmapsto x_1 \cdots x_n$$

e dimostriamo che si tratta di un isomorfismo.
Ora, $f((x_1, \dots, x_n)(y_1, \dots, y_n)) = f((x_1y_1, \dots, x_ny_n)) = x_1y_1 \cdots x_ny_n = x_1 \cdots x_ny_1 \cdots y_n = f(x_1, \dots, x_n)f(y_1, \dots, y_n)$ per l'Osservazione 4.
Proviamo l'iniettività di f : sia $f(x_1, \dots, x_n) = x_1 \cdots x_n = 1$ allora $x_2 \cdots x_n = {x_1}^{-1}$ quindi ${x_1}^{-1}$ appartiene $H_1 \cap \langle H_i \,|\, i \neq 1 \rangle$ e perciò è uguale ad 1. Allora $x_1 = 1 = x_2 \cdots x_n$. Ripetendo il ragionamento partendo da $x_2 \cdots x_n = 1$ si prova che $(x_1, \dots, x_n) = 1$.
Infine dimostriamo la suriettività: per il Corollario 1.1.15 si ha che $H_1 \cdots H_n$ è un sottogruppo di H, quindi $H = H_1 \cdots H_n$ perchè $H_1 \cdots H_n$ contiene tutti i generatori di H. □

Dati due interi m e n indichiamo con $\mathrm{mcm}(m, n)$ il minimo comune multiplo tra m e n.

Ricordiamo, senza dimostrarlo, il seguente risultato.

Lemma 1.2.3. *Se G è un gruppo e $x \in G$ è del tipo $x = x_1x_2$, con $[x_1, x_2] = 1$, allora $|x|$ divide $\mathrm{mcm}(|x_1|, |x_2|)$ e se $|x_1|$ e $|x_2|$ sono coprimi allora $|x| = |x_1||x_2|$.*

Osservazione 5. Sia G un gruppo e sia $x \in G$ di ordine $m = rs$ con r e s primi tra loro. Allora per il Teorema di Bézout esistono due interi a e b tali che $ar + bs = 1$ quindi $x = x^{ar+bs} = x^{ar}x^{bs}$. Ponendo $x_1 = x^{ar}$ e $x_2 = x^{bs}$ abbiamo scritto x come $x = x_1x_2$ con x_1 e x_2 potenze di x. Osserviamo che $|x_1|$ divide s e $|x_2|$ divide r, ma poiché $rs = |x| = |x_1x_2|$ per il Lemma 1.2.3 segue che $|x_1| = r$ e $|x_2| = s$. Inoltre $[x_1, x_2] = 1$ quindi dal Lemma 1.2.3 si ha $rs = |x| = |x_1||x_2|$.

Proposizione 1.2.4. *Sia G un gruppo, $G = A \times B$ con A e B sottogruppi di G tali che gli elementi di A hanno ordine potenza di 2, mentre gli elementi di B hanno ordine dispari. Se H è un sottogruppo di G allora $H = (H \cap A) \times (H \cap B)$.*

Dimostrazione. Osserviamo che se $x \in G$ ha ordine potenza di 2, allora $x \in A$. Infatti se $x = x_1x_2$ con $x_1 \in A, x_2 \in B$ e $|x| = 2^r$ si ha che ${x_1}^{2^r}{x_2}^{2^r} = 1$, quindi ${x_1}^{2^r} = 1 = {x_2}^{2^r}$, ma poiché x_2 ha ordine dispari deve essere $x_2 = 1$. Segue che $x = x_1 \in A$. Analogamente se $x \in G$ ha ordine dispari allora $x \in B$. Sia ora $x \in H$. Per l'Osservazione 5 si ha che $x = x_1x_2$, ove x_1 e x_2 sono potenze di x, $|x_1|$ è potenza di 2, mentre $|x_2|$ è dispari. Allora $x_1 \in H \cap A$ e $x_2 \in H \cap B$. □

Proposizione 1.2.5. *Sia G un gruppo, $G = A \times B$ con A e B sottogruppi di G. Sia H un sottogruppo di G tale che $H = (H \cap A) \times (H \cap B)$ con $H \cap A \trianglelefteq A$ e $H \cap B \trianglelefteq B$. Allora $H \trianglelefteq G$.*

Dimostrazione. Sia $x \in H$, allora esistono $x_1 \in H \cap A$ e $x_2 \in H \cap B$ tali che $x = x_1x_2$. Sia $g \in G$, allora esistono $g_1 \in A$ e $g_2 \in B$ tali che $g = g_1g_2$. Ora: $gxg^{-1} = g_1g_2x_1x_2(g_1g_2)^{-1} = g_1g_2x_1x_2{g_2}^{-1}{g_1}^{-1}$.
Ricordiamo che per le proprietà del prodotto diretto $[A, B] = 1$ quindi $[H \cap A, H \cap B] = [H \cap B, A] = [H \cap A, B] = 1$.
Proseguendo con le uguaglianze si ha:
$gxg^{-1} = g_2g_1x_1x_2{g_1}^{-1}{g_2}^{-1} = g_2g_1x_2x_1{g_1}^{-1}{g_2}^{-1} = g_2x_2g_1x_1{g_1}^{-1}{g_2}^{-1}$

Ora: ${g_1}x_1{g_1}^{-1} \in H \cap A$ per ipotesi, ${g_2}^{-1} \in B$ quindi per commutatività $g_2x_2g_1x_1{g_1}^{-1}{g_2}^{-1} = g_2x_2{g_2}^{-1}g_1x_1{g_1}^{-1}$;
osserviamo poi che $g_2x_2{g_2}^{-1} \in H \cap B$ per ipotesi e ${g_1}x_1{g_1}^{-1} \in H \cap A$, quindi $gxg^{-1} \in H$ per ogni $g \in G$ e per ogni $x \in H$. Dunque $H \trianglelefteq G$. □

1.3 Sui gruppi commutativi

Proposizione 1.3.1. *Sia G un gruppo tale che ogni elemento diverso dall'unità ha ordine 2, allora G è commutativo.*

Dimostrazione. Siano $a, b \in G$, dobbiamo provare che $ab = ba$. Abbiamo che $(ab)(ab) = (ab)^2 = 1$ per ipotesi; ne viene che $bab = a^{-1}$ quindi $ab = b^{-1}a^{-1}$, ma poiché a e b hanno ordine al più 2 coincidono con i loro inversi. Si ha allora $ab = ba$. □

Proposizione 1.3.2. *Siano G un gruppo e N un sottogruppo normale di G. Allora il gruppo quoziente G/N è commutativo se e solo se $G' \subseteq N$.*

Dimostrazione. G/N è commutativo se e solo se $gxN = xgN$ per ogni $x, g \in G$, ma $gxN = xgN \Leftrightarrow g^{-1}x^{-1}gxN = N \Leftrightarrow g^{-1}x^{-1}gx \in N$. Ora, $g^{-1}x^{-1}gx$ è proprio il commutatore $[g, x]$ e quindi abbiamo provato che G/N è commutativo se e solo se $[g, x] \in N$ per ogni $x, g \in G$. Questa ultima condizione è equivalente a $G' \subseteq N$.

□

Proposizione 1.3.3. *Se E è un gruppo i cui elementi hanno ordine al più 2 allora E è spazio vettoriale sul campo $\mathbb{F}_2$ con due elementi.*

Dimostrazione. Consideriamo su E l'operazione di prodotto che lo rende gruppo e osserviamo che E è commutativo per la Proposizione 1.3.1. Definiamo poi l'operazione prodotto per scalare:

$$*\colon \mathbb{F}_2 \times E \to E$$

$$(0, v) \mapsto 1$$

$$(1, v) \mapsto v$$

Mostriamo che valgono per questa operazione le proprietà di spazio vettoriale.

1. $\lambda * (\mu * v) = \lambda\mu * v, \quad \lambda, \mu \in \mathbb{F}_2, \quad v \in E.$

   - $\lambda = 0, \mu = 1$
     $0 * (1 * v) = 0 * v$
     $0 * v = 0 * v$

- $\lambda = 0, \mu = 0$
  $0 * (0 * v) = 0 * 1 = 1$
  $0 * v = 1$

- $\lambda = 1, \mu = 0$
  $1 * (0 * v) = 1 * 1 = 1$
  $0 * v = 1$

- $\lambda = 1, \mu = 1$
  $1 * (1 * v) = 1 * v$
  $1 * v = 1 * v$

2. $1 * v = v$ per definizione

3. $\lambda * (uv) = (\lambda * u) \cdot (\lambda * v), \quad \lambda \in \mathbb{F}_2, \quad u, v \in E.$

   - $\lambda = 0$
     $0 * (uv) = 1$
     $(0 * u) \cdot (0 * v) = 1$

   - $\lambda = 1$
     $1 * (uv) = uv$
     $(1 * u) \cdot (1 * v) = uv$

4. $(\lambda + \mu) * v = (\lambda * v) \cdot (\mu * v), \quad \lambda, \mu \in \mathbb{F}_2, \quad v \in E.$

- $\lambda = 0, \mu = 1$
  $1 * v = v$
  $(0 * v) \cdot (1 * v) = v$

- $\lambda = 0, \mu = 0$
  $0 * v = 1$
  $(0 * v) \cdot (0 * v) = 1$

- $\lambda = 1, \mu = 0$
  $1 * v = v$
  $1 * v = v$

- $\lambda = 1, \mu = 1$
  $0 * v = 1$
  $(1 * v) \cdot (1 * v) = v^2 = 1$ poiché in E gli elementi hanno ordine al più 2.

□

Osservazione 6. Dalla definizione di prodotto per uno scalare segue immediatamente che un sottoinsieme di E è un sottogruppo se e solo se è un sottospazio.

Teorema 1.3.4. *Se V è uno spazio vettoriale e S un sottoinsieme di V costituito da vettori linearmente indipendenti, allora esiste una base B di V tale che $S \subseteq B$.*

Dimostrazione. Sia:

$\mathcal{A} = \{ X \subseteq V \mid \quad S \subseteq X \quad$ e i vettori di X sono linearmente indipendenti $\}$.

Si ha che $\mathcal{A}$ è un insieme poiché $\mathcal{A} \subseteq \mathcal{P}(V)$; $\mathcal{A}$ non è vuoto perchè $S \in \mathcal{A}$. Consideriamo la relazione di inclusione su $\mathcal{A}$ e la seguente catena $\mathcal{C} = \{ X_\lambda \}_{\lambda \in \Lambda}$

$$X_1 \subseteq X_2 \subseteq \ldots \subseteq X_r \subseteq \ldots$$

Sia poi $X = \cup X_\lambda$; mostriamo che $X \in \mathcal{A}$. Ovviamente $S \subseteq X$. Supponiamo per assurdo $X \notin \mathcal{A}$, allora i vettori di X sono linearmente dipendenti quindi esiste $v \in X$ tale che v è combinazione lineare di vettori in X, ossia $v = a_1 v_1 + \ldots + a_n v_n$. Considerando un insieme $X_\mu \in \mathcal{C}$ che contiene $v, v_1, \ldots, v_n$ abbiamo trovato l'assurdo poiché i vettori di X_μ sono linearmente indipendenti. Segue per il lemma di Zorn che esiste un elemento massimale Y in $\mathcal{C}$. Dimostriamo che Y è una base di V; l'unica cosa da provare è che i vettori di Y sono un sistema di generatori per V. Sia $v \in V$ allora $Y \cup \{ v \}$ è un insieme di vettori linearmente dipendenti, quindi esistono $(a, a_1, \ldots, a_n) \neq (0, \ldots, 0)$ tali che $av + a_1 v_1 + \ldots + a_n v_n = 0$. Osserviamo che necessariamente $a \neq 0$ altrimenti $v_1, \ldots, v_n$ non sarebbero linearmente indipendenti perciò $v = a^{-1} a_1 v_1 + \ldots + a^{-1} a_n v_n$. □

Corollario 1.3.5. *Dato un sottospazio vettoriale W di V allora W è addendo diretto.*

Dimostrazione. Se X è una base di W sia B una base di V tale che $X \subseteq B$. Allora se U è il sottospazio di V generato da $B \backslash X$ si ha che $V = W \oplus U$. □

Ricordiamo ora un importante teorema sui gruppi commutativi. Per la dimostrazione si veda [1].

Teorema 1.3.6. *Sia G un gruppo commutativo finitamente generato. Allora G è isomorfo alla somma diretta di un numero finito di gruppi ciclici di ordine $m_1, \ldots, m_k$, con $m_1 > 1$ e $m_1 | m_2 | \ldots | m_k$.*

1.4 Teoria di Galois

Richiamiamo alcune definizioni ed enunciati riguardanti la teoria di Galois. Per le dimostrazioni si faccia riferimento al testo [2]. Assumiamo che i gradi delle estensioni che tratteremo siano tutti finiti.

Teorema 1.4.1 (*della torre*)**.** *Supponiamo di avere le estensioni di campi* $K \subseteq L \subseteq F$*, allora vale*

$$[F : K] = [F : L][L : K].$$

Definizione 1.4.1. Data un'estensione di campi $F \subseteq E$ definiamo $\mathrm{Gal}(E/F)$ come il gruppo degli automorfismi di E che fissano F.

Notazione: dato un sottogruppo H di $\mathrm{Gal}(E/F)$ indichiamo con E^H il sottocampo degli elementi di E fissati dagli automorfismi in H.

Definizione 1.4.2. Un'estensione di campi $F \subseteq E$ si dice *normale* se ogni polinomio irriducubile di $F[x]$ che ha una radice in E si spezza in fattori lineari in $E[x]$.

Definizione 1.4.3. Un polinomio si dice *separabile* se non ha radici multiple nel suo campo di spezzamento.

Definizione 1.4.4. Sia $F \subseteq E$ un'estensione di campi; $\alpha \in E$ si dice *separabile su* F se il polinomio minimo di α su F è separabile.

Definizione 1.4.5. Un'estensione di campi $F \subseteq E$ si dice *separabile* se ogni $\alpha \in E$ è separabile.

Proposizione 1.4.2. *Ogni estensione di un campo di caratteristica 0 è separabile.*

Definizione 1.4.6. Un' estensione si dice di *Galois* se è normale e separabile.

Osservazione 7. Se E è il campo di spezzamento di un polinomio separabile $p(x)$ a coefficienti nel campo F allora l'estensione $F \subseteq E$ è di Galois.

Teorema 1.4.3 (*Corrispondenza di Galois*)**.** *Sia $F \subseteq E$ un' estensione di Galois.*
Allora esiste una corrispondenza biunivoca tra i sottogruppi di $\mathrm{Gal}(E/F)$ *e i campi intermedi dell'estensione $F \subseteq E$, ossia i campi K tali che $F \subseteq K \subseteq L$:*

$$\{\textit{sottogruppi di } \mathrm{Gal}(E/F)\} \longrightarrow \{\textit{campi intermedi dell'estensione } F \subseteq E\}$$

$$H \longmapsto E^H$$

L'inversa di tale corrispondenza è:

$$\{\textit{campi intermedi dell'estensione } F \subseteq E\} \longrightarrow \{\textit{sottogruppi di } \mathrm{Gal}(E/F)\}$$

$$K \longmapsto \mathrm{Gal}(E/K)$$

Inoltre valgono le seguenti proprietà:

- *Sia K un'estensione intermedia. Allora* $\mathrm{Gal}(E/K) \trianglelefteq \mathrm{Gal}(E/F)$ *se e solo se $F \subseteq K$ è un'estensione normale.*
- *Sia K un'estensione intermedia. Allora* $|\mathrm{Gal}(E/K)| = [E : K]$.

Assumiamo ora che i campi in questione abbiamo caratteristica 0.

Proposizione 1.4.4. *Sia $f(x)$ un polinomio a coefficienti nel campo F e sia E il campo di spezzamento di $f(x)$. Allora* $\mathrm{Gal}(E/F)$ *è isomorfo ad un sottogruppo del gruppo di permutazioni sull'insieme delle radici di $f(x)$.*

Definizione 1.4.7. Sia $f(x)$ un polinomio a coefficienti nel campo F; sia poi E il campo di spezzamento di $f(x)$ e siano $\alpha_1, \ldots, \alpha_n$ le radici di $f(x)$. Chiamiamo *discriminante* di $f(x)$ l'elemento

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

L'elemento $\sqrt{\Delta}$ indicherà $\sqrt{\Delta} = \prod_{i<j}(\alpha_i - \alpha_j)$.

Osservazione 8. La definizione di $\sqrt{\Delta}$ dipende da come sono state numerate le radici, ma la sua appartenenza o meno ad F no.

Teorema 1.4.5. *Si ha che $\Delta \in F$ mentre $\sqrt{\Delta}$ appartiene ad F se e solo se $\mathrm{Gal}(L/F)$ è contenunto nel gruppo alterno su n lettere.*

Lemma 1.4.6. *Consideriamo a e $b \in F$ tali che $\sqrt{a}$ e $\sqrt{b} \notin F$. Allora $F(\sqrt{a}) = F(\sqrt{b})$ se e solo se a/b è un quadrato in F.*

Dimostrazione. Supponiamo $F(\sqrt{a}) = F(\sqrt{b})$. Allora $\sqrt{a} \in F(\sqrt{b})$ cioè $\sqrt{a} = \alpha_1 + \sqrt{b}\beta_1$ per certi $\alpha_1, \beta_1 \in F$. Ne viene che $a = {\alpha_1}^2 + b{\beta_1}^2 + 2\alpha_1\beta_1\sqrt{b}$, quindi $\alpha_1\beta_1 = 0$ poiché $a \in F$. Essendo F un campo si ha che o $\alpha_1 = 0$ oppure $\beta_1 = 0$. Se $\alpha_1 = 0$ allora $\sqrt{a} = \sqrt{b}\beta_1$ perciò $\sqrt{a}/\sqrt{b} = \beta_1 \in F$ quindi a/b è un quadrato in F. Se invece $\beta_1 = 0$ allora $\sqrt{a} = \alpha_1 \in F$, ma questo è assurdo per ipotesi.
Viceversa supponiamo che a/b sia un quadrato in F. Allora esiste $x \in F$ tale che $a/b = x^2$, quindi possiamo supporre $\sqrt{a}/\sqrt{b} = x$. Ne viene che $\sqrt{a} = x\sqrt{b}$ quindi $\sqrt{a} \in F(\sqrt{b})$ e $\sqrt{b} = \sqrt{a}x^{-1}$ quindi $\sqrt{b} \in F(\sqrt{a})$. Segue che $F(\sqrt{a}) = F(\sqrt{b})$. □

Definizione 1.4.8. L'estensione di campi $F \subseteq E$ si dice *estensione ciclica* se e solo se è di Galois e $\mathrm{Gal}(E/F)$ è ciclico.

Riportiamo ora una proposizione sulle permutazioni che verrà utilizzata nel capitolo 4. Indichiamo con S_n il gruppo simmetrico su n lettere.

Proposizione 1.4.7. *Sia $\sigma \in S_n$, $\sigma = (a_1a_2 \dots a_r)(b_1 \dots b_s) \cdots (c_1 \dots c_t)$. Allora, per ogni $\tau \in S_n$ vale*

$$\sigma^\tau = (\tau^{-1}(a_1)\tau^{-1}(a_2) \dots \tau^{-1}(a_r))(\tau^{-1}(b_1) \dots \tau^{-1}(b_s)) \cdots (\tau^{-1}(c_1) \dots \tau^{-1}(c_t)).$$

Dimostrazione. Poniamo

$$\omega = (\tau^{-1}(a_1)\tau^{-1}(a_2) \dots \tau^{-1}(a_r))(\tau^{-1}(b_1) \dots \tau^{-1}(b_s)) \cdots (\tau^{-1}(c_1) \dots \tau^{-1}(c_t)).$$

Se $d \in \{1, \dots, n\}$, $d \neq \tau^{-1}(a_i)$ per ogni $i = 1, \dots, r$, $d \neq \tau^{-1}(b_j)$ per ogni $j = 1, \dots, s$, $\dots, d \neq \tau^{-1}(c_k)$ per ogni $k = 1, \dots, t$, allora $\omega(d) = d$;

d'altra parte $\tau(d) \neq a_i$, $\tau(d) \neq b_j$ e $\tau(d) \neq c_k$ per ogni $i = 1, \ldots, r$, per ogni $j = 1, \ldots, s$ e per ogni $k = 1, \ldots, t$. Ne viene che $\tau^{-1}\sigma\tau(d) = \tau^{-1}\sigma(\tau(d)) = \tau^{-1}(\tau(d)) = d$. Si ha poi $\tau^{-1}\sigma\tau(\tau^{-1}(a_1)) = \tau^{-1}\sigma(a_1) = \tau^{-1}(a_2) = \omega(\tau^{-1}(a_1))$ e analogamente si prova che le due permutazioni $\tau^{-1}\sigma\tau$ e ω coincidono su tutti gli altri elementi. □

Capitolo 2

Il gruppo dei quaternioni

In questo capitolo verrà descritto il gruppo dei quaternioni attraverso la sua struttura e le proprietà che lo rendono notevole per molti aspetti. Nel capitolo successivo approfondiremo infatti la sua caratteristica principale.

2.1 Il gruppo e le sue proprietà

Definizione 2.1.1. Consideriamo l'anello delle matrici quadrate di ordine 2 sul campo complesso. Denotiamo con:

$$\mathbf{1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

$$\mathbf{i} = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$$

$$\mathbf{j} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$$

$$\mathbf{k} = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right).$$

Si dice *gruppo dei quaternioni* l'insieme

$$Q_8 = \{\, \mathbf{1}, -\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}, -\mathbf{i}, -\mathbf{j}, -\mathbf{k} \,\}$$

dotato del prodotto tra matrici.

È facile verificare che l'insieme Q_8 con il prodotto così definito è un gruppo. Infatti il prodotto è ben definito in Q_8, ed è associativo per definizione.

Inoltre $\mathbf{1}$ è l'elemento neutro e gli inversi sono $\mathbf{i}^{-1} = -\mathbf{i}, \mathbf{j}^{-1} = -\mathbf{j}, \mathbf{k}^{-1} = -\mathbf{k}$.
Dalla definizione si trova che valgono queste relazioni :
$\mathbf{i}^4 = \mathbf{1}, \quad \mathbf{i}^2 = \mathbf{j}^2, \quad \mathbf{i}^{\mathbf{j}} = \mathbf{j}^{-1}\mathbf{ij} = \mathbf{j}^3\mathbf{ij} = (-\mathbf{1})\mathbf{jij} = (-\mathbf{1})\mathbf{jk} = -\mathbf{i} = \mathbf{i}^{-1}$.
Tali relazioni implicano che Q_8 è chiuso rispetto al prodotto, come si evince dalla seguente tavola di moltiplicazione.

2.1.1 Tavola di moltiplicazione

La tavola di moltiplicazione di Q_8 è data da:

	1	**-1**	**i**	**-i**	**j**	**-j**	**k**	**-k**
1	**1**	**−1**	**i**	**−i**	**j**	**−j**	**k**	**−k**
-1	**−1**	**1**	**−i**	**i**	**−j**	**j**	**−k**	**k**
i	**i**	**−i**	**−1**	**1**	**k**	**−k**	**−j**	**j**
-i	**−i**	**i**	**1**	**−1**	**−k**	**k**	**j**	**−j**
j	**j**	**−j**	**−k**	**k**	**−1**	**1**	**i**	**−i**
-j	**−j**	**j**	**k**	**−k**	**1**	**−1**	**−i**	**i**
k	**k**	**−k**	**j**	**−j**	**−i**	**i**	**−1**	**1**
-k	**−k**	**k**	**−j**	**j**	**i**	**−i**	**1**	**−1**

Le seguenti proposizioni sono ora ovvie.

Proposizione 2.1.1. *Q_8 non è un gruppo commutativo.*

Proposizione 2.1.2. *Gli elementi in Q_8 hanno il seguente ordine:*
$\mathbf{1}$ *ha ordine* 1
$-\mathbf{1}$ *ha ordine* 2
$\mathbf{i}, \mathbf{j}, \mathbf{k}, -\mathbf{i}, -\mathbf{j}, -K$ *hanno ordine* 4.

2.1.2 I sottogruppi del gruppo dei quaternioni

Nel gruppo dei quaternioni vi sono tre sottogruppi ciclici di ordine 4:

$$\langle \mathbf{i} \rangle = \{ \mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i} \} \quad \langle \mathbf{j} \rangle = \{ \mathbf{1}, -\mathbf{1}, \mathbf{j}, -\mathbf{j} \} \quad \langle \mathbf{k} \rangle = \{ \mathbf{1}, -\mathbf{1}, \mathbf{k}, -\mathbf{k} \}$$

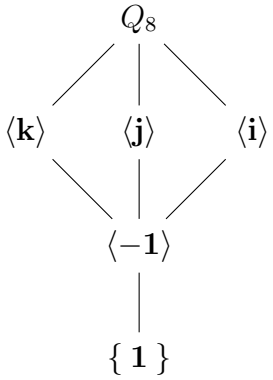
un sottogruppo ciclico di ordine 2:

$$\langle -\mathbf{1} \rangle = \{ \mathbf{1}, -\mathbf{1} \}$$

il sottogruppo banale e il gruppo stesso.

Questi sono tutti e soli i sottogruppi di Q_8. Consideriamo infatti un sottogruppo proprio H di G; per il teorema di Lagrange gli ordini possibili per H sono 1,2 oppure 4. Se l'ordine di H è 1 banalmente $H = \langle \mathbf{1} \rangle$.
Se l'ordine di H è 2 allora H deve contenere $\mathbf{1}$ e un altro elemento di G di ordine necessariamente 2, ma allora $H = \langle -\mathbf{1} \rangle$.
Osserviamo che se H è un gruppo di ordine 4 allora o H contiene un elemento di ordine 4 e quindi è ciclico, oppure H contiene l'identità e tre elementi distinti di ordine 2, il che è impossibile perchè in Q_8 c'è un solo elemento di ordine 2. Ne viene che H necessariamente contiene almeno uno tra $\mathbf{i}, \mathbf{j}, \mathbf{k}$ perchè se per assurdo così non fosse, allora conterrebbe almeno uno tra $-\mathbf{i}, -\mathbf{j}, -\mathbf{k}$ e sicuramente $-\mathbf{1}$ quindi anche il loro prodotto. Se H contiene un elemento x di ordine 4 allora $\langle x \rangle$ è contenuto in H, ma avendo H ordine 4 si ha $H = \langle x \rangle$.

Il reticolo dei sottogruppi di Q_8 è quindi il seguente:



Osservazione 9. I sottogruppi non identici di Q_8 contengono tutti il sottogruppo ciclico $\{ -\mathbf{1}, \mathbf{1} \}$ di ordine 2.

2.1.3 Centro e derivato

Indichiamo con Z il sottogruppo di Q_8 di sostegno $\{ -\mathbf{1}, \mathbf{1} \}$.

Proposizione 2.1.3. *Z è il centro di Q_8.*

Dimostrazione. Basta osservare la tavola di moltiplicazione. □

Proposizione 2.1.4. *Z è il derivato di Q_8.*

Dimostrazione. Mostriamo che Q_8' è contenuto in Z. Si ha che Z è normale in Q_8 in quanto centro; Q_8/Z è un gruppo non ciclico di ordine 4 quindi i suoi elementi hanno tutti ordine al più 2, allora per la Proposizione 1.3.2 Q_8' è contenuto in Z.
Essendo Q_8' non banale e Z di ordine 2 ne viene che $Q_8' = Z$. □

Enunciamo ora la proprietà più importante del gruppo dei quaternioni, proprietà di cui gode pur non essendo commutativo.

Proposizione 2.1.5. *Tutti i sottogruppi di Q_8 sono normali.*

Dimostrazione. Consideriamo i sottogruppi propri di Q_8:
$\{ -\mathbf{1}, \mathbf{1} \}$ è sottogruppo normale di Q_8 poiché centro.
$H = \{ -\mathbf{1}, \mathbf{1}, \mathbf{i}, -\mathbf{i} \}$ è sottogruppo normale di Q_8 poiché ha ordine metà di quello di Q_8 quindi $[Q_8 : H] = 2$ e questo implica che H è normale in Q_8.
Analogamente lo si dimostra per gli altri due sottogruppi di ordine 4. □

2.2 I quozienti del gruppo dei quaternioni

Consideriamo la famiglia $\mathcal{A}$ dei gruppi G tali che G è generato da due elementi x e y che soddisfano le seguenti relazioni:

$$x^4 = 1, x^2 = y^2, x^y = x^{-1}.$$

Osservazione 10. La famiglia $\mathcal{A}$ è non vuota. Infatti il gruppo identico generato da $x = y = 1$ appartiene ad $\mathcal{A}$.

Osservazione 11.
- Poiché $x^4 = 1$ si ha che x^j con $j \in \mathbb{Z}$ è del tipo x^α, con α in $\{ 0, 1, 2, 3 \}$. Analogamente per y.
- Se $\beta \in \{ 0, 2 \}$ dalle relazioni segue che $x^{y^\beta} = x$, se invece $\beta \in \{ 1, 3 \}$ si ha che $x^{y^\beta} = x^{-1}$.

Proposizione 2.2.1. *Sia G in $\mathcal{A}$ generato da x e y. Indichiamo con S il seguente sottoinsieme di G*

$$S = \left\{ x^\alpha y^\beta, \alpha, \beta \in \{0, 1, 2, 3\}, x^4 = 1, x^2 = y^2, x^y = x^{-1} \right\}.$$

Allora $G = S$.

Dimostrazione. Dimostriamo per prima cosa che S è un sottogruppo di G.
$1 \in S$ poichè $1 = x^0 y^0$.
Siano $x^{\alpha_1} y^{\beta_1}$ e $x^{\alpha_2} y^{\beta_2}$ due elementi di S, $x^{\alpha_1} y^{\beta_1} x^{\alpha_2} y^{\beta_2} = x^{\alpha_1} y^{\beta_1} x^{\alpha_2} y^{-\beta_1} y^{\beta_1} y^{\beta_2} = x^{\alpha_1} (x^{\alpha_2})^{y^{-\beta_1}} y^{(\beta_1 + \beta_2)}$.
Se β_1 è pari allora $(x^{\alpha_2})^{y^{-\beta_1}} = x^{\alpha_2}$ quindi $x^{\alpha_1} y^{\beta_1} x^{\alpha_2} y^{\beta_2} = x^{\alpha_1 + \alpha_2} y^{\beta_1 + \beta_2}$.
Se β_1 è dispari allora $(x^{\alpha_2})^{y^{-\beta_1}} = x^{-\alpha_2}$ perciò $x^{\alpha_1} y^{\beta_1} x^{\alpha_2} y^{\beta_2} = x^{\alpha_1 - \alpha_2} y^{\beta_1 + \beta_2}$.
In ogni caso $x^{\alpha_1} y^{\beta_1} x^{\alpha_2} y^{\beta_2} \in S$.

Preso $x^\alpha y^\beta \in S$ il suo inverso è:
se β è pari $x^{-\alpha} y^{-\beta} \in S$, se β è dispari $x^\alpha y^{-\beta} \in S$.
Ora, poiché i generatori di G x e y appartengono ad S ne viene che $G = S$. □

Proposizione 2.2.2. *L'ordine di un gruppo G in $\mathcal{A}$ é al massimo 8.*

Dimostrazione. Apparentemente l'ordine é al massimo 16, ma sfruttando le relazioni di cui godono gli elementi del gruppo si possono dimostrare alcune uguaglianze.
Osserviamo infatti che $y^2 = x^2$ e che $y^3 = y^2 y = x^2 y$. Si ottengono quindi otto coincidenze:
$x^2 = y^2, y^3 = x^2 y, xy^2 = x^3, xy^3 = x^3 y, x^2 y^2 = 1, x^2 y^3 = y, x^3 y^2 = x, x^3 y^3 =$

xy.
Gli elementi di G sono così al massimo 8.

□

Proposizione 2.2.3. *Il gruppo Q_8 dei quaternioni appartiene ad $\mathcal{A}$.*

Dimostrazione. Mostriamo che

$$Q_8 = \left\{ x^\alpha y^\beta \;\middle|\; \alpha, \beta \in \{0,1,2,3\}, x^4 = 1, x^2 = y^2, x^y = x^{-1} \right\}$$

Poniamo $x = \mathbf{i}$ e $y = \mathbf{j}$. Si ha che:

$$\mathbf{i}^4 = \mathbf{1}, \mathbf{i}^2 = \mathbf{j}^2, \mathbf{i}^\mathbf{j} = \mathbf{i}^{-1}.$$

Inoltre tutti gli elementi di Q_8 si scrivono in termini di $\mathbf{i}$ e $\mathbf{j}$:

$$\mathbf{1} = \mathbf{i}^0\mathbf{j}^0, -\mathbf{1} = \mathbf{i}^2\mathbf{j}^0, \mathbf{i} = \mathbf{i}^1\mathbf{j}^0, \mathbf{j} = \mathbf{i}^0\mathbf{j}^1, \mathbf{k} = \mathbf{i}^1\mathbf{j}^1, -\mathbf{i} = \mathbf{i}^3\mathbf{j}^0, -\mathbf{j} = \mathbf{i}^0\mathbf{j}^3, -\mathbf{k} = \mathbf{i}^3\mathbf{j}^1.$$

□

Proposizione 2.2.4. *Sia G in $\mathcal{A}$ generato da x e y. Allora esiste un epimorfismo da Q_8 a G.*

Dimostrazione. Consideriamo la funzione:

$$\varphi \colon Q_8 \to G$$
$$\mathbf{i}^\alpha\mathbf{j}^\beta \mapsto x^\alpha y^\beta$$

Mostriamo che si tratta di un epimorfismo. Siano $\mathbf{i}^{\alpha_1}\mathbf{j}^{\beta_1}$ e $\mathbf{i}^{\alpha_2}\mathbf{j}^{\beta_2}$ elementi di Q_8 :
se β_1 è pari $\varphi(\mathbf{i}^{\alpha_1}\mathbf{j}^{\beta_1}\mathbf{i}^{\alpha_2}\mathbf{j}^{\beta_2}) = \varphi(\mathbf{i}^{\alpha_1+\alpha_2}\mathbf{j}^{\beta_1+\beta_2}) = x^{\alpha_1+\alpha_2}y^{\beta_1+\beta_2} = x^{\alpha_1}y^{\beta_1}x^{\alpha_2}y^{\beta_2} = \varphi(\mathbf{i}^{\alpha_1}\mathbf{j}^{\beta_1})\varphi(\mathbf{i}^{\alpha_2}\mathbf{j}^{\beta_2})$;
se β_1 è dispari $\varphi(\mathbf{i}^{\alpha_1}\mathbf{j}^{\beta_1}\mathbf{i}^{\alpha_2}\mathbf{j}^{\beta_2}) = \varphi(\mathbf{i}^{\alpha_1-\alpha_2}\mathbf{j}^{\beta_1+\beta_2}) = x^{\alpha_1-\alpha_2}y^{\beta_1+\beta_2} = x^{\alpha_1}y^{\beta_1}x^{\alpha_2}y^{\beta_2} = \varphi(\mathbf{i}^{\alpha_1}\mathbf{j}^{\beta_1})\varphi(\mathbf{i}^{\alpha_2}\mathbf{j}^{\beta_2})$.

Mostriamo ora la suriettività:
Sia $g \in G$; allora per la Proposizione 2.2.1 g è del tipo $g = x^\alpha y^\beta$ perciò $g = \varphi(\mathbf{i}^\alpha\mathbf{j}^\beta)$. □

Indichiamo con D_4 il gruppo delle isometrie del quadrato. Numerando i vertici del quadrato da 1 a 4 in senso orario si ha che ogni isometria dl quadrato è individuata dalla corrispondente permutazione sui vertici. Si ha che D_4 ha ordine 8 e le permutazioni (1234) e (12)(34) appartenenti al gruppo simmetrico su 4 lettere generano D_4. Il gruppo D_4 contiene solo due elementi di ordine 4 distinti, precisamente (1234) e $(1234)^{-1}$, quindi D_4 ha solo un sottogruppo ciclico di ordine 4.

Osservazione 12. Esattamente con le stesse tecniche utilizzate in questa sezione si dimostra che se G è un gruppo generato da due elementi x e y tali che $x^4 = 1 = y^2, \quad x^y = x^{-1}$ allora esiste un epimorfismo da D_4 a G.

Indichiamo con C_i il gruppo ciclico di ordine i.

Proposizione 2.2.5. *Il gruppo dei quaternioni è l'unico gruppo di ordine 8 ad avere tre sottogruppi ciclici di ordine 4.*

Dimostrazione. Analizziamo la struttura di un gruppo G di ordine 8 che ha almeno un elemento di ordine 4.

- Se G contiene un elemento di ordine 8 allora G è un gruppo ciclico quindi G ha un solo sottogruppo di ordine 4.

- Se G non è un gruppo ciclico, ma contiene un elemento x di ordine 4 allora $\langle x \rangle$ è normale in G perchè ha indice 2. Sia $y \in G, y \notin \langle x \rangle$ allora $x^y \in \langle x \rangle$ e x^y ha ordine 4 perchè il coniugio è un automorfismo. Ne viene che $x^y = x$ oppure $x^y = x^{-1}$. Se $x^y = x$ allora il gruppo G è commutativo e per il Teorema 1.3.6 $G = C_4 \times C_2$. In tal caso se $G = \langle a \rangle \times \langle b \rangle$ con $|a| = 4$ e $|b| = 2$ si ha che gli unici sottogruppi di G di ordine 4 sono $\langle a \rangle$ e $\langle ab \rangle$.
  Se invece $x^y = x^{-1}$ si presentano due possibilità: se $y^2 \neq 1$ allora y ha ordine 4 e $y^2 \in \langle x \rangle$ poiché il gruppo quoziente $G/\langle x \rangle$ ha ordine 2, quindi $x^2 = y^2$, ma allora $G \cong Q_8$. Se invece $y^2 = 1$ per l'Osservazione 12 c'è un epimorfismo da D_4 a G e quindi $G \cong D_4$. In quest'ultimo caso G ha solo un sottogruppo ciclico di ordine 4.

□

Dalla dimostrazione della Proposizione 2.2.5 segue la classificazione dei gruppi di ordine 8.

Proposizione 2.2.6. *Se G è un gruppo di ordine 8 allora G è isomorfo ad uno dei seguenti gruppi:*

- *Se G è commutativo allora* $G \cong C_8$ oppure $G \cong C_4 \times C_2$ oppure $G \cong C_2 \times C_2 \times C_2$.
- *Se G non è commutativo allora* $G \cong Q_8$ oppure $G \cong D_4$.

Dimostrazione. Resta solo da dimostrare che se G non ha elementi di ordine 4 allora $G \cong C_2 \times C_2 \times C_2$. Ma questo è vero perchè in tal caso gli elementi di G hanno ordine al più 2 e quindi per la Proposizione 1.3.1 G è commutativo. □

Capitolo 3

Gruppi in cui tutti i sottogruppi sono normali

Il nostro obiettivo è quello di classificare i gruppi con la proprietà di avere tutti i sottogruppi normali. Troveremo che non si allontanano molto dal gruppo dei quaternioni.

Teorema 3.0.7. *Tutti i sottogruppi di un gruppo G sono normali se e solo se G è commutativo o prodotto diretto del gruppo dei quaternioni, di un gruppo i cui elementi hanno ordine al più 2 e di un gruppo commutativo i cui elementi hanno tutti ordine dispari.*

Dimostrazione. Supponiamo che ogni sottogruppo di G sia normale, ma G non sia commutativo. Siano x e y due elementi in G che non commutano tra loro e poniamo $c = [x, y]$. Per la Proposizione 1.1.2, poiché $\langle x \rangle$ e $\langle y \rangle$ sono sottogruppi normali di G, si ha che $c \in \langle x \rangle \cap \langle y \rangle$. Si ha quindi che $x^r = c = y^s$ con r e s entrambi diversi da 0 e diversi da 1, poiché c commuta con x e con y. Consideriamo $Q = \langle x, y \rangle$ e osserviamo che c appartiene al centro di Q e che $Q' = \langle c \rangle$. Per provare che c appartiene al centro basta mostrare che commuta con x e y, e questo è banale poiché $c = x^r$ e x commuta con le sue potenze, ma si ha anche $c = y^s$ e y commuta con le sue potenze. Inoltre per la Proposizione 1.1.11 si ha che $Q' = \langle c \rangle$ e quindi Q è nilpotente di classe 2. Per il Lemma 1.1.6 si ha che $c^r = [x, y]^r = [x^r, y] = [c, y] = 1$, ma allora c, x e

y hanno ordine finito e quindi per la Proposizione 1.1.10 Q ha ordine finito. Siano $|x| = m$ e $|y| = n$. Tra tutti gli elementi che non commutano scegliamo x e y tali che $m + n$ sia il minimo valore per cui $c = [x, y] \neq 1$. Sia p un divisore primo di m, allora $1 = [x^p, y] = c^p$ e c ha esattamente ordine p; infatti se x^p e y non commutassero formerebbero una coppia che contraddice l'ipotesi di minimalità di $m + n$ poiché $|x^p| = \frac{m}{p} < m$. Questo ci dice che $|x|$ e $|y|$ sono potenze di p. Per dimostrarlo premettiamo un osservazione:

Osservazione 13. In G elementi di ordine coprimo commutano tra loro. Infatti siano u e v tali elementi, allora $\langle u\rangle \cap \langle v\rangle = 1$ poiché altrimenti avrei in uno dei due sottogruppi un elemento il cui ordine non divide l'ordine del gruppo e questo è assurdo per il teorema di Lagrange. Inoltre $[u, v] \in \langle u\rangle$ perchè ogni sottogruppo di G è normale, analogamente $[u, v] \in \langle v\rangle$ poiché $\langle v\rangle$ è normale; si ha quindi che $[u, v] = 1$.

Supponiamo per assurdo che $|x|$ e $|y|$ non siano potenze del primo p. Possiamo allora dire per l'Osservazione 5:
$x = x_1x_2$ con $|x_1| = p^m, |x_2| = r,$ r e p primi tra loro, x_1 e x_2 potenze di x.
$y = y_1y_2$ con $|y_1| = p^n, |y_2| = s,$ s e p primi tra loro, y_1 e y_2 potenze di y.
Si ha quindi che $[x, y] = [x_1x_2, y_1y_2] = ([x_1, y_2][x_1, y_1]^{y_2})^{x_2}[x_2, y_2][x_2, y_1]^{y_2}$; per l'Osservazione 13 abbiamo che $[x_1, y_2] = 1 = [x_2, y_1]$, quindi $[x, y] = [x_1, y_1][x_2, y_2]$.
Ora, $[x_2, y_2]$ ha ordine coprimo con p poiché appartiene a $\langle x_2\rangle \cap \langle y_2\rangle$, mentre $[x_1, y_1]$ ha ordine potenza di p poiché appartiene a $\langle x_1\rangle \cap \langle y_1\rangle$. Osserviamo che $[x_1, y_1]$ e $[x_2, y_2]$ commutano perchè x_1, x_2 e y_1, y_2 sono potenze di x e di y rispettivamente e quindi per la Proposizione 1.1.11 $[x_1, y_1]$ e $[x_2, y_2]$ sono entrambi potenze di $[x, y]$. Ne viene che $p = |[x, y]| = |[x_1, y_1]||[x_2, y_2]|$ per il Lemma 1.2.3, ma allora $[x_2, y_2] = 1$ e quindi $[x, y] = [x_1, y_1]$. Per non contraddire la minimalità di $|x| + |y|$ si ha che $x_1 = x$ e $y_1 = y$ quindi x e y hanno ordine potenza di p.
Dal momento che c è potenza sia di x che di y esistono k, l, r, s interi tali che $x^{kp^r} = c = y^{lp^s}$ con k e p primi tra loro come pure l e p. Poiché k ed l sono primi con p sono invertibili modulo p, cioè esistono k' ed l' tali

che $kk' \equiv 1$ modulo p e $ll' \equiv 1$ modulo p. Indicando con $x' = x^{l'}$ e con $y' = y^{k'}$, abbiamo che $c^{k'l'} = ([x,y]^{k'})^{l'} = [x, y^{k'}]^{l'} = [x^{l'}, y^{k'}] = [x', y']$; inoltre $(x')^{p^r} = (x^{p^r})^{l'} = c^{k'l'}$ poiché $c^{k'} = x^{kk'p^r} = x^{p^r}$(sono tutte uguaglianze visto che c ha ordine p), analogamente $(y')^{p^s} = c^{k'l'}$. Possiamo allora assumere, sostituendo x con x' e y con y', che

$$x^{p^r} = c = y^{p^s} \quad (r, s > 0).$$

E' chiaro che $|x| = p^{r+1}$ e $|y| = p^{s+1}$. Senza perdere di generalità supponiamo $r \geq s$.
Se y_1 denota $x^{-p^{r-s}}y$, allora $[x, y_1] = [x, y] = c$ per la Proposizione 1.1.1, quindi per la minimalità di $|x| + |y|$ si ha che $|y_1| \geq |y| = p^{s+1}$; allora ${y_1}^{p^s} \neq 1$. Per la Proposizione 1.1.12 si ha:

$${y_1}^{p^s} = x^{-p^r} y^{p^s} [y, x^{-p^{r-s}}]^{\binom{p^s}{2}} = c^{-1} c [x,y]^{p^{r-s}\binom{p^s}{2}} = c^{-p^r(p^s-1)/2}.$$

Se p è dispari allora divide $-\frac{1}{2}p^r(p^s - 1)$ e quindi ${y_1}^{p^s} = 1$ che è assurdo. Necessariamente $p = 2$ e $2^{r-1}(2^s - 1)$ deve essere dispari per non ritrovare l'assurdo, ossia $r = 1$. Poiché avevamo supposto $r \geq s$ segue che anche $s = 1$. Sono quindi valide le seguenti relazioni: $x^4 = 1$, $x^2 = y^2$, $x^y = x^{-1}$. Sappiamo allora che esiste un epimorfismo da Q_8 a Q, quindi l'ordine di Q è al massimo 8. Inoltre Q non può avere ordine 2 o 4 perchè altrimenti sarebbe commutativo. Ne viene che Q_8 è isomorfo a Q.

Consideriamo ora $C = C_G(Q)$; allora per la Proposizione 1.1.13 CQ è un sottogruppo. Supponiamo $g \in G \backslash CQ$. Allora g non commuta con entrambi x e y perchè altrimenti g commuterebbe con ogni elemento di Q e quindi apparterrebbe a $C \subseteq CQ$; supponiamo ad esempio che sia $y^g \neq y$. Poiché y ha ordine 4 si ha che $y^g = y^{-1}$; infatti y^g appartiene a $\langle y \rangle$ perchè $\langle y \rangle$ è normale in G e il coniugio è un automorfismo, quindi $|y^g| = |y|$, allora $y^g = y$ oppure $y^g = y^3 = y^{-1}$, ma per evitare l'assurdo si ha sicuramente $y^g = y^{-1}$. Possiamo allora dire che gx commuta con y, infatti $y^{gx} = (y^g)^x = (y^{-1})^x = (y^x)^{-1} = (y^{-1})^{-1} = y$. Necessariamente gx non può commutare con

x altrimenti apparterrebbe a C e quindi g apparterrebbe a CQ. Ne viene che, poiché $x^{gx} \in \langle x \rangle$, $x^{gx} = x^{-1}$ quindi $x^{gxy} = (x^{-1})^y = (x^{-1})^y = x$ cioè gxy commuta con x. Dal momento che gx commuta con y si ha che gxy commuta con y. Allora $gxy \in C$ e $g \in CQ$ poiché $g = (gxy)(y^{-1}x^{-1})$, ma questo è assurdo perciò $G = CQ$.
Se $g \in C$ allora $[x, gy] = [x, y] = c \neq 1$ e per quanto provato all'inizio, poiché c ha ordine finito, anche gy ha ordine finito e quindi g ha ordine finito. Supponiamo che $g \in C$ abbia ordine 4. Allora $[x, gy] \neq 1$ e $(gy)^4 = 1$, da cui segue che $(gy)^x = (gy)^{-1}$ripetendo il ragionamento appena visto. Allora $[gy, x] = (gy)^{-2} = g^{-2}y^{-2}$, ma anche $[gy, x] = [y, x] = y^{-2}$ quindi $g^2 = 1$, una contraddizione. Abbiamo quindi mostrato che in C non ci sono elementi di ordine 4.

Osservazione 14. Gli elementi di C di ordine dispari commutano tra loro e formano un sottogruppo di G che indichiamo con O.
Proviamo prima di tutto che gli elementi di O commutano tra loro. Siano x_1 e x_2 in O di ordine rispettivamente m ed n; ripercorriamo la dimostrazione del teorema supponendo che x_1 e x_2 non commutino tra loro e scegliendoli in modo che $m + n$ assuma il valore minimo per cui $[x_1, x_2] \neq 1$. Allora troviamo che entrambi hanno ordine potenza di 2, ma questo è assurdo. Ora, l'insieme O è non vuoto poiché vi appartiene 1. Siano g_1 e g_2 in O di ordine rispettivamente m ed n; allora per il Lemma 1.2.3 $|g_1g_2|$ divide mn quindi $|g_1g_2|$ è dispari. Infine dato $c \in O$, c^{-1} ha lo stesso ordine di c, dunque dispari.

Osservazione 15. Gli elementi di C aventi ordine al più 2 formano un sottogruppo commutativo di G che indichiamo con E_1.
L'insieme E_1 è non vuoto poiché 1 sta in E_1. Siano ora a e b in E_1, ripercorrendo la dimostrazione del teorema con $x = a$ e $y = b$ troviamo che $a^b = a^{-1} = a$ poiché a ha ordine 2. Allora a e b commutano tra loro, quindi $(ab)^2 = a^2b^2 = 1$. Infine dato $d \in E_1$, d^{-1} ha lo stesso ordine di d perciò al più 2. Quindi E_1 è un sottogruppo di C. Inoltre E_1 è commutativo per la Proposizione 1.3.1.

A questo punto vogliamo provare che $C = E_1 \times O$:

- E_1 ed O sono normali perchè sottogruppi di G.
- $E_1 \cap O = 1$ per definizione dei due sottogruppi.
- Sia $x \in C$ di ordine $m = 2^u v$, con v dispari. Dall' Osservazione 5 sappiamo che $x = x_1 x_2$ con x_1 e x_2 potenze di x di ordine rispettivamente v e 2^u. Inoltre x_1 e x_2 appartengono a C quindi $x_1 \in O$ e x_2 deve avere ordine 2 perchè in C non vi sono elementi di ordine 4. Dunque $x_1 \in O$ e $x_2 \in E_1$.

Ora, $G = CQ = (E_1 \times O)Q = (QE_1) \times O$. Infatti preso $z \in (E_1 \times O)Q$ allora $z = uvw$ con $u \in E_1, v \in O, w \in Q$; sappiamo che O e Q commutano, ma anche E_1 e Q commutano, quindi $z = uvw = uwv = wuv$ perciò $z \in (QE_1)O$. Inoltre $QE_1 \cap O = 1$ perchè sono sottogruppi i cui elementi hanno ordine coprimo. Per la Proposizione 1.3.3 E_1 è spazio vettoriale sul campo $\mathbb{F}_2$ e $Q \cap E_1$ è un sottogruppo di E_1, quindi anche un sottospazio di E_1. Si ha allora per il Teorema 1.3.4 che $Q \cap E_1$ è addendo diretto di E_1 come spazio vettoriale, cioè $E_1 = (Q \cap E_1) \times E$ per un certo sottogruppo E di E_1. Analogamente a prima si dimostra che $QE_1 = Q \times E$ quindi si ha che $G = (QE_1) \times O = Q \times E \times O$.

Dimostriamo ora il viceversa. Supponiamo $G = Q \times E \times O$ ove Q è il gruppo dei quaternioni, E è un gruppo commutativo i cui elementi hanno ordine al più 2, O è un gruppo i cui elementi hanno tutti ordine dispari. Sia H un sottogruppo di G.

Per la Proposizione 1.2.4 si ha:

$$H = (H \cap (Q \times E)) \times (H \cap O).$$

Vogliamo ora dimostrare che H è normale in G. Si ha che $H \cap O$ è normale in O poiché O è commutativo e quindi ogni suo sottogruppo è normale. Proviamo ora che $H \cap (Q \times E)$ è normale in $Q \times E$.

- Caso 1: $H \cap Q = 1$.

  Osservazione 16. L'insieme $T = \{ g \in G \mid g^2 = 1 \}$ è un sottogruppo di G contenuto nel centro di G.

  Dimostrazione. Osserviamo che $T = Q' \times E$. Sia $t \in T, \quad t = x_1x_2x_3$ con $x_1 \in Q, x_2 \in E, x_3 \in O$, allora $t^2 = 1$ implica che ${x_1}^2 = {x_2}^2 = {x_3}^2 = 1$ quindi $x_1 \in Q'$ e $x_3 = 1$. Quindi $T \subseteq Q' \times E$. D'altra parte ogni elemento di $Q' \times E$ ha ordine 2, perciò $T = Q' \times E$. Abbiamo poi che T è contenuto nel centro di G, poiché presi $g_1 = r_1s_1 \in T$ e $g_2 = r_2s_2t_2 \in G$ si ha che ${r_1s_1}^{r_2s_2t_2} = {r_1}^{r_2}{s_1}^{s_2} = r_1r_2$, ove abbiamo utilizzato il fatto che $Q' \subseteq Z(Q)$. □

  Poiché $H \cap Q = 1$ allora $H \cap (Q \times E)$ è isomorfo ad un sottogruppo di E. Infatti se si considera la proiezione

  $$\pi \colon Q \times E \to E$$

  si ha che la sua restrizione a $H \cap (Q \times E)$ è iniettiva. Ne viene che gli elementi di $H \cap (Q \times E)$ hanno tutti ordine al più 2, quindi per l'Osservazione 16 $H \cap (Q \times E)$ è contenuto nel centro di $Q \times E$ perciò per la Proposizione 1.1.5 $H \cap (Q \times E)$ è normale in $Q \times E$.

- Caso 2: $H \cap Q \neq 1$.

  $H \cap (Q \times E)$ è un sottogruppo non banale di Q e per struttura di Q ogni sottogruppo non banale di Q contiene l'unico elemento di Q di ordine 2 e quindi contiene il derivato di Q. Poichè E è commutativo $Q' = (Q \times E)'$. Perciò $H \cap (Q \times E)$ contiene $(Q \times E)'$ quindi per la Proposizione 1.1.5 $H \cap (Q \times E)$ è normale in $Q \times E$.

Sfruttando la Proposizione 1.2.5 abbiamo così provato che H è normale in G e la dimostrazione è conclusa.

□

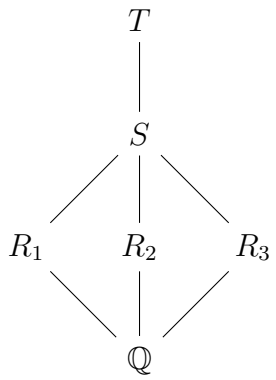
Capitolo 4

Il gruppo dei quaternioni come gruppo di Galois

In questo capitolo determineremo un polinomio a coefficienti razionali il cui gruppo di Galois è proprio il gruppo dei quaternioni.

4.1 Condizioni necessarie e teoremi notevoli

Iniziamo a cercare condizioni necessarie affinchè un estensione T dei razionali $\mathbb{Q}$ abbia i quaternioni come gruppo di automorfismi. Sfruttiamo per questo il Teorema 1.4.3. I campi intermedi corrispondono ai sottogruppi di $\mathrm{Gal}(T/\mathbb{Q})$, che vogliamo siano il gruppo dei quaternioni. Dobbiamo determinare l'immagine dei tre sottogruppi di ordine 4 di Q_8 (che indicheremo con Q_1, Q_2, Q_3) e del sottogruppo di ordine 2 (che indicheremo con Q). L'immagine di Q_1 è T^{Q_1}. Poiché $|Q_1| = [T : T^{Q_1}]$ si ha che $[T : T^{Q_1}] = 4$. Analogamente per Q_2, Q_3, mentre per Q si ha $[T : T^Q] = 2$.
Osserviamo poi che, poiché Q è contenuto in Q_1,Q_2,Q_3 si ha che T^{Q_1},T^{Q_1},T^{Q_1} sono contenuti in T^{Q_1}. Inoltre poiché tutti i sottogruppi di Q_8 sono normali, ogni estensione di $\mathbb{Q}$ dovrà essere normale. Utilizzando la seguente notazione: $R_i = T^{Q_i}$,$S = T^Q$, si ha quindi il diagramma:



L'osservazione fondamentale è che T è estensione ciclica di grado 4 su ogni sottocampo T^{Q_i}. Andiamo ora a studiare la struttura delle estensioni cicliche di grado 4. Sono necessari i seguenti teoremi.

Teorema 4.1.1. *Sia T un'estensione ciclica di grado 4 di un campo R, con $\mathbb{Q} \subseteq R$.*
Allora esistono d, e ed $f \in R$ tali che :

- *d non è un quadrato in R.*
- *$T = R(\sqrt{e + f\sqrt{d}})$ ove $d(e^2 - f^2 d)$ è un quadrato in R.*

Il prossimo teorema è il viceversa del teorema precedente con qualche informazione in più.

Teorema 4.1.2. *Sia T un'estensione ciclica di grado 4 di un campo R, con $\mathbb{Q} \subseteq R$. Se $d \in R$, ma non è un quadrato in R e se per $e, f \in R$ si ha che $d(e^2 - f^2 d)$ è un quadrato in R, allora $T = R(\sqrt{e + f\sqrt{d}})$ è un estensione ciclica di grado 4 su R e $p(x) = x^4 - 2ex^2 + (e^2 - f^2 d)$ è il polinomio minimo di $\sqrt{e + f\sqrt{d}}$ su R.*

Iniziamo dimostrando il primo teorema.

Dimostrazione del Teorema 4.1.1. Sia T un'estensione ciclica di grado 4 su R. Per il Teorema 1.4.3, al sottogruppo di ordine 2 di $\mathrm{Gal}(T/R)$ corrisponde un campo intermedio P tale che $R \subseteq P \subseteq T$; le estensioni $R \subseteq P$ e $P \subseteq T$

sono entrambe di grado 2, quindi $P = R(\sqrt{d})$ ove d non è un quadrato in R e $T = P(\theta)$ con $\theta^2 = e + f\sqrt{d} \in P$ per qualche $e, f \in R$. Si ha che $\theta^2 - e = f\sqrt{d}$ perciò θ è una radice di

$$p(x) = x^4 - 2ex^2 + (e^2 - f^2 d).$$

Questo polinomio è irriducibile su R. Infatti le sue radici sono $\theta, -\theta, \phi, -\phi$ dove $\phi^2 = e - f\sqrt{d}$ e nessuna di esse appartiene ad R, quindi sicuramente $p(x)$ non si fattorizza come prodotto di un polinomio di grado 3 e di un polinomio di grado 1. Non si può nemmeno fattorizzare come prodotto di due polinomi di grado 2 perchè nè θ^2, nè $\theta\phi$ appartengono ad R.
Il discriminante di $p(x)$ è

$$\Delta = (2\theta)^2(2\phi)^2(\theta - \phi)^2(\theta + \phi)^2(-\theta - \phi)^2(-\theta + \phi)^2 = 16\theta^2\phi^2(\theta^2 - \phi^2)^4 =$$

$$16^2(e^2 - f^2 d)f^4 d^2$$

Dal momento che $\mathrm{Gal}(T/R)$ è ciclico di ordine 4, non è un sottogruppo del gruppo alterno su 4 lettere. Quindi per il Teorema 1.4.5 $\sqrt{\Delta} \notin R$ e allora $e^2 - f^2 d$ non è un quadrato in R.
Resta da provare che invece $d(e^2 - f^2 d)$ è un quadrato in R.
Poiché $T = P(\theta) = P(\phi)$ e $[T : P] = 2$ segue per il Lemma 1.4.6 che ϕ^2/θ^2 è un quadrato in P. Ora, $\phi^2/\theta^2 = (e - f\sqrt{d})/(e + f\sqrt{d}) = (e - f\sqrt{d})^2/(e^2 - f^2 d)$. Quindi $e^2 - f^2 d$ è un quadrato in P, ossia:

$$e^2 - f^2 d = (r + s\sqrt{d})^2 = r^2 + s^2 d + 2rs\sqrt{d}, \quad \text{per qualche} \quad r, s \in R.$$

Poiché $e^2 - f^2 d \in P$, si ha che $rs = 0$. Se $s = 0$ allora $e^2 - f^2 d = r^2$ è un un quadrato in R, ma questo è assurdo per quanto appena provato. Allora $r = 0$ e così $e^2 - f^2 d = s^2 d$. Moltiplicando per d si ha che $d(e^2 - f^2 d) = s^2 d^2$, quindi $d(e^2 - f^2 d)$ è un quadrato in R.

□

Non resta che provare il secondo teorema.

Dimostrazione del Teorema 4.1.2. Per ipotesi abbiamo che $d(e^2 - f^2d)$ è un quadrato in R, mentre d non è un quadrato in R. Allora $(e^2 - f^2d)$ non è un quadrato in R. Inoltre $e + f\sqrt{d}$ non ha radice quadrata in $R(\sqrt{d})$, infatti se

$$e + f\sqrt{d} = (r + s\sqrt{d})^2 = r^2 + s^2d + 2rs\sqrt{d}$$

allora $f = 2rs$ e $e = r^2 + s^2d$ quindi

$$e^2 - f^2d = (r^2 + s^2d)^2 - 4r^2s^2d = (r^2 - s^2d)^2$$

sarebbe un quadrato perfetto in R, ma questo è assurdo per ipotesi. Analogamente si dimostra che anche $e - f\sqrt{d}$ non ha radice quadrata in $R(\sqrt{d})$. Si ha quindi la seguente catena di estensioni quadratiche:

$$R \subseteq R(\sqrt{d}) = S \subseteq S(\sqrt{e + f\sqrt{d}}).$$

Ora sia $\theta^2 = e + f\sqrt{d}$. Come mostrato nel teorema precedente, θ è una radice del seguente polinomio in $R[x]$

$$p(x) = x^4 - 2ex^2 + (e^2 - f^2d) = (x^2 - (e + f\sqrt{d}))(x^2 - (e - f\sqrt{d})).$$

Poiché ciascuno dei due fattori di grado 2 è irriducibile su $R(\sqrt{d})$, segue che $p(x)$ è irriducibile su R. Dal momento che

$$(e-f\sqrt{d})/(e+f\sqrt{d}) = (e-f\sqrt{d})^2/(e^2-f^2d) = (\sqrt{d})^2(e-f\sqrt{d})^2/d(e^2-f^2d)$$

e $d(e^2 - f^2d)$ è un quadrato in R, per il Lemma 1.4.6 segue che

$$P(\sqrt{e - f\sqrt{d}}) = P(\sqrt{e + f\sqrt{d}}) = R(\sqrt{e + f\sqrt{d}}) = T.$$

Allora $p(x)$ si fattorizza completamente su T e su nessun sottocampo proprio, perciò T è campo di spezzamento di $p(x)$ su R ed è un estensione normale di grado 4 di R. Allora per il Teorema 1.4.3 l'ordine di $\mathrm{Gal}(T/R)$ è 4. Ne viene quindi che $\mathrm{Gal}(T/R)$ o è il gruppo ciclico di ordine 4 o è il gruppo di *Klein* $\mathbb{Z}_2 \times \mathbb{Z}_2$. Se fosse il gruppo di *Klein* allora sarebbe isomorfo ad un sottogruppo

del gruppo alterno su 4 lettere, ma allora $\sqrt{\Delta}$ dovrebbe appartenere ad R. Abbiamo però calcolato nel Teorema 4.1.1

$$\Delta = 16^2(e^2 - f^2 d)f^4 d^2$$

e dal momento che $(e^2 - f^2 d)$ non è un quadrato in R, si ha che $\sqrt{\Delta} \notin R$. Perciò $\mathrm{Gal}(T/R)$ è gruppo ciclico di ordine 4.

□

4.2 Costruzione

Cerchiamo ora di costruire un polinomio di $\mathbb{Q}[x]$ il cui campo di spezzamento T sia tale che $\mathrm{Gal}(T/\mathbb{Q}) = Q_8$. Partiamo cercando un campo intermedio S. Prendiamo $S = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $d_1 = 2, d_2 = 3, d_3 = 6$ e sia $R_i = \mathbb{Q}(\sqrt{d_i})$ per ogni $i \in \{ 1, 2, 3 \}$. L'obiettivo ora è quello di trovare un estensione quadratica T di S, $T = S(\theta)$, tale che per ogni $i \in \{ 1, 2, 3 \}$ θ^2 possa essere espresso come

$$\theta^2 = e_i + f_i\sqrt{d_i}$$

con $\sqrt{d_i} \notin R_i$, mentre $d_i({e_i}^2 - {f_i}^2 d)$ è un quadrato in R_i.
In questo modo, utilizzando il Teorema 4.1.2 concludiamo che $T = S(\theta)$ è estensione ciclica di grado 4 su ogni R_i e quindi $[T : \mathbb{Q}] = 8$ per il Teorema 1.4.1.
Scegliamo θ^2 in S come

$$\theta^2 = (2 + \sqrt{2})(2 + \sqrt{3})(3 + \sqrt{6}) = 18 + 12\sqrt{2} + 10\sqrt{3} + 7\sqrt{6}.$$

Mostriamo che possiamo riscrivere θ^2 in 3 modi, definendo quindi e_i e f_i per ogni $i \in \{ 1, 2, 3 \}$.

$$\theta^2 = \begin{cases} (18 + 12\sqrt{2}) + (10 + 7\sqrt{2})\sqrt{3} \\ (18 + 10\sqrt{3}) + (12 + 7\sqrt{3})\sqrt{2} \\ (18 + 7\sqrt{6}) + (12 + 5\sqrt{6})\sqrt{2} \end{cases}$$

Ora verifichiamo direttamente che, per ogni $i \in \{ 1, 2, 3 \}$, $d_i({e_i}^2 - {f_i}^2 d)$ è un quadrato in R_i.

In $R_1 = \mathbb{Q}(\sqrt{2})$, si ha $3((18 + 12\sqrt{2})^2 - (10 + 7\sqrt{2})^2 3) = (3(2 + \sqrt{2}))^2$

In $R_2 = \mathbb{Q}(\sqrt{3})$, si ha $2((18 + 10\sqrt{3})^2 - (12 + 7\sqrt{3})^2 2) = (2(3 + 2\sqrt{3}))^2$

In $R_3 = \mathbb{Q}(\sqrt{6})$, si ha $2((18 + 7\sqrt{6})^2 - (12 + 5\sqrt{6})^2 2) = (2(3 + \sqrt{6}))^2$

Il prossimo passo è quello di trovare un polinomio $p(x) \in \mathbb{Q}[x]$ che abbia T come campo di spezzamento. Una volta trovato $p(x)$ segue automaticamente che T è un'estensione di Galois su $\mathbb{Q}$ e che $\mathrm{Gal}(T/\mathbb{Q})$ è il gruppo dei quaternioni poiché ha tre sottogruppi ciclici di ordine 4 che corrispondono alle tre estensioni $R_i \subseteq T$ di grado 4 (si veda il Teorema 1.4.3).

Per il Teorema 4.1.2 sappiamo che T è campo di spezzamento del polinomio

$$p(x) = x^4 - 2e_1 x^2 + (e_1^2 - 3f_1^2)$$

su $R_1 = \mathbb{Q}(\sqrt{2})$ e $p(\theta) = 0$. Siano

$$\overline{e_1} = 18 - 12\sqrt{2}, \quad \overline{f_1} = 10 - 7\sqrt{2};$$

si tratta delle immagini di e_1 ed f_1 attraverso l'automorfismo di S che manda $\sqrt{2}$ in $-\sqrt{2}$ e fissa $\sqrt{3}$.

Definiamo

$$\phi^2 = (2 - \sqrt{2})(2 + \sqrt{3})(3 - \sqrt{6}) = \overline{e_1} + \overline{f_1}\sqrt{3}$$

così che ϕ è radice di

$$\overline{p(x)} = x^4 - 2\bar{e_1} x^2 + (\overline{e_1}^2 - 3\overline{f_1}^2)$$

su $R_1 = \mathbb{Q}(\sqrt{2})$. Osserviamo che $\theta^2\phi^2 = 6(2+\sqrt{3})^2$ quindi $\theta\phi = (2+\sqrt{3})\sqrt{6} \in T$. Poiché $\theta, \sqrt{6}, 2 + \sqrt{3} \in T$ segue che anche $\phi \in T$. Usando il Teorema 4.1.2 si ha che $\overline{p(x)}$ è irriducibile su $\mathbb{Q}(\sqrt{2})$. Allora θ e ϕ sono radici di

$$q(x) = p(x)\overline{p(x)} = x^8 - 72x^6 + 180x^4 - 144x^2 + 36$$

candidato ad essere il polinomio desiderato.
Ora per il Teorema 4.1.2 T è il campo di spezzamento sia di $p(x)$ che di $\overline{p(x)}$ su R_1 quindi T è il campo di spezzamento di $q(x)$ su $\mathbb{Q}$. Infatti $q(x)$ si fattorizza completamente su T. Inoltre se consideriamo un'estensione P di $\mathbb{Q}$ contenente tutte le radici di $q(x)$ allora contiene $\theta^2, \eta^2, \theta^2+\eta^2$ ove $\eta^2 = e_1 - f_1\sqrt{3}$. Poiché $\theta^2+\eta^2 = 2e_1 \in P$ si ha che anche $\sqrt{2} = ((2e_1/2) - 18) \in P$ quindi $\mathbb{Q}(\sqrt{2}) \subseteq P$; poiché T è il campo di spezzamento di $p(x)$ e di $\overline{p(x)}$ su $R_1 = \mathbb{Q}(\sqrt{2})$ si ha che $T \subseteq P$. Allora T è il campo di spezzamento di $q(x)$ su $\mathbb{Q}$. La costruzione è così conclusa.

Vogliamo ora determinare gli automorfismi che generano $\mathrm{Gal}(T/Q)$, visti come permutazioni delle radici di $q(x)$.

Osservazione 17. Abbiamo che $T = R_1(\theta) = R_1(\phi)$. Consideriamo infatti le seguenti estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \theta)$, dal Teorema 1.4.1 si ha che $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \theta) : \mathbb{Q}(\sqrt{2})] = 4$ poiché $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \theta) : \mathbb{Q}] = 8$. Prendiamo ora la catena di estensioni $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \theta) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \theta)$; sfruttando il risultato precedente e il Teorema 1.4.1 abbiamo che $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \theta) : \mathbb{Q}(\sqrt{2}, \theta)] = 1$ poiché $[\mathbb{Q}(\sqrt{2}, \theta) : \mathbb{Q}(\sqrt{2})] = 4$ e $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \theta) : \mathbb{Q}(\sqrt{2})] = 4$. Ne viene che $T = R_1(\theta)$ e analogamente si dimostra che $T = R_1(\phi)$.

Indichiamo con $\theta, -\theta, \eta, -\eta$ le radici del polinomio $p(x)$, ove $\theta^2 = e_1 + f_1\sqrt{3}, \eta^2 = e_1 - f_1\sqrt{3}$ e con $\psi, -\psi, \gamma, -\gamma$ le radici del polinomio $\overline{p(x)}$, ove $\psi^2 = \overline{e_1} + \overline{f_1}\sqrt{3}, \gamma^2 = \overline{e_1} - \overline{f_1}\sqrt{3}$. Per ora le radici sono determinate a meno del segno. Osserviamo che $\mathbb{Q}(\theta^2) = \mathbb{Q}(\eta^2) = \mathbb{Q}(\psi^2) = \mathbb{Q}(\gamma^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = S$.

Cerchiamo prima di tutto l'unico automorfismo $\sigma \in \mathrm{Gal}(T/Q)$ di ordine 2. Dal Teorema 1.4.3 segue che $\langle\sigma\rangle = \mathrm{Gal}(T/S)$ è immmagine di S. Necessariamente $\sigma(\theta) \in \{\, \theta, -\theta \,\}$, ma se $\sigma(\theta) = \theta$ allora σ coincide con l'identità è questo è assurdo. Ne viene che $\sigma(\theta) = -\theta$ e per quanto appena osservato $\sigma(\psi) = -\psi, \sigma(\eta) = -\eta, \sigma(\gamma) = -\gamma$.
Cerchiamo ora gli automorfismi di ordine 4 che generano il gruppo di Ga-

lois $\mathrm{Gal}(T/Q)$. Dal Teorema 1.4.3 sappiamo che essi sono i generatori di $\mathrm{Gal}(T/R_1)$ e di $\mathrm{Gal}(T/R_2)$.

Sia i un generatore di $\mathrm{Gal}(T/R_2)$. Si ha che $i(\sqrt{3}) = \sqrt{3}$ e $i(\sqrt{2}) = -\sqrt{2}$, altrimenti i fissa S, cioè $i \in \mathrm{Gal}(T/S)$ che per il Teorema 1.4.3 ha ordine 2, quindi i ha ordine 2, il che è assurdo. Dobbiamo ora stabilire l'immagine di θ attraverso i; saranno così determinate le immagini attraverso i di tutte le altre radici del polinomio $q(x)$. Poiché $(i(\theta))^2 = i(\theta^2) = \psi^2$ segue che $i(\theta) \in \{\, \psi, -\psi \,\}$, ma anche $i^{-1}(\theta) \in \{\, \psi, -\psi \,\}$. Poniamo $i(\theta) = \psi$, si avrà allora $i^{-1}(\theta) = -\psi$. Poiché $i^2(\theta) = \sigma(\theta) = -\theta$ si ha che $i(\psi) = -\theta$.
Sia ora j un generatore di $\mathrm{Gal}(T/R_1)$. Si ha che $j(\sqrt{2}) = \sqrt{2}$ e $j(\sqrt{3}) = -\sqrt{3}$, altrimenti j fissa S, cioè $j \in \mathrm{Gal}(T/S)$ che per il Teorema 1.4.3 ha ordine 2, quindi j ha ordine 2, ma questo è assurdo. Stabiliamo quindi l'immagine di θ; poiché $(j(\theta))^2 = j(\theta^2) = \eta^2$ segue che $j(\theta) \in \{\, \eta, -\eta \,\}$, ma anche $j^{-1}(\theta) \in \{\, \eta, -\eta \,\}$. Fissiamo $j(\theta) = \eta$ allora $j^{-1}(\theta) = -\eta$. Torniamo ad i. Dal momento che $(i(\eta))^2 = i(\eta^2) = \gamma^2$ segue che $i(\eta) \in \{\, \gamma, -\gamma \,\}$. Indichiamo con γ l'immagine di η attraverso i, cioè $i(\eta) = \gamma$; si ha poi che $i(\gamma) = -\eta$ perchè $i^2(\eta) = \sigma(\eta) = -\eta$. Abbiamo così determinato le immagini delle radici di $q(x)$ attraverso i. Non resta che trovare l'immagine di ψ attraverso j. Sappiamo che $j(\psi) \in \{\, \gamma, -\gamma \,\}$ poichè $(j(\psi))^2 = j(\psi^2) = \gamma^2$. Sfruttando l'uguaglianza $j^2(\psi) = \sigma(\psi) = -\psi$ saranno poi determinati $j(\gamma)$ e $j(-\gamma)$. Indichiamo con $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8$ rispettivamente $\theta, -\theta, \psi, -\psi, \eta, -\eta, \gamma, -\gamma$; chiamiamo ω la permutazione su 8 lettere associata ad i, ossia la permutazione sulle radici di $q(x)$; siano infine τ_1 la permutazione su 8 lettere associata a j con $j(\psi) = \gamma$ e τ_2 la permutazione su 8 lettere associata a j con $j(\psi) = -\gamma$. Si ha che $\omega = (1324)(5768)$, $\tau_1 = (1526)(3748)$, $\tau_2 = (1526)(3847)$. Poiché i e j sono generatori deve valere $i^j = i^{-1}$. Dalla Proposizione 1.4.7 si ha che $\omega^{\tau_1} = \omega$ e $\omega^{\tau_2} = \omega^{-1}$. Ne viene che $j(\psi) = -\gamma$.

In conclusione i due automorfismi che generano $\mathrm{Gal}(T/\mathbb{Q})$ visti come permutazioni sulle radici di $q(x)$ sono:

$$\omega = (1324)(5768) \quad \tau = (1526)(3847).$$

Bibliografia

[1] D.Robinson, *A Course in the Theory of Groups*, Springer, 1996.

[2] D.Cox, *Galois Theory*, Wiley, 2004.

[3] R.A.Dean, *A rational polynomial whose group is the quaternions*, Amer. Math. Monthly 88 (1981), no. 1, 42-45.