# 1 La corrispondenza di Galois

Sia $K$ un campo. Un *automorfismo di* $K$ è un omomorfismo biiettivo $\alpha\colon K \to K$. Ogni campo ha almeno un automorfismo, l'identità.

Indicheremo con $\mathrm{Gal}(K)$ l'insieme di tutti gli automorfismi di $K$. Questo insieme è un gruppo rispetto alla composizione di applicazioni. Infatti, se $\alpha$ e $\beta$ sono automorfismi di $K$, anche $\alpha \circ \beta$ lo è e così per $\alpha^{-1}$.

**Esempi 1.** Se $\mathbf{Q}$ è il campo razionale, l'unico elemento di $\mathrm{Gal}(\mathbf{Q})$ è l'identità. Sia infatti $\alpha$ un automorfismo di $\mathbf{Q}$. Allora $\alpha(1) = 1$ e, per induzione su $m$, $\alpha(m) = m$ per ogni $m$ intero non negativo. Inoltre $\alpha(-m) = -\alpha(m) = -m$ e quindi $\alpha$ induce l'identità su $\mathbf{Z}$. Se poi $m/n \in \mathbf{Q}$, si ha

$$n\alpha\left(\frac{m}{n}\right) = \alpha\left(n\frac{m}{n}\right) = \alpha(m) = m$$

da cui $\alpha(m/n) = m/n$.

Lo stesso vale per il campo reale $\mathbf{R}$. Se $\alpha$ è un automorfismo di $\mathbf{R}$ la medesima argomentazione dimostra che $\alpha$ induce l'identità su $\mathbf{Q}$. Inoltre in $\mathbf{R}$ ogni elemento non negativo è un quadrato; perciò $a \leq b$ se e solo se $b - a = c^2$ per qualche $c \in \mathbf{R}$. Sia dunque $a \leq b$ con $b - a = c^2$:

$$\alpha(b) - \alpha(a) = \alpha(b - a) = \alpha(c^2) = \alpha(c)^2$$

cosicché $\alpha(a) \leq \alpha(b)$. Dunque $\alpha$ è un'applicazione crescente e biiettiva di $\mathbf{R}$ in $\mathbf{R}$, quindi è continua. Poiché $\mathbf{Q}$ è denso in $\mathbf{R}$ e $\alpha$ induce l'identità su $\mathbf{Q}$, $\alpha$ è l'identità.

Si può dimostrare invece che $\mathrm{Gal}(\mathbf{C})$ ha la cardinalità del continuo.

Chiameremo $\mathrm{Gal}(K)$ *gruppo di Galois* di $K$. Se $H$ è un sottogruppo di $\mathrm{Gal}(K)$, porremo

$$K^H = \{\, a \in K : \alpha(a) = a, \text{ per ogni } \alpha \in H \,\}.$$

L'insieme $K^H$ è un sottocampo di $K$, come si vede facilmente.

Viceversa, se $L$ è un sottocampo di $K$, l'insieme

$$\mathrm{Gal}(K/L) = \{\, \alpha \in \mathrm{Gal}(K) : \alpha(a) = a, \text{ per ogni } a \in L \,\}$$

è un sottogruppo di $\mathrm{Gal}(K)$ (esercizio).

Indicheremo con $\mathcal{L}(K)$ l'insieme dei sottocampi di $K$; più in generale, se $L$ è un sottocampo di $L$, $\mathcal{L}(K/L)$ sarà l'insieme dei sottocampi di $K$ che contengono $L$. Se $G$ è un gruppo, $\mathcal{L}(G)$ indica l'insieme dei sottogruppi di $G$. Abbiamo perciò definito due applicazioni:

$$\begin{aligned} \mathcal{L}(K) &\to \mathcal{L}(\mathrm{Gal}(K)) & \qquad \mathcal{L}(\mathrm{Gal}(K)) &\to \mathcal{L}(K) \\ L &\mapsto \mathrm{Gal}(K/L) & \qquad H &\mapsto K^H \end{aligned}$$

e possiamo facilmente verificare che, per ogni sottocampo $L$ di $K$ e ogni sottogruppo $H$ di $\mathrm{Gal}(K)$, si ha

$$L \subseteq L^{\mathrm{Gal}(K/L)}, \qquad H \subseteq \mathrm{Gal}(K/K^H).$$

Uno degli scopi della teoria di Galois è di dare condizioni necessarie e sufficienti affinché nelle relazioni precedenti valga l'uguaglianza, quindi che le due applicazioni siano biiettive, una inversa dell'altra.

Indichiamo, solo per il momento, con $f\colon \mathcal{L}(\mathrm{Gal}(K)) \to \mathcal{L}(K)$ e $g\colon \mathcal{L}(K) \to \mathcal{L}(\mathrm{Gal}(K))$ le due applicazioni. Una conseguenza delle inclusioni appena viste è che, per ogni $H \in \mathcal{L}(\mathrm{Gal}(K))$ e ogni $L \in \mathcal{L}(K)$ si ha

$$f(g(f(H))) = f(H), \qquad g(f(g(L))) = g(L).$$

Infatti $H \subseteq g(f(H))$, da cui $f(H) \supseteq f(g(f(H))$; ma, siccome $f(H) \in \mathcal{L}(K)$, abbiamo $f(H) \subseteq f(g(f(H))$. Analogamente per $L$.

Dunque, per verificare che $f$ e $g$ sono biiettive, basta verificare che sono suriettive. Infatti, per $L = f(H)$ vale che $L = f(g(L))$ e, per $H = g(L)$ vale $g(f(H)) = H$.

Un esempio banale in cui non si ha l'uguaglianza è il caso di $K = \mathbf{R}$. Infatti $\mathrm{Gal}(\mathbf{R}/\mathbf{Q}) = \{id\}$ e $\mathbf{R}^{\mathrm{Gal}(\mathbf{R}/\mathbf{Q})} = \mathbf{R} \neq \mathbf{Q}$.

Di solito però non ci interesserà l'intero gruppo di Galois di un campo $K$, ma considereremo fin dall'inizio il gruppo $\mathrm{Gal}(K/F)$, dove $F$ è un fissato sottocampo di $K$. È chiaro che si hanno le due applicazioni

$$\begin{array}{ccc} \mathcal{L}(K/F) \to \mathcal{L}(\mathrm{Gal}(K/F)) & \qquad & \mathcal{L}(\mathrm{Gal}(K/F)) \to \mathcal{L}(K/F) \\ L \mapsto \mathrm{Gal}(K/L) & & H \mapsto K^H \end{array}$$

con le stesse proprietà di prima. Saremo in particolare interessati al caso in cui $K/F$ è un'estensione finita perché, in tal caso, anche $\mathrm{Gal}(K/F)$ è finito.

**Esempi 2.** Consideriamo $K = \mathbf{Q}[\sqrt{-2}]$, che è un'estensione finita di $\mathbf{Q}$. Cerchiamo gli automorfismi in $\mathrm{Gal}(K/\mathbf{Q})$. Se $\alpha$ è un automorfismo di $K$ su $\mathbf{Q}$ (cioè lascia fissi gli elementi di $\mathbf{Q}$), ci basta determinare $\alpha(\sqrt{-2})$, perché ogni elemento di $K$ si scrive in modo unico come $a + b\sqrt{-2}$, con $a, b \in \mathbf{Q}$.

Ora $\alpha(\sqrt{-2})^2 = \alpha((\sqrt{-2})^2) = \alpha(-2) = -2$ e quindi abbiamo $\alpha(\sqrt{-2}) = \sqrt{-2}$ oppure $\alpha(\sqrt{-2}) = -\sqrt{-2}$. Entrambe le possibilità sono realizzate, dall'identità e dalla restrizione del coniugio. Quindi $|\mathrm{Gal}(K/\mathbf{Q})| = 2$.

Si provi che $\mathbf{Q}[\sqrt[3]{2}]$ ha un solo automorfismo.

**Teorema 1.1.** *Sia $\phi\colon F \to F'$ un isomorfismo di campi e siano $E$ ed $E'$ estensioni di $F$ e $F'$ rispettivamente. Sia $b \in E$ un elemento algebrico su $F$, con polinomio minimo $f \in F[X]$ e sia $g$ il polinomio corrispondente in $F'[X]$. Allora $\phi$ può essere esteso a un omomorfismo $\bar{\phi}\colon F[b] \to E'$ se e solo se $g$ ha una radice in $E'$; in tal caso il numero di estensioni possibili coincide con il numero delle radici distinte di $g$ in $E'$.*

*Dimostrazione.* Supponiamo che un'estensione $\bar{\phi}$ esista. Allora

$$g(\bar{\phi}(b)) = \bar{\phi}(f(b)) = \phi(0) = 0$$

e quindi $\bar{\phi}(b)$ è una radice di $g$ in $E'$.

Viceversa, sia $c \in E'$ una radice di $g$. Se indichiamo con $h^*$ il polinomio corrispondente a $h \in F[X]$ applicando $\phi$ ai suoi coefficienti, abbiamo l'omomorfismo $\eta\colon h \mapsto h^*(c)$ da $F[X]$ in $E'$. Il nucleo di $\eta$ contiene l'ideale generato da $f$, poiché evidentemente $\eta(f) = f^*(c) = g(c) = 0$. Siccome l'ideale $I = fF[X]$ è massimale, il nucleo coincide con quest'ideale.

Quindi, per il teorema di omomorfismo, abbiamo un omomorfismo (iniettivo) $\tilde{\eta}\colon F[X]/I \to E'$ e inoltre il dominio di $\tilde{\eta}$ è un campo.

In modo simile abbiamo un omomorfismo $\theta\colon F[X] \to F[b]$ che induce un isomorfismo $\tilde{\theta}\colon F[X]/I \to F[b]$. Considerando la composizione $\tilde{\eta} \circ \tilde{\theta}^{-1}\colon F[b] \to E'$, questa è un'estensione di $\phi$. Chiaramente il numero di queste estensioni coincide con il numero di scelte possibili della radice $c$ di $g$ in $E'$. □

**Teorema 1.2.** *Sia $f \in F[X]$ e sia $\phi\colon F \to F'$ un isomorfismo di campi. Indichiamo con $h^*$ il corrispondente in $F'[X]$ del polinomio $h \in F[X]$. Se $K$ e $K'$ sono campi di riducibilità completa di $f$ e $f^*$ rispettivamente, allora esiste un isomorfismo $\bar{\phi}\colon K \to K'$ che estende $\phi$. Il numero di tali estensioni è $\leq [K : F]$ e vale l'uguaglianza se e solo se $f^*$ ha radici distinte in $K'$.*

*Dimostrazione.* Si procede per induzione su $[K : F]$, ma ometteremo la dimostrazione. □

Una conseguenza di questo teorema è che se $K$ è un campo di riducibilità di un polinomio irriducibile $f \in F[X]$, allora il numero di automorfismi di $K$ che lasciano fisso $F$ è al massimo $[K : F]$ e che coincide con questa dimensione se $f$ ha radici distinte in $K$.

Supponiamo ora $f$ monico qualsiasi; lo possiamo decomporre in prodotto di polinomi irriducibili $f = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ dove i $p_i$ sono monici e a due a due distinti. È evidente che il campo di riducibilità completa $K$ di $f$ su $F$ coincide con il campo di riducibilità completa di $p_1 p_2 \dots p_r$. Inoltre i fattori distinti non hanno radici in comune; infatti due polinomi irriducibili monici distinti $p$ e $q$ hanno massimo comun divisore 1 e quindi esistono $a, b \in F[X]$ tali che $ap + bq = 1$; una radice in comune in qualche estensione contraddirebbe questa identità.

**Definizione 1.** Un polinomio $f \in F[X]$ si dice *separabile* se i suoi fattori irriducibili hanno radici distinte nel campo di riducibilità completa di $f$ su $F$.

In caratteristica 0 ogni polinomio è separabile. Infatti, se $f$ è irriducibile, $f'$ ha grado minore del grado di $f$ e quindi non può dividere $f$ a meno che non sia costante. Dunque il massimo comun divisore fra $f$ e $f'$ è 1 e quindi $f$ non ha radici multiple in alcuna estensione di $F$.

Un campo $F$ si dice *perfetto* se ogni polinomio $f \in F[X]$ è separabile.

**Teorema 1.3.** *Sia $a \in F$, campo di caratteristica $p$. Allora esiste $b \in F$ tale che $b^p = a$ oppure il polinomio $f = X^p - a$ è irriducibile in $F[X]$.*

*Dimostrazione.* Se $a = b^p$, abbiamo $X^p - a = X^p - b^p = (X - b)^p$ e quindi $f$ non è irriducibile.

Supponiamo che $f = gh$, con $g$ monico di grado $k < p$. Sia $K$ un campo di riducibilità completa di $f$ su $F$ e sia $c \in K$ una radice di $f$. Allora $c^p = a$ e quindi $f = X^p - c^p = (X - c)^p = g(X)h(X)$ in $K[X]$. Ne segue che $g(X) = (X - c)^k \in F[X]$. Sviluppando il binomio, otteniamo che $c^k \in F$. Siccome $k < p$, esistono $x, y \in \mathbf{Z}$ tali che $kx + py = 1$ e quindi

$$c = c^{kx+py} = (c^k)^x (c^p)^y \in F,$$

da cui $a = c^p$ con $c \in F$. □

Se $F$ ha caratteristica $p > 0$ indichiamo con $F^p$ l'insieme delle potenze $p$-esime in $F$.

**Teorema 1.4.** *Un campo $F$ di caratteristica $p > 0$ è perfetto se e solo se $F = F^p$.*

*Dimostrazione.* Se $F$ è perfetto, il polinomio $X^p - a$ è separabile per ogni $a \in F$; ma allora $X^p - a$ non è irriducibile, perché altrimenti avrebbe radici coincidenti nel campo di riducibilità completa. Quindi è riducibile e $a \in F^p$.

Se $F$ non è perfetto, sia $f$ un polinomio irriducibile non separabile. Questo implica $f' = 0$, cioè che $f = a_0 + a_1 X^p + \cdots + a_n X^{p^n}$. Allora uno dei coefficienti non appartiene a $F^p$ e quindi $F \neq F^p$. Infatti, se $a_i = b_i^p$, per $i = 0, 1, \ldots, n$, avremmo

$$a_0 + a_1 X^p + \cdots + a_n X^{p^n} = (b_0 + b_1 X + \cdots + b_n X^n)^p$$

contro l'ipotesi che $f$ sia irriducibile. □

Come conseguenza abbiamo che ogni campo finito è perfetto. Infatti $F^p$ è l'immagine dell'omomorfismo di Frobenius che è iniettivo, avendo come dominio un campo. Per la finitezza, esso è anche suriettivo.

Vale anche un risultato nella direzione opposta.

**Teorema 1.5** (Artin)**.** *Sia $H$ un sottogruppo finito del gruppo* $\mathrm{Gal}(K)$ *e sia $F = K^H$. Allora $[K : F] \leq |H|$.*

*Dimostrazione.* Sia $n = |H|$. Dimostreremo che ogni insieme di $m$ elementi di $K$ è linearmente dipendente su $F$; quindi una base di $K$ su $F$ ha al massimo $n$ elementi, come richiesto.

Sia $H = \{\alpha_1 = id, \alpha_2, \ldots, \alpha_n\}$ e siano $b_1, b_2, \ldots, b_m$ elementi a due a due distinti di $K$, con $m > n$.

Siccome $m > n$, il sistema omogeneo con equazioni

$$\sum_{j=1}^{m} \alpha_i(u_j) x_j = 0, \qquad i = 1, 2, \ldots, n$$

ha una soluzione non banale (le incognite dominanti sono al massimo $n$). Fra queste ne scegliamo una $[b_1 \ b_2 \ \ldots \ b_m]^T$ con il minimo numero di coefficienti non nulli. Non è restrittivo, riordinando le incognite, supporre che $b_1 \neq 0$; ma anche $b_1^{-1}[b_1 \ b_2 \ \ldots \ b_m]^T$ è una soluzione, quindi possiamo supporre $b_1 = 1$.

Vogliamo a questo punto dimostrare che tutti i $b_i$ appartengono a $F$; se così è, infatti, l'equazione in cui $\alpha_h = id$ dà la richiesta relazione di dipendenza lineare.

Supponiamo dunque, per assurdo, che uno dei coefficienti non appartenga a $F$, cioè non sia tenuto fisso da tutti gli elementi di $H$. Non è restrittivo, cambiando l'ordine delle incognite, supporre che sia $b_2$. Allora esiste un indice $k$ tale che $\alpha_k(b_2) \neq b_2$.

Se applichiamo $\alpha_k$ a tutte le relazioni $\sum_j \alpha_i(u_j) b_j = 0$, otteniamo

$$\sum_{j=1}^{m} \alpha_k \alpha_i(u_j) \alpha_k(b_j) = 0 \qquad i = 1, 2, \ldots, n$$

e quindi $[1\ \alpha_k(b_2)\ \dots\ \alpha_k(b_m)]^T$ è una soluzione del sistema omogeneo di equazioni

$$\sum_{j=1}^{m} \alpha_k\alpha_i(u_j)x_j = 0 \qquad i = 1, 2, \dots, n$$

che è lo stesso di prima, solo con le equazioni in ordine diverso. Infatti, per ogni $\alpha \in H$, si ha $\alpha = \alpha_k(\alpha_k^{-1}\alpha)$ e $(\alpha_k^{-1}\alpha) \in H$.

Siccome il sistema è omogeneo, la differenza di due soluzioni è ancora una soluzione e abbiamo una contraddizione, perché

$$\begin{bmatrix} 1 \\ b_2 \\ \dots \\ b_m \end{bmatrix} - \begin{bmatrix} 1 \\ \alpha_k(b_2) \\ \dots \\ \alpha_k(b_m) \end{bmatrix} = \begin{bmatrix} 0 \\ b_2 - \alpha_k(b_2) \\ \dots \\ b_m - \alpha_k(b_m) \end{bmatrix}$$

è una soluzione non nulla con meno coefficienti non nulli di quella da cui siamo partiti, che ne aveva il numero minimo: assurdo. □

Diamo una nuova definizione: un'estensione $K/F$ si dice *normale* se ogni polinomio irriducibile in $F[X]$ che ammette una radice in $K$ si fattorizza in $K[X]$ nel prodotto di polinomi di grado 1. Equivalentemente, se $K$ contiene un campo di riducibilità completa per ogni polinomio irriducibile in $F[X]$ che abbia una radice in $K$.

Diremo anche che $K$ è *separabile su* $F$ se è algebrica su $F$ e il polinomio minimo su $F$ di ogni elemento di $K$ è separabile.

**Teorema 1.6.** *Sia $K$ un'estensione del campo $F$. Le seguenti condizioni sono equivalenti:*

(a) *$K$ è il campo di riducibilità completa di un polinomio separabile $f \in F[X]$;*

(b) *$F = K^H$ per un sottogruppo finito $H$ di* $\mathrm{Gal}(K)$*;*

(c) *$K$ è un'estensione finita, normale e separabile di $F$.*

*Se tali condizioni valgono, allora:*

(1) *con le stesse notazioni di* (a) *e posto $G = \mathrm{Gal}(K/F)$ si ha $F = K^G$;*

(2) *con le stesse notazioni di* (b)*, si ha $H = \mathrm{Gal}(K/F)$.*

*Dimostrazione.* (a) $\Longrightarrow$ (b) Sia $G = \mathrm{Gal}(K/F)$ e sia $F' = K^G$. È evidente che $F' \supseteq F$ e che $K$ è il campo di riducibilità completa di $f$ anche su $F'$; inoltre $G = \mathrm{Gal}(K/F')$. Dunque, per un risultato precedente, $|G| = [K : F']$ e $|G| = [K : F]$. Perciò, da

$$[K : F] = [K : F'][F' : F]$$

segue che $[F' : F] = 1$, cioè che $F' = F$. Abbiamo anche l'asserzione (1).

(b) $\Longrightarrow$ (c) Per il lemma di Artin, $[K : F] \leq |H|$, quindi $K$ ha dimensione finita su $F$. Sia $f \in F[X]$ un polinomio irriducibile monico che abbia una radice $b \in K$. Siano $b_1$, $b_2$,..., $b_r$ gli elementi distinti di $K$ che si ottengono applicando gli automorfismi appartenenti a $K$: in altre parole

$$\{b_1, \dots, b_r\} = \{\, \alpha(b) : \alpha \in H \,\}.$$

Se $\alpha \in H$, gli insiemi $\{b_1, \ldots, b_r\}$ e $\{\alpha(b_1), \ldots, \alpha(b_r)\}$ sono evidentemente uguali e tutti gli elementi $b_i$ sono radici di $f$ in $K$. Ne segue che il polinomio

$$g(X) = (X - b_1)(X - b_2) \ldots (X - b_r)$$

ha i coefficienti lasciati fissi da ogni automorfismo in $H$ e quindi, per definizione di $F$, $g \in F[X]$. Inoltre $g$ divide $f$ in $K[X]$ ma, appartenendo a $F[X]$ lo divide anche in questo anello. Poiché $f$ è irriducibile monico, abbiamo $f = g$. Ciò dimostra che $K$ è un'estensione normale e separabile di $F$.

(c) $\Longrightarrow$ (a) Dal momento che $K$ è un'estensione finita di $F$, possiamo scrivere $K = F[b_1][b_2] \ldots [b_r]$, dove i $b_i$ $(i = 1, 2, \ldots, r)$ sono algebrici su $F$. Sia $f_i$ il polinomio minimo di $b_i$ su $F$ $(i = 1, 2, \ldots, r)$. Per ipotesi, ogni $f_i$ è prodotto, in $K[X]$, di fattori monici distinti di grado 1 e quindi il polinomio $f = f_1 f_2 \ldots f_r$ è separabile. Ma allora $K$ è il campo di riducibilità completa di $f$ su $F$.

Rimane da dimostrare l'asserzione (2). Sappiamo già che $[K : F] \leq |H|$; siccome vale la (c), abbiamo che $|\operatorname{Gal}(K/F)| = [K : F]$. Siccome $H \subseteq \operatorname{Gal}(K/F)$ e $|H| \geq [K : F] = |\operatorname{Gal}(K/F)|$, deduciamo l'uguaglianza $H = \operatorname{Gal}(K/F)$. □

**Definizione 2.** Un'estensione finita $K$ del campo $F$ si dice *estensione di Galois* se è normale e separabile.

Dal teorema precedente è chiara l'importanza di questo tipo di estensioni e infatti per esse vale la biiettività della corrispondenza di Galois.

**Teorema 1.7** (Teorema fondamentale della teoria di Galois)**.** *Sia $K$ un'estensione di Galois del campo $F$. Allora le applicazioni*

$$\begin{aligned} \mathcal{L}(K/F) &\to \mathcal{L}(\operatorname{Gal}(K/F)) & \qquad \mathcal{L}(\operatorname{Gal}(K/F)) &\to \mathcal{L}(K/F) \\ L &\mapsto \operatorname{Gal}(K/L) & \qquad H &\mapsto K^H \end{aligned}$$

*sono biiettive, una inversa dell'altra. Inoltre, per ogni $H, H_1, H_2 \in \mathcal{L}(\operatorname{Gal}(K/F))$, si ha:*

(1) *$H_1 \subseteq H_2$ se e solo se $K^{H_1} \supseteq K^{H_2}$;*

(2) *$|H| = [K : K^H]$ e $[G : H] = [K^H : F]$;*

(3) *$H$ è normale in $\operatorname{Gal}(K/F)$ se e solo se $K^H$ è un'estensione normale di $F$ e, in tal caso,*

$$\operatorname{Gal}(K^H/F) \cong \operatorname{Gal}(K/F)/H.$$

*Dimostrazione.* Sia $H$ un sottogruppo di $G = \operatorname{Gal}(K/F)$. Allora $F' = K^H$ è un sottocampo di $K$ contenente $F$. Per l'asserzione (2) del teorema precedente, $H = \operatorname{Gal}(K/F')$ e abbiamo inoltre $|H| = |\operatorname{Gal}(K/F')| = [K : F']$.

□

# 2 Alcuni risultati di teoria dei gruppi

Un gruppo $G$ si dice *risolubile* se esistono sottogruppi $G_0 = G$, $G_1$, $\ldots$, $G_{n-1}$, $G_n = \{1\}$ tali che

(1) $G_i$ è normale in $G_{i-1}$, per $i = 1, 2, \ldots, n$;

(2) $G_{i-1}/G_i$ è abeliano.

La successione $G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n$ si chiama una *serie abeliana* per $G$.

Dati $x, y \in G$, si chiama *commutatore* di $x$ e $y$ l'elemento

$$[x, y] = xyx^{-1}y^{-1}.$$

Il *derivato* di $G$ è il minimo sottogruppo $G'$ di $G$ che contiene tutti i commutatori fra gli elementi di $G$. Dal momento che

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

è evidente che gli elementi di $G'$ sono i prodotti di commutatori.

Nel seguito è conveniente usare la notazione $x^g = gxg^{-1}$, se $x, g \in G$. Un sottogruppo $H$ di $G$ è normale se e solo se, per ogni $x \in H$ e ogni $g \in G$, $x^g \in H$. Si ricordi anche che, se $x, y \in G$, $(xy)^g = x^g y^g$.

**Proposizione 2.1.** *Il derivato $G'$ di $G$ è un sottogruppo normale di $G$ e $G/G'$ è abeliano.*

*Dimostrazione.* Siano $x, y \in G$ e sia $g \in G$. Allora

$$[x, y]^g = g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [x^g, y^g] \in G'.$$

Un elemento generico di $G'$ è del tipo

$$h = [x_1, y_1][x_2, y_2] \dots [x_n, y_n]$$

e quindi

$$h^g = ([x_1, y_1][x_2, y_2] \dots [x_n, y_n])^g = [x_1, y_1]^g [x_2, y_2]^g \dots [x_n, y_n]^g = [x_1^g, y_1^g][x_2^g, y_2^g] \dots [x_n^g, y_n^g]$$

perciò $h^g \in G'$.

Per dimostrare che $G/G'$ è abeliano, basta vedere che, per ogni $x, y \in G$, $xy \sim_{G'} yx$, cioè che

$$(xy)(yx)^{-1} \in G'.$$

Questo è ovvio, perché $(xy)(yx)^{-1} = [x, y]$. □

**Proposizione 2.2.** *Se $H$ è un sottogruppo normale di $G$ e $G/H$ è abeliano, allora $G' \subseteq H$.*

*Dimostrazione.* Siano $x, y \in G$. Allora $xy \sim_H yx$, quindi $(xy)(yx)^{-1} \in H$. Ma allora $[x, y] \in H$, e quindi $H$ contiene tutti i commutatori. □

Possiamo ora ripetere la costruzione del derivato induttivamente: $G^{(0)} = G$, $G^{(k+1)} = (G^{(k)})'$. Per quanto visto prima, $G^{(k+1)}$ è un sottogruppo normale di $G^{(k)}$ e $G^{(k)}/G^{(k+1)}$ è abeliano.

**Teorema 2.3.** *Se $G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n$ è una serie abeliana per $G$, allora $G^{(n)} = \{1\}$. Di conseguenza $G$ è risolubile se e solo se esiste $m$ tale che $G^{(m)} = \{1\}$.*

*Dimostrazione.* Abbiamo già visto che $G' = G^{(1)} \subseteq G_1$. Supponiamo di aver dimostrato che $G^{(k)} \subseteq G_k$. Allora $G^{(k+1)} = (G^{(k)})' \subseteq G_{k+1}$, perché per ipotesi $G_k/G_{k+1}$ è abeliano. L'induzione permette di arrivare al passo $n$.

Se poi $G^{(m)} = \{1\}$, la successione

$$G = G^{(0)} \supseteq G' = G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(m-1)} \supseteq G^{(m)} = \{1\}$$

è una serie abeliana per $G$ e quindi $G$ è risolubile. □

**Teorema 2.4.** *Sia $G$ un gruppo. Se $G$ è risolubile e $H$ è un sottogruppo di $G$, allora $H$ è un gruppo risolubile. Se $H$ è un sottogruppo normale di $G$ tale che $H$ e $G/H$ siano risolubili, allora $G$ è risolubile.*

*Dimostrazione.* Nel primo caso è evidente che $H^{(k)} \subseteq G^{(k)}$, da cui la tesi.

Supponiamo ora che $H$ e $\bar{G} = G/H$ siano risolubili. Sia

$$\bar{G}_0 \supseteq \bar{G}_1 \supseteq \cdots \supseteq \bar{G}_n$$

una serie abeliana per $G/H$ e poniamo $G_i = \pi^{\rightarrow}(\bar{G}_i)$. Sia poi

$$H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r$$

una serie abeliana per $H$. Allora

$$G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n \supseteq H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r$$

è una serie abeliana per $G$. Infatti il teorema di omomorfismo mostra che $G_i$ è normale in $G_{i-1}$ e che $G_{i-1}/G_i$ è isomorfo a $\bar{G}_{i-1}/\bar{G}_i$ che è abeliano. □

È evidente che se inseriamo termini dentro una serie abeliana del gruppo $G$, la serie che si ottiene è ancora abeliana. Esaminiamo allora ciò che si può fare quando un gruppo $G$ è abeliano e finito.

Sia $n = |G|$ e supponiamo $n > 1$. Allora fra gli elementi di $G$ diversi da 1, ce n'è uno $x$ di ordine minimo $m$. Affermo che $m$ è primo: infatti, se $m = ab$, con $a > 1$, si ha $(x^a)^b = x^m = 1$ e quindi $x^a$ ha ordine minore di $m$. Quindi $x^a = 1$ e perciò $a = m$. Il sottogruppo $\langle x \rangle$ è normale in $G$ e possiamo ripetere lo stesso ragionamento su $G/\langle x \rangle$, ottenendo una serie abeliana con quozienti ciclici.

**Proposizione 2.5.** *Un gruppo finito è risolubile se e solo se ammette una serie abeliana con quozienti ciclici.*

*Dimostrazione.* Se $G$ è finito e risolubile, consideriamo una sua serie abeliana $G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n$. Indichiamo con $\pi_i \colon G_{i-1} \to G_{i-1}/G_i$ la proiezione canonica. Il gruppo $H = G_{i-1} \to G_{i-1}/G_i$ ha una serie con quozienti ciclici: $H_0 = H \supseteq H_1 \supseteq \cdots \supseteq H_k = \{1\}$. Possiamo allora inserire fra $G_{i-1}$ e $G_i$ i sottogruppi $\pi_i^{\leftarrow}(H_j)$ $(i = 1, \ldots, n)$, ottenendo la serie abeliana richiesta. □

**Esempi 3.** Esistono gruppi non risolubili: per esempio $S_5$. In virtù dei risultati precedenti, ci basta vedere che $A_5$, insieme delle permutazioni pari in $S_5$ non è risolubile. Sarà sufficiente dimostrare che $A_5' = A_5$.

La struttura ciclica di una permutazione pari è $(ab)(cd)$ oppure $(abc)$ oppure $(abcde)$ (con lettere distinte indichiamo elementi distinti di $\{1,2,3,4,5\}$). Abbiamo

$$[(acebd),(ace)(bd)] = (ab)(cd) \in A_5'$$
$$[(acb),(ab)(de)] = (abc) \in A_5'$$
$$[(aebdc),(ac)(bd)] = (abcde) \in A_5'$$

e quindi ogni elemento di $A_5$ è un commutatore.

Nessun gruppo $S_n$, per $n \geq 5$ è allora risolubile, perché $S_5$ è isomorfo a un sottogruppo di $S_n$.

Un altro teorema importantissimo di teoria dei gruppi è dovuto al norvegese Sylow.

Diremo che un gruppo $G$ *agisce sull'insieme* $X$ se è dato un omomorfismo $\phi\colon G \to S_X$. Per ogni $g \in G$, porremo $\hat{g} = \phi(g)$; questo perché $\hat{g}$ è un'applicazione biiettiva $X \to X$ e quindi avremo bisogno di calcolare $\hat{g}$ sugli elementi di $X$. Siccome $\phi$ è un omomorfismo, abbiamo che

$$\widehat{gh} = \hat{g} \circ \hat{h}$$

cioè che, per ogni $g, h \in G$ e per ogni $x \in X$,

$$\widehat{gh}(x) = \hat{g} \circ \hat{h}(x) = \hat{g}(\hat{h}(x)).$$

Inoltre $\hat{1} = id$, quindi $\hat{1}(x) = x$. L'azione $\phi$ definisce una relazione di equivalenza su $X$: poniamo $x \sim_\phi y$ quando

$$y = \hat{g}(x) \text{ per qualche } g \in G.$$

La proprietà riflessiva discende dal fatto che $\hat{1} = id$, quella simmetrica dal fatto che $\widehat{g^{-1}} = \hat{g}^{-1}$ e quella transitiva dal fatto che $\phi$ è un omomorfismo. Indicheremo con $\mathrm{Orb}_\phi(x)$ la classe di equivalenza di $x \in X$ e la chiameremo *orbita di* $x$. Poniamo

$$\mathrm{Stab}_\phi(x) = \{\, g \in G : \hat{g}(x) = x \,\}.$$

È un facile esercizio dimostrare che $\mathrm{Stab}_\phi(x)$ è un sottogruppo di $G$.

**Proposizione 2.6.** *Se $\phi\colon G \to S_X$ è un'azione del gruppo $G$ sull'insieme $X$ e $x \in X$, allora*

$$|\,\mathrm{Orb}_\phi(x)| = \frac{|G|}{|\,\mathrm{Stab}_\phi(x)|} = [G : \mathrm{Stab}_\phi(x)].$$

*In particolare $|\,\mathrm{Orb}_\phi(x)|$ divide l'ordine di $G$.*

*Dimostrazione.* Si tratta di contare gli elementi di $\mathrm{Orb}_\phi(x) = \{\, \hat{g}(x) : g \in G \,\}$. Si ha $\hat{h}(x) = \hat{g}(x)$ se e solo se $\hat{g}^{-1}(\hat{h}(x)) = x$, cioè se e solo se $g^{-1}h \in \mathrm{Stab}_\phi(x)$. Perciò otteniamo una biiezione

$$G/_H \sim \to \mathrm{Orb}_\phi(x)$$

dove $H = \mathrm{Stab}_\phi(x)$ e ${}_H\sim$ è proprio una delle due relazioni di equivalenza legate al teorema di Lagrange. □

**Esempi 4.** Un'azione molto importante è quella di Cayley: si prende $X = G$ e si pone $\hat{g}(x) = gx$. La verifica che $g \mapsto \hat{g}$ è un omomorfismo di $G$ in $S_G$ è banale. Inoltre questo omomorfismo è iniettivo e ciò dimostra che ogni gruppo è isomorfo a un sottogruppo di un gruppo di permutazioni. In particolare, se $G$ è finito di ordine $n$, $G$ si può pensare come sottogruppo di $S_n$. In questa azione c'è un'unica orbita.

Un'altra azione di $G$ su sé stesso è quella per coniugio. Si pone, per $g \in G$,

$$\hat{g}(x) = gxg^{-1}$$

ed è ancora immediata la verifica che $g \mapsto \hat{g}$ è un omomorfismo di $G$ in $S_G$. In questo caso le orbite si chiamano *classi di coniugio*. Nel caso particolare di $G = S_3$, le classi di coniugio sono

$$\{id\}, \quad \{(12), (13), (23)\}, \quad \{(123), (132)\}.$$

Un terzo esempio si ottiene considerando come $X$ l'insieme potenza di $G$. Se $A \subseteq X$ e $g \in G$, poniamo

$$\hat{g}(A) = \{\, gx : x \in A \,\}$$

e, naturalmente, $\hat{g}(\emptyset) = \emptyset$. Ci sono altre azioni dello stesso tipo, per esempio possiamo prendere come $X$ l'insieme dei sottoinsiemi di $G$ di una data cardinalità; infatti è chiaro che $|\hat{g}(A)| = |A|$.

**Proposizione 2.7.** *Siano $p$, $m$ e $a$ numeri naturali. Se $p$ è primo, allora*

$$\binom{p^a m}{p^a} \equiv m \pmod{p}.$$

*Dimostrazione.* Sia $A$ l'anello $\mathbf{Z}/p\mathbf{Z}$ e consideriamo il polinomio $f \in A[X, Y]$:

$$f(X, Y) = (X + Y)^{qm}$$

dove $q = p^a$. Possiamo sviluppare $f$ in due modi; il primo è quello della formula di Newton:

$$f(X, Y) = \sum_{i=0}^{qm} \binom{qm}{i} X^i Y^{qm-i}.$$

Il secondo tiene conto che, in caratteristica $p$, si ha $(x + y)^p = x^p + y^p$ e quindi

$$f(X, Y) = (X^q + Y^q)^m = \sum_{j=0}^{m} \binom{m}{j} X^{qj} Y^{q(m-j)}.$$

I coefficienti di $X^q Y^{q(m-1)}$ nei due sviluppi devono essere uguali (modulo $p$) e quindi

$$\binom{qm}{m} \equiv \binom{m}{1} \pmod{p},$$

come richiesto. □

**Teorema 2.8.** *Sia $G$ un gruppo finito; siano $p$ un numero primo e $k \geq 0$ tali che $p^k$ divide $|G|$. Allora esiste un sottogruppo $H$ di $G$ con $|H| = p^k$.*

*Dimostrazione.* Faremo induzione su $|G|$; il passo base, quando $|G| = 1$ è ovvio. Supponiamo allora $|G| > 1$.

Vediamo prima un caso speciale: $G$ abeliano e $k = 1$. Prendiamo $x \in G$, $x \neq 1$. Se l'ordine $r$ di $x$ è divisibile per $p$, avremo $r = pq$ e $(x^q)^p = 1$ con $x^q \neq 1$; perciò $x^q$ ha ordine $p$ e $\langle x^q \rangle$ soddisfa alla richiesta. Se invece $p$ non divide $r$, allora $p$ divide l'ordine del gruppo $G/\langle x \rangle$ e quindi questo gruppo, per ipotesi induttiva, ha un sottogruppo di ordine $p$, cioè un elemento $[y] \neq [1]$ tale che $[y]^p = [1]$. Allora $[y^p] = [1]$; se $s$ è l'ordine di $y$, abbiamo $[y]^s = [y^s] = [1]$ e quindi $s$ è un multiplo di $p$. Allora in $\langle y \rangle$ esiste un elemento di ordine $p$ per quanto visto prima.

Consideriamo l'azione $\phi$ di $G$ su sé stesso per coniugio: $\hat{g}(x) = gxg^{-1}$ e siano $C_1 = \mathrm{Orb}_\phi(1) = \{1\}$, $C_2, \ldots, C_n$ le orbite. Le ordiniamo mettendo per prime quelle con un solo elemento, diciamo che sono quelle da 1 a $m$ e poniamo $Z = C_1 \cup \cdots \cup C_m$.

Allora $Z$ è un sottogruppo di $G$: infatti dire che $x \in Z$ significa dire che $\hat{g}(x) = gxg^{-1} = x$, cioè $gx = xg$, per ogni $g \in G$. Inoltre ogni sottogruppo di $Z$ è normale in $G$.

Indichiamo con $H_i$ lo stabilizzatore degli elementi dell'orbita $C_i$ ($i = m + 1, \ldots, n$). Allora possiamo scrivere

$$|G| = |Z| + \sum_{i=m+1}^{n} [G : H_i].$$

Se $p$ non divide $|Z|$, allora $p$ non divide $[G : H_i]$ per qualche $i$, dunque $p^k$ divide $|H_i|$. Siccome $|H_i| < |G|$, perché $|C_i| > 1$, l'ipotesi induttiva dice che $H_i$ ha un sottogruppo di ordine $p^k$.

Supponiamo ora che $p$ divida $Z$. Allora esiste un sottogruppo $Z_0$ di $Z$ di ordine $p$ che è quindi normale in $G$. Per ipotesi induttiva, esiste un sottogruppo $K$ di $G/Z_0$ di ordine $p^{k-1}$. Se $\pi\colon G \to G/Z_0$ è la proiezione canonica, $H = \pi^{\leftarrow}$ è un sottogruppo di $G$ con $p^k$ elementi. □

Il sottogruppo la cui esistenza è garantita da questo teorema si chiama un *p-sottogruppo di Sylow* di $G$.

Usiamo questo teorema per dimostrare che $\mathbf{C}$ è algebricamente chiuso.

La prima cosa da vedere è che ogni numero complesso ha radici quadrate. Questo è evidente se il numero è reale. Se $a + bi \in \mathbf{C}$ con $b \neq 0$, dobbiamo trovare $x$ e $y$ tali che $(x + yi)^2 = a + bi$, cioè

$$x^2 - y^2 = a, \qquad 2xy = b.$$

Sostituendo $y = b/(2x)$, si trova

$$4x^4 - 4ax^2 - b^2 = 0,$$

che dà

$$x^2 = \frac{a + \sqrt{a^2 + b^2}}{2}$$

da cui ricaviamo due valori per $x$ e due corrispondenti valori per $y$.

Vogliamo dimostrare che se $K$ è un'estensione finita di $\mathbf{C}$, allora $K = \mathbf{C}$. Non è restrittivo supporre che $K$ sia normale, quindi un'estensione di Galois di $\mathbf{C}$. Siccome $\mathbf{C}$ è normale su $\mathbf{R}$, $K$ è anche un'estensione normale di $\mathbf{R}$; sia

$G = \mathrm{Gal}(K/\mathbf{R})$. Sia $H$ il 2-sottogruppo di Sylow di $G$, quindi $[G : H]$ è dispari. Sia $F = K^H$: allora $[F : \mathbf{R}] = [G : H]$ è dispari e quindi il polinomio minimo su $R$ di ogni elemento di $F$ ha grado dispari. Siccome ogni polinomio di grado dispari in $\mathbf{R}[X]$ ha radici, concludiamo che $F = \mathbf{R}$. Dunque $G$ ha ordine una potenza di 2.

Quindi anche $G_1 = \mathrm{Gal}(K/\mathbf{C})$ ha ordine una potenza di 2, diciamo $|G_1| = 2^n$. Supponiamo $n > 1$. Sempre per il teorema di Sylow, esiste un sottogruppo $H_1$ di $G_1$ che ha ordine $2^{n-1}$, quindi indice 2; perciò $H_1$ è normale in $G_1$ e $K^{H_1}$ è un'estensione normale di $\mathbf{C}$ di grado 2. Questo è impossibile, perché ogni polinomio di grado 2 è riducibile in $\mathbf{C}$. Resta dunque solo il caso di $G_1 = \{1\}$ e perciò $K = \mathbf{C}$, come richiesto.