Capitolo 2

Teoria di Galois delle equazioni

In questo capitolo K sarà un campo di caratteristica zero e $f(x) = x^n + e_1 x^{n-1} + \cdots + e_n$ un polinomio separabile (cioè a radici distinte) ma non necessariamente irriducibile di grado n a coefficienti in K, e $\alpha_1, \alpha_2, \ldots, \alpha_n$ le sue radici in un ampliamento di K. Come abbiamo visto nel precedente capitolo, le α_i soddisfano certe relazioni algebriche a coefficienti in K, ad esempio le relazioni simmetriche

$$\sum \alpha_i + e_1 = 0, \ \sum \alpha_i \alpha_j - e_2 = 0, \ldots, \alpha_1 \alpha_2 \cdots \alpha_n \pm e_n = 0$$

(e anzi queste relazioni caratterizzano i numeri α_i come le radici di $f(x)$). Permutando comunque le α_i queste relazioni restano soddisfatte, e dunque una radice α_i non può essere individuata dal fatto di soddisfare una delle relazioni. Esistono in generale altre relazioni a coefficienti in K, ma in ogni caso, come vedremo, le radici che non appartengono a K non possono essere determinate dalle relazioni che esse soddisfano. Possono esserlo soltanto con un certo grado di ambiguità. Questa ambiguità è dovuta al fatto che se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n) = 0$ è una relazione, e $\alpha_i \notin K$, esiste almeno una permutazione $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_j}, \ldots, \alpha_{i_n}$ delle α_i che porta α_i in una $\alpha_{i_j} \neq \alpha_i$ e tale che la relazione $\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_j}, \ldots, \alpha_{i_n}) = 0$ è ancora soddisfatta. Il grado di ambiguità che esiste nella determinazione delle radici a partire dalle relazioni è dunque misurato dalle permutazioni che mutano le relazioni tra le radici ancora in relazioni. Queste permutazioni formano gruppo, sottogruppo di S^n, il *gruppo di Galois del polinomio* $f(x)$.

2.1 Il gruppo di Galois

Fissiamo una volta per tutte un ordinamento $\alpha_1 \alpha_2 \cdots \alpha_n$ delle radici del polinomio $f(x)$. Siano $f_1(x)$ il polinomio irriducibile monico su K che ammette la radice α_1, $f_2(\alpha_1, x)$ il polinomio irriducibile monico su $K(\alpha_1)$ che ammette la radice α_2, $\ldots$, $f_n(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x)$ il polinomio irriducibile monico su $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ che ammette la radice α_n.

Il lemma che segue mostra come gli elementi del campo $K(\alpha_1)$, che sono funzioni razionali di α_1, si possono ridurre a polinomi in α_1 di grado inferiore al grado di $f_1(x)$. Analogamente, gli elementi di $K(\alpha_1, \alpha_2)$ sono funzioni razionali di α_1 e α_2 ma si possono ridurre a polinomi in α_1 e α_2 di grado in α_1 inferiore al grado di $f_1(x)$, e in α_2 inferiore al grado di $f_2(\alpha_1, x)$. In generale, gli elementi del campo $K(\alpha_1, \alpha_2, \ldots, \alpha_k)$, sono funzioni razionali in $\alpha_1, \alpha_2, \ldots, \alpha_k$ e si possono ridurre a polinomi in $\alpha_1, \alpha_2, \ldots, \alpha_k$ di grado in α_1 inferiore al grado di $f_1(x)$, in α_2 inferiore al grado di $f_2(\alpha_1, x)$,..., in α_k inferiore al grado di $f_k(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x)$.

2.1 Lemma. *Sia $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_k)$ una funzione razionale delle α_i. Allora φ si esprime come un polinomio $r(\alpha_1, \alpha_2, \ldots, \alpha_k)$ il cui grado in α_i è inferiore al grado di $f_i(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, x)$.*

Dim. Siano $k = 1$ e $\varphi(\alpha_1) = \frac{g(\alpha_1)}{h(\alpha_1)}$ una funzione razionale. Si ha intanto $h(\alpha_1) \neq 0$, e dunque $f_1(x)$ non divide $h(x)$, per cui i due polinomi sono primi tra loro. Ne segue $h(x)k_1(x) + f_1(x)k_2(x) = 1$, per certi $k_1(x)$ e $k_2(x)$, da cui $k(\alpha_1)h(\alpha_1) = 1$ e $\varphi(\alpha_1) = \frac{g(\alpha_1)}{h(\alpha_1)} = g(\alpha_1)k(\alpha_1) = u(\alpha_1)$. Dividendo ora $u(x)$ per $f_1(x)$ si ha $u(x) = f_1(x)q(x) + r(x)$, con $\partial r(x) < \partial f_1(x)$, e, calcolando in α_1, $\varphi = u(\alpha_1) = r(\alpha_1)$, dove $r(\alpha_1)$ è un'espressione polinomiale in α_1 che ha il grado richiesto.

Se $k = 2$ e $\varphi(\alpha_1, \alpha_2) = \frac{g(\alpha_1, \alpha_2)}{h(\alpha_1, \alpha_2)}$ è una funzione razionale, $h(\alpha_1, x)$ e $f_2(\alpha_1, x)$ sono primi tra loro, e si ha $h(\alpha_1, x)k_1(\alpha_1, x) + f_2(\alpha_1, x)k_2(\alpha_1, x) = 1$ e calcolando in α_2, $h(\alpha_1, \alpha_2)k_1(\alpha_1, \alpha_2) = 1$. φ si riduce allora a un polinomio $u(\alpha_1, \alpha_2)$. Scrivendo u come polinomio in α_2 a coefficienti polinomi $p_i(\alpha_1)$, i p_i si possono ridurre a un grado minore di $f_1(x)$. Dividendo ora $u(\alpha_1, x)$ per $f_2(\alpha_1, x)$ si ha un resto $r(\alpha_1, x)$ con $\partial r < \partial f_2$, e calcolando in α_2 si trova $\varphi(\alpha_1, \alpha_2) = r(\alpha_1, \alpha_2)$, con $\partial_{\alpha_1} r < \partial f_1$ e $\partial_{\alpha_2} r < \partial f_2$.

Procedendo in modo analogo (o per induzione) si ha il risultato. $\diamondsuit$

2.2 Nota. **1.** I polinomi $f_k(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x)$ sono a priori a coefficienti funzioni razionali. Dividendo per il coefficiente direttore, si ha un polinomio monico a coefficienti funzioni razionali nelle $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ che come visto nel Lemma 2.1 possono ridursi a polinomi.

2. Avendosi $\partial r(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x) < \partial f_k(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x)$, r e f_k sono relativamente primi; dunque $rk_1 + f_k k_2 = 1$; calcolando in α_k si trova $k_1(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k)$ come inverso di $r(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k)$.

Il seguente risultato di Abel sarà fondamentale in tutta la nostra discussione.

2.3 Teorema. (ABEL) *Siano $g(x)$ e $p(x)$ sono due polinomi a coefficienti in* *un campo K con $p(x)$ irriducibile. Se $g(x)$ ammette una radice di $p(x)$, allora $p(x)$ divide $g(x)$, e quindi $g(x)$ ammette anche tutte le altre radici di $p(x)$.*

Dim. Se α è una radice comune dei due polinomi, il $MCD(g,p) = d(x)$ è divisibile per $x - \alpha$, e dunque non è costante. Poiché $d(x)$ si calcola a partire dai coefficienti dei due polinomi senza uscire da K (ad esempio con il metodo di Euclide), $d(x)$ è a coefficienti in K, e dunque, dividendo $p(x)$, coincide con esso (a meno di una costante). $\diamondsuit$

Una delle conseguenze di questo teorema è che non è possibile distinguere algebricamente un numero algebrico su un campo K dai suoi coniugati (radici dello stesso polinomio irriducibile): se infatti uno di questi è radice di un polinomio $g(x)$ su K anche gli altri lo sono. Ad esempio, non c'è modo di distinguere tra $\sqrt{2}$ e $-\sqrt{2}$: se uno di questi è radice di un polinomio $g(x)$ a coefficienti razionali anche l'altro lo è: sono infatti entrambi radici del polinomio irriducibile $x^2 - 2$ che per il teorema divide $g(x)$.

2.4 Lemma. *Sia φ come nel* Lemma 2.1. *Allora se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ il polinomio $r(x_1, x_2, \ldots, x_n)$ è il polinomio identicamente nullo.*

Dim. Il polinomio $r(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x)$ ha la la radice α_n in comune con $f_n(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x)$, che è irriducibile, e dunque è divisibile per questo polinomio. Ma essendo r di grado inferiore al grado di f_n ciò è possibile solo se r non dipende da x. Ne segue $r(x_1, x_2, \ldots, x_{n-1}, x) = r(x_1, x_2, \ldots, x_{n-1})$. Analogamente $r(\alpha_1, \alpha_2, \ldots, \alpha_{n-2}, x)$ ha una radice in comune con $f_{n-1}(\alpha_1, \alpha_2, \ldots, \alpha_{n-2}, x)$, e dunque è divisibile per questo polinomio. Ma essendo r di grado inferiore ciò è possibile solo se r non dipende da x. Proseguendo in questo modo r non dipende da alcuna variabile, e dunque è costante, ma essendo uguale a zero, questa costante è lo zero. $\diamondsuit$

2.5 Corollario. *Se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_k) = a \in K$, il polinomio $r(x_1, x_2, \ldots, x_n)$ del* Lemma 2.4 *è la costante a di K.*

Dim. Per il Lemma 2.4, il polinomio $r_1 = r - a$ relativo a $\varphi_1 = \varphi - a$ è il polinomio nullo. $\diamondsuit$

Siano ora $\alpha_{i_1} \in S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una radice di $f_1(x)$ (eventualmente la stessa α_1), $\alpha_{i_2} \in S \setminus \{\alpha_{i_1}\}$ una radice di $f_2(\alpha_{i_1}, x)$ (eventualmente la stessa α_2 se $\alpha_{i_1} \neq \alpha_2$),..., $\alpha_{i_k} \in S \setminus \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{n-1}}\}$ una radice di $f_n(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{n-1}}, x)$.

2.6 Lemma. *I polinomi $f_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}}, x)$ sono irriducibili sul campo $K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}})$, $k = 1, 2, \ldots, n$.*

Dim. $f_1(x)$ è irriducibile. Sia $f_2(\alpha_{i_1}, x) = g(\alpha_{i_1}, x)h(\alpha_{i_1}, x)$. Il polinomio $f_2(x_1, x) - g(x_1, x)h(x_1, x)$ in x_1 ha per ogni valore di x in K la radice α_{i_1}, e dunque è divisibile per $f_1(x_1)$. Ma allora ha anche la radice α_1, e dunque $f_2(\alpha_1, x) = g(\alpha_1, x)h(\alpha_1, x)$, che contraddice l'irriducibilità di $f_2(\alpha_1, x)$. Vediamo ora f_3; gli altri f_k si vedono in modo analogo. Se $f_3(\alpha_{i_1}, \alpha_{i_2}, x) = g(\alpha_{i_1}, \alpha_{i_2}, x)h(\alpha_{i_1}, \alpha_{i_2}, x)$, per ogni valore $x = a \in K$ il polinomio in x_2

$$f_3(\alpha_{i_1}, x_2, a) - g(\alpha_{i_1}, x_2, a)h(\alpha_{i_1}, x_2, a)$$

ammette la radice α_{i_2}, e dunque è divisibile per $f_2(\alpha_{i_1}, x_2)$ (che abbiamo appena visto essere irriducibile). Ne segue

$$f_3(\alpha_{i_1}, x_2, a) - g(\alpha_{i_1}, x_2, a)h(\alpha_{i_1}, x_2, a) - f_2(\alpha_{i_1}, x_2)h_2'(\alpha_{i_1}, x_2) = 0.$$

Per ogni $x_2 = b \in K$ si ha allora un polinomio che ammette la radice α_{i_1}, e perciò è divisibile per $f_1(x_1)$. Ma allora ammette anche la radice α_1:

$$f_3(\alpha_1, b, a) - g(\alpha_1, b, a)h(\alpha_1, b, a) - f_2(\alpha_1, b)h_2'(\alpha_1, b) = 0.$$

Ma ciò vale per ogni $b \in K$, e dunque identicamente

$$f_3(\alpha_1, x_2, a) = g(\alpha_1, x_2, a)h(\alpha_1, x_2, a) + f_2(\alpha_1, x_2)h_2'(\alpha_1, x_2).$$

Per $x_2 = \alpha_2$ si ha, essendo $f_2(\alpha_1, \alpha_2)$,

$$f_3(\alpha_1, \alpha_2, a) = g(\alpha_1, \alpha_2, a)h(\alpha_1, \alpha_2, a),$$

e ciò per ogni $a \in K$, e dunque identicamente

$$f_3(\alpha_1, \alpha_2, x) = g(\alpha_1, \alpha_2, x)h(\alpha_1, \alpha_2, x),$$

contro l'irriducibilità di $f_3(\alpha_1, \alpha_2, x)$. Si procede analogamente nel caso generale. $\diamondsuit$

2.7 Nota. I polinomi del Lemma 2.6 sono irriducibili ed essendo il campo a caratteristica zero sono separabili (hanno radici distinte).

2.8 Teorema. *Se* $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$, *allora* $\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}) = 0$.

Dim. La dimostrazione è analoga a quella del Lemma 2.6 per dimostrare l'irriducibilità dei polinomi $f_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}}, x)$.

Sia $k = 1$ e sia $\varphi(\alpha_1) = 0$. Vogliamo dimostrare che $\varphi(\alpha_{i_1}) = 0$. Avendosi $\varphi(\alpha_1) = 0$, $f_1(x)$ divide $\varphi(x)$: $\varphi(x) = f_1(x)q(x)$, da cui $\varphi(\alpha_{i_1}) = f_1(\alpha_{i_1})q(\alpha_{i_1}) = 0$.

Sia $k = 2$ e sia $\varphi(\alpha_1, \alpha_2) = 0$. Allora $\varphi(\alpha_1, x)$ ha la radice α_2 e dunque è divisibile per $f_2(\alpha_1, x)$:

$$\varphi(\alpha_1, x) = f_2(\alpha_1, x)q(\alpha_1, x),$$

e il polinomio differenza è il polinomio nullo:

$$\varphi(\alpha_1, x) - f_2(\alpha_1, x)q(\alpha_1, x) \equiv 0.$$

Allora il polinomio:

$$\varphi(x_1, x) - f_2(x_1, x)q(x_1, x),$$

ammette, per ogni valore $x = a \in K$ la radice α_1:

$$\varphi(\alpha_1, a) - f_2(\alpha_1, a)q(\alpha_1, a) = 0,$$

e perciò $\varphi(x_1, a) - f_2(x_1, a)q(x_1, a)$ è divisibile per $f_1(x_1)$. Ne segue che questo polinomio ammette anche la radice α_{i_1}:

$$\varphi(\alpha_{i_1}, a) - f_2(\alpha_{i_1}, a)q(\alpha_{i_1}, a) = 0.$$

Ma ciò vale per ogni $a \in K$, e dunque identicamente:

$$\varphi(\alpha_{i_1}, x) = f_2(\alpha_{i_1}, x)q(\alpha_{i_1}, x),$$

e pertanto, essendo α_{i_2} radice di $f_2(\alpha_{i_1}, x)$,

$$\varphi(\alpha_{i_1}, \alpha_{i_2}) = 0,$$

come richiesto. Analogamente per $k > 2$. $\diamondsuit$

Il Teor. 2.8 si inverte:

2.9 Teorema. *Se da ogni relazione*

$$\varphi(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0$$

segue la relazione

$$\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}) = 0,$$

allora α_{i_1} è radice di $f_1(x)$, α_{i_2} di $f_2(\alpha_{i_1}, x)$, $\ldots$, α_{i_k} di $f_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}}, x)$.

Dim. Poiché dalla relazione $f_1(\alpha_1) = 0$ segue per ipotesi $f_1(\alpha_{i_1}) = 0$, α_{i_1} è radice di $f_1(x)$. Analogamente, poiché dalla $f_k(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k) = 0$ segue $f_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}) = 0$, α_{i_k} è radice di $f_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}}, x)$. $\diamondsuit$

2.10 Teorema. *Le permutazioni delle α_i che mutano relazioni in relazioni formano gruppo.*

Dim. Se

$$\sigma = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_{i_1} & \alpha_{i_2} & \ldots & \alpha_{i_n} \end{pmatrix}, \quad \tau = \begin{pmatrix} \alpha_{i_1} & \alpha_{i_2} & \ldots & \alpha_{i_n} \\ \alpha_{j_1} & \alpha_{j_2} & \ldots & \alpha_{j_n} \end{pmatrix}$$

conservano le relazioni, dalla $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ segue $\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}) = 0$, e applicando τ a quest'ultima, $\varphi(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_n}) = 0$, risultato equivalente a quello ottenuto applicando a $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ il prodotto $\sigma\tau$. L'insieme delle permutazioni delle α_i che conservano le relazioni è chiuso rispetto al prodotto ed è dunque un gruppo (si ricordi che questo insieme di permutazioni è finito). $\diamondsuit$

2.11 Definizione. Il gruppo del Teor. 2.10 è il *gruppo di Galois* del polinomio $f(x)$.

2.12 Corollario. *La permutazione*

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_k & \ldots & \alpha_n \\ \alpha_{i_1} & \alpha_{i_2} & \ldots & \alpha_{i_k} & \ldots & \alpha_{i_n} \end{pmatrix} \tag{2.1}$$

appartiene al gruppo di Galois di $f(x)$ se e solo se α_{i_k} è una radice di $f_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}}, x)$, $k = 1, 2, \ldots, n$. $\diamondsuit$

Il grado n di $f(x)$, che dà il numero delle radici di $f(x)$ e dunque il numero di elementi su cui agisce il gruppo di Galois G, è il *grado di G*.

Per quanto riguarda l'ordine di G osserviamo che l'immagine di α_1 in (2.1) si può scegliere in $d_1 = \partial f_1$ modi, e per ciascuna di queste scelte vi sono $d_2 = \partial f_2$ scelte per α_{i_2},..., per ciascuna scelta di $\alpha_{i_{k-1}}$ vi sono d_k scelte per α_{i_k}.

2.13 Corollario. *L'ordine del gruppo di Galois è dato dal prodotto dei gradi dei polinomi f_k.* $\diamondsuit$

Il gruppo simmetrico S^n agisce sulle radici $\alpha_1, \alpha_2, \ldots, \alpha_n$ di $f(x)$. Se però si considera una funzione razionale $\gamma = \gamma(\alpha_1, \alpha_2, \ldots, \alpha_n)$ di queste radici, l'azione di $\sigma \in S^n$ su γ definita come l'azione indotta da quella di σ sulle radici,$\gamma^\sigma = \gamma(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$, non è detto che sia ben definita.

Si consideri il seguente esempio.

Esempio. Con $f(x) = x^4 - 2$, $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = -\alpha_1$, $\alpha_3 = i\alpha_1$, $\alpha_4 = -i\alpha_1$, l'elemento $\gamma = \sqrt{2} - 2$ è rappresentato da $\alpha_1^2 - 2$ e anche $\alpha_2^2 - 2$. Una permutazione σ che porti α_1 in α_2 e α_2 in α_3 fornisce per γ^σ due valori distinti: $\sqrt{2} - 2$ nel primo caso, $-\sqrt{2} - 2$ nel secondo.

Il punto è che se un elemento γ ha due diverse rappresentazioni come funzione razionale delle α_i, e siano $\gamma = g(\alpha_i)$ e $\gamma = h(\alpha_i)$, la differenza $g(\alpha_i) - h(\alpha_i) = 0$ è una relazione su K che se σ non appartiene al gruppo di Galois non viene in generale mutata, per azione di σ sulle α_i, ancora in una relazione, per cui $g(\alpha_{\sigma(i)}) - h(\alpha_{\sigma(i)}) \neq 0$, cioè $g(\alpha_{\sigma(i)}) \neq h(\alpha_{\sigma(i)})$. Il risultato dell'azione dipenderebbe quindi dalla rappresentazione di γ come funzione razionale delle α_i. Se invece σ appartiene al gruppo di Galois, allora σ muta la relazione suddetta ancora in una relazione: $g(\alpha_{\sigma(i)}) - h(\alpha_{\sigma(i)}) = 0$, e dunque $g(\alpha_{\sigma(i)}) = h(\alpha_{\sigma(i)})$. Il risultato dell'azione indotta su γ non dipende dalla rappresentazione di γ, e pertanto l'azione indotta è ben definita.

Nota. Per come è definito, è chiaro che il gruppo di Galois, come gruppo di permutazioni, dipende dall'ordinamento scelto per le radici. Se quest'ultimo viene modificato, e dall'ordinamento $\alpha_1, \alpha_2, \ldots, \alpha_n$ si passa a $\alpha_{\tau(1)}, \alpha_{\tau(2)}, \ldots, \alpha_{\tau(n)}$, per una certa permutazione τ delle n radici, allora se $G = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$, il nuovo gruppo sarà il *coniugato* di G: $\{\tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_2\tau, \ldots, \tau^{-1}\sigma_m\tau\}$, isomorfo a G.

2.2 I moduli fondamentali

Consideriamo i polinomi f_k del paragrafo precedente come polinomi dell'anello $A = K[x_1, x_2, \ldots, x_n]$. Sia $\varphi(x_1)$ un polinomio di A e dividiamolo per $f_1(x_1)$; otteniamo:

$$\varphi(x_1) = f_1(x_1)q(x_1) + r_1(x_1)$$

con $\partial r_1 < \partial f_1$. Analogamente, dividendo $\varphi(x_1, x_2) \in A$ per $f_2(x_1, x_2)$ considerati come polinomi in x_2, abbiamo $\varphi(x_1, x_2) = f_2(x_1, x_2)q_2(x_1, x_2) + r_2(x_1, x_2)$, con $\partial r_2 < \partial f_2$. Dividendo ora $r_2(x_1, x_2)$ come polinomio in x_1 per f_1 si ha un resto $r_3(x_1, x_2)$ con $\partial_{x_1} r_1 < \partial f_1$ e $\partial_{x_2} r_2 < \partial_{x_2} f_2$:

$$\varphi(x_1, x_2) = f_2(x_1, x_2)q_2(x_1, x_2) + f_1(x_1)q_1(x_1, x_2) + r_3(x_1, x_2).$$

In generale:

$$\begin{aligned} \varphi(x_1, x_2, \ldots, x_k) \;=\;& f_1(x_1)q_1(x_1, x_2, \ldots, x_k) \\ +\;& f_2(x_1, x_2)q_2(x_1, x_2, \ldots, x_k) \\ \vdots\;& \\ +\;& f_k(x_1, x_2, \ldots, x_k)q_k(x_1, x_2, \ldots, x_k) \\ +\;& r_k(x_1, x_2, \ldots, x_k), \end{aligned}$$

con $\partial_{x_i} r_k < \partial_{x_i} f_i$, $i = 1, 2, \ldots, k$. Si scrive anche:

$$\varphi(x_1, x_2, \ldots, x_k) \equiv r_k(x_1, x_2, \ldots, x_k) \bmod f_1, f_2, \ldots f_k.$$

2.14 Definizione. I polinomi

$$f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \ldots, x_n)$$

sono i *moduli fondamentali* di $f(x)$.

Se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0$ il polinomio $r_k(x_1, x_2, \ldots, x_k)$ è identicamente nullo (Lemma 2.4). Abbiamo allora il seguente teorema.

2.15 Teorema. *Ogni polinomio $\varphi(x_1, x_2, \ldots, x_k)$ in k indeterminate tale che $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0$ si scrive nella forma:*

$$\begin{aligned}\varphi(x_1, x_2, \ldots, x_k) &= f_1(x_1)q_1(x_1, x_2, \ldots, x_k) \\ &+ f_2(x_1, x_2)q_2(x_1, x_2, \ldots, x_k) \\ &\vdots \\ &+ f_k(x_1, x_2, \ldots, x_k)q_k(x_1, x_2, \ldots, x_k)\end{aligned}$$

dove i q_i sono polinomi nelle x_i e gli f_i, $i = 1, 2, \ldots, k$, i primi k moduli fondamentali del polinomio $f(x)$. ♢

I polinomi $\varphi(x_1, x_2, \ldots, x_n)$ tali che $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ formano un ideale di A, l'*ideale delle relazioni*. Il Teor. 2.15 si può dunque enunciare dicendo che *i moduli fondamentali del polinomio $f(x)$ sono una base per l'ideale delle relazioni tra le radici di $f(x)$*.

Dal Teor. 2.15 si ha inoltre che se una permutazione delle α_i conserva le relazioni:

$$f_1(\alpha_1) = 0,\ f_2(\alpha_1, \alpha_2) = 0, \ldots,\ f_n(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0 \tag{2.2}$$

allora conserva ogni relazione $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ tra le α_i. Viceversa, se una permutazione conserva ogni relazione tra le α_i conserva in particolare le (2.2). Le infinite relazioni su K tra le α_i si riportano così a un numero finito. Abbiamo quindi:

2.16 Corollario. *Il gruppo di Galois di $f(x)$ consta delle permutazioni delle α_i che conservano le relazioni* (2.2). ♢

Dal teorema delle funzioni simmetriche (Teor. 1.5) segue che se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) - a$ è una funzione simmetrica delle α_i, allora a appartiene al campo K. Infatti per il teorema detto φ è un polinomio a coefficienti in K nelle funzioni simmetriche elementari delle α_i, e queste sono i coefficienti e_i del polinomio $f(x)$. Ma le e_i sono elementi di K e dunque a, come polinomio a coefficienti in K delle e_i, appartiene anch'esso a K. Questo fatto viene generalizzato da Galois nel senso che non è necessario che il valore a di φ resti invariato per tutte le permutazioni delle α_i; basta che resti invariato per le permutazioni delle α_i che appartengono al gruppo di Galois di $f(x)$.

2.17 Teorema. *Se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = a$, e questo valore resta invariato per le permutazioni del gruppo di Galois, allora $a \in K$. In particolare, se il gruppo di*

Galois si riduce all'identità allora le α_i appartengono a K e dunque il polinomio si spezza in fattori lineari su K.

Dim. Si ha:

$$\begin{aligned} \varphi(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x) &= f_n(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x) q(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x) \\ &+ r(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x), \end{aligned}$$

con $\partial r < \partial f_n = 1$, e dunque r è costante e pertanto non dipende da x. Calcolando in α_n si ha $f_n = 0$ e

$$a = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) = r(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}).$$

Supponiamo allora, per induzione, $a = r(\alpha_1, \alpha_2, \ldots, \alpha_{n-k})$, e dimostriamo che $r(\alpha_1, \alpha_2, \ldots, \alpha_{n-k}) = r(\alpha_1, \alpha_2, \ldots, \alpha_{n-(k+1)})$. Dividiamo per f_{n-k}:

$$\begin{aligned} r(\alpha_1, \alpha_2, \ldots, \alpha_{n-k-1}, x) &= f_{n-k}(\alpha_1, \alpha_2, \ldots, \alpha_{n-k-1}, x) q(\alpha_1, \alpha_2, \ldots, \alpha_{n-k-1}, x) \\ &+ r'(\alpha_1, \alpha_2, \ldots, \alpha_{n-k-1}, x), \end{aligned}$$

con $\partial f_{n-k} = d \leq k$ e $\partial r' < d$. Il gruppo di Galois contiene le permutazioni che fissano $\alpha_1, \alpha_2, \ldots, \alpha_{n-(k+1)}$ e portano α_{n-k} in una delle d radici di f_{n-k}:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_{n-(k+1)} & \alpha_{n-k} & \alpha_{n-(k-1)} & \ldots \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{n-(k+1)} & \alpha_{i_{n-k}} & \ldots & \ldots \end{pmatrix}$$

Poiché il valore $a = r(\alpha_1, \alpha_2, \ldots, \alpha_{n-(k+1)}, \alpha_{n-k})$ non cambia sostituendo α_{n-k} con una delle d radici di f_{n-k}, e poiché f_{n-k} si annulla su queste radici, il resto $r'(\alpha_1, \alpha_2, \ldots, \alpha_{n-(k+1)}, x)$, di grado minore di d assume lo stesso valore su d punti diversi, e dunque non dipende da x. $\diamondsuit$

Il Teor. 2.17 si inverte:

2.18 Teorema. *Se $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = a \in K$, allora il valore a non cambia permutando le α_i secondo gli elementi del gruppo di Galois. In particolare, se il polinomio $f(x)$ si spezza in fattori lineari su K, allora il suo gruppo di Galois si riduce all'identità.*

Dim. La relazione $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) - a = 0$ è a coefficienti in K e si muta ancora in una relazione per una qualunque permutazione del gruppo di Galois: $\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}) - a = 0$, cioè $\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}) = a$.

In particolare, se $f(x) = \prod_{i=1}^{n}(x - c_i)$, $c_i \in K$, si ha $\alpha_i - c_i = 0$, $i = 1, 2, \ldots, n$, e un elemento del gruppo di Galois deve mutare queste relazioni ancora in relazioni. Ma se un elemento σ del gruppo porta una radice α_i in $\alpha_j \neq \alpha_i$, si ha $\alpha_j - c_i \neq 0$. Dunque $\alpha_{\sigma(i)} = \alpha_i$, per ogni i, e σ è l'identità. $\diamondsuit$

Se $\alpha_i = a \notin K$ allora esiste almeno una permutazione del gruppo di Galois che porta α_i in una $\alpha_j \neq \alpha_i$, e muta quindi una relazione in cui compare α_i in una in cui compare α_j. Le $\alpha_i \notin K$ non possono quindi essere individuate dalle relazioni che esse soddisfano.

2.19 Definizione. Un gruppo di permutazioni $G \subseteq S^n$ si dice *transitivo* se dati comunque i, j esiste $\sigma \in G$ che porta i su j. Si dice $k-$ *transitivo* se date comunque due $k-$ple (ordinate) di elementi distinti $(i_1, i_2, \dots, i_k)$ e $(j_1, j_2, \dots, j_k)$ esiste una permutazione di G che porta i_1 su j_1, i_2 su j_2,...,i_k su j_k.

2.20 Teorema. *Il gruppo di Galois G è k–transitivo se e solo se i moduli fondamentali $f_1, f_2, \dots, f_k$ coincidono ordinatamente con i moduli di Cauchy $X_1, X_2, \dots, X_k$.*

Dim. Sia $k = 1$. Se G è transitivo, tutte le radici di $f(x)$ sono anche radici di $f_1(x)$ e dunque, poiché f_1 divide f, $f_1 = f$, cioè f è irriducibile. Inoltre, essendo $f = X_1$, si ha $f_1 = X_1$.

Sia $k = 2$, e G 2–transitivo. Allora data comunque la coppia α_i, α_j esiste una permutazione:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_i & \alpha_j & \dots & \dots & \dots \end{pmatrix},$$

ed essendo α_i una qualunque delle n radici di $f(x)$, $f_1(x)$ ha n radici e dunque grado n, e coincide perciò con $f(x) = X_1$. α_j deve essere radice di $f_2(\alpha_i, x)$,e può essere una qualunque delle $n-1$ radici di $f(x)$ diverse da α_i. Dunque $f_2(\alpha_i, x)$ ha grado $n-1$ e concide quindi con X_2.

Viceversa, se $f_1 = X_1 = f$ e $f_2 = X_2$, dati α_{i_1} e α_{i_2} esiste una permutazione di G che porta α_1 in α_{i_1}, e tra tutte queste almeno una che porta α_2 in α_{i_2}. Dunque G è $2-$transitivo.

In generale, se G è $k-$transitivo la $k-$pla $\alpha_1, \alpha_2, \dots, \alpha_k$ può andare, ordinatamente, su una qualunque altra $k-$pla $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}$. Poiché allora vi sono n scelte per l'immagine α_{i_1} di α_1, e poiché queste immagini sono radici di f_1, f_1 ha grado n e perciò coincide con $f = X_1$. inoltre α_{i_2} deve essere radice di $f_2(\alpha_{i_1}, x)$, e poiché vi sono $n-1$ scelte per α_{i_2}, f_2 ha grado $n-1$ e coincide quindi con X_2. In generale, scelte le immagini di $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$, vi sono $n-k$ scelte per α_{i_k}; queste ultime sono radici di $f_k(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_{k-1}}, x)$, che dunque ha grado $n-k$ e pertanto coincide con X_k.

Viceversa, se $f_1 = f = X_1, f_2 = X_2, \dots, f_k = X_k$, poiché allora l'immagine α_{i_1} di α_1 può essere una qualunque delle n radici di f, l'immagine α_{i_2} di α_1 una qualunque delle $n-1$ radici di f_2,...,l'immagine α_{i_k} di α_1 una qualunque delle $n-(k-1)$ radici di f_k, esiste una permutazione di G che porta ordinatamente la $k-$pla $\alpha_1, \alpha_2, \dots, \alpha_k$ su una qualunque altra $k-$pla $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}$. Dunque G è $k-$transitivo. $\diamondsuit$

Il solo gruppo $n-$transitivo su n elementi è il gruppo simmetrico; ne segue:

2.21 Corollario. *Il gruppo di Galois di un polinomio $f(x)$ è l'intero gruppo simmetrico se e solo se i moduli fondamentali e i moduli di Cauchy di $f(x)$ concidono: $f_k = X_k,\ k = 1, 2, \ldots, n$.*

2.22 Esempi. 1. Consideriamo il polinomio $f(x) = x^4 - 2$ sul campo razionale $\mathcal{Q}$. Le sue radici sono:

$$\alpha_1 = \sqrt[4]{2},\ \alpha_2 = -\alpha_1,\ \alpha_3 = i\alpha_1,\ \alpha_4 = -i\alpha_1.$$

Poiché $f(x)$ è irriducibile, $f_1(x) = f(x)$. Abbiamo intanto la relazione $\alpha_1^4 - 2 = 0$. La fattorizzazione in $\mathcal{Q}(\alpha_1)$ è $f(x) = (x - \alpha_1)(x + \alpha_1)(x^2 + \alpha_1^2)$. Il polinomio che ammette la radice α_2 è $x + \alpha_1$; dunque $f_2(\alpha_1, x) = x + \alpha_1$, che dà la relazione $\alpha_2 + \alpha_1 = 0$. Aggiungendo α_2 a $\mathcal{Q}(\alpha_1)$ si ottiene di nuovo $\mathcal{Q}(\alpha_1)$ per cui $x^2 + \alpha_1^2$ resta irriducibile, ed è il fattore che ammette la radice α_3. Aggiungendo ora α_3 il polinomio si spezza completamente in fattori lineari $f(x) = (x - \alpha_1)(x + \alpha_1)(x - \alpha_3)(x + \alpha_3)$, e $f_4(\alpha_1, \alpha_2, \alpha_3, x) = x + \alpha_3$, che dà la relazione $\alpha_4 + \alpha_3 = 0$. Si verifica facilmente che le pemutazioni di S^4 che conservano tutte e quattro le relazioni:

$$\alpha_1^4 = 2,\ \alpha_2 + \alpha_1 = 0,\ \alpha_3^2 + \alpha_1^2 = 0,\ \alpha_4 + \alpha_3 = 0$$

sono le

$$I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1)(2)(3,4), (1,2)(3)(4), (1,3,2,4), (1,4,2,3),$$

che costituiscono uno dei tre gruppi diedrali D_4 contenuti in S^4. Questo D_4 è dunque il gruppo di Galois del polinomio $x^4 - 2$ su $\mathcal{Q}$. Vediamo ora come esprimere una relazione in termini delle quattro trovate, ad esempio la $\alpha_1\alpha_2 + \alpha_3\alpha_4 = 0$, che si verifica subito essere conservata da D_4. Dividiamo il polinomio $x_1x_2 + x_3x_4$ come polinomio in x_4 per l'ultimo modulo fondamentale $f_4(x_1, x_2, x_3, x_4) = x_4 + x_3$, anch'esso considerato come polinomio in x_4; si ha:

$$x_3x_4 + x_1x_2 = (x_4 + x_3)x_3 - x_3^2 + x_1x_2.$$

Dividiamo ora il resto $-x_3^2 + x_1x_2$ come polinomio in x_3 per $f_3 = x_3^2 - x_1x_2$:

$$-x_3^2 + x_1x_2 = (x_3^2 - x_1x_2) \cdot (-1) + 0,$$

che sostituito nella precedente dà l'espressione richiesta:

$$x_1x_2 + x_3x_4 = (x_4 + x_3)x_3 + (x_3^2 - x_1x_2) \cdot (-1),$$

cioè $f_4 \cdot x_3 + f_3 \cdot (-1)$ (i q_i del Teor. 2.15 sono ora $q_1 = q_2 = 0, q_3 = -1, q_4 = x_3$). La corrispondente espressione nelle α_i è

$$\alpha_1\alpha_2 + \alpha_3\alpha_4 = (\alpha_4 + \alpha_3)\alpha_3 + (\alpha_3^2 - \alpha_1\alpha_2) \cdot (-1),$$

cioè $f_4(\alpha_4)\cdot\alpha_3 + f_3(\alpha_3)\cdot(-1)$.

Come altro esempio consideriamo la relazione $\alpha_2\alpha_4 - \alpha_1\alpha_3 = 0$. Si ha:

$$x_2x_4 - x_1x_3 = (x_4 + x_3)x_2 - (x_1 + x_2)x_3.$$

Il resto r è di grado 1 in x_3, mentre f_3 è di grado 2 in x_3. La divisione di r per f_3 dà quoziente zero e resto lo stesso r. Considerando allora r come polinomio in x_2 e dividendo per f_2 abbiamo $-x_3x_2 - x_1x_3 = (x_2 + x_1)(-x_3) + 0$, da cui $x_2x_4 - x_1x_3 = (x_4+x_3)x_2+(x_2+x_1)(-x_3)$, con $q_4 = x_2, q_3 = 0, q_2 = -x_3, q_1 = 0$. Infine,

$$\alpha_2\alpha_4 - \alpha_1\alpha_3 = (\alpha_4 + \alpha_3)\alpha_2 + (\alpha_2 + \alpha_1)(-\alpha_3).$$

2. Sia $f(x) = x^8 - 1$ su $\mathcal{Q}$. Si tratta di un polinomio riducibile su $\mathcal{Q}$:

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$$

le cui radici sono:

$$\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = i, \alpha_4 = -i, \alpha_5 = \sqrt{i}, \alpha_6 = -\sqrt{i}, \alpha_7 = \sqrt{-i}, \alpha_8 = -\sqrt{-i}.$$

Si ha, con le relative relazioni:

$f_1(x) = x - 1,\ \alpha_1 - 1 = 0$
$f_2(\alpha_1, x) = x + \alpha_1,\ \alpha_2 + 1 = 0;$
$f_3(\alpha_1, \alpha_2, x) = x^2 + 1,\ \alpha_3^2 + 1 = 0;$
$f_4(\alpha_1, \alpha_2, \alpha_3, x) = x + \alpha_3,\ \alpha_4 + \alpha_3 = 0.$

Il fattore irriducibile su $\mathcal{Q}(i)$ che ha la radice $\alpha_5 = \sqrt{i}$ è $x^2 - i$ in quanto $x^4 + 1$ si spezza su $\mathcal{Q}(i)$ in $(x^2 - i)(x^2 + i)$:

$f_5(\alpha_1, \ldots, \alpha_4, x) = x^2 - \alpha_3,\ \alpha_5^2 - \alpha_3 = 0.$

Aggiungendo $\sqrt{i}$ resta il fattore $x + \sqrt{i}$, irriducibile su $\mathcal{Q}(i, \sqrt{i}) = \mathcal{Q}(\sqrt{i})$:

$f_6(\alpha_1, \ldots, \alpha_5, x) = x + \alpha_5,\ \alpha_6 + \alpha_5 = 0.$

Ma su $\mathcal{Q}(\sqrt{i})$ si spezza anche $x^2 + i$, in quanto $\sqrt{-i} = i\sqrt{i}$, e perciò $x^2 + i = (x - \sqrt{-i})(x + \sqrt{-i})$:

$f_7(\alpha_1, \ldots, \alpha_6, x) = x - i\sqrt{i} = x - \alpha_3\alpha_5,\ \alpha_7 - \alpha_3\alpha_5 = 0.$

Infine,

$f_8(\alpha_1, \ldots, \alpha_7, x) = x + i\sqrt{i} = x + \alpha_7 = x + \alpha_3\alpha_5,\ \alpha_8 + \alpha_3\alpha_5 = 0.$

Il gruppo che conserva le otto relazioni è il gruppo di Klein, di ordine 4:

$$G = \{I, (1)(2)(3,4)(5,8)(6,7), (1)(2)(3,4)(5,7)(6,8), (1)(2)(3)(4)(5,6)(7,8)\}.$$

Si osservi che le cifre 1 e 2 sono fissate da ogni elemento di G, ciò che corrisponde al fatto che $\alpha_1 = 1$ e $\alpha_2 = -1$ appartengono a $\mathcal{Q}$. Inoltre, il gruppo ha quattro orbite: due corrispondenti alle radici razionali, cioè ai due fattori irriducibili $x-1$ e $x+1$, le orbite $\{1\}$ e $\{-1\}$, e le altre due $\{3,4\}$ e $\{5,6,7,8\}$ corrispondenti alle radici degli altri due fattori.

Se consideriamo come $f_3(\alpha_1, \alpha_2, x)$ il polinomio x^4+1 invece di x^2+1, aggiungendo la radice $\sqrt{i}$ il polinomio $f(x)$ si spezza completamente, e con calcoli analoghi si trova che il gruppo è

$$G_1 = \{I, (1)(2)(3,6)(4,5)(7,8), (1)(2)(7,8)(3,5)(4,6), (1)(2)(7)(8)(3,4)(5,6)\},$$

coniugato del precedente tramite la permutazione:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 8 & 3 & 4 & 5 & 6 \end{pmatrix}$$

che esprime il passaggio dall'ordinamento delle α_i indicato dalla prima riga di σ a quello indicato dalla seconda.

Le otto radici α_i sono tutte potenze della radice primitiva $\zeta = \sqrt{i}$, che abbiamo denotato con α_5. Il gruppo di Galois che abbiamo visto consta delle permutazioni indotte dalle quattro corrispondenze:

$$\sigma_k : \zeta^i \longrightarrow (\zeta^i)^k, \quad i = 1, 2, \ldots, 8, \quad (\text{mod } 8),$$

per $k = 1, 3, 5, 7$. Così ad esempio si ha per σ_3:

$$\begin{array}{rcl} \zeta \longrightarrow \zeta^3 \longrightarrow \zeta^9 & = & \zeta, \\ \zeta^2 \longrightarrow \zeta^6 \longrightarrow \zeta^{18} & = & \zeta^2, \\ \zeta^4 \longrightarrow \zeta^{12} = \zeta^4, & & \\ \zeta^5 \longrightarrow \zeta^{15} = \zeta^7 \longrightarrow \zeta^{21} & = & \zeta^5 \\ \zeta^8 = 1 \longrightarrow 1 & & , \end{array}$$

cioè la permutazione (1)(2)(3,4)(5,8)(6,7) delle α_i, e analogamente per le altre σ_k.

3. Determiniamo il gruppo di Galois G del polinomio ciclotomico su $\mathcal{Q}$:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

con p primo, a partire dai suoi moduli fondamentali. Consideriamo dapprima il caso particolare $p = 5$; le radici del polinomio sono allora le quattro radici quinte dell'unità: $\alpha_1 = \epsilon, \alpha_2 = \epsilon^2, \alpha_3 = \epsilon^3, \alpha_4 = \epsilon^4$, (con $\epsilon = e^{\frac{2i\pi}{5}}, \epsilon^5 = 1$, una qualunque delle radici dà con le sue potenze tutte le altre). In $\mathcal{Q}(\epsilon)$ il polinomio $\Phi_p(x)$ si spezza completamente: $\Phi_p(x) = (x-\epsilon)(x-\epsilon^2)(x-\epsilon^3)(x-\epsilon^4)$. I moduli fondamentali sono:

$f_1(x) = \Phi_p(x)$, radice α_1, $\alpha_1^4 + \alpha_1^3 + \alpha_1^2 + \alpha_1^1 + 1 = 0$;

$f_2(\alpha_1, x) = x - \alpha_1^2$, radice α_2, $\alpha_2 - \alpha_1^2 = 0$;

$f_3(\alpha_1, \alpha_2, x) = x - \alpha_1^3$, radice α_3, $\alpha_3 - \alpha_1^3 = 0$;

$f_4(\alpha_1, \alpha_2, \alpha_3, x) = x - \alpha_1^4$, radice α_4, $\alpha_4 - \alpha_1^4 = 0$.

Il prodotto dei gradi di questi polinomi è $4 \cdot 1 \cdot 1 \cdot 1$, e dunque il gruppo di Galois ha ordine 4. Vediamo quali sono le permutazioni $\sigma \in S^4$ che lasciano invariate le quattro relazioni viste sopra. Sia $\sigma(1) = 2$ (cioè $\sigma(\alpha_1 = \alpha_{\sigma(1)} = \alpha_2)$; dimostriamo che allora le immagini di tutte le altre radici sono determinate. Dalla seconda relazione abbiamo:

$$\alpha_{\sigma(2)} - \alpha_{\sigma(1)}^2 = \alpha_{\sigma(2)} - \alpha_2^2 = \alpha_{\sigma(2)} - \alpha_1^4 = 0,$$

e dunque l'immagine di 2 è 4. Analogamente, dalla terza relazione si ha che 3 va in 1, e infine 4 in 3. L'immagine 2 di 1 determina dunque il ciclo (1,2,4,3). Se $\sigma(1) = 3$ si ha il ciclo inverso del precedente (1,3,4,2), e infine $\sigma(1) = 4$ determina l'involuzione (1,4)(2,3). Il gruppo di Galois del polinomio è dunque il gruppo ciclico di ordine 4

$$C_4 = \{I, \sigma = (1,3,2,4), \sigma^2 = (1,2)(3,4), \sigma^3 = (1,4,2,3)\}.$$

La relazione $\alpha_3 - \alpha_1\alpha_2 = 0$ è invariante per σ (e quindi per tutte le sue potenze). La relazione si trasforma infatti in $\alpha_1 - \alpha_2\alpha_4 = \epsilon - \epsilon^2\epsilon^4 = \epsilon - \epsilon^6 = \epsilon - \epsilon = 0$.

Scriviamo il polinomio $x_3 - x_1x_2$ in termini dei moduli fondamentali. Poiché x_4 non compare dividiamo per $f_3 = x_3 - x_1^3$ come polinomi in x_3. Otteniamo quoziente 1 e resto $-x_1x_2 + x_1^3$. Diviamo ora questo resto per $f_2 = x_2 - x_1^2$ come polinomi in x_2; si ottiene quoziente $-x_1$ e resto zero. Dunque,

$$x_3 - x_1x_2 = (x_3 - x_1^3) \cdot 1 + (x_2 - x_1^2) \cdot (-x_1).$$

In generale, per il polinomio $\Phi_p(x)$ e con le radici $p-$esime dell'unità $\alpha_k = \epsilon^k$, $k = 1, 2, \ldots, p-1$, abbiamo i polinomi $f_k = x_k - \alpha_1\alpha_{k-1}$ e le relazioni $\alpha_k - \alpha_1\alpha_{k-1} = 0$, $(\alpha_0 = 1)$. Il gruppo ha quindi ordine $(p-1) \cdot 1 \cdot 1 \cdots 1 = p-1$. Sia s una radice primitiva della congruenza $x^{p-1} - 1 \equiv 0 \bmod p$; le cifre $1, 2, \ldots, p-1$ sono in un certo ordine le potenze $1, , g^2, \ldots, g^{p-2}$. La corrispondenza $\sigma : \alpha \to \alpha^g$ ha ordine $p-1$ (in quanto $g^{p-1} \equiv 1 \bmod p$) e induce la permutazione ciclica $\alpha \to \alpha^g \to \alpha^{g^2} \to \cdots \to \alpha^{g^{p-2}} \to \alpha^{g^{p-2}} = \alpha$. Le $p-1$ potenze di σ esauriscono il gruppo di Galois, che dunque è ciclico di ordine $p-1$, ed è generato da un ciclo di ordine $p-1$. In particolare il gruppo è transitivo, e dunque $\Phi_p(x)$ è irriducibile (come d'altra parte si può verificare direttamente sostituendo x con $x+1$ e applicando il criterio di Eisenstein; v. oltre, Teor. 3.13). Nel caso precedente $(p = 5)$, una radice primitiva è $g = 2$, che con le sue potenze dà $2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 3, 2^4 = 16 \equiv 1 \bmod 5$, cioè il ciclo (1,2,4,3). Anche 3 è una radice primitiva e fornisce il ciclo inverso (1,3,4,2) (si noti che 3 è l'inverso di 2 mod 5).

2.3 Riduzione del gruppo di Galois

(D'ora in poi scriveremo $\underline{\alpha}$ per indicare l'insieme delle radici $\alpha_1, \alpha_2, \ldots, \alpha_n$). Le permutazioni di S^n che lasciano invariato il valore numerico di una funzione razionale delle radici di un polinomio $f(x)$ non formano in generale un gruppo.

2.23 Esempio. Con $f(x)$ come nell'Es. 1 di 2.22, siano $\gamma = \alpha_1^2$ e $\sigma = (1,2,3)(4)$. Il valore $\sqrt{2}$ di α_1^2 resta invariato: $\alpha_{\sigma(1)}^2 = \alpha_2^2 = \sqrt{2}$. Ma $\alpha_{\sigma^{-1}(1)} = \alpha_3^2 = -\sqrt{2}$. L'insieme delle permutazioni che lasciano invariato il valore di γ contiene σ ma non σ^{-1}, e dunque non è un gruppo.

Se però ci si limita alle permutazioni appartenenti al gruppo di Galois di $f(x)$ si ottiene un gruppo.

2.24 Teorema. *L'insieme G_γ degli elementi del gruppo di Galois G di un polinomio $f(x)$ che lasciano invariato il valore numerico di una funzione razionale $\gamma = \gamma(\underline{\alpha})$ delle radici di $f(x)$ è un sottogruppo di G.*

Dim. Dimostriamo che se σ e τ sono elementi di G che lasciano invariato il valore di γ, anche il loro prodotto lascia invariato il valore di γ (essendo G_γ finito, ciò implica che G_γ è un sottogruppo). Se $\gamma^\sigma = \gamma(\underline{\alpha}^\sigma) = \gamma$, allora $\gamma^\sigma - \gamma = 0$ è una relazione tra le radici di $f(x)$ e dunque τ, come elemento di G, la conserva: $0 = \gamma^{\sigma\tau} - \gamma^\tau = \gamma^{\sigma\tau} - \gamma$. Ne segue $\gamma^{\sigma\tau} = \gamma$, e anche $\sigma\tau$ fissa γ. $\diamondsuit$

Sia ancora $\gamma = \gamma(\underline{\alpha})$ una funzione razionale delle radici di $f(x)$. Ci proponiamo di determinare il gruppo di Galois G_1 di $f(x)$ su $K(\gamma)$, considerando cioè $f(x)$ a coefficienti in $K(\gamma)$. Per il Teor. 2.18 gli elementi di G_1 devono lasciare fisso il valore di γ, e dunque $G_1 \subseteq G_\gamma$. D'altra parte se $\sigma \in G_\gamma$ e $h(\underline{\alpha})$ è una funzione razionale $\vartheta(\gamma)$ di γ a coefficienti in K, si ha $h = \vartheta(\gamma) = \vartheta(\varphi(\underline{\alpha})) = \vartheta_1(\underline{\alpha})$ con ϑ_1 a coefficienti in K. La differenza $h - \vartheta_1$ è zero, e questo valore zero si conserva applicando σ:

$$0 = h^\sigma - \vartheta_1^\sigma = h^\sigma - \vartheta(\gamma^\sigma) = h^\sigma - \vartheta(\gamma) = h^\sigma - h,$$

ovvero $h^\sigma = h$ e $G_\gamma \subseteq G_1$. Si ha così il teorema:

2.25 Teorema. *Se si amplia il campo K aggiungendo una funzione razionale γ a coefficienti in K delle radici di $f(x)$ il gruppo di Galois di $f(x)$ sul campo ampliato $K(\gamma)$ si abbassa al sottogruppo G_γ.*

2.26 Corollario. (LAGRANGE) *Se $\eta = \eta(\underline{\alpha})$ non cambia il proprio valore numerico permutando le α_i secondo gli elementi di G_γ, cioè se $G_\gamma \subseteq G_\eta$, allora $\eta = \vartheta(\gamma)$, dove ϑ è a coefficienti in K, e dunque $K(\eta) \subseteq K(\gamma)$.*

Dim. $K(\gamma)$ consta degli elementi di $K(\underline{\alpha})$ che conservano il proprio valore numerico sotto l'azione degli elementi di G_γ. Dunque $\eta \in K(\gamma)$. $\diamondsuit$

In particolare,

2.27 Corollario. *Se $G_\gamma = \{1\}$ allora*

$$K(\underline{\alpha}) = K(\gamma). \tag{2.3}$$

Ogni elemento di $K(\underline{\alpha})$ è cioè una funzione razionale (polinomio) di γ a coefficienti in K. In particolare ciò accade per le radici α_i:

$$\alpha_1 = \vartheta_1(\gamma),\ \alpha_2 = \vartheta_2(\gamma), \ldots,\ \alpha_n = \vartheta_n(\gamma). \quad \diamondsuit \tag{2.4}$$

2.28 Definizione. Un elemento γ tale che sussista la (2.3) o la (2.4) è un elemento *primitivo* del campo $K(\underline{\alpha})$.

Il Cor. 2.27 si inverte. Se infatti γ è primitivo e $\gamma^\sigma = \gamma$, dalle (2.4) segue $\alpha_i^\sigma = \vartheta_i(\gamma^\sigma) = \vartheta_i(\gamma) = \alpha_i$, per ogni $i = 1, 2, \ldots, n$, e dunque $\sigma = 1$. Abbiamo così:

2.29 Teorema. *γ è primitivo se e solo se $G_\gamma = \{1\}$.* $\diamondsuit$

2.30 Corollario. *γ è primitivo se e solo se le sue immagini secondo gli elementi di G sono tutte distinte.*

Dim. Se γ è primitivo, $G_\gamma = \{1\}$, e dunque poiché da $\gamma^\sigma = \gamma^\tau$ segue $\gamma^{\sigma\tau^{-1}} = \gamma$, si ha $\sigma\tau^{-1} = 1$ e $\sigma = \tau$. Viceversa, se le immagini sono tutte distinte $\gamma^\sigma = \gamma = \gamma^1$ implica $\sigma = 1$, e perciò $G_\gamma = \{1\}$. $\diamondsuit$

Un elemento primitivo esiste sempre, e si può costruire in questo modo. Si considerino i polinomi $\alpha_1 + \alpha_2 x + \cdots + \alpha_n x^{n-1}$ e $\alpha_{i_1} + \alpha_{i_2} x + \cdots + \alpha_{i_n} x^{n-1}$ per le distinte permutazioni di G. Nessuna delle differenze $(\alpha_1 - \alpha_{i_1}) + (\alpha_2 - \alpha_{i_2})x + \cdots + (\alpha_n - \alpha_{i_n})x^{n-1}$ è il polinomio nullo, e dunque esistono valori di x per i quali nessuno di questi polinomi si annulla. Se $x = c \in K$ è uno di questi valori, l'elemento $\gamma = \alpha_1 + \alpha_2 c + \cdots + \alpha_n c^{n-1}$ è fissato solo dall'identità di G, e quindi per il Teor. 2.29 γ è primitivo. Si osservi che potendo scegliersi c in infiniti modi, esistono infiniti elementi primitivi.

2.31 Esempio. Consideriamo il polinomio $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$; le radici sono dunque $\alpha_{1,2} = \pm\sqrt{2}, \alpha_{3,4} = \pm\sqrt{3}$. Sia $f_1(x) = x^2 - 2$, e la relazione $\alpha_1^2 - 2 = 0$. In $\mathcal{Q}(\sqrt{2})$ il polinomio $f(x)$ si spezza in $(x - \sqrt{2})(x + \sqrt{2})(x^2 - 3)$, e dunque $f_2(\sqrt{2}, x) = x + \sqrt{2}$, e la relazione $\alpha_2 + \alpha_1 = 0$. Aggiungendo $-\sqrt{2}$ il campo resta lo stesso, e quindi $f_3(\sqrt{2}, -\sqrt{2}, x) = x^2 - 3$, e la relazione $\alpha_3^2 - 3 = 0$. Su $\mathcal{Q}(\sqrt{2}, \sqrt{3})$ il polinomio si spezza completamente, e $f_4(\sqrt{2}, -\sqrt{2}, \sqrt{3}, x) = x + \sqrt{3}$, e si ha la relazione $\alpha_4 + \alpha_3 = 0$. Il gruppo di Galois è $G = \{I, (1,2)(3,4), (1,2)(3)(4), (1)(2)(3,4)\}$.

Sia $\gamma = \alpha_1 + \alpha_3 = \sqrt{2} + \sqrt{3}$. Nessun elemento del gruppo di Galois conserva il valore di γ. Dunque $G_\gamma = \{1\}$, e γ è primitivo: $\mathcal{Q}(\sqrt{2}, \sqrt{3}) = \mathcal{Q}(\sqrt{2} + \sqrt{3})$. Il polinomio minimo di γ è $x^4 - 10x^2 + 1$; aggiungendo $\sqrt{2} + \sqrt{3}$ esso si spezza completamente: $(x - (\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (\sqrt{3} - \sqrt{2}))$.

Sia $\gamma = \sqrt{2}$; si ha $\gamma = ((\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3}))/2$, e poiché scambiando $\sqrt{3}$ con $-\sqrt{3}$, cioè α_3 con α_4, il valore di γ non cambia, mentre cambia per altre permutazioni di G, è $G_\gamma = \{I, (1)(2)(3,4)\}$.

Dato ora un elemento $\gamma \in K(\underline{\alpha})$ (non necessariamente primitivo) consideriamo il polinomio

$$\psi(x) = \prod_{\sigma \in G} (x - \gamma^\sigma). \tag{2.5}$$

I suoi coefficienti $\sum \gamma^\sigma, \sum \gamma^\sigma \gamma^\tau, \ldots$ sono invarianti per ogni elemento di G e dunque appartengono a K. Questo polinomio ammette la radice γ (in corrispondenza ad esempio di $\sigma = 1$). Sia $J(x)$ il fattore irriducibile monico su K che ammette la radice γ; allora $J(x)$ divide $\psi(x)$. Sia $J(x)^t$ la massima potenza di $J(x)$ che divide $\psi(x)$: $\psi(x) = J(x)^t L(x)$. Se J e L hanno una radice in comune, J divide L, e dunque t non sarebbe più massimo. Inoltre, $J(\gamma) = 0$ è una relazione su K, che dunque conserva il valore 0 per ogni $\sigma \in G$: $J(\gamma^\sigma) = 0$. Ne segue che $J(x)$ ammette tutte le radici di $\psi(x)$ e perciò ha lo stesso grado di $\psi(x)$. Allora $L(x)$ è una costante, la quale, essendo J e ψ monici, uguale a 1. Quindi $\psi(x) = J(x)^t$. Se J è di grado s, si ha st uguale al grado di ψ, cioè all'ordine di G. Ne segue:

2.32 Teorema. *Se γ è una funzione razionale delle α_i e $J(x)$ è il polinomio irriducibile monico su K che ammette la radice γ, allora esiste un intero t tale che $J(x)^t = \prod_{\sigma \in G}(x - \gamma^\sigma)$.* ♢

2.33 Corollario. *Per γ come nel* Teor. 2.32 *si ha:*

$$J(x) = \prod_{i=1}^{s} (x - \gamma^{\sigma_i})$$

dove $1 = \sigma_1, \sigma_2, \ldots, \sigma_s$ un sistema di rappresentanti dei laterali di G_γ in G. Il grado di $J(x)$ è dunque uguale all'indice $[G : G_\gamma]$ di G_γ in G.

Dim. Il polinomio $\psi(x)$ si può scrivere $\psi(x) = \prod_{i=1}^{s}(x - \gamma^{\sigma_i})^{|G_\gamma|}$. Poiché $J(x)$ è irriducibile e ha la radice γ in comune con il polinomio $\psi_1 = \prod_{i=1}^{s}(x - \gamma^{\sigma_i})$, J divide ψ_1, ma avendo le stesse radici γ^{σ_i}, $i = 1, 2, \ldots, s$, lo uguaglia. ♢

Si ritrova il Cor. 2.30 perché se γ è primitivo si ha $G_\gamma = \{1\}$ e dunque $J(x)$ ha grado $|G|$, ed essendo a radici distinte in quanto è irriducibile le γ^σ

sono tutte distinte, e viceversa. Un elemento γ primitivo soddisfa dunque un polinomio di grado $|G|$, e viceversa.

2.34 Corollario. *Se $K(\underline{\alpha})$ contiene una radice di un polinomio irriducibile, allora le contiene tutte.*

Dim. Sia $p(x)$ il polinomio e γ una sua radice in $K(\underline{\alpha})$. Allora $p(x) = J(x)$ (Cor. 2.33) e le altre radici sono le γ^{σ_i}, e queste appartengono a $K(\underline{\alpha})$. ◊

Sia $\gamma = \vartheta(\underline{\alpha})$ un elemento di $K(\underline{\alpha})$ e $J(y)$ il suo polinomio minimo. Nel campo $K(\gamma)$ questo polinomio si spezza completamente in fattori lineari:

$$J(y) = \prod_{i=1}^{s}(y - \gamma^{\sigma_i})$$

(v. Cor. 2.33). Gli elementi di $K(\gamma)$ sono polinomi in γ; sia $\gamma^\sigma = g(\gamma)$. Ci proponiamo di determinare i polinomi $g(y)$, e a questo scopo faremo uso dei moduli fondamentali del polinomio $f(x)$.

Scriviamo $\gamma^\sigma - g(\gamma) = 0$ come:

$$\vartheta(\underline{\alpha}) - g(\vartheta(\underline{\alpha})) = 0.$$

Per il Teor. 2.15 il resto $r(\underline{x})$ che si ottiene dividendo

$$\vartheta(\underline{x}^\sigma) - g(\vartheta(\underline{x}))$$

successivamente per $f_n, f_{n-1}, \ldots, f_1$ è il polinomio nullo. Questo resto $r(\underline{x})$ dipende linearmente dai coefficienti di $g(y)$; imponendo allora che i suoi coefficienti siano nulli si ottiene un sistema di equazioni lineari risolvendo il quale si determinano i coefficenti di $g(y)$.

2.35 Esempio. Sia $f(x) = (x^2-2)(x^2-3)$ (v. *Es.* 2.31). I moduli fondamentali di $f(x)$ sono

$$f_1 = x_1^2 - 2,\ f_2 = x_2 + x_1,\ f_3 = x_3^2 - 3,\ f_4 = x_4 + x_3.$$

Il gruppo di Galois è di ordine $m = 2 \cdot 1 \cdot 2 \cdot 1 = 4$. Sia $\gamma = \alpha_1 + \alpha_3$ $(= \sqrt{2} + \sqrt{3})$, e dunque $\vartheta(\underline{x}) = x_1 + x_3$. Il polinomio minimo di γ è $J(y) = y^4 - 10y^2 + 1$, e il gruppo di Galois è il Klein dell'*Es.* 2.31. Sia $\gamma^{\sigma_i} = g_i(\gamma)$, $i = 1, \ldots, 4$. Con $\sigma_1 = 1$ abbiamo $g_1(\gamma) = \gamma$; cerchiamo quindi i polinomi g_2, g_3, g_4. Per dividere $\vartheta(\underline{x}^\sigma) - g(\vartheta(\underline{x}))$ per gli f_i dividiamo i due membri e poi prendiamo la differenza. Sia $g(y) = a_1y^3 + a_2y^2 + a_3y + a_4$, e calcoliamo il resto $R(x_i, a_i)$ delle divisioni successive di

$$g(x_1 + x_3) = a_1(x_1 + x_3)^3 + a_2(x_1 + x_3)^2 + a_3(x_1 + x_3) + a_4$$

per f_4, f_3, f_2, f_1. Dividendo addendo per addendo abbiamo:

$$(x_1 + x_3)^3 = x_1^3 + 3x_1^2 x_3 + 3x_1 x_3^2 + x_3^3,$$

che diviso per f_4 (come polinomio in x_4) dà come resto lo stesso polinomio. Dividendo poi per f_3 (come polinomio in x_3) si ha il resto $x_1^3+3x_1^2x_3+9x_1+3x_3$, e questo diviso per f_2 (come polinomio in x_2) dà come resto lo stesso polinomio. Infine, dividendo per f_1 (come polinomio in x_1) si ottiene:

$$2x_1 + 6x_3 + 9x_1 + 3x_3 = 11x_1 + 9x_3.$$

Analogamente, $(x_1 + x_3)^2$ si riduce a $2x_1x_3 + 5$. Gli altri due addendi danno come resto gli addendi stessi. La riduzione di $g(x_1 + x_3)$ fornisce dunque il polinomio

$$R(x_i, a_i) = 2a_2x_1x_3 + (11a_1 + a_3)x_1 + (9a_1 + a_3)x_3 + 5a_2 + a_4.$$

Le immagini di $\vartheta_1 = x_1 + x_3$ secondo gli elementi del gruppo di Galois sono

$$\vartheta_1 = x_1 + x_3, \vartheta_2 = x_2 + x_4, \vartheta_3 = x_2 + x_3, \vartheta_4 = x_1 + x_4.$$

Riduciamo ϑ_2 modulo gli f_i; otteniamo $-x_1 - x_3$, e dunque imponendo

$$-x_1 - x_3 - R(x_i, a_i) = 0$$

otteniamo il sistema:

$$\begin{array}{lcr} 2a_2 & = & 0, \\ 11a_1 + a_3 & = & -1, \\ 9a_1 + a_3 & = & -1, \\ 5a_2 + a_4 & = & 0. \end{array}$$

Risolvendo si trova $a_1 = a_2 = a_4 = 0$ e $a_3 = -1$, e dunque $g_2(y) = -y$ (come si poteva dedurre anche dal fatto che, modulo gli f_i, $\vartheta_2 + \vartheta_1 = 0$).

Per $\vartheta_3 = x_2 + x_3$ la riduzione modulo gli f_i dà $-x_1 + x_3$ e si ottiene il sistema:

$$\begin{array}{lcr} 2a_2 & = & 0, \\ 11a_1 + a_3 & = & -1, \\ 9a_1 + a_3 & = & 1, \\ 5a_2 + a_4 & = & 0, \end{array}$$

che fornisce $a_2 = a_4 = 0$, $a_1 = -1$ e $a_3 = 10$. Dunque $g_3(y) = -y^3 + 10$, e poiché, modulo gli f_i, $\vartheta_4 = -\vartheta_3$ si ha $g_4(y) = -g_3(y)$.

$J(x)$ si spezza dunque in $K(\gamma)$ come:

$$J(y) = (y - \gamma)(y - g_2(\gamma))(y - g_3(\gamma))(y - g_4(\gamma)).$$

Questi fattori danno anche i moduli fondamentali di $J(x)$:

$$\begin{aligned} F_1(x_1) &= J(x_1), \\ F_2(x_1,x_2) &= x_2+x_1, \\ F_3(x_1,x_2,x_3) &= x_3-(-x_1^3+10x_1), \\ F_4(x_1,x_2,x_3,x_4) &= x_4-(x_1^3-10x_1). \end{aligned}$$

Essi si annullano ponendo $x_1=\alpha_1+\alpha_3, x_2=\alpha_2+\alpha_4, x_3=\alpha_2+\alpha_3, x_4=\alpha_1+\alpha_4$. Le permutazioni delle x_i che mutano le relazioni ottenute in questo modo ancora in relazioni sono quelle del gruppo $\{I,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$, isomorfo al precedente (ma questa volta *regolare*, e ciò è dovuto al fatto che γ è primitivo; v. oltre, §2.4).

2.36 Definizione. Se γ è primitivo, l'equazione $\psi(x)=0$, dove $\psi(x)$ è il polinomio (2.5), si chiama *risolvente di Galois* di $f(x)$.

Se infatti si conosce una radice di $\psi(x)=0$ le radici di $f(x)$ si esprimono come funzioni razionali di questa.

Il Teor. 2.24 ammette un inverso:

2.37 Teorema. *Sia H un sottogruppo di G. Allora esiste γ tale che $H=G_\gamma$.*

Dim. Sia η primitivo, e sia $g(x)=\prod_{\tau\in H}(x-\eta^\tau)$. Se $1=\sigma_1,\sigma_2,\ldots,\sigma_r$ è un sistema di rappresentanti dei laterali di H in G, i polinomi $g(x)^{\sigma_i}=\prod_{\tau\in H}(x-\eta^{\tau\sigma_i})$ sono tutti distinti. Infatti se fossero uguali avrebbero le stesse radici, ma da $\eta^{\tau_i\sigma_j}=\eta^{\tau_h\sigma_k}$ segue $\tau_i\sigma_j\sigma_k^{-1}\tau_h^{-1}\in H$ e $\sigma_j\sigma_k^{-1}\in H$, escluso. Sia $c\in K$ tale che i $g(c)^{\sigma_i}$ siano tutti distinti (se $g(c)^{\sigma_i}=g(c)^{\sigma_j}$ per ogni $c\in K$, allora $g(x)^{\sigma_i}=g(x)^{\sigma_j}$). L'elemento $\gamma=g(c)$ è fissato dagli elementi di H e solo da questi: essendo $c\in K$, per $\sigma\in G$ abbiamo

$$g(c)^\sigma=g(c^\sigma)=g(c).$$

Ma $g(c)^\sigma=\prod_{\tau\in H}(c^\sigma-\eta^{\tau\sigma})$, e $g(c)=\prod_{\tau\in H}(c-\eta^\tau)$, e dunque dato $\eta^{\tau\sigma}$ deve aversi $\tau\sigma=\tau'\in H$ e quindi $\sigma=\tau^{-1}\tau'\in H$. ♢

Gli elementi di S^n che fissano il valore numerico di γ non formano in generale un sottogruppo (v. *Es.* 2.23), ma per ogni sottogruppo H di S^n, e non solo di G, esiste γ fissato da tutti e soli gli elementi di H. L'argomento è lo stesso di quello del Teor. 2.37, considerando η tale che $\eta^\sigma\neq\eta$ per ogni $\sigma\in S^n$ (cioè tale che $H_\eta=\{1\}$).

2.4 Proprietà del gruppo di Galois

2.38 Definizione. Un polinomio su K si dice *normale* se le sue radici si possono esprimere come funzioni razionali (polinomi) su K di una qualunque di esse.

2.39 Esempi. 1. Il polinomio $g(x) = (x^2+1)(x^2+4)$ su $\mathcal{Q}$ è normale: mediante una qualunque delle radici $\pm i, \pm 2i$ si possono esprimere tutte le altre.

2. Il polinomio $x^3 - 2$ su $\mathcal{Q}$ non è normale. Gli elementi di $\mathcal{Q}(\sqrt[3]{2})$ sono reali, mentre le altre due radici sono complesse.

2.40 Teorema. *I fattori irriducibili di un polinomio normale hanno tutti lo stesso grado.*

Dim. Siano $h(x)$ e $k(x)$ due fattori irriducibili del polinomio normale $g(x)$, e siano $\alpha_1, \alpha_2, \ldots, \alpha_t$ le radici di $h(x)$. Se β è una radice di $k(x)$, è $\beta = \vartheta(\alpha_1)$, in quanto β e le α_i sono radici anche di $g(x)$ e $g(x)$ è normale. Allora $h(\alpha_1) = 0 = k(\vartheta(\alpha_1))$, e dunque il polinomio $k(\vartheta(x))$ ammette la radice α_1 di $h(x)$, e pertanto le ammette tutte. Ne segue che $\vartheta(\alpha_1), \vartheta(\alpha_2), \ldots, \vartheta(\alpha_t)$ sono radici di $k(x)$, e dunque $\partial k(x) \geq \partial h(x)$, e analogamente $\partial h(x) \geq \partial k(x)$. $\diamondsuit$

Se $G_\alpha = \{1\}$ per ogni radice di $f(x)$ allora tutte le α_i sono elementi primitivi e $f(x)$ è normale, e viceversa (Cor. 2.27 e Teor. 2.29).

2.41 Definizione. Un gruppo di permutazioni nel quale ogni elemento è fissato solo dall'identità si dice *semiregolare.* Un gruppo semiregolare e transitivo si dice *regolare.*

2.42 Teorema. *In un gruppo semiregolare i cicli di una permutazione hanno tutti la stessa lunghezza, e questa è pari all'ordine della permutazione.*

Dim. Se una pemutazione σ ha un ciclo di lunghezza h e uno di lunghezza k con $h < k$, allora σ^h è diversa dall'identità e fissa almeno h elementi. $\diamondsuit$

2.43 Teorema. *Il gruppo di Galois di $f(x)$ è semiregolare se e solo se $f(x)$ è un polinomio normale, e in tal caso l'equazione $f(x) = 0$ è essa stessa una risolvente di Galois di $f(x)$* (v. Def. 2.36). $\diamondsuit$

2.44 Esempio. $f(x) = (x^2+1)(x^2+4)$ è normale, e le sue radici $\alpha_1 = i, \alpha_2 = -i, \alpha_3 = 2i, \alpha_4 = -2i$ soddisfano le relazioni

$$\alpha_1^2 + 1 = 0,\ \alpha_2 + \alpha_1 = 0,\ \alpha_3 - 2\alpha_1 = 0,\ \alpha_4 + 2\alpha_1 = 0.$$

La permutazione $(1,2)(3,4)$ lascia inalterato il valore zero di tutte e quattro. Poiché né α_1 né α_2 possono andare in α_3 o in α_4 (la prima relazione, o rispettivamente la seconda, cambiano di valore), in una permutazione di G deve necessariamente comparire il ciclo (1,2). Deve allora esserci anche il ciclo (3,4), altrimenti la terza relazione cambia di valore. D'altra parte, $|G| > 1$ in quanto nessuna radice appartiene a $\mathcal{Q}$. Dunque $G = \{I, (1,2)(3,4)\}$, che è semiregolare.

2.45 Lemma. *Sia G un gruppo (anche infinito) che agisce su un insieme Ω. Allora la cardinalità di un'orbita α^G dell'azione di G è uguale all'indice dello* *stabilizzatore G_α di un (qualunque) elemento appartenente all'orbita:*

$$|\alpha^G| = [G : G_\alpha]. \tag{2.6}$$

Dim. Sia $\alpha \in \Omega_i$, e sia $h \in G_\alpha g$. Allora $h = xg$, $x \in G_\alpha$, e $\alpha^h = \alpha^{xg} = \alpha^{xg} = \alpha^g$. Un elemento dell'orbita α^G è dunque ripetuto un numero di volte pari alla cardinalità di G_α. Gli elementi distinti sono allora in numero pari all'indice di G_α in G. ♢

Mediante la (2.6) possiamo dare un'altra dimostrazione del fatto che l'ordine del gruppo di Galois è dato dal prodotto dei gradi dei moduli fondamentali di $f(x)$. L'orbita di α_1 sotto l'azione di G consta delle radici di f_1; per la (2.6) si ha allora:

$$d_1 = [G : G_{\alpha_1}],$$

Aggiungendo α_1 a K il gruppo di Galois di $f(x)$ su $K(\alpha_1)$ è G_{α_1}. Le permutazioni di G_{α_1} hanno la forma:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_k & \dots & \alpha_n \\ \alpha_1 & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

e poiché l'immagine di α_2 può essere una qualunque radice di $f_2(\alpha_1, x)$ l'orbita di α_2 sotto l'azione di G_{α_1} ha cardinalità

$$d_2 = [G_{\alpha_1} : (G_{\alpha_1})_{\alpha_2}].$$

Poniamo $G_{k+1} = (G_k)_{\alpha_{k+1}}$ $(G_0 = G)$. Si ha, analogamente, che le permutazioni di G_{k-1} hanno la forma:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{k-1} & \alpha_k & \alpha_{k+1} & \dots & \alpha_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_{k-1} & \dots & \dots & \dots & \dots \end{pmatrix}$$

e l'orbita di α_k sotto l'azione di G_{k-1} ha cardinalità d_k. Poiché

$$|G| = \frac{|G|}{|G_1|} \cdot \frac{|G_1|}{|G_2|} \cdots \frac{|G_{n-1}|}{|G_n|}$$

ritroviamo il risultato $|G| = d_1 d_2 \cdots d_n$. Si osservi che $G_n = \{1\}$, e che anche $G_{n-1} = \{1\}$ in quanto essendo lasciate fisse le prime $n-1$ radici anche l'ultima deve restare fissa. Infine, se solo l'identità fissa α_1 $(G_1 = \{1\})$, allora l'ordine di G è pari al grado d_1 del polinomio $f_1(x)$.

Se il Gruppo di Galois è noto, allora il procedimento ora esposto permette di determinare i gradi dei moduli fondamentali di $f(x)$.

2.46 Corollario. *Se G è semiregolare, le orbite di G su Ω hanno tutte la stessa cardinalità, e questa cardinalità è quella di G. In particolare, se G è finito la* *cardinalità di Ω è un multiplo di quella di G. Se inoltre G è regolare, allora la cardinalità di Ω è uguale a quella di G.*

Dim. Se G è semi-regolare, $G_\alpha = \{1\}$ per ogni α. Il risultato segue. $\diamondsuit$

Se il gruppo di Galois G di $f(x)$ è semiregolare, ogni radice di $f(x)$ ha $|G|$ immagini distinte (gli elementi della propria orbita). Le n radici si dividono dunque in orbite di cardinalità $|G|$, per cui $|G|$ divide il grado n di $f(x)$, e si ritrova il Cor. 2.46. Nell'esempio qui sopra questa cardinalità è 2. Se G è transitivo, e solo l'identità fissa α_i, allora anche ogni altra radice α_j è fissata solo dall'identità. Infatti, se $\alpha_j^\tau = \alpha_j$, avendosi per la transitività $\alpha_i^\sigma = \alpha_j$ per un certo σ, si ha $\alpha_i^{\sigma\tau} = \alpha_i^\sigma$, $\alpha_i^{\sigma\tau\sigma^{-1}} = \alpha_i$, $\sigma\tau\sigma^{-1} = 1$ e $\tau = 1$. Dunque una qualunque radice è fissata solo dall'identità, e G è regolare.

2.47 Corollario. *Il gruppo di Galois di $f(x)$ è regolare, e dunque di ordine pari al grado di $f(x)$, se e solo se $f(x)$ è irriducibile e normale.*

2.48 Definizione. Sia $\gamma \in K(\underline{\alpha})$ e $\sigma \in G$. L'elemento γ^σ è il *coniugato* di γ mediante σ. Se G_γ è lo stabilizzatore di γ, lo stabilizzatore di γ^σ è $\sigma^{-1}G_\gamma\sigma$, il sottogruppo coniugato di G_γ in G mediante σ.

Il gruppo di Galois di $f(x)$ su $K(\gamma^{\sigma_1}, \gamma^{\sigma_2}, \ldots, \gamma^{\sigma_m})$ è $\bigcap_{\sigma\in G}\sigma^{-1}G_\gamma\sigma$, che è un sottogruppo normale di G. Se G_γ è esso stesso un sottogruppo normale, allora $G_{\gamma^\sigma} = \sigma^{-1}G_\gamma\sigma = G_\gamma$, e dal Cor. 2.26 si ha $K(\gamma) = K(\gamma^\sigma)$, cioè ogni radice del polinomio (2.5) si esprime razionalmente in funzione di una qualunque di esse, e perciò $\psi(x)$ è un polinomio normale. Viceversa, se $\psi(x)$ è normale, l'aggiunta di γ equivale all'aggiunta di una qualunque γ^σ. Il gruppo di Galois di $f(x)$ su $K(\gamma)$ si abbassa a G_γ, ma anche a G_γ^σ, per ogni $\sigma \in G$ e dunque $G_\gamma = G_\gamma^\sigma$, per ogni $\sigma \in G$. In altri termini G_γ è un sottogruppo normale. Si ha allora:

2.49 Teorema. *i) Aggiungendo al campo tutte le radici di un polinomio il gruppo di Galois di $f(x)$ sul campo ampliato si riduce a un sottogruppo normale di G;*

ii) il polinomio (2.5) *è un polinomio normale se e solo se G_γ è un sottogruppo normale di G.* $\diamondsuit$

2.50 Esempi. 1. Se $\gamma = \alpha_i$ è una delle radici di $f(x)$, $\bigcap_{\sigma\in G}\sigma^{-1}G_{\alpha_i}\sigma = \{1\}$ in quanto la sola permutazione che fissa tutte le α_i è l'identità, e dunque G si abbassa a $\{1\}$. Si ritrova così il fatto ovvio che il gruppo di Galois di $K(\underline{\alpha})$ su $K(\underline{\alpha})$ è l'identità.

2. Riprendiamo l'*Es.* 1 di 2.22. Sia $\gamma = i = \frac{\alpha_3}{\alpha_1}$. Le permutazioni di D_4 che non fanno cambiare il valore i di γ sono quelle del gruppo ciclico C_4 generato da $(1,3,2,4)$, che è normale in D_4. $J(x)$ è in questo caso x^2+1, che è normale.

Aggiungendo i il gruppo di Galois di $f(x)$ su $\mathcal{Q}(i)$ si abbassa a questo C_4

(Teor. 2.25), e $f(x)$ resta irriducibile (per via dell'irrazionale $\sqrt[4]{2}$), ma ora si tratta di un polinomio normale in quanto le radici si esprimono tutte in termini di α_1 a coefficienti in $\mathcal{Q}(i)$: $\alpha_1, \alpha_2 = -\alpha_1, \alpha_3 = i\alpha_1, \alpha_4 = -i\alpha_1$. Il gruppo C_4 è infatti regolare. La radice α_1 è fissata da $C_2 = \{I, (1)(2)(3,4)\}$, gruppo al quale si riduce G aggiungendo α_1.

2.51 Definizione. Siano G e G_1 due gruppi che operano su due insiemi Ω e Ω_1 rispettivamente. L'azione di G su Ω si dice *simile* a quella di G_1 su Ω_1 se esistono un isomorfismo φ di G su G_1 e una corrispondenza biunivoca θ tra Ω e Ω_1 tali che $\theta(\alpha)^{\varphi(g)} = \theta(\alpha^g)$, per ogni $\alpha \in \Omega$ e $g \in G$.

2.52 Teorema. *Sia $\gamma \in K(\underline{\alpha})$. Allora il gruppo di Galois G_1 su K del polinomio $J(x)$ di γ è isomorfo al gruppo quoziente G/H, dove $H = \bigcap_{\sigma \in G} \sigma^{-1} G_\gamma \sigma$ è l'intersezione dei coniugati di G_γ in G. Inoltre, come gruppo di permutazioni, l'azione di G_1 sulle γ^{σ_i}, $i = 1, 2, \ldots, s$ è simile all'azione di G sui laterali di G_γ.*

Dim. Costruiamo un omomorfismo di G su G_1. Sia $\gamma = h(\underline{\alpha})$, e siano $\gamma_i = \gamma^{\sigma_i} = h(\alpha_{(1)\sigma_i}, \ldots, \alpha_{(n)\sigma_i})$ le radici di $J(x)$, $i = 1, 2, \ldots, s$, con $s = [G : G_\gamma]$ (Cor. 2.31). G_1 consta delle permutazioni delle γ_i che lasciano invariato il valore di una qualunque funzione razionale delle γ_i a valore in K. Sia $g(\gamma_1, \ldots, \gamma_s) = a \in K$ una tale funzione. Allora

$$g(h(\alpha_{(1)\sigma_1}, \ldots, \alpha_{(n)\sigma_1}), \ldots, h(\alpha_{(1)\sigma_s}, \ldots, \alpha_{(n)\sigma_s})) = a$$

è una funzione razionale delle α_i a valore in K, e sia $g_1(\alpha_1, \ldots, \alpha_n) = a$. Il valore a resta dunque invariato permutando le α_i secondo G. Poichè l'immagine di α_i secondo $\sigma \in G$ è $\alpha_{(i)\sigma}$, si ha

$$\gamma^{\sigma_i} = \gamma_i = h(\alpha_{(1)\sigma_i}, \ldots, \alpha_{(n)\sigma_i}) \xrightarrow{\sigma} h(\alpha_{(1)\sigma_i\sigma}, \ldots, \alpha_{(n)\sigma_i\sigma}) = \gamma^{\sigma_i\sigma}.$$

La corrispondenza $\psi : G \longrightarrow G_1$ data da

$$\sigma \longrightarrow \pi = \begin{pmatrix} \gamma^{\sigma_1} & \gamma^{\sigma_2} & \ldots & \gamma^{\sigma_s} \\ \gamma^{\sigma_1\sigma} & \gamma^{\sigma_2\sigma} & \ldots & \gamma^{\sigma_s\sigma} \end{pmatrix} \tag{2.7}$$

è ovviamente un omomorfismo. Dimostriamo che è surgettivo. Se $\pi \in G_1$, π permuta le γ^{σ_i} lasciando inalterato il valore a, e induce sulle α_i una permutazione σ che lascia invariato a (permutando le γ si permutano automaticamente le α_i), e dunque $\sigma \in G$. Ma se

$$h(\alpha_{(1)\sigma_i}, \ldots, \alpha_{(n)\sigma_i})^\pi = h(\alpha_{(1)\sigma_j}, \ldots, \alpha_{(n)\sigma_j}),$$

allora:

$$h(\alpha_{(1)\sigma_i\sigma}, \ldots, \alpha_{(n)\sigma_i\sigma}) = h(\alpha_{(1)\sigma_j}, \ldots, \alpha_{(n)\sigma_j}),$$

e pertanto π è la permutazione (1.6) e quindi proviene da σ.

Il nucleo è $\bigcap_{\sigma\in G}\sigma^{-1}G_\gamma\sigma$. Infatti π è l'identità se e solo se $\gamma^{\sigma_i}=\gamma^{\sigma_i\sigma}$, per ogni i, cioè se e solo se $\sigma_i\sigma\sigma_i^{-1}\in G_\gamma$, ovvero $\sigma\in\bigcap_{i=1}^s\sigma_i^{-1}G_\gamma\sigma_i=\bigcap_{\sigma\in G}\sigma^{-1}G_\gamma\sigma=H$.

G agisce sulle σ_i come segue: $\sigma_i\sigma=\sigma_j$, dove σ_j è il rappresentante scelto per il laterale che contiene il prodotto $\sigma_i\sigma$. L'azione di G_1 sulle γ^{σ_i} per come è definita è equivalente a questa. $\diamondsuit$

Se G_γ è normale in G, allora in particolare $G_1\simeq G/G_\gamma$, ed essendo allora $J(x)$ irriducibile e normale, il gruppo G_1, come gruppo di pemutazioni delle radici di $J(x)$, è regolare. Se $G_\gamma=\{1\}$ si ha $G\simeq G_1$ e la (2.7) fornisce la *rappresentazione regolare* di G. In altri termini, la considerazione di un elemento primitivo ($G_\gamma=\{1\}$) permette di trasformare il gruppo di Galois in un gruppo regolare.

Se $f(x)$ è irriducibile e G_{α_i} è normale per una radice α_i di $f(x)$, allora per la transitività $G_{\alpha_j}=G_{\alpha_i^\sigma}=\sigma^{-1}G_{\alpha_i}\sigma=G_{\alpha_i}$, per ogni j, e dunque $\{1\}=\bigcap_{k=1}^n G_{\alpha_k}=G_{\alpha_i}$. Dunque G è regolare.

2.53 Esempi. 1. A illustrazione del Teor. 2.52 riprendiamo il polinomio x^4-2 dell'*Es.* 1 di 2.22. Con $\alpha=\alpha_1$, l'elemento $\gamma=2\alpha_1+\alpha_3=(2+i)\alpha$ è primitivo in quanto le sue immagini secondo D_4 sono $\pm(2+i)\alpha,\pm(2-i)\alpha,\pm(2i+1)\alpha,\pm(2i-1)\alpha$, tutte distinte. Dunque $G_\gamma=\{1\}$. Un semplice calcolo mostra che il polinomio che ha come radici gli otto coniugati di $\gamma=(2+i)\alpha$ è $\varphi(x)=x^8-28x^4+2500$. Per il teorema, il gruppo di Galois G_1 di $J(x)$ è isomorfo al gruppo di Galois D_4 di $f(x)$, e fornisce la rappresentazione regolare di G. Ad esempio, posto $a=(2+i)\alpha, b=-(2+i)\alpha$, e analogamente $c,d,\dots,h$ per gli altri sei coniugati si ha

$$\begin{array}{cccc} a=\gamma, & b=\gamma^{(1,2)(3,4)}, & c=\gamma^{(1,3)(2,4)}, & d=\gamma^{(1,4)(2,3)},\\ e=\gamma^{(1)(2)(3,4)}, & f=\gamma^{(1,2)(3)(4)}, & g=\gamma^{(1,3,2,4)}, & h=\gamma^{(1,4,2,3)}, \end{array}$$

e se $\sigma=(1,2)(3,4)$, si ha $a^\sigma=b$, $b^\sigma=a,\dots,g^\sigma=h$, $h^\sigma=g$, e dunque σ agisce sui γ^{σ_i} come l'involuzione senza punti fissi $(a,b)(c,d)(e,f)(g,h)$. Analogamente, (1,3,2,4) si rappresenta come $(a,g,b,h)(c,f,d,e)$, ecc.

Se consideriamo $\gamma=\frac{\alpha_3}{\alpha_1}=i$ come nell'*Es.* 2 di 2.46 abbiamo due sole immagini di γ secondo gli elementi di D_4: i e $-i$. Allora $J(x)=(x-i)(x+i)=x^2+1$, e il gruppo di Galois G_1 ha ordine 2:

$$G_1=\{I,\begin{pmatrix} i & -i\\ -i & i\end{pmatrix}\},$$

immagine omomorfa di D_4 ottenuta mandando σ in I se $\sigma\in C_4$ e in π altrimenti.

2. Nell'esempio precedente cerchiamo ora, dato $H=\{I,(1,2)(3)(4)\}$, un elemento γ tale che $G_\gamma=H$. Seguendo la dimostrazione del Teor. 2.37 sia

$\eta = (2+i)\alpha$, che sappiamo essere primitivo, e costruiamo il polinomio

$$g(x) = (x-\eta)(x-\eta^{(1,2)(3)(4)}) = (x-(2+i)\alpha)(x+(2-i)\alpha) = x^2 - 2i\alpha x - 5\alpha^2.$$

Gli altri tre polinomi, ottenuti applicando a η gli elementi delle altre tre classi laterali di H sono

$$g_2(x) = x^2 + 2i\alpha x - 5\alpha^2,\ g_3(x) = x^2 + 2\alpha x + 5\alpha^2,\ g_4(x) = x^2 - 2\alpha x + 5\alpha^2.$$

Per $x = 1$, i $g_i(x)$ sono tutti distinti e posto

$$\gamma = g(1) = 1 - 2i\alpha - 5\alpha^2 = 1 - 2\alpha_3 - 5\alpha_1^2,$$

si vede subito che γ è fissato solo dagli elementi di H.

3. Sia $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$ il discriminante di un polinomio $f(x)$. Poiché Δ è una funzione simmetrica delle α_i, $\Delta \in K$. Se Δ è un quadrato in K, allora $\sqrt{\Delta} \in K$ e dunque è lasciato inalterato dagli elementi del gruppo di Galois G di $f(x)$. Ma le permutazioni che lasciano inalterato $\sqrt{\Delta} = \prod_{i<j}(\alpha_i - \alpha_j)$ sono necessariamente pari, e dunque se Δ è un quadrato in K il gruppo G è contenuto nel gruppo alterno A^n. In generale, aggiungendo $\sqrt{\Delta}$ il gruppo di Galois si riduce a $G \bigcap A^n$.

4. Sia $f(x) = x^3 + bx + c$. Un semplice calcolo mostra che $\Delta = -4b^3 - 27c^2$. Se $f(x)$ non ha radici in K allora è irriducibile, e dunque il suo gruppo di Galois è S^3 se e solo se Δ non è un quadrato in K.

Con $f(x) = x^3 - 2$ su $\mathcal{Q}$ si trova $D = -108$, che non è un quadrato in $\mathcal{Q}$, e dunque $G \not\subseteq A^3$. Essendo G transitivo ($f(x)$ è irriducibile), $|G| \geq 3$, e dunque non resta che $|G| = 6$ e $G = S^3$. Aggiungiamo a $\mathcal{Q}$ una radice terza dell'unità ϵ. Poiché $\sqrt{-108} = 6\sqrt{-3} = 6(\epsilon - \epsilon^2)$, $\sqrt{\Delta}$ ha valore in $\mathcal{Q}(\epsilon)$, e dunque non varia sotto l'azione del nuovo gruppo G_1. Ne segue che G_1 non può contenere trasposizioni, e dunque è contenuto in $A^3 = \{I, (1,2,3), (1,3,2)\}$. Non potendo essere $\{1\}$ in quanto il polinomio resta irriducibile su $\mathcal{Q}(\epsilon)$, il gruppo è A^3. D'altra parte, su $\mathcal{Q}(\epsilon)$ il polinomio è normale, e infatti A^3 è regolare.

5. Sia $f(x) = x^4 + 1$, che ha le radici $\alpha_1 = \sqrt{i}$, $\alpha_2 = -\sqrt{i}$, $\alpha_3 = \sqrt{-i}$, $\alpha_4 = -\sqrt{-i}$. Si ha $D = 16$, che è un quadrato in $\mathcal{Q}$, e dunque $G \subseteq A^4$. Inoltre, $f(x)$ è normale in quanto si ha α_1, $\alpha_2 = -\alpha_1$, $\alpha_3 = \frac{1}{\alpha_1}$, $\alpha_4 = -\frac{1}{\alpha_1}$, e irriducibile. Dunque G è regolare. Ma il solo sottogruppo regolare di A^4 è il gruppo di Klein V, e dunque $G = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

Troviamo ora lo stesso risultato determinando le relazioni che provengono dai moduli fondamentali. L'aggiunta di $\alpha_1 = \sqrt{i}$ spezza completamente il polinomio; le altre radici sono α_1^3, α_1^5 e α_1^7. Possiamo allora rinumerare le radici come $\alpha_2 = \alpha_1^3$, $\alpha_3 = \alpha_1^5$, $\alpha_4 = \alpha_1^7$ e ottenere le relazioni $\alpha_1^4 + 1 = 0$, $\alpha_2 - \alpha_1^3 = 0$, $\alpha_3 - \alpha_1^5 = 0$, $\alpha_4 - \alpha_1^7 = 0$. Si può verificare che il gruppo è gruppo di Klein trovato sopra.

6. $f(x) = x^4 - 2$ è normale su $\mathcal{Q}(i)$, e restando irriducibile il gruppo di Galois G_1 è regolare. Avendosi $G_1 \subseteq D_4$ è $G_1 = V$ oppure $G_1 = C_4$. $\gamma = \frac{\alpha_3}{\alpha_1} = i$ ha valore in $\mathcal{Q}(i)$, e perciò non deve variare per G_1, e poiché (1,3)(2,4) porta i in $-i$, G_1 non può essere V, e dunque è C_4. Con $\sigma_1 = I$ e $\sigma_2 = (1,3)(2)(4)$ come rappresentanti dei laterali di C_4 abbiamo che il polinomio $J(x)$ (Cor. 2.33) è il polinomio $(x-i)(x+i) = x^2+1$.

2.5 Gruppi abeliani

Se il gruppo di Galois G è abeliano tutti i suoi sottogruppi sono normali. In particolare lo è lo stabilizzatore G_γ per ogni γ, e dunque $G_{\gamma^\sigma} = G_\gamma$, per $\sigma \in G$. Allora $\gamma^\sigma \in K(\gamma)$ (Cor. 2.26) e perciò γ^σ è una certa funzione razionale $\vartheta_\sigma(\gamma)$ di γ.

2.54 Teorema. *Se G è abeliano,*

$$\vartheta_\sigma(\vartheta_\tau(\gamma)) = \vartheta_\tau(\vartheta_\sigma(\gamma)). \tag{2.8}$$

Dim.

$$\begin{aligned}\gamma^{\sigma\tau} &= (\gamma^\sigma)^\tau = \vartheta_\sigma(\gamma^\tau) = \vartheta_\sigma(\vartheta_\tau(\gamma))\\ \gamma^{\tau\sigma} &= (\gamma^\tau)^\sigma = \vartheta_\tau(\gamma^\sigma) = \vartheta_\tau(\vartheta_\sigma(\gamma))\end{aligned}$$

ed essendo $\sigma\tau = \tau\sigma$ il risultato segue. ♢

2.55 Teorema. *Se G_γ è normale in G e sussiste la* (2.8) *per ogni $\sigma, \tau \in G$, allora il gruppo quoziente G/G_γ è abeliano.*

Dim. Essendo G_γ normale in G si ha che, per ogni σ, γ^σ è una funzione razionale di γ, $\vartheta_\sigma(\gamma)$. Se sussiste la (2.8) si ha, per ogni $\sigma, \tau \in G$ $\gamma^{\sigma\tau} = \gamma^{\tau\sigma}$, da cui $\sigma\tau\sigma^{-1}\tau^{-1} \in G_\gamma$. Allora $G_\gamma\sigma\tau\sigma^{-1}\tau^{-1} = G_\gamma$, da cui $G_\gamma\sigma\tau = G_\gamma\tau\sigma$ e dunque $G_\gamma\sigma G_\gamma\tau = G_\gamma\tau G_\gamma\sigma$, cioè il quoziente G/G_γ è abeliano. ♢

2.56 Teorema. *Sia $f(x)$ irriducibile e G ciclico. Allora G è generato da un ciclo di lunghezza n.*

Dim. Essendo $f(x)$ irriducibile G è transitivo, e se il generatore ha più di un ciclo, G non può essere transitivo. ♢

Un'equazione $f(x) = 0$ con $f(x)$ irriducibile e G ciclico, e dunque, per il teorema, generato da un ciclo di lunghezza n si dice *equazione ciclica.*

2.57 Corollario. *Un'equazione $f(x) = 0$ con $f(x)$ normale e di grado primo è ciclica.*

Dim. G è semi-regolare (Teor. 2.43), e dunque un suo elemento ha tutti i cicli della stessa lunghezza, per cui se non è l'identità ha un solo ciclo, di lunghezza p. Allora G è transitivo (e il polinomio è irriducibile) e dunque regolare e perciò ha ordine p. G coincide allora con il gruppo generato da un ciclo di lunghezza p. ♢

2.58 Lemma. *Un gruppo abeliano transitivo è regolare.*

Dim. Basta far vedere che G è semi–regolare, cioè che se $\sigma \in G$ fissa un elemento α, allora è l'identità, cioè fissa tutti gli elementi. Sia β un qualunque elemento. Allora per la transitività $\beta = \alpha^\tau$, per un certo τ, e dunque $\beta = \alpha^\tau = \alpha^{\sigma\tau} = \alpha^{\tau\sigma} = \beta^\sigma$. ♢

Ne segue:

2.59 Teorema. *Se il gruppo di Galois di un polinomio irriducibile è abeliano, allora il polinomio è normale.*

2.6 Gruppi primitivi e imprimitivi

2.60 Definizione. Sia G un gruppo transitivo su un insieme Ω. Un sottoinsieme Δ di Ω si chiama *blocco* o *sistema di imprimitività* di G se

$$\Delta^\sigma = \Delta \ \text{ oppure } \ \Delta^\sigma \cap \Delta = \emptyset,$$

per ogni $\sigma \in G$ (con Δ^σ denotiamo l'insieme $\{\alpha^\sigma, \alpha \in \Delta\}$). I sottoinsiemi a un solo elemento, l'insieme Ω e l'insieme vuoto sono blocchi *banali*. Se questi sono i soli blocchi il gruppo è *primitivo* (più precisamente, l'azione di G su Ω è primitiva); altrimenti G è *imprimitivo*.

I blocchi sono le classi di un'equivalenza su Ω compatibile con l'azione di G (cioè tale che se $\alpha \sim \beta$ allora $\alpha^\sigma \sim \beta^\sigma$). In particolare, i blocchi hanno tutti la stessa cardinalità, che dunque divide n, e G è transitivo sui blocchi.

2.61 Esempi. 1. Un gruppo può essere imprimitivo in più modi, nel senso che può avere diversi sistemi di imprimitività. Il gruppo ciclico generato dal ciclo $\sigma = (1,2,3,4,5,6)$ in S^6 ammette i sistemi di imprimitività $\Delta_1 = \{1,3,5\}, \Delta_2 = \{2,4,6\}$, e anche i sistemi $\Delta'_1 = \{1,4\}, \Delta'_2 = \{2,5\}, \Delta'_3 = \{3,6\}$ (i due sistemi corrispondono ai cicli di σ^2 e σ^3, rispettivamente).

2. Il gruppo diedrale D_4 dell'*Es.* 1 di 2.22 ammette i blocchi $\Delta_1 = \{1,2\}$, $\Delta_2 = \{3,4\}$, che corrispondono alle orbite del sottogruppo normale $\{I, (1,2)(3,4)\}$.

2.62 Teorema. *Sia G transitivo su Ω. Allora:*
i) Se $|\Omega|$ è primo, G è primitivo.

ii) Se G è imprimitivo, Δ è un blocco, e $\alpha \in \Delta$, allora $G_\alpha \subseteq G_\Delta$ (G_Δ è l'insieme degli elementi che lasciano fisso Δ come insieme). Più in generale, se $\alpha \in \Delta$ e $\alpha^\sigma \in \Delta$, allora $\sigma \in G_\Delta$.

iii) Se G è imprimitivo e Δ è un blocco, allora G_Δ è transitivo su Δ. In particolare, $G_\Delta \neq \{1\}$.

Sia H un sottogruppo normale di G.

iv) G agisce sull'insieme delle orbite di H e questa azione è transitiva. In particolare, le orbite di H hanno tutte la stessa cardinalità.

v) le azioni di H su queste orbite sono tutte tra loro simili.

vi) Se G è primitivo, H è transitivo oppure banale su Ω.

Dim. i) Ovvio.

ii) Se $\alpha \in \Delta$ e $\sigma \in G_\alpha$, si ha $\alpha^\sigma = \alpha$, cioè σ porta $\alpha \in \Delta$ in un elemento ancora di Δ. Ciò deve allora accadere per ogni elemento del blocco Δ.

iii) Siano $\alpha, \beta \in \Delta$. Per la transitività di G, esiste $\sigma \in G$ tale che $\alpha^\sigma = \beta$. Ma allora σ deve portare ogni elemento di Δ in un elemento ancora di Δ, e dunque $\sigma \in G_\Delta$.

iv) Siano Ω_1 e Ω_2 due orbite di H, $\alpha \in \Omega_1$ e $\beta \in \Omega_2$. Per la transitività di G esiste $\sigma \in G$ tale che $\alpha^\sigma = \beta$, e se $\alpha_1 \in \Omega_1$ allora, per certi $\tau, \tau' \in H$, $\alpha_1 = \alpha^\tau$ e $\alpha_1^\sigma = (\alpha^\tau)^\sigma = (\alpha^\sigma)^{\tau'} = \beta^\tau$. Ne segue che Ω_1^σ è contenuto nell'orbita Ω_2 di β secondo H. Analogamente, $\Omega_2^{\sigma^{-1}} \subseteq \Omega_1$, ed essendo $|\Omega_1^\sigma| = |\Omega_1|$ per ogni $\sigma \in G$ si ha $\Omega_1^\sigma = \Omega_2$. Ciò dimostra che G agisce sull'insieme delle orbite di H transitivamente.

v) Sia $\Delta_2 = \Delta_1^\sigma$ e $\varphi : \Delta_1 \to \Delta_2$ l'applicazione data da $\alpha \to \alpha^\sigma$, e θ l'automorfismo di H dato dal coniugio di G indotto da σ: $\theta(\tau) = \sigma^{-1}\tau\sigma$, $\tau \in H$. Con questi φ e θ si ha l'equivalenza richiesta:

$$\varphi(\alpha^\tau) = \alpha^{\tau\sigma} = (\alpha^\sigma)^{\sigma^{-1}\tau\sigma} = \varphi(\alpha)^{\theta(\tau)}.$$

vi) Se k è la cardinalità di un'orbita di H, allora k divide $|\Omega|$, e se $|\Omega|$ è primo, o $k = |\Omega|$ e c'è una sola orbita e quindi H è transitivo, oppure $k = 1$, e H è banale su Ω. ◊

2.63 Corollario. *Le orbite di un sottogruppo normale $H \neq \{1\}$ di un gruppo transitivo G costituiscono un sistema di imprimitività di G.* ◊

L'aggettivo "primitivo" è già stato usato per un elemento di un ampliamento i cui coniugati sono tutti distinti. Vediamo che relazione c'è tra questa nozione e quella di gruppo primitivo. Sia γ un elemento primitivo di $Q(\underline{\alpha})$ e sia η un elemento non primitivo. Si ha $\eta = \varphi(\gamma)$ per una certa φ, Poiché η non è primitivo, il suo stabilizzatore G_η è diverso da $\{1\}$; siano $\tau_1 = 1, \tau_2, \ldots \tau_r$ i suoi elementi. Siano poi $\sigma_1 = 1, \sigma_2, \ldots, \sigma_s$ rappresentanti dei laterali destri di G_η in G. Fissato σ_j si ha $\eta^{\sigma_j} = \eta^{\tau_i\sigma_j}$ per ogni $\tau_i \in G_\eta$. Ne segue, avendosi per ogni

$\sigma \in G$, $\eta^\sigma = \varphi(\gamma)^\sigma = \varphi(\gamma^\sigma)$:

$$\begin{array}{rcl}
\eta^{\sigma_1} & = & \varphi(\gamma^{\tau_1\sigma_1}) = \varphi(\gamma^{\tau_2\sigma_1}) = \ldots = \varphi(\gamma^{\tau_r\sigma_1}),\\
\eta^{\sigma_2} & = & \varphi(\gamma^{\tau_1\sigma_2}) = \varphi(\gamma^{\tau_2\sigma_2}) = \ldots = \varphi(\gamma^{\tau_r\sigma_2}),\\
\vdots & & \vdots \qquad\qquad \vdots \qquad \vdots\\
\eta^{\sigma_s} & = & \varphi(\gamma^{\tau_1\sigma_s}) = \varphi(\gamma^{\tau_2\sigma_s}) = \ldots = \varphi(\gamma^{\tau_r\sigma_s}),
\end{array}$$

per ogni σ_j. Essendo γ primitivo, gli $r \cdot s$ elementi $\gamma^{\tau_i\sigma_j}$ sono tutti distinti. Posto $\gamma^{\tau_i\sigma_j} = \gamma_{i,j}$, si ha

$$\begin{array}{rcl}
\Delta_1 & = & \{\gamma_{1,1}, \quad \gamma_{2,1}, \quad \ldots, \quad \gamma_{r,1}\},\\
\Delta_2 & = & \{\gamma_{1,2}, \quad \gamma_{2,2}, \quad \ldots, \quad \gamma_{r,2}\},\\
\vdots & & \vdots \qquad \vdots \qquad \vdots \qquad \vdots\\
\Delta_s & = & \{\gamma_{1,s}, \quad \gamma_{2,s}, \quad \ldots, \quad \gamma_{r,s}\},
\end{array}$$

e i Δ_i formano un sistema di imprimitività per il gruppo G. Facendo infatti agire un elemento $\sigma \in G$, si ha $\gamma_{i,j}^\sigma = (\gamma^{\tau_i\sigma_j})^\sigma$, e se $\sigma_j\sigma = \tau_k\sigma_l$ allora

$$\gamma^{(\tau_i\sigma_j)\sigma} = \gamma^{\tau_i(\sigma_j\sigma)} = \gamma^{\tau_i(\tau_h\sigma_l)} = \gamma^{(\tau_i\tau_h)\sigma_l} = \gamma^{\tau_k\sigma_l},$$

per un certo $\tau_k \in G_\eta$, e dunque nell'azione di σ l'intera $j-$esima riga va nella $l-$esima. Dunque, il gruppo G è imprimitivo.

Viceversa, sia G imprimitivo, Δ un blocco, $H = G_\Delta$, e sia β tale che $H = G_\beta$ (Teor. 2.37). Allora $G_\beta \neq \{1\}$ (Teor. 2.62, *iii*)), e dunque β non è primitivo (Teor. 2.29).

2.64 Definizione. Diremo che un ampliamento $K(\underline{\alpha})$ è *primitivo* se ogni suo elemento è primitivo, cioè se $K(\underline{\alpha}) = K(\gamma)$ per ogni $\gamma \in K(\alpha)$; lo diremo *imprimitivo* nell'altro caso.

Quanto appena visto dimostra allora il seguente risultato:

2.65. Teorema. *Il gruppo di Galois G è primitivo se e solo se il campo $K(\underline{\alpha})$ è primitivo.*

Il teorema seguente caratterizza i polinomi a gruppo di Galois imprimitivo.

2.66. Teorema. *Il gruppo di Galois G è di un polinomio $f(x)$ è imprimitivo se e solo se $f(x)$ divide la composizione $g(h(x))$ di due polinomi di grado minore del grado di $f(x)$ e con $g(x)$ irriducibile. In tal caso le radici di $f(x)$ si suddividono in un numero di blocchi pari al grado di $g(x)$.*

Dim. Sia G imprimitivo, con r blocchi di cardinalità s. Sia α una radice, Δ il blocco che contiene α, e β tale che $H = G_\Delta = G_\beta$. Avendosi $G_\alpha \subseteq G_\Delta$ (Teor.

2.62, *ii*)) si ha $\beta = h(\alpha)$ per un certo polinomio $h(x)$. Sia $g(x)$ il polinomio minimo di β; allora il grado di $g(x)$ è $[G : G_\Delta]$, ed essendo G transitivo sui blocchi questo indice è pari al numero dei blocchi. Ma $g(h(\alpha)) = g(\beta) = 0$, e dunque $f(x)$ divide $g(h(x))$.

Viceversa, supponiamo che $f(x)$ divida una composizione $g(h(x))$, con $g(x)$ irriducibile, e sia r il grado di $g(x)$. Per ipotesi $g(h(x)) = f(x)k(x)$, e dunque se α è una radice di $f(x)$, $h(\alpha)$ lo è di $g(x)$. Sia:

$$\beta_1 = h(\alpha_{1,1}) = h(\alpha_{1,2}) = \ldots = h(\alpha_{1,s})$$

Allora β_1 è una radice di $g(x)$, ed essendo $\beta_1 \in K(\underline{\alpha})$, per l'irriducibilità di $g(x)$ tutte le sue radici $\beta_1, \beta_2, \ldots, \beta_r$ sono in $K(\underline{\alpha})$. Ne segue che il gruppo di Galois G agisce sulle β_i. Poniamo:

$$\Delta_i = \{\alpha_{i,j} \mid h(\alpha_{i,j}) = \beta_i\}.$$

Gli insiemi Δ_i costituiscono una partizione delle radici di $f(x)$; dimostriamo che si tratta di blocchi di G. Siano $\alpha_{i,k}, \alpha_{i,l} \in \Delta_i$ e $\beta_i^\sigma = \beta_j$. Allora $h(\alpha_{i,k}^\sigma) = h(\alpha_{i,l}^\sigma) = \beta_i^\sigma = \beta_j$, e dunque $\alpha_{i,k}^\sigma, \alpha_{i,l}^\sigma \in \Delta_j$. Pertanto, il gruppo G permuta i Δ_i, e dunque è imprimitivo. $\diamondsuit$

2.67 Esempio. Il gruppo di Galois del polinomio $f(x) = x^4 - 2$ è imprimitivo (*Es.* 2 di 2.61). La radice $\alpha_1 = \sqrt[4]{2}$ appartiene al blocco $\Delta = \{\alpha_1, -\alpha_1\}$, e $G_{\Delta_1} = \{I, (1,2), (3,4), (1)(2)(3,4), (1,2)(3)(4)\}$. Questo gruppo stabilizza l'elemento $-\alpha_1\alpha_2 = \alpha_1^2$, e $\alpha_1^2 = h(\alpha_1)$, con $h(x) = x^2$. Il polinomio minimo di α_1^2 $(=\sqrt{2})$ è $g(x) = x^2 - 2$, per cui $f(x) = g(h(x))$.

2.68 Nota. Una volta noto il polinomio $h(x)$, un modo per determinare $g(x)$ come polinomio minimo di $h(\alpha)$, dove α è una radice di $f(x)$, è considerare il risultante $R = R(f(y), x - h(y))$ rispetto alla variabile x. Se α non è un elemento primitivo, R è una potenza di $g(x)$. Occorre allora dividere R per il massimo comun divisore tra R stesso e la sua derivata.

Se G è imprimitivo con blocchi $\Delta_i = \{\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,s}\}, i = 1, 2 \ldots, r$, consideriamo lo stabilizzatore G_{Δ_i} di Δ_i, e gli elementi:

$$\gamma_i = (a - \alpha_{i,1})(a - \alpha_{i,2}) \cdots (a - \alpha_{i,s}),$$

$i = 1, 2 \ldots, r$ e $a \in K$. Scegliendo opportunamente l'elemento a (al di fuori di un numero finito di elementi di K), si può fare in modo che i γ_i siano tutti distinti. Si tratta allora dei $[G : G_{\Delta_i}] = r$ coniugati di γ_i. I coefficienti del polinomio:

$$g_i(x) = (x - \alpha_{i,1})(x - \alpha_{i,2}) \cdots (x - \alpha_{i,s})$$

appartengono al campo $K(\gamma_i)$, in quanto funzioni razionali delle radici di $f(x)$ che restano invariate sotto l'azione di G_{Δ_i} (che è il gruppo di Galois di $f(x)$ su

$K(\gamma_i)$). Scriviamo allora $g(x,\gamma_i)$ invece di $g_i(x)$. Inoltre, $g(x,\gamma_i)$ è irriducibile su $K(\gamma_i)$, in quanto G_{Δ_i} è transitivo su Δ_i. Se ne conclude che nella fattorizzazione

$$f(x) = (x-\alpha_{1,1})(x-\alpha_{1,2})(x-\alpha_{1,s})\cdots(x-\alpha_{r,1})(x-\alpha_{r,2})(x-\alpha_{r,s})$$

di $f(x)$ su $K(\underline{\alpha})$, si possono raggruppare i termini e scrivere

$$f(x) = g(x,\gamma_1)g(x,\gamma_2)\cdots g(x,\gamma_r)$$

dove $g(x,\gamma_i)$ è di grado s e irriducibile su $K(\gamma_i)$, $i = 1, 2\ldots, r$.

2.7 Automorfismi di un ampliamento

Se $\sigma \in S^n$, l'applicazione $K(\underline{\alpha}) \to K(\underline{\alpha})$ data da:

$$g(\underline{\alpha}) \longrightarrow g(\underline{\alpha}^\sigma) \tag{2.9}$$

non è in generale ben definita.

2.69 Esempio. Con $f(x) = x^4 - 2$, $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = -\alpha_1$, $\alpha_3 = i\alpha_1$, $\alpha_4 = -i\alpha_1$, l'elemento $\gamma = \sqrt{2} - 2$ rappresenta $\alpha_1^2 - 2$ e anche $\alpha_2^2 - 2$. Una permutazione σ che porti α_1 in α_2 e α_2 in α_3 fornisce per γ^σ due valori distinti: $\sqrt{2} - 2$ nel primo caso, $-\sqrt{2} - 2$ nel secondo.

Se però ci si limita alle permutazioni del gruppo di Galois del polinomio, allora:

2.70 Teorema. *i) Sia σ una permutazione del gruppo di Galois di $f(x)$ su K. Allora la (2.13) è ben definita, e σ si estende a un automorfismo τ del campo $K(\underline{\alpha})$ che lascia fissi gli elementi di K.*

ii) Viceversa, sia τ un automorfismo di $K(\underline{\alpha})$ che lascia fissi gli elementi di K. Allora la restrizione di τ all'insieme delle α_i è una permutazione delle α_i che appartiene al gruppo di Galois di $f(x)$.

Dim. *i)* Se $g(\underline{\alpha})$ e $g_1(\underline{\alpha})$ hanno lo stesso valore numerico, la differenza $g(\underline{\alpha}) - g_1(\underline{\alpha}) = 0$ è una relazione su K tra le α_i. Essa resta allora soddisfatta applicando σ: $g(\underline{\alpha}^\sigma) - g_1(\underline{\alpha}^\sigma) = 0$, cioè $g(\underline{\alpha}^\sigma) = g_1(\underline{\alpha}^\sigma)$.

L'applicazione $g(\underline{\alpha}) \longrightarrow g(\underline{\alpha}^\sigma)$ è quindi ben definita. Inoltre è suriettiva ($g(\underline{\alpha})$ proviene da $g(\underline{\alpha}^{\sigma^{-1}})$) e iniettiva (se $\gamma^\sigma = \eta^\sigma$, allora applicando σ^{-1} alla relazione $\gamma^\sigma - \eta^\sigma = 0$ si ottiene $\gamma - \eta = 0$ e $\gamma = \eta$). Infine, per definizione di gruppo di Galois, gli elementi di K sono fissati da σ.

ii) τ conserva somme e prodotti, fissa gli elementi di K e induce una permutazione delle radici di $f(x)$: da $f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n\alpha = 0$ si ha infatti

$$\begin{aligned} 0 = \tau(0) = \tau(f(\alpha)) &= \tau(a_0)\tau(\alpha)^n + \tau(a_1)\tau(\alpha)^{n-1} + \cdots + \tau(a_n) \\ &= a_0\tau(\alpha)^n + a_1\tau(\alpha)^{n-1} + \cdots + a_n \\ &= f(\tau(\alpha)), \end{aligned}$$

e dunque $\tau(\alpha)$ è ancora radice di $f(x)$. Se $\varphi(\underline{\alpha}) = 0$ è una relazione, segue allora

$$0 = \tau(0) = \tau(\varphi(\underline{\alpha})) = \varphi(\alpha_{\tau(1)}, \alpha_{\tau(2)}, \ldots, \alpha_{\tau(n)}).$$

Se ne conclude che la permutazione indotta da τ porta relazioni in relazioni e appartiene pertanto al gruppo di Galois di $f(x)$. $\diamondsuit$

Il teorema ora dimostrato permette di definire il gruppo di Galois in termini del campo $K(\underline{\alpha})$ come *il gruppo degli automorfimi di* $K(\underline{\alpha})$ *che lasciano fissi gli elementi di* K (gruppo degli automorfismi di $K(\underline{\alpha})$ *su* K).