Capitolo 3

Risolubilità per radicali e teorema fondamentale

3.1 Equazioni binomie

3.1 Definizione. Se a è un elemento non nullo di un campo K l'equazione $x^n - a = 0$ si chiama *equazione binomia* (o *equazione pura*).

3.2 Definizione. La *funzione di Eulero* è definita per ogni intero positivo n come segue:

$\varphi(1) = 1$;

$\varphi(n) =$ numero degli interi minori di n e primi con n.

Gli interi minori di n e primi con n formano gruppo rispetto alla moltiplicazione mod n; si denota con $U(n)$.

3.3 Teorema. *Il gruppo di Galois G dell'equazione binomia è un sottogruppo del gruppo delle trasformazioni lineari $\mathcal{L}_n$ su $\mathbf{Z}_n$:*

$$x \to kx + t, \quad (k, n) = 1, \ t = 0, 1, \ldots, n-1 \bmod n. \tag{3.1}$$

$\mathcal{L}_n$ ha ordine $n\varphi(n)$, e dunque $|G|$ è un divisore di $n\varphi(n)$.

Dim. Se α è una radice di $f(x)$, le altre si ottengono moltiplicando questa per le potenze di una radice primitiva $n-$esima dell'unità ε:

$$\alpha, \varepsilon\alpha, \varepsilon^2\alpha, \ldots, \varepsilon^{n-1}\alpha,$$

(posto $x = ay$ l'equazione data si trasforma nella $y^n - 1$). Sia $\alpha_i = \varepsilon^i\alpha$, $i = 0, 1, \ldots, n-1$. Il campo $K(\underline{\alpha})$ si ottiene dunque aggiungendo α e ε a K:

$$K(\underline{\alpha}) = K(\varepsilon, \alpha).$$

Si osservi che ε è una funzione razionale delle α_i (ad esempio, $\varepsilon = \frac{\alpha_1}{\alpha_0}$). Il polinomio minimo di ε su K è il polinomio ciclotomico $\Phi_n(x)$, che per il Cor. 2.33 è uguale a $\prod_{i=1}^{s}(x - \varepsilon^{\sigma_i})$. Allora $s = \varphi(n)$, G permuta le radici di $\Phi_n(x)$, e dunque porta radici primitive dell'unità in radici primitive dell'unità. Sia $\sigma \in G$; allora $\sigma(\varepsilon) = \varepsilon^k$, per un certo k primo con n. Inoltre,

$$\sigma(\varepsilon) = \sigma(\frac{\varepsilon\alpha}{\alpha}) = \sigma(\frac{\alpha_1}{\alpha}) = \frac{\sigma(\alpha_1)}{\sigma(\alpha)} = \frac{\sigma(\varepsilon\alpha)}{\sigma(\alpha)},$$

da cui

$$\sigma(\varepsilon\alpha) = \sigma(\varepsilon)\sigma(\alpha),$$

e perciò $\sigma(\varepsilon\alpha) = \varepsilon^k\sigma(\alpha)$. Sia $\sigma(\alpha) = \varepsilon^t\alpha$; allora l'elemento σ di G determina univocamente due interi k e t. Per la generica radice $\alpha_h = \varepsilon^h\alpha$ si ha allora:

$$\sigma(\alpha_h) = \sigma(\varepsilon^h\alpha) = \sigma(\varepsilon^h)\sigma(\alpha) = \sigma(\varepsilon)^h\sigma(\alpha) = \varepsilon^{kh}\sigma(\alpha) = \varepsilon^{kh+t}\alpha = \alpha_{kh+t}$$

ciò che permette di identificare σ con la trasformazione $x \to kx + t$ di $\mathcal{L}_n$, e stabilire quindi un isomorfismo tra G e un sottogruppo di $\mathcal{L}_n$. $\diamondsuit$

Le trasformazioni (3.1) con $k = 1$ formano un sottogruppo ciclico $\mathcal{T}_n$ di $\mathcal{L}_n$, di ordine n, generato dalla trasformazione $x \to x + 1$ (o da una qualunque $x \to x + t$ con $(t, n) = 1$). $\mathcal{T}_n$ è il sottogruppo delle *traslazioni*, ed è ovviamente isomorfo a $\mathbf{Z}_n$.

3.4 Teorema. *i) $\mathcal{T}_n$ è normale in $\mathcal{L}_n$;*

ii) se $n = p$, primo, un sottogruppo transitivo H di $\mathcal{L}_p$ contiene $\mathcal{T}_p$.

Dim. i) Sia $\sigma : x \to kx + s$, $\tau : x \to x + t$. Allora $\sigma^{-1} : x \to k^{-1}x - k^{-1}s$, e $\sigma^{-1}\tau\sigma : x \to x + kt$, ancora una traslazione.

ii) Avendosi $|H| \mid p(p-1)$, se H non contiene traslazioni il suo ordine divide $p - 1$ e dunque è minore di p. H non può allora essere transitivo. $\diamondsuit$

Estendiamo ora il campo K aggiungendo ε.

3.5 Teorema. *Il gruppo di Galois $\mathcal{T}$ su $K(\varepsilon)$ dell'equazione binomia è dato dall'intersezione del gruppo di Galois G su K con $\mathcal{T}_n$, e dunque, come sottogruppo di $\mathcal{T}_n$, è ciclico. Inoltre, $\mathcal{T}$ è normale in G e il quoziente $G/\mathcal{T}$ è abeliano.*

Dim. Poiché gli elementi di $\mathcal{T}$ sono gli elementi di G che lasciano fissi gli elementi di $K(\varepsilon)$, si ha $\tau(\varepsilon) = \varepsilon$ per $\tau \in \mathcal{T}$. Allora $\tau(\varepsilon\alpha) = \varepsilon\tau(\alpha)$, e pertanto la trasformazione associata a τ è del tipo $x \longrightarrow x + t$, per un certo t. Ne segue $\tau \in \mathcal{T}_n$. Inoltre, il polinomio ciclotomico è normale, e dunque il gruppo di Galois $\mathcal{T}$ su $K(\varepsilon)$ è normale in G, e il quoziente è abeliano perché isomorfo al gruppo di Galois del polinomio ciclotomico (*Es.* 3 di 2.22). $\diamondsuit$

3.6 Teorema. *L'ordine f di $\mathcal{T}$ è un divisore di n ed è il più piccolo intero k tale che α_i^k appartiene a $K(\varepsilon)$, dove α è una qualunque radice dell'equazione binomia.*

Dim. Intanto $(\varepsilon^s\alpha)^k \in K(\varepsilon)$ se e solo se $(\varepsilon^t\alpha)^k \in K(\varepsilon)$, e ciò permette di considerare una radice α qualunque; inoltre, c'è almeno la potenza $n-$esima di α che appartiene a K, e dunque a $K(\varepsilon)$. Poiché $\mathcal{T}$ è un sottogruppo di $\mathbf{Z}_n$, $|\mathcal{T}|$ divide n. Sia $\mathcal{T}$ generato da τ. Allora α^k appartiene a $K(\epsilon)$ se e solo se $\tau(\alpha^k) = \alpha^k$. Sia (notazione del Teor. 3.3): $\tau(\alpha) = \alpha_t = \epsilon^t\alpha$. Allora:

$$\tau(\alpha^k) = \tau(\alpha)^k = \alpha_t^k = \varepsilon^{tk}\alpha^k,$$

e dunque $\tau(\alpha^k) = \alpha^k$ se e solo se $\varepsilon^{tk} = 1$. D'altra parte se f è l'ordine di τ, f è il più piccolo intero tale che $\tau^f = I$ e perciò

$$\alpha^k = \tau^f(\alpha^k) = (\tau^f(\alpha))^k = \alpha_{ft}^k = \varepsilon^{ft}\alpha^k,$$

da cui $\varepsilon^{ft} = 1$. f è dunque il più piccolo intero tale che $\varepsilon^{ft} = 1$. $\diamondsuit$

Il quoziente $G/\mathcal{T}$ è isomorfo al gruppo di Galois di $\Phi(x)$ su K, e dunque il suo ordine è $\varphi(n)$. Ne segue:

3.7 Teorema. *L'ordine del gruppo di Galois su K dell'equazione binomia è uguale al prodotto $f \cdot \varphi(n)$.*

3.8 Esempio. Sia $f(x) = x^4 - a$ su $\mathcal{Q}$, e siano

$$\alpha_1 = \alpha, \alpha_2 = i\alpha, \alpha_3 = i^2\alpha, \alpha_4 = i^3\alpha,$$

le radici di $f(x)$. Se $\sigma \in G$, allora $\sigma(i) = i$, oppure $\sigma(i) = -i$.

(i) Sia $\sigma(i) = i$; l'intero k del Teor. 3.3 è uguale a 1.
Se $\sigma(\alpha) = i\alpha = \alpha_2$, si ha $t = 1$ e σ determina la trasformazione $x \longrightarrow x + 1$. Ne segue:

$$\sigma(\alpha_2) = \sigma(i\alpha) = \sigma(i)\sigma(\alpha) = i\sigma(\alpha) = i \cdot i\alpha = i^2\alpha = \alpha_3$$

e analogamente $\sigma(\alpha_3) = \alpha_4$, $\sigma(\alpha_4) = \alpha_1$ e dunque $\sigma = (1, 2, 3, 4)$.

Se $\sigma(\alpha) = \alpha_3$ vengono determinate la trasformazione $x \longrightarrow x + 2$, e la permutazione (1,3)(2,4). Se $\sigma(\alpha) = \alpha_4$, la trasformazione è $x \longrightarrow x + 3$, e la permutazione $(1, 4, 3, 2)$.

(ii) Se $\sigma(i) = i^3$, si hanno analogamente le trasformazioni $x \longrightarrow 3x$, $x \longrightarrow 3x + 1$, $x \longrightarrow 3x + 2$, e $x \longrightarrow 3x + 3$. Si ottiene così il gruppo diedrale D_4:

{I,(1,2,3,4),(1,3)(2,4),(1,4,3,2),(1,2)(3,4),(1,3)(2)(4),(1)(2)(3,4),(1,4)(2,3)}.

Il gruppo di Galois di $x^4 - a$ è perciò un sottogruppo di D_4. Ad esempio, per $a = 2$ sappiamo che è tutto D_4 (*Es.* 1 di 2.22), mentre per $a = -1$ abbiamo visto (*Es.* 5 di 2.53) che il gruppo di $x^4 + 1$ è il gruppo di Klein

$$V = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

(*Es.* 5 di 2.53). In questo secondo caso infatti si ha $\alpha = \sqrt[4]{-1} = \sqrt{i}$, e dunque $\alpha_1\alpha_2 + 1 = 0$. Il ciclo (1,2,3,4) porta $\alpha_1\alpha_2$ in $\alpha_2\alpha_3$ che è uguale a 1., e perciò non appartiene al gruppo di Galois. Si vede analogamente che le sole permutazioni di D_4 ammesse sono quelle di V.

Aggiungiamo ora i a $\mathcal{Q}$. Dovendo i restare fisso, il gruppo di Galois G_1 di $x^4 - 1$ su $\mathcal{Q}(i)$ è un sottogruppo di $\{I, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$. Dunque $G_1 = G \cap V = \{I, (1,3)(2,4)\}$. Si osservi che G_1 ha ordine 2, e infatti $\alpha^f \in \mathcal{Q}(i)$ con $f = 2$: $\alpha^2 = (\sqrt{i})^2 = i \in \mathcal{Q}(i)$.

Può ben accadere che un'equazione binomia irriducibile su K si spezzi su $K(\varepsilon)$.

3.9 Esempio. Con $K = \mathcal{Q}$, il polinomio $x^4 + 1$, irriducibile su K si spezza su $K(i)$: $x^4 + 1 = (x^2 - i)(x^2 + i)$. Il gruppo di Galois di questo polinomio su K è il gruppo di Klein, e dunque è abeliano.

Se però il polinomio resta irriducibile su $K(\epsilon)$, allora:

3.10 Corollario. *i) Se l'equazione binomia è irriducibile su $K(\varepsilon)$, allora il gruppo di Galois G su $K(\varepsilon)$ coincide con $\mathcal{T}_n$;*

ii) se $\varepsilon \notin K$, il gruppo di Galois G su K non può essere abeliano;

iii) se $n = p$, primo, allora su $K(\varepsilon)$ l'equazione o è irriducibile oppure si spezza in fattori lineari su $K(\varepsilon)$ (le radici appartengono a $K(\varepsilon)$).

Dim. i) Su $K(\varepsilon)$ è $G = \mathcal{T}$; essendo $f(x)$ irriducibile e G ciclico, G è generato da un ciclo di lunghezza n (Teor. 2.56), e dunque $G = \mathcal{T}_n$.

ii) Su K, se G fosse abeliano, essendo transitivo sarebbe regolare, e quindi avrebbe ordine n, e perciò $G = \mathcal{T}_n$. Ma allora $K = K(\varepsilon)$, contro l'ipotesi.

iii) Se l'equazione non è irriducibile, per *i)* il gruppo di Galois su $K(\varepsilon)$ non può essere $\mathcal{T}_p$, e dunque è l'identità; l'equazione si spezza allora in fattori lineari. ♢

3.11. Teorema. *Se p è un primo ed ε una radice primitiva $p-$esima dell'unità, allora un'equazione binomia $x^p - a$ irriducibile su K resta irriducibile su $K(\varepsilon)$.*

Dim. (Se $p = 2$, poiché $-1 \in K$ non c'è niente da dimostrare). Se l'equazione è irriducibile su K il gruppo di Galois è transitivo e dunque (Teor. 3.4) contiene $\mathcal{T}_p$. Ma per il Teor. 3.5 $\mathcal{T}_p$ è il gruppo di Galois di $x^p - a$ su $K(\varepsilon)$, ed essendo transitivo il polinomio è irriducibile. ♢

Un importante caso particolare di equazione binomia si ha per $a = -1$. Il polinomio $x^n - 1$ ha come radici le radici $n-$esime dell'unità. Il prodotto delle radici primitive $n-$esime è il *polinomio ciclotomico* $\Phi_n(x)$ (abbiamo già considerato il caso $n = p$; v. *Es.* 3 di 2.22). Se d divide n, e ε è una radice primitiva $n-$esima, allora $\varepsilon^{\frac{n}{d}}$ è una radice primitiva $d-$esima; si ha:

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{3.2}$$

3.12 Esempi. 1. Per $n = 1$ c'è la sola radice $x = 1$, ovviamente primitiva, e $\Phi_1(x) = x - 1$. Per $n = 2$ abbiamo due radici, 1 e -1, delle quali solo la seconda è primitiva; dunque $\Phi_2(x) = x + 1$. Una radice prima o seconda è anche radice quarta: i e $-i$ sono primitive quarte, $\Phi_4(x) = (x-i)(x+i) = x^2+1$ e $x^4 - 1 = (x-1)(x+1)(x-i)(x+i) = \Phi_1(x)\Phi_2(x)\Phi_4(x)$.

2. Per $n = 8$ si hanno le quattro radici primitive $\sqrt{i}, -\sqrt{i}, \sqrt{-i}, -\sqrt{i}$ (v. *Es.* 2 di 2.22) e il polinomio $\Phi_8(x) = x^4 + 1$.

3.13 Teorema. *Il polinomio $\Phi_n(x)$ è:*

i) a coefficienti interi;

ii) irriducibile su $\mathcal{Q}$;

il gruppo di Galois G di $\Phi_n(x)$ è:

iii) abeliano, isomorfo al gruppo $U(n)$ degli interi minori di n e primi con n (dunque ha ordine $\varphi(n)$);

iv) regolare.

Dim. i) Induzione su n. Se $n = 1$, $\Phi_1(x) = x - 1$, che è a coefficienti interi. Supponiamo il teorema vero per $\Phi_m(x)$, $m < n$. Dalla (4.2) abbiamo

$$x^n - 1 = \prod_{d|n, d<n} \Phi_d(x) \cdot \Phi_n(x).$$

Per induzione i $\Phi_d(x)$ sono a coefficienti interi e di coefficiente direttore 1, e dunque anche il loro prodotto è a coefficienti interi e di coefficient direttore 1. Il quoziente di $x^n - 1$ per questo prodotto è allora a coefficienti interi; ma questo quoziente è proprio $\Phi_n(x)$.

ii) Facciamo vedere che se ε è una radice primitiva $n-$esima dell'unità, ogni altra radice primitiva è radice di ogni polinomio a coefficienti razionali (interi) di cui è radice ε. Diamo una dimostrazione che si basa sul teorema di Dirichlet secondo il quale se $(r, n) = 1$, nella progressione aritmetica $r + kn$, $k = 1, 2, \ldots$, compaiono infiniti numeri primi. Per ogni primo p della progressione si ha $\varepsilon^p = \varepsilon^{r+kn} = \varepsilon^r \cdot \varepsilon^{kn} = \varepsilon^r$. Se ora $f(x)$ è un polinomio che ammette ε come radice, da $f(\varepsilon) = 0$ si ha $0 = f(\varepsilon)^p \equiv f(\varepsilon^p) = f(\varepsilon^r) \bmod p$ (la congruenza segue da note proprietà dei campi finiti). Il numero $f(\varepsilon^r)$ è dunque divisibile per infiniti primi, e perciò è zero, cioè ε^r è radice di $f(x)$. Poiché, essendo

$(r,n) = 1$, ε^r è primitiva, abbiamo quanto richiesto. Se $f(x)$ è il polinomio minimo irriducibile su $\mathcal{Q}$ che ammette la radice ε esso divide $\Phi_n(x)$, e dunque avendo tutte le radici di $\Phi_n(x)$ lo uguaglia.

iii) Se $\varepsilon_1 = \varepsilon$ è una radice di $\Phi_n(x)$, le altre sono $\varepsilon_2 = \varepsilon^{k_2}, \varepsilon_3 = \varepsilon^{k_3}, \ldots, \varepsilon_m = \varepsilon^{k_m}$, con $m = \varphi(n)$ e $k_1, k_2, \ldots, k_m$ gli interi minori di n e primi con n. Se $\sigma \in G$, allora se $\sigma(\varepsilon) = \varepsilon_i$ si ha

$$\sigma(\varepsilon_j) = \sigma(\varepsilon^{k_j}) = (\sigma(\varepsilon))^{k_j} = (\varepsilon_i)^{k_j} = \varepsilon^{k_i k_j}.$$

L'immagine di ε determina quindi l'immagine di ogni altra radice ε_j. Fissato k_i, i prodotti $k_i k_j$ riproducono, al variare di j, tutti gli interi k_l, $l = 1, 2, \ldots, m$. Inoltre $\Phi_n(x)$ è irriducibile, e dunque G è transitivo. La corrispondenza $\sigma \longrightarrow k_i$ è univoca perché se σ e τ determinano lo stesso k_i allora determinano anche le stesse immagini di tutte le ε_k, e dunque sono la stessa permutazione. Inoltre è suriettiva per via della transitività di G. Si vede poi facilmente che se a τ corrisponde k_j, al prodotto $\sigma\tau$ corrisponde il prodotto $k_i k_j$. La corrispondenza è perciò un isomorfismo. (Che il gruppo sia abeliano si vede anche direttamente come segue: da $\varepsilon^\sigma = \varepsilon^k$ e $\varepsilon^\tau = \varepsilon^h$ abbiamo $\varepsilon^{\sigma\tau} = (\varepsilon^\sigma)^\tau = (\varepsilon^k)^\tau = (\varepsilon^k)^h = \varepsilon^{kh} = \varepsilon^{hk} = (\varepsilon^h)^k = (\varepsilon^\tau)^k = (\varepsilon^\tau)^\sigma = \varepsilon^{\tau\sigma}$, e dunque $\sigma\tau = \tau\sigma$ e il gruppo è abeliano; v. Teor. 2.54, con $\theta_\sigma(\varepsilon) = \varepsilon^k$)

iv) Il gruppo è regolare perché è transitivo e abeliano (Lemma 2.58). ♢

3.14 Esempi. 1. Il polinomio $\Phi_8(x)$ è il polinomio $x^4 + 1$ (v. *Es.* 5 di 2.53). Il suo gruppo di Galois è il gruppo di Klein, isomorfo al gruppo degli interi minori di 8 e primi con 8: $\{1, 3, 5, 7\}$.

2. Se p è primo, il gruppo di $\Phi_p(x)$ è ciclico di ordine $p - 1$ (v. *Es.* 3 di 2.22).

3.2 Risolubilità per radicali

Vediamo ora per quali polinomi le radici si possono esprimere per mezzo di operazioni razionali ed estrazioni di radici. A priori, è possibile che i radicali riguardino elementi non appartenenti a $K(\underline{\alpha})$, cioè elementi che non sono funzioni razionali delle radici. In questo caso tuttavia le radici si esprimono anche per radicali di elementi di $K(\underline{\alpha})$: è quanto afferma un teorema di Abel (teorema delle irrazionalità naturali) sul quale torneremo nel Cap. 4 (Teor. 4.3).

Si tratta quindi di raggiungere il campo di spezzamento $K(\underline{\alpha})$ a partire da K attraverso successive aggiunte di radicali $\sqrt[t]{a}$ in modo tale che a ogni passo a appartenga al campo già costruito.

3.15 Definizione. L'equazione $f(x) = 0$ a coefficienti in K si dice *risolubile*

per radicali (o *risolubile algebricamente*) se esiste una successione di campi:

$$K \subset K_1 = K(a_1) \subset K_2 = K_1(a_2) \subset \ldots \subset K_s = K_{s-1}(a_s) \subset K_s = K(\underline{\alpha}), \tag{3.3}$$

e $a_1^{r_1} \in K$, $a_2^{r_2} \in K_2, \ldots$, $a_s^{r_s} \in K_{s-1}$ per opportuni interi $r_i, i = 1, 2, \ldots, s$. Un campo K_i è un *ampliamento* (o *estensione*) *radicale* dei campi K_{i-1}, $i = 1, 2, \ldots, s$, $K_0 = K$, che lo precedono.

Gli a_i sono soluzioni di equazioni del tipo $x^r = c$. Se $r = pk$, p primo, una tale equazione è equivalente alle due: $x^p = c$ e $x^k = \gamma$, dove γ è un'opportuna radice $p-$esima di c (in altri termini, si può ridurre $\sqrt[pk]{c}$ a $\sqrt[k]{\sqrt[p]{c}}$). Se k non è primo si può procedere allo stesso modo, e concludere che gli esponenti r_i della Def. 3.15 si possono supporre numeri primi.

Può ben accadere che si possa trovare un'espressione delle radici di un polinomio per radicali di elementi non appartenenti a $K(\underline{\alpha})$. Ma allora si può anche trovare un'espressione per radicali di elementi di $K(\underline{\alpha})$ (v. Cap. 4, Teor. 4.3). Ciò giustifica la limitazione a $K(\underline{\alpha})$ della definizione di ampliamento radicale. Pertanto un'equazione è risolubile per radicali se le radici si trovano in un ampliamento radicale di K, cioè se $K(\underline{\alpha})$ è un ampliamento radicale di K.

Veniamo ora al:

3.16 Teorema. *Un'equazione ciclica è risolubile per radicali.*

Dim. Diamo una dimostrazione dovuta a Lagrange. Possiamo supporre che il polinomio sia irriducibile. Siano le radici della forma $\alpha, \vartheta(\alpha), \vartheta^2(\alpha), \ldots, \vartheta^{n-1}(\alpha)$, per una data funzione razionale $\vartheta(x)$ con $\vartheta^n(x) = x$. Sia ζ una qualunque radice $n-$esima dell'unità (non necessariamente primitiva), e sia

$$\varphi(x) = x + \zeta\vartheta(x) + \zeta^2\vartheta^2(x) + \cdots + \zeta^{n-1}\vartheta^{n-1}(x).$$

Allora

$$\varphi(\vartheta(x)) = \vartheta(x) + \zeta\vartheta^2(x) + \zeta^2\vartheta^3(x) + \cdots + \zeta^{n-1}x$$

e dunque $\varphi(\vartheta(x)) = \zeta^{-1}\varphi(x)$, e in generale $\varphi(\vartheta^k(x)) = \zeta^{-k}\varphi(x)$. Elevando alla potenza $n-$esima

$$\varphi(\vartheta^k(x))^n = \varphi(x)^n$$

Posto $\psi(x) = \varphi(x)^n$, la funzione $\psi(x)$ è tale che $\psi(\vartheta^k(x)) = \psi(x)$; ne segue:

$$n\psi(x) = \psi(x) + \psi(\vartheta(x)) + \psi(\vartheta^2(x)) + \cdots + \psi(\vartheta^{n-1}(x)).$$

Sia $x = \alpha$. Le permutazioni del gruppo di Galois (che è generato dal ciclo $(\alpha, \vartheta(\alpha), \vartheta^2(\alpha), \ldots, \vartheta^{n-1}(\alpha))$, mutano $n\psi(\alpha)$ in sé e dunque $n\psi(\alpha) \in K(\zeta)$ e perciò anche $\psi(\alpha) \in K(\zeta)$. Ponendo successivamente ζ uguale a tutte le radici

$n-$esime dell'unità ζ_i, $i = 0, 1, \ldots, n-1$, e detti $c_i \in K(\zeta)$ i valori di $\psi(\alpha)$ che così si ottengono, abbiamo le n uguaglianze:

$$\begin{array}{ccccccccccc}
\alpha & + & \vartheta(\alpha) & + & \vartheta^2(\alpha) & + & \cdots & + & \vartheta^{n-1}(\alpha) & = & \sqrt[n]{c_0}, \\
\alpha & + & \zeta_1\vartheta(\alpha) & + & \zeta_1^2\vartheta^2(\alpha) & + & \cdots & + & \zeta_1^{n-1}\vartheta^{n-1}(\alpha) & = & \sqrt[n]{c_1}, \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\alpha & + & \zeta_{n-1}\vartheta(\alpha) & + & \zeta_{n-1}^2\vartheta^2(\alpha) & + & \cdots & + & \zeta_{n-1}^{n-1}\vartheta^{n-1}(\alpha) & = & \sqrt[n]{c_{n-1}}.
\end{array}$$

Sommando queste uguaglianze, e ricordando che $\sum_{i=0}^{n} \zeta_i^k = 0$, per ogni intero k, si ha

$$\alpha = \frac{1}{n}(\sqrt[n]{c_0} + \sqrt[n]{c_1} + \cdots + \sqrt[n]{c_{n-1}})$$

(si può scegliere arbitariamente uno solo degli n radicali). Le altre radici si ottengono formando $\vartheta(\alpha), \vartheta^2(\alpha)$, ecc., oppure, sommando le precedenti equazioni moltiplicate rispettivamente per $1, \zeta_1^{-r}, \zeta_2^{-r}, \ldots, \zeta_{n-1}^{-r}$; si ottiene l'$r-$esima radice come

$$\vartheta^r(\alpha) = \frac{1}{n}(\sqrt[n]{c_0} + \zeta_1^{-r}\sqrt[n]{c_1} + \zeta_2^{-r}\sqrt[n]{c_2} + \cdots + \zeta_{n-1}^{-r}\sqrt[n]{c_{n-1}}), \qquad (3.4)$$

che è l'espressione per radicali richiesta. ♢

3.17 Corollario. *Le radici p-esime dell'unità, p primo, si esprimono mediante radicali di indice inferiore a p.*

Dim. Si tratta, a parte la radice 1, delle radici del polinomio ciclotomico $\Phi_p(x)$, il cui gruppo di Galois è ciclico di ordine $p-1$. ♢

3.18 Esempio. Calcoliamo, con il metodo del teorema, le radici terze dell'unità. Il gruppo di Galois è il gruppo ciclico $G = \{I, (\alpha, \vartheta(\alpha))\}$ di ordine 2 con $\vartheta(\alpha) = \alpha^2$. Siano 1 e -1 le due radici seconde dell'unità; allora, con $\zeta = 1$:

$$\psi_0(\alpha) = (\alpha + 1 \cdot \alpha^2)^2 = \alpha^2 + 2\alpha^3 + \alpha^4 = \alpha^2 + \alpha + 2 = 1,$$

ricordando che $\alpha^3 = 1$ e $\alpha^2 + \alpha + 1 = 0$. Con $\zeta = -1$:

$$\psi_1(\alpha) = (\alpha - \alpha^2)^2 = \alpha^2 - 2\alpha^3 + \alpha^4 = \alpha^2 - 2 + \alpha = \alpha^2 + \alpha + 1 - 3 = -3,$$

e dunque:

$$\alpha = \frac{1}{2}(\sqrt[2]{1} + \sqrt[2]{-3}).$$

Ma sappiamo che $\alpha + \alpha^2 = -1$, e dunque la determinazione di $\sqrt[2]{1}$ da prendere è -1:

$$\alpha_1 = \frac{1}{2}(-1 + \sqrt[2]{-3}).$$

Per l'altra radice,

$$\alpha_2 = \vartheta(\alpha) = \alpha^2 = \frac{1}{2}(-1 - \sqrt[2]{-3});$$

o anche, applicando la (3.4):

$$\alpha_2 = \frac{1}{2}(-1 + (-1)^{-1}\sqrt[2]{-3}).$$

3.19 Corollario. *Le radici n-esime dell'unità, per ogni n, si esprimono mediante radicali.*

Dim. Se $n = p$, primo, si tratta del corollario precedente. Se $n = p^h$, una radice p^h-esima è radice di $x^p - \zeta = 0$, con ζ radice $p^{h-1}-$esima, e per induzione si ha il risultato. Se $n = p_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$ e ζ_i è una radice $p_i^{h_i}-$esima dell'unità espressa per radicali, allora il prodotto $\zeta_1\cdot\zeta_2\cdots\zeta_t$ è una radice $n-$esima espressa per radicali. ♢

3.20 Nota. Se nel Cor. 3.19 le ζ_i sono radici primitive $p_i^{h_i}-$esime, allora $\zeta_i^{p_i^{h_i}} = 1$, e $p_i^{h_i}$ è il minimo per cui ciò accade. Ne segue che per il prodotto ζ delle ζ_i si ha $\zeta^n = 1$, con n minimo, e ζ è primitiva.

Consideriamo ora un'equazione $f(x)$ risolubile per radicali. Per l'osservazione fatta dopo la Def. 3.15 possiamo supporre che gli r_i siano numeri primi. Sappiamo che le radici $p-$esime dell'unità si esprimono per radicali su K di indice primo inferiore a p: l'ampliamento $K(\varepsilon)$ di K, con una radice primitiva $p-$esima si ottiene pertanto mediante ampliamenti normali successivi ottenuti aggiungendo radici $q-$esime con $q < p$:

$$K \subseteq K_1 = K(\varepsilon_1) \subseteq K_2 = K(\varepsilon_2) \subseteq \ldots \subseteq K_t = K(\varepsilon).$$

Se $p_1, p_2, \ldots, p_t$ sono i primi che compaiono nella fattorizzazione degli esponenti $r_i,\ i = 1, 2, \ldots, s$ della Def. 3.15, operando come sopra si ottiene un ampliamento K' di K che contiene tutte le radici p_k-esime dell'unità, $k = 1, 2, \ldots, t$ ed è ottenuto mediante successivi ampliamenti normali. Se ora $a \in K$ è uno degli a_i della (3.3), l'ampliamento di K' con una radice $\sqrt[p]{a}$ di $x^p - a$, p primo, è normale. Infatti, per il Cor. 3.10, *iii*), se $x^p - a$ si spezza, allora si spezza in fattori lineari, e dunque poiché in tal caso $\sqrt[p]{a}$ appartiene già a K' non si tratta di un effettivo ampliamento. Altrimenti $x^p - a$ è irriducibile, e poiché $K'(\sqrt[p]{a})$ contiene anche le altre radici del polinomio, l'ampliamento è normale, e di grado primo. Aggiungendo ora a $K'(\sqrt[p]{a})$ una radice $q-$esima di a o una radice $r-$esima di un altro elemento di K, e così per tutti gli elementi $a_1, a_2, \ldots, a_s$ della (3.3), si ottiene un campo $\overline{K}$ che contiene il campo $K(\underline{\alpha})$ ed è tale che

$$K \subseteq K^{(1)} \subset K^{(2)} \subset \ldots \subset K^{(i)} \subset K^{(i+1)} \subset \ldots \subset K^{(m)} \subset \overline{K} \qquad (3.5)$$

dove il gruppo di Galois di $K^{(i+1)}$ su $K^{(i)}$ è ciclico di ordine primo. Alla serie di sottocampi di $\overline{K}$ della (3.5) corrisponde una serie di sottogruppi,

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_m \supset \{1\} \tag{3.6}$$

ciascuno normale nel precedente e tale che il quoziente G_i/G_{i+1} è ciclico di ordine primo.

3.21 Definizione. Una serie come la (3.6) nella quale ogni sottogruppo è normale nel precedente si dice *serie normale*. Un gruppo che ammette una serie normale a quozienti ciclici di ordine primo si dice *risolubile*.

3.22 Teorema.

(*i*) *Sottogruppi e quozienti di gruppi risolubili sono risolubili;*

(*ii*) *se* $N \trianglelefteq G$ *e* G/N *sono risolubili, allora* G *lo è;*

(*iii*) *se* G *è abeliano allora è risolubile.*

Dim. (*i*) Se la (3.6) è una serie normale di G, e $H \leq G$, allora $H_{i+1} = H \cap G_{i+1} \trianglelefteq H \cap G_i = H_i$. Inoltre,

$$\frac{H_i}{H_{i+1}} = \frac{H_i}{H \cap G_{i+1}} = \frac{H_i}{H_i \cap G_{i+1}} \simeq \frac{H_i G_{i+1}}{G_{i+1}} \subseteq \frac{G_i}{G_{i+1}}.$$

Pertanto, essendo G_i/G_{i+1} di ordine primo, o $H_i/H_{i+1} = \{1\}$, e dunque $H_i = H_{i+1}$, oppure $H_i/H_{i+1} \simeq G_i/G_{i+1}$ ciclico di ordine primo.

Se $N \trianglelefteq G$, $G_{i+1}N \trianglelefteq G_iN$; inoltre, $NG_i = (NG_{i+1})G_i$ e dunque,

$$\frac{NG_i}{NG_{i+1}} = \frac{(NG_{i+1})G_i}{NG_{i+1}} \simeq \frac{G_i}{NG_{i+1} \cap G_i} \simeq \frac{G_i/G_{i+1}}{(NG_{i+1} \cap G_i)/G_{i+1}}$$

(sia NG_{i+1} che G_i contengono G_{i+1} e dunque anche l'intersezione lo contiene). NG_i/NG_{i+1} è allora isomorfo a un quoziente di G_i/G_{i+1}, ciclico di ordine primo, e pertanto o è il gruppo identico o è ciclico di ordine primo.

(*ii*). Dalla serie normale di G/N a quozienti di ordine primo

$$G/N \supset H_1/N \supset H_2/N \supset \ldots \supset H_{k-1}/N \supset N/N$$

segue $H_{i+1} \lhd H_i$ e H_i/H_{i+1} ciclico di ordine primo. Abbiamo così parte della serie richiesta per G:

$$G \supset H_1 \supset H_2 \supset \ldots \supset H_{k-1} \supset N,$$

che si può completare aggiungendo una serie $N \supset H_{k+1} \supset H_{k+2} \supset \ldots \supset H_m = \{1\}$ per N.

(*iii*) G ha un sottogruppo N di ordine primo (Cauchy), che è risolubile (la serie è $N \supset \{1\}$). Per induzione G/N è risolubile, e dunque per (*ii*) G lo è. $\diamondsuit$

Se dunque un'equazione è risolubile per radicali, allora il campo $K(\underline{\alpha})$ è un sottocampo di un campo come $\overline{K}$ della (3.5). Sia $\overline{G}$ il gruppo di Galois di $\overline{K}$ su K. Allora $\overline{K}$ contiene una serie di sottocampi tali che i corrispondenti sottogruppi di $\overline{G}$ costituiscono una serie normale a quozienti di ordine primo. Il gruppo $\overline{G}$ è dunque risolubile. Inoltre, avendosi $K \subseteq K(\underline{\alpha}) \subseteq \overline{K}$, ed essendo $K(\underline{\alpha})$ un ampliamento normale (si aggiungono a K tutte le radici α_i di $f(x)$), il gruppo di Galois G di $K(\underline{\alpha})$ è un quoziente di $\overline{G}$, e dunque anch'esso risolubile.

Viceversa, sia il gruppo di Galois G di $K(\underline{\alpha})$ su K risolubile, e sia (3.6) una serie normale. Induzione su m. Se $m = 1$ il gruppo è ciclico (di ordine primo) e dunque l'equazione è risolubile per radicali (Teor. 3.16). Sia $m > 1$, e sia γ un elemento di $K(\underline{\alpha})$ tale che $G_\gamma = G_1$. Il gruppo di Galois su K del polinomio $J(x)$ di γ è isomorfo a G/G_1, ciclico di ordine p, e pertanto il polinomio è risolubile per radicali. L'ampliamento $K(\gamma)$ di K si ottiene dunque mediante aggiunzioni di radici. Il gruppo di Galois di $f(x)$ su $K(\gamma)$ è G_1, che ha una serie di lunghezza $m-1$, e pertanto è risolubile per radicali. Il campo $K(\underline{\alpha})$ si ottiene allora da $K(\gamma)$ per aggiunzione di radici.

In conclusione:

3.23 Teorema. *Un'equazione è risolubile per radicali se e solo se il suo gruppo di Galois è risolubile.* ♢

3.24 Definizione. Siano $a_1, a_2, \ldots, a_n$ elementi algebricamente indipendenti su un campo K. L'equazione

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

prende il nome di *equazione generale di grado n su K.*

L'equazione generale di grado n sul campo K è dunque un'equazione particolare sul campo $K(a_1, a_2, \ldots, a_n)$ (quella che ha come coefficienti gli a_i).

Nel risultato seguente sta il motivo per il quale non esiste una formula risolutiva per l'equazione generale di grado $n \geq 5$ che faccia intervenire soltanto operazioni razionali ed estrazioni di radici.

3.25 Teorema. *Il gruppo simmetrico S^n, $n \geq 5$, non è risolubile.* ♢

3.26 Teorema. (Ruffini–Abel) *L'equazione generale di grado $n \geq 5$ su K non è risolubile per radicali.*

Dim. Dimostriamo che il gruppo di Galois su $K(a_1, a_2, \ldots, a_n)$ dell'equazione generale è il gruppo simmetrico S^n. Il risultato seguirà allora dal Teor. 3.25. Le radici dell'equazione sono distinte (l'annullarsi del discriminante darebbe una relazione algebrica tra le a_i che invece sono indipendenti); ha senso dunque parlare di gruppo di Galois. Sia

$$g(\alpha_1, \alpha_2, \ldots, \alpha_n, a_1, a_2, \ldots, a_n) = 0 \tag{3.7}$$

una relazione a coefficienti in $K(a_1, a_2, \ldots, a_n)$ tra le radici α_i dell'equazione. Facciamo vedere che essa resta soddisfatta per ogni permutazione delle α_i. Le a_i sono le funzioni simmetriche elementari delle α_i, e sostituendo nella g le loro espressioni in termini delle α_i si ottiene un polinomio nelle α_i a coefficienti in K:

$$G(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0. \tag{3.8}$$

Se dimostriamo che tutti i coefficienti del polinomio G sono uguali a zero, cioè che il polinomio a coefficienti in K:

$$G(x_1, x_2, \ldots, x_n) \tag{3.9}$$

è il polinomio nullo, allora permutando comunque le α_i la (3.8) resterà soddisfatta, e dunque anche la (3.7) (poiché le a_i restano inalterate per qualunque permutazione delle α_i, dall'annullarsi della (3.7) seguirà

$$g(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}, a_1, a_2, \ldots, a_n) = 0.$$

Se (3.9) non è il polinomio nullo, consideriamo i polinomi che si ottengono permutando in tutti i modi possibili le x_i in (3.9). Nessuno è nullo; facendone il prodotto si ottiene un polinomio non nullo che è ovviamente simmetrico, e che dunque è un polinomio nelle funzioni simmetriche elementari b_i delle x_i:

$$\prod_{\sigma \in S^n} G(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = F(b_1, b_2, \ldots, b_n) \tag{3.10}$$

dove F è a coefficienti in K. Sostituendo in questa identità le x_i con le α_i si ottiene:

$$\prod_{\sigma \in S^n} G(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) = F(a_1, a_2, \ldots, a_n).$$

Ma ora il primo membro contiene il fattore (3.8), e dunque è nullo. Ne segue $F(a_1, a_2, \ldots, a_n) = 0$, contro l'indipendenza algebrica delle a_i. ♢

Di questo teorema daremo anche la dimostrazione originale di Ruffini e Abel (Teor. 4.5).

Nella dimostrazione del teorema precedente è contenuto il seguente risultato che inverte il Teor. 1.1:

3.27 Teorema. *Se le funzioni simmetriche elementari delle indeterminate x_i sono algebricamente indipendenti, anche le x_i lo sono.* ♢

3.28 Teorema. *Un'equazione di grado primo è risolubile per radicali se e solo se le sue radici si possono esprimere come funzioni razionali di due qualunque di esse.*

Questo teorema è una conseguenza di alcuni risultati di teoria dei gruppi che ora dimostriamo.

3.29 Lemma. *Un gruppo transitivo G di grado primo è risolubile se e solo se contiene un gruppo ciclico di ordine primo C_p come sottogruppo normale. G è allora un sottogruppo del gruppo lineare $\mathcal{L}_p$.*

Dim. Sia $c = (1, 2, \ldots, p)$, $C_p =< c > \trianglelefteq G$, e sia N il più grande sottogruppo di S^p che contiene C_p come sottogruppo normale (N è il normalizzante di C_p in S^p). Sia $\sigma \in N$; allora $\sigma^{-1} c \sigma = c^k$, $(p, k) = 1$. Sia $U(p)$ il gruppo degli interi minori di p (e dunque primi con p), e sia $N \to U(p)$ la corrispondenza data da $\sigma \to k$. Si tratta di un omomorfismo, che è suriettivo in quanto, dato k, $(1, 2, \ldots, p)^k = (i_1, i_2, \ldots, i_p) = c^k$ ha ordine p ed è coniugato a c mediante $\sigma = \begin{pmatrix} 1 & 2 & \ldots & p \\ i_1 & i_2 & \ldots & i_p \end{pmatrix}$. Dunque σ appartiene a N e induce k. Il nucleo consta dei $\sigma \in N$ tali che $k = 1$, cioè dai σ che permutano con c. Ma dovendo ora essere $(i_1, i_2, \ldots, i_p) = (1, 2, \ldots, p)$, una tale σ non può essere che una delle p potenze di c. Dunque il nucleo è lo stesso C_p, e pertanto $|N| = p \cdot \varphi(p) = p(p-1)$. Ora C_p è ciclico, dunque risolubile, e N/C_p è isomorfo al gruppo degli interi minori di p e primi con p che è abeliano, quindi risolubile. Allora N è risolubile, e dunque anche $G \leq N$. (Questa dimostrazione vale per ogni n: il normalizzante in S^n di un $n-$ciclo ha ordine $n\varphi(n)$).

Ora da $\sigma^{-1} c \sigma = c^k$, cioè $c\sigma = \sigma c^k$ si ha

$$c\sigma = \begin{pmatrix} 1 & 2 & \ldots & p-1 & p \\ i_2 & i_3 & \ldots & i_p & i_1 \end{pmatrix} = \sigma c^k = \begin{pmatrix} 1 & 2 & \ldots & p-1 & p \\ i_{1+k} & i_{2+k} & \ldots & i_{p-1}+k & i_p+k \end{pmatrix}$$

da cui $i_{s+1} \equiv i_s + k \mod p$, e poiché $i_{s+1} \equiv ks + i_1 \mod p$ abbiamo

$$\sigma = \begin{pmatrix} s \\ ks + i_1 - k \end{pmatrix}.$$

La corrispondenza $\sigma \to (x \to kx + t)$, con $t = i_1 - k$ mostra che si tratta di un gruppo lineare.

Viceversa, sia G di grado primo p e risolubile,

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_{n-1} \supset G_n = \{1\}$$

una serie normale a quozienti ciclici di ordine primo (per certi primi $q, r, \ldots$). Il gruppo G_1 è transitivo (è normale e ha grado primo); lo stesso accade per G_2 (ha grado primo ed è un sottogruppo normale del gruppo transitivo G_1), e analogamente per tutti gli altri gruppi della serie. Ne segue che G_{n-1}, essendo transitivo e ciclico di grado primo p è necessariamente generato da un $p-$ciclo, e dunque è ciclico di ordine p; sia esso C_p. Allora per quanto dimostrato sopra, G_{n-2} è contenuto nel gruppo lineare $\mathcal{L}_p$, che ammette un solo sottogruppo di ordine p (il sottogruppo delle traslazioni). Se ora $\sigma \in G_{n-3}$ si ha, per la

normalità di G_{n-2} in G_{n-3}, $\sigma^{-1}G_{n-2}\sigma = G_{n-2}$ da cui $\sigma^{-1}C_p\sigma \subseteq G_{n-2}$ e quindi $\sigma^{-1}C_p\sigma = C_p$, essendo C_p l'unico sottogruppo di ordine p. Dunque $C_p \trianglelefteq G_{n-3}$, e così proseguendo si ha $C_p \trianglelefteq G$. ♢

3.30 Lemma. *Nel gruppo lineare $\mathcal{L}_p$ un elemento non identico ha al più un punto fisso.*

Dim. Supponiamo che la trasformazione $x \to ax + b$ abbia due punti fissi r e s, $0 \leq r, s \leq p-1$:

$$ar + b \equiv r \mod p$$
$$as + b \equiv s \mod p.$$

Allora, sottraendo, $a(r-s) \equiv r - s \mod p$, e poiché p non divide $r - s < p$, dividendo per $r - s$ si ha $a \equiv 1 \bmod p$. Ne segue $r + b \equiv r \bmod p$, e perciò $b \equiv 0 \bmod p$, per cui $a = 1, b = 0$, e la trasformazione è l'identità. ♢

3.31 Lemma. *Sia G un gruppo transitivo di grado primo p nel quale un elemento non identico fissa al più un punto. Allora G è un sottogruppo di $\mathcal{L}_p$, e in particolare è risolubile.*

Dim. Se i e j sono due punti, i loro stabilizzatori G_i e G_j hanno intersezione $\{1\}$. Per la transitività $[G : G_i] = p$; inoltre i G_i sono tutti tra loro coniugati e hanno perciò lo stesso ordine, e sia h. Ne segue $|G| = ph$, e siccome i G_i sono in numero di p e ciascuno contiene $h - 1$ elementi non identici, $|\cup G_i| = p(h-1)+1 = ph-(p-1)$. Restano $p-1$ elementi che non fissano alcun punto; sia σ uno di questi. Se σ ha due cicli di lunghezza diversa, t e s, con $2 \leq t < s$, allora σ^h fissa almeno due punti e non è l'identità. Allora i cicli di σ hanno tutti la stessa lunghezza, ma essendo p primo ciò è possibile solo se c'è un solo ciclo. Dunque σ è un $p-$ciclo, e i $p-1$ elementi che non fissano alcun punto sono allora le sue potenze. Infine, il sottogruppo $< \sigma >$ è normale. Infatti, se τ fissa i allora $\eta^{-1}\tau\eta$ fissa i^η; due elementi coniugati fissano dunque lo stesso numero di punti, e pertanto se σ non fissa alcun punto, lo stesso accade per i suoi coniugati. Il gruppo G è allora contenuto in $\mathcal{L}_p$. ♢

Dimostriamo ora il Teor. 3.28.

Dim. Se l'equazione è risolubile per radicali, il gruppo di Galois G è risolubile. Per il Lemma 3.29 G è un sottogruppo di $\mathcal{L}_p$. Aggiungendo al campo K due qualunque radici α_i, α_j il gruppo G si abbassa a un sottogruppo H che lascia fisse queste due radici. H è allora un sottogruppo di $\mathcal{L}_p$ che fissa due punti e perciò è l'identità. In altri termini,

$$K(\alpha_i, \alpha_j) = K(\underline{\alpha}), \tag{3.11}$$

cioè ogni radice è una funzione razionale di α_i e α_j.

Viceversa, sussista la (3.11) per ogni coppia di radici α_i e α_j. Una permutazione che fissa α_i e α_j fissa tutti gli elementi di $K(\underline{\alpha})$, e dunque è l'identità. G è allora un gruppo nel quale un elemento che fissa due punti è l'identità. per il Lemma 3.31, G è risolubile. ♢

3.32 Corollario. (KRONECKER) *Sia $f(x) = 0$ un'equazione a coefficienti razionali irriducibile di grado primo e risolubile per radicali. Allora o $f(x)$ ha esattamente una radice reale, oppure tutte le radici sono reali.*

Dim. Se α_1 e α_2 sono due radici reali, allora $\mathcal{Q}(\alpha_1, \alpha_2)$ consta solo di numeri reali. Per il Teor. 3.28 $\mathcal{Q}(\alpha_1, \alpha_2) = \mathcal{Q}(\underline{\alpha})$, e dunque tutte le radici sono reali.♢

3.3 Teorema fondamentale

Siano Δ un sottocampo di $K(\underline{\alpha})$, $K \subseteq \Delta \subseteq K(\underline{\alpha})$, G il gruppo di Galois di $f(x)$ su K e H il gruppo di Galois di $f(x)$ su Δ. Allora H lascia fissi gli elementi di Δ (Teor. 2.18, con Δ al posto di K), e viceversa, se un elemento di $K(\underline{\alpha})$ è fissato da ogni elemento di H allora appartiene a Δ (Teor. 2.17). Il sottocampo Δ resta dunque determinato come l'insieme degli elementi di $K(\underline{\alpha})$ fissati da ogni elemento di H (e dunque un sottogruppo di G non può essere gruppo di Galois di $f(x)$ su due sottocampi diversi). D'altra parte sappiamo che H è gruppo di Galois di $f(x)$ su $\Delta = K(\gamma)$, dove γ è un elemento tale che $G_\gamma = H$ (Teor. 2.25), e pertanto dato $H \leq G$, esiste ed è unico il sottocampo Δ di $K(\underline{\alpha})$ tale che H è il gruppo di Galois di $f(x)$ su Δ. Abbiamo così:

3.33 Teorema. (TEOREMA FONDAMENTALE DELLA TEORIA DI GALOIS) *La corrispondenza che associa a un sottocampo Δ, $K \subseteq \Delta \subseteq K(\underline{\alpha})$, il gruppo di Galois di $f(x)$ su Δ, è una corrispondenza biunivoca tra l'insieme dei sottocampi di $K(\underline{\alpha})$ che contengono K e l'insieme dei sottogruppi H del gruppo di Galois G di $f(x)$ su K.* ♢

A $K(\underline{\alpha})$ corrisponde $H = \{1\}$, a K corrisponde $H = G$.

3.34 Nota. Ai sottocampi di $K(\underline{\alpha})$, cioè contenuti in $K(\underline{\alpha})$, contenenti K, corrispondono i sottogruppi di G che contengono $\{1\}$ e sono contenuti in G (cioè tutti i sottogruppi di G).

3.35 Definizione. La corrispondenza stabilita nel Teor. 3.33 prende il nome di *corrispondenza di Galois.*

Se $\Delta_1 \subseteq \Delta_2$, il gruppo di Galois di $f(x)$ su Δ_2 è un sottogruppo del gruppo di Galois di $f(x)$ su Δ_1 (un elemento di G che fissa gli elementi di Δ_2 è tra quelli che fissano gli elementi di Δ_1). Se $H_1 \subseteq H_2$, il sottocampo Δ_2 per il quale H_2 è il gruppo di Galois di $f(x)$ è un sottocampo di Δ_1 per il quale H_1

è il gruppo di Galois di $f(x)$ (un elemento fissato da H_2 è fissato in particolare da H_1). Si ha così:

3.36 Corollario. *La corrispondenza di Galois inverte la relazione di inclusione*:

$$\Delta_1 \subseteq \Delta_2 \Rightarrow H_1 \supseteq H_2, \quad H_1 \subseteq H_2 \Rightarrow \Delta_1 \supseteq \Delta_2$$

3.37 Corollario. *Vi sono soltanto un numero finito di campi intermedi tra K e $K(\underline{\alpha})$.*

Dim. Il gruppo di Galois è finito, e quindi ha un numero finito di sottogruppi. Essendo questi in corrispondenza biunivoca con i sottocampi di $K(\underline{\alpha})$ che contengono K si ha il risultato. ♢

3.38 Corollario. *Nella corrispondenza di Galois, a sottogruppi normali di G corrispondono ampliamenti normali di K.*

Dim. A $\Delta = K(\gamma)$ corrisponde $H = G_\gamma$. Il risultato segue dalla *ii*) del Teor. 2.49. ♢

3.39 Esempio. Consideriamo gli *Es.* 1 di 2.22 e 6 di 2.53. Il gruppo di Galois è il gruppo diedrale D_4; denotiamo con $\kappa(H)$ il campo fisso del sottogruppo H.

I tre sottogruppi di ordine 4 di D_4 sono normali (indice 2); se $K(\gamma)$ è l'ampliamento corrispondente a uno di questi, il polinomio di γ sarà un polinomio normale (perché ha grado 2).

$C_4 = \{I, (1,3,2,4), (1,2)(3,4), (1,4,2,3)\}$ fissa $\gamma = \frac{\alpha_3}{\alpha_1} = i$ (infatti, $\frac{\alpha_{\sigma(3)}}{\alpha_{\sigma(1)}} = \frac{\alpha_2}{\alpha_3} = \frac{-\alpha}{\imath\alpha} = -\frac{1}{i} = i$). Dunque

$$\kappa(C_4) = \mathcal{Q}(i).$$

Sotto l'azione di D_4, l'elemento $\frac{\alpha_3}{\alpha_1} = i$ assume due valori, i e $-i$. Il polinomio di i è $(x-i)(x+i) = x^2+1$.

$V_1 = \{I, (1,2)(3)(4), (1)(2)(3,4), (1,2)(3,4)\}$ fissa $\sqrt{2}$, valore di α_1^2:

$$\kappa(V_1) = \mathcal{Q}(\sqrt{2}).$$

L'elemento α_1^2 assume due valori: $\sqrt{2}, -\sqrt{2}$, e il polinomio è x^2-2.

$V_2 = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ fissa $\alpha_1\alpha_3 = i\sqrt{2}$:

$$\kappa(V_2) = \mathcal{Q}(i\sqrt{2}).$$

Anche $\alpha_1\alpha_3$ assume due valori $i\sqrt{2}, -i\sqrt{2}$, e il polinomio è x^2+2.

$C_2^{(1)} = \{I, (1)(2)(3,4)\}$ fissa $\alpha_1 = \sqrt[4]{2}$:

$$\kappa(C_2^{(2)}) = \mathcal{Q}(\sqrt[4]{2}).$$

$C_2^{(2)} = \{I, (1,2)(3)(4)\}$ fissa $\alpha_3 = i\sqrt[4]{2}$:

$$\kappa(C_2^{(1)}) = \mathcal{Q}(i\sqrt[4]{2}).$$

Al variare di σ in D_4, α_3 percorre le quattro radici di $f(x)$ (D_4 è transitivo); il polinomio di α_3 è dunque lo stesso $f(x)$.

$C_2^{(3)} = \{I, (1,2)(3,4)\}$ fissa $\sqrt{2} = \alpha_1^2 = \alpha_2^2$ e $i = \frac{\alpha_3}{\alpha_1} = \frac{\alpha_4}{\alpha_2}$:

$$\kappa(C_2^{(3)}) = \mathcal{Q}(i, \sqrt{2}) = \mathcal{Q}(i + \sqrt{2}).$$

Il polinomio di $i + \sqrt{2}$ è $x^4 - 2x^2 + 9$ le cui radici sono $\pm i \pm \sqrt{2}$; poiché $(i + \sqrt{2})^3 = 5i - \sqrt{2}$, aggiungendo $i + \sqrt{2}$ si ottiene i, quindi $\sqrt{2}$ e perciò anche le altre radici. Analogamente se si aggiunge una qualunque altra radice. Il polinomio è normale.

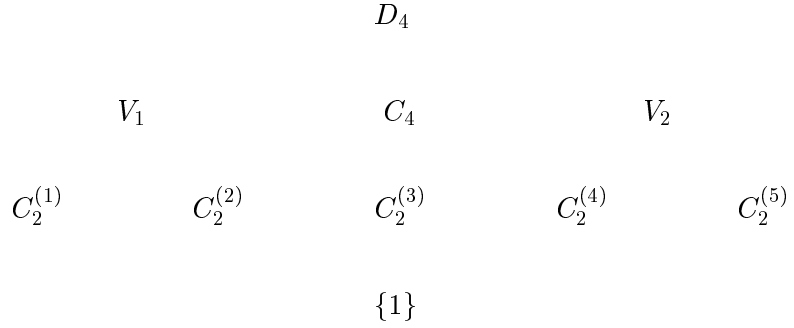
$C_2^{(4)} = \{I, (1,4)(2,3)\}$ fissa $\alpha_1^2\alpha_3 + \alpha_1^3 = \sqrt{i}\sqrt[4]{2}$ (ricordando che $\sqrt{i} = \frac{\sqrt{2}}{2}(i + 1)$ e $i = \frac{\alpha_3}{\alpha_1}$):

$$\kappa(C_2^{(4)}) = \mathcal{Q}(\sqrt{i\sqrt{2}}\,).$$

Infine $C_2^{(5)} = \{I, (1,3)(2,4)\}$ fissa $\alpha_1^2\alpha_3 - \alpha_1^3 = \sqrt{-i}\sqrt[4]{2}$ ($\sqrt{-i} = \frac{\sqrt{2}}{2}(i - 1)$):

$$\kappa(C_2^{(5)}) = \mathcal{Q}(\sqrt{-i\sqrt{2}}\,).$$

Al reticolo dei sottogruppi:



corrisponde il reticolo dei sottocampi:

$$K(i, \sqrt[4]{2})$$

$$\mathcal{Q}(\sqrt[4]{2}) \qquad \mathcal{Q}(i\sqrt[4]{2}) \qquad \mathcal{Q}(i, \sqrt{2}) \qquad \mathcal{Q}(\sqrt{i\sqrt{2}}) \qquad \mathcal{Q}(\sqrt{-i\sqrt{2}})$$

$$\mathcal{Q}(\sqrt{2}) \qquad \mathcal{Q}(i) \qquad \mathcal{Q}(i\sqrt{2})$$

$$\mathcal{Q}$$

3.40 Nota. $\mathcal{Q}' = \mathcal{Q}(\sqrt{2})$ è un ampliamento normale di $\mathcal{Q}$ (V_2 è un sottogruppo normale di D_4), $\mathcal{Q}'(i\sqrt[4]{2})$ è un ampliamento normale di $\mathcal{Q}'$ ($C_2^{(2)}$ è normale in V_2), ma $\mathcal{Q}(i\sqrt[4]{2})$ non è un ampliamento normale di $\mathcal{Q}$ ($C_2^{(2)}$ non è un sottogruppo normale di D_4): la normalità non è transitiva.

L'ampliamento $\mathcal{Q}(i, \sqrt{2})$, corrispondente a $C_2^{(3)} \trianglelefteq C_4$, è invece normale in D_4, e ciò perché $C_2^{(3)}$ è non solo normale, ma anche caratteristico in C_4.

3.4 Gruppi di Galois su $\mathbf{Z_p}$

Ricordiamo alcune proprietà dei campi finiti che ci serviranno in questo paragrafo.

1. Un campo finito ha un numero di elementi che è una potenza di un numero primo p. E' uno spazio vettoriale di dimensione finita, e se questa dimensione è m esso coincide a meno di isomorfismi con l'insieme delle radici del polinomio $x^{p^m} - x$. Si denota con $\mathbf{F}_{p^m}$. Il gruppo moltiplicativo di $\mathbf{F}_{p^m}$ è ciclico. Se γ è un generatore, allora è un elemento primitivo (ogni elemento del campo è potenza di γ), ma possono esistere elementi primitivi η che non sono generatori del gruppo moltiplicativo (ogni elemento del campo è un polinomio in η, non necessariamente una potenza).

2. Si ha $(a+b)^p = a^p + b^p$, e più in generale $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ per ogni k.

3. Un polinomio in x^p, $f(x^p)$, su $\mathbf{F}_p$ è la potenza $p-$esima del polinomio $f(x)$: $f(x^p) = f(x)^p$. Più in generale, $f(x^{p^m}) = f(x)^{p^m}$. Su $\mathbf{F}_{p^m}$, $f(x^p)$ è la potenza $p-$esima di un polinomio $g(x)$.

4. Il campo $\mathbf{F}_{p^m}$ si può ottenere come segue. Sia $f(x)$ un polinomio irriducibile di grado m a coefficienti in $\mathbf{F}_p$, e si consideri l'insieme dei polinomi di grado al più $m-1$ a coefficienti in $\mathbf{F}_p$ con la somma usuale e il prodotto mod $f(x)$: questo insieme è un campo a p^m elementi. In questo campo $f(x)$ ammette una radice, il polinomio $p(x) = x$. Più precisamente, il campo in questione è il quoziente $\mathbf{F}_p[x]/I$, dove I è l'ideale generato da $f(x)$, e la radice è la classe $x + I$. Detta α questa radice, scriviamo $\mathbf{F}_{p^m} = \mathbf{F}_p(\alpha)$; in questo campo $f(x)$ si spezza completamente. Infatti, dalla $f(\alpha) = 0$ si ha $f(\alpha)^{p^k} = 0$, e per la proprietà 3., anche $f(\alpha^{p^k}) = 0$, $k = 0, 1, 2, \ldots, p-1$. Le radici sono dunque $\alpha, \alpha^p, \ldots, \alpha^{p^{m-1}}$ (dove α^{p^k} indica la classe che contiene il resto della divisione di x^{p^k} per $f(x)$). L'ampliamento $\mathbf{F}_p(\alpha)$ è allora un ampliamento normale.

5. Il gruppo degli automorfismi di $\mathbf{F}_{p^m}$ è ciclico di ordine m, generato dalla corrispondenza che associa ad ogni elemento β la sua potenza $p-$esima $\sigma : \beta \to \beta^p$ (*automorfismo di Frobenius*). E' chiaro che σ è un automorfismo (v. proprietà 2.); dimostriamo che ha ordine m. Sia α un generatore del gruppo ciclico del campo, radice di un polinomio irriducibile di grado m su $\mathbf{F}_p$. Applicando σ si ottengono m elementi distinti $\sigma^k(\alpha) = \alpha^{p^k}$, $k = 0, 1, \ldots, m-1$ (se $\alpha^{p^i} = \alpha^{p^j}$, $i < j$, allora elevando alla p^{m-j} si ha $\alpha^{p^{m-j+i}} = \alpha^{p^m} = \alpha$; con $k = m - j + i < m$ si ha $\alpha^{p^k - 1} = 1$, escluso perché α è di ordine $p^m - 1$). Inoltre un automorfismo fissa 1, e dunque tutti gli elementi di $\mathbf{F}_p$. Ne segue che se τ è un automorfismo, allora se $f(\alpha) = 0$ è anche $0 = \tau(0) = \tau(f(\alpha)) = f(\tau(\alpha))$, per cui $\tau(\alpha)$ è una radice di $f(x)$, cioè una α^{p^k} per un certo k. Ne segue $\tau = \sigma^k$, e le potenze di σ esauriscono quindi il gruppo degli automorfismi di $\mathbf{F}_{p^m}$.

6. Un elemento di $\mathbf{F}_{p^m}$ appartiene a $\mathbf{F}_p$ se e solo se è fissato da tutti gli automorfismi di $\mathbf{F}_{p^m}$. Infatti, abbiamo già osservato che un automorfismo fissa gli elementi di $\mathbf{F}_p$. Se poi $\beta^p = \beta$, allora β è radice di $x^p - x$, che è di grado p e ha come radici gli elementi di $\mathbf{F}_p$. Dunque anche $\beta \in \mathbf{F}_p$.

7. Per ogni primo p e n, p primo, esistono polinomi di grado n irriducibili su $\mathbf{F}_p$.

La proprietà 6. ora vista è tipica del gruppo di Galois. In realtà il gruppo degli automorfismi di $\mathbf{F}_{p^m}$ è un gruppo di Galois, come dimostrano i teoremi che seguono.

3.41 Teorema. *Il gruppo di Galois $G^{(p)}$ di un polinomio irriducibile $f(x)$ di grado m su $\mathbf{F}_p$ è ciclico di ordine m.*

Dim. Il campo $\mathbf{F}_p(\alpha)$, α radice di $f(x)$, è normale (v. proprietà 4). Il gruppo di Galois $G^{(p)}$ di $f(x)$ su $\mathbf{F}_p$ è il gruppo che lascia invariate le relazioni $\varphi(\alpha, \alpha^p, \ldots, \alpha^{p^{m-1}}) = 0$. Per il polinomio $\varphi(x_0, x_1, \ldots, x_{m-1})$ si ha

$$\varphi(x_0^p, x_1^p, \ldots, x_{m-1}^p) = \varphi(x_0, x_1, \ldots, x_{m-1})^p.$$

Sostituendo x_k con α^{p^k}:

$$\varphi(\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}, \alpha) = \varphi(\alpha, \alpha^p, \ldots, \alpha^{p^{m-1}}),$$

per cui se $\varphi(\alpha, \alpha^p, \ldots, \alpha^{p^{m-1}}) = 0$ è anche $\varphi(\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}, \alpha) = 0$. $G^{(p)}$ contiene allora il ciclo $\sigma = (\alpha, \alpha^p, \ldots, \alpha^{p^{m-1}})$, di ordine m, e perciò anche le m potenze di questo. L'ampliamento è normale e $f(x)$ irriducibile, il gruppo $G^{(p)}$ è regolare e di ordine pari al grado di $f(x)$: $|G^{(p)}| = m$. $\diamondsuit$

Che $G^{(p)}$ sia ciclico anche se $f(x)$ si riduce si vede osservando che una permutazione σ del gruppo di Galois si estende a un automorfismo $\bar{\sigma}$ del campo $\mathbf{F}_p(\alpha)$ (Teor. 2.68); dunque $G^{(p)}$ è (isomorfo a) un sottogruppo di $\mathcal{A}$. Viceversa, un elemento $\bar{\sigma}$ di $\mathcal{A}$ lascia fissi gli elementi di $\mathbf{F}_p$, e quindi induce una permutazione σ delle radici di $f(x)$ che porta relazioni in relazioni. $\mathcal{A}$ è allora isomorfo a un sottogruppo di $G^{(p)}$. Ne segue $\mathcal{A} \simeq G^{(p)}$. Se $f(x) = f_1(x) f_2(x) \cdots f_t(x)$,

con gli $f_i(x)$ irriducibili di grado m_i, il campo di spezzamento di $f(x)$ è $\mathbf{F}_{p^m}$, dove $m = \text{mcm}(m_1, m_2, \ldots, m_t)$. Se α_i è una radice di $f_i(x)$ il gruppo di Galois di $f(x)$ è generato dalla permutazione i cui cicli sono quelli corrispondenti ai singoli fattori come nel Teor. 3.41.

Sia $f(x)$ un polinomio a coefficienti interi e sia p un primo che non divide il discriminante Δ di $f(x)$. Ci chiediamo che relazione c'è tra il gruppo di Galois G di $f(x)$ su $\mathcal{Q}$ e il gruppo di Galois $G^{(p)}$ di $\bar{f}(x) \bmod p$ su $\mathbf{F}_p$. Vedremo che con una opportuna numerazione delle radici $G^{(p)}$ è un sottogruppo di G.

Siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ le radici di $f(x)$ in un dato ordine. Sia inoltre $f(x) = f_1(x)g(x)$, con $f_1(x)$ irriducibile, di radice α_1, che prendiamo come primo modulo fondamentale di $f(x)$. Modulo p, $f_1(x)$ si può spezzare: $\bar{f}_1(x) = \bar{\varphi}_1(x)\bar{h}(x)$, con $\bar{\varphi}_1(x)$ fattore irriducibile e che prenderemo come primo modulo fondamentale del polinomio $\bar{f}(x)$:

$$\bar{f}(x) = \bar{f}_1(x)\bar{g}(x) = \bar{\varphi}_1(x)\bar{h}(x)\bar{g}(x). \tag{3.12}$$

Detta $\bar{\alpha}_1$ una radice di $\bar{\varphi}_1(x)$, facciamo corrispondere α_1 ad $\bar{\alpha}_1$. Da una relazione $\psi(\alpha_1) = 0$ segue $\bar{\psi}(\bar{\alpha}_1) = 0$, in quanto da $\psi(x) = 0$ segue $f_1(x)|\psi(x)$, e dunque $\bar{\varphi}_1(x)|\bar{\psi}(x)$. Sia ora $f(x) = f_2(\alpha_1, x)g_2(\alpha_1, x)$ in $\mathcal{Q}(\alpha_1)$, con $f_2(\alpha_1, x)$ il secondo modulo fondamentale di $f(x)$, di radice α_2. Dalla corrispondenza $\alpha_1 \to \bar{\alpha}_1$ abbiamo $\bar{f}(x) = \bar{f}_2(\bar{\alpha}_1, x)\bar{g}_2(\bar{\alpha}_1, x)$. Sia $\bar{\varphi}_2(\alpha_1, x)$ un fattore irriducibile di $\bar{f}_2(\bar{\alpha}_1, x)$; denotiamo con $\bar{\alpha}_2$ una sua radice, e facciamo corrispondere α_2 ad $\bar{\alpha}_2$. Una relazione $\psi_2(\alpha_1, \alpha_2) = 0$ implica allora $\bar{\psi}_2(\bar{\alpha}_1, \bar{\alpha}_2) = 0$. Infatti, $f_2(\alpha_1, x)$ divide $\psi_2(\alpha_1, x)$ e dunque $\bar{\varphi}_2(\bar{\alpha}_1, x)$ divide $\bar{\psi}_2(\bar{\alpha}_1, x)$ e perciò $\bar{\psi}_2(\bar{\alpha}_1, \bar{\alpha}_2) = 0$. In generale, sia $f_k(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x)$ il $k-$esimo modulo fondamentale di $f(x)$, $\bar{f}_k(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_{k-1}, x)$ la sua immagine determinata come sopra, $\bar{\varphi}_k(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_{k-1}, x)$ un suo fattore irriducibile in $\mathbf{F}_p(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_{k-1})$ e $\bar{\alpha}_k$ una sua radice. Facendo corrispondere α_k ad $\bar{\alpha}_k$, ad una relazione $\psi(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0$ corrisponde una relazione $\bar{\psi}(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_k) = 0$.

3.42 Teorema. *Se una permutazione delle $\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n$ lascia invariate le relazioni $\bar{\varphi}_k(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_k) = 0$, $k = 1, 2, \ldots, n$, cioè appartiene al gruppo di Galois $G^{(p)}$ di $\bar{f}(x)$, allora appartiene al gruppo di Galois G di $f(x)$. In altre parole $G^{(p)}$ è un sottogruppo di G.*

Dim. Sia $\sigma \in G^{(p)}$, $\bar{\alpha}_{\sigma(1)} = \bar{\alpha}_i$, e dunque $\bar{\varphi}_1(\bar{\alpha}_1) = 0$. Ne segue che α_i, corrispondente di $\bar{\alpha}_i$, è radice di $f_1(x)$. Se infatti $f_1(\alpha_i) \neq 0$, allora $g(\alpha_i) = 0$ e $\bar{g}(\bar{\alpha}_i) = 0$ (v. (3.12)). Ma allora $\bar{\alpha}$ è radice doppia di $\bar{f}(x)$, escluso. Dunque è anche $\alpha_{\sigma(1)} = \alpha_i$; in altri termini, σ porta la relazione $f_1(\alpha_1) = 0$ ancora in una relazione, la $f_1(\alpha_i) = 0$. Se $\bar{\alpha}_{\sigma(2)} = \bar{\alpha}_j$, allora per definizione $\bar{\alpha}_j$ è radice di $\bar{\varphi}_2(\bar{\alpha}_i, x)$. Ora $\bar{f}_2(\bar{\alpha}_1, x) = \bar{\varphi}_2(\bar{\alpha}_1, x)\bar{h}(\bar{\alpha}_1, x)$ implica $\bar{f}_2(\bar{\alpha}_i, x) = \bar{\varphi}_2(\bar{\alpha}_i, x)\bar{h}(\bar{\alpha}_i, x)$ (il polinomio $\bar{f}_2(x_1, x) - \bar{\varphi}_2(x_1, x)\bar{g}_2(x_1, x)$ ha la radice $\bar{\alpha}_1$, dunque è divisibile per $\bar{f}_1(x)$ e perciò ha la radice $\bar{\alpha}_i$), per cui

$\alpha_{\sigma(2)}$ è una radice di $f_2(\alpha_i, x)$ (se $f_2(\alpha_i, \alpha_{\sigma(2)}) \neq 0$ allora $0 \neq f_2(\bar{\alpha}_i, \bar{\alpha}_{\sigma(2)}) = \bar{\phi}_2(\bar{\alpha}_i, \bar{\alpha}_{\sigma(2)})\bar{g}(\bar{\alpha}_i, \bar{\alpha}_{\sigma(2)}) = 0$). Procedendo in questo modo, si vede come le relazioni tra le α_i si conservano permutando le α_i secondo gli elementi di $G^{(p)}$. Dunque $G^{(p)} \subseteq G$. ♢

Per la determinazione del gruppo di Galois su $\mathcal{Q}$ risulta particolarmente utile il seguente corollario.

3.43 Corollario. *Se $f(x)$ a coefficienti interi si spezza modulo p in fattori irriducibili $\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_k$ di gradi rispettivamente $m_1, m_2, \ldots, m_k$, allora il gruppo di Galois $G^{(p)}$ di $\bar{f}$ è ciclico e generato da una permutazione di struttura ciclica $(m_1, m_2, \ldots, m_k)$, e una permutazione con questa struttura ciclica compare anche nel gruppo di Galois G di $f(x)$.*

3.44 Esempio. Sia $f(x) = x^5 - x - 1$, che è irriducibile su $\mathcal{Q}$, e sia $p = 2$. Si ha $\bar{f}(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$, che non ha fattori multipli. G contiene allora una permutazione di struttura ciclica (2,3), cioè del tipo (1,2)(3,4,5). Per $p = 3$ esso resta irriducibile, e dunque G contiene un $5-$ciclo. Inoltre, se $\tau = (i, j)(k, l, m)$ allora $\tau^3 = (i, j)$. Applichiamo allora la *ii*) del lemma che segue.

3.45 Lemma. *i) Un sottogruppo transitivo di S^n che contiene una trasposizione e un $(n-1)-$ciclo coincide con S^n;*

ii) un sottogruppo G di S^p, p primo, che contiene una trasposizione e un ciclo di lunghezza p, coincide con S^p.

Dim. i) Per la transitività la trasposizione deve contenere la cifra fissata dall'$(n-1)-$ciclo. Sia allora $\sigma = (1)(2, 3, \ldots, n)$ e $\tau = (1, i)$. Coniugando τ con le potenze di σ si ottengono le trasposizioni $(1, 2), (1, 3), \ldots (1, n)$ che generano S^n (una permutazione è prodotto di trasposizioni e una trasposizione (i, j) si scrive come $(1, i)(1, j)(1, i)$).

ii) Siano $\sigma = (1, 2, \ldots, p)$, $\tau = (i, i + s)$; allora coniugando con σ^s si ottengono successivamente le p trasposizioni $(i, i + s), (i + s, i + 2s), (i + 2s, i + 3s), \ldots, (i + (p - 1)s, i)$ che contengono tutte le p cifre, e che possiamo scrivere $(1, i), (i, j), (j, k), \ldots, (r, 1)$. Il prodotto di tutte queste, nell'ordine scritto, è il $(p-1)-$ciclo $\sigma' = (1)(i, r, \ldots, j)$. Con la trasposizione $(1, i)$ siamo nelle condizioni di *i*) (la transitività si ottiene perché il sottogruppo G contiene anche il prodotto $(1, i)$ per τ, che è un ciclo di lunghezza p). Dunque $G = S^p$. ♢

3.46 Nota. Nella *ii*) del lemma, se p non è primo, applicando ripetutamente alla trasposizione $(i, i+s)$ la potenza $s-$esima del ciclo $(1, 2, \ldots, p)$ si ottengono $\frac{p}{(p,s)}$ trasposizioni, che contengono in tutto $\frac{p}{(p,s)}$ cifre. Se $(p, s) \neq 1$ queste non possono generare S^p.

Questo lemma si può utilizzare per costruire polinomi su $\mathcal{Q}$ il cui gruppo di Galois è il gruppo simmetrico.

3.47 Teorema. *Per ogni n esistono polinomi di grado n su $\mathcal{Q}$ il cui gruppo di Galois su $\mathcal{Q}$ è il gruppo simmetrico S^n.*

Dim. Sappiamo che per ogni p e n esistono polinomi di grado n irriducibili mod p. Siano f_1, f_2, f_3 polinomi monici di grado n tali che f_1 sia irriducibile mod 2; f_2 sia prodotto di un fattore lineare e uno di grado $n-1$ mod 3; f_3 sia prodotto di un polinomio di secondo grado e uno o due fattori di grado dispari mod 5. (Tutti questi fattori siano irriducibili). Consideriamo allora il polinomio $f = 15f_1 + 10f_2 + 6f_3$. Mod 2 questo polinomio è f_1, e dunque è irriducibile, e pertanto è irriducibile su $\mathcal{Q}$. Il gruppo di Galois è dunque transitivo. Esso contiene inoltre un $(n-1)-$ciclo, derivante dalla fattorizzazione mod 3, e una permutazione $\rho = (i,j)c_1c_2$ con i c_i di lunghezza d_i dispari, derivante dalla fattorizzazione mod 5. Allora $\rho^{d_1d_2} = (i,j)$, e per il lemma il gruppo di Galois di f è il gruppo simmetrico S^n. ♢

3.48 Esempio. Con $n = 6$, sia $f_1 = x^6 + x + 1$, $f_2 = (x+1)(x^5 - x + 1)$, $f_3 = (x^2 - 4x + 1)(x^3 + x + 1)(x - 1)$. Allora $f(x) = 31x^6 + 10x^5 + 6x^4 - 10x^2 + 9x + 19$ è un polinomio con le proprietà richieste.

3.5 Il problema inverso di Galois

Il *problema inverso di Galois* richiede di stabilire se dato un gruppo finito G esistono un campo K e un polinomio $f(x)$ tali che G sia isomorfo al gruppo di Galois di $f(x)$ su K. In caso affermativo si dirà che G è un *gruppo di Galois su K*.

Con questa terminologia il Teor. 3.47 si può enunciare dicendo che per ogni n il gruppo S^n è un gruppo di Galois su $\mathcal{Q}$.

3.49 Corollario. *Sia G un gruppo finito, $f(x)$ un polinomio a coefficienti in $\mathcal{Q}$. Allora G è gruppo di Galois di $f(x)$ su un ampliamento di $\mathcal{Q}$.*

Dim. Per un opportuno n, sia $G \subseteq S^n$, e sia sia $f(x)$ un polinomio su $\mathcal{Q}$ che ammette S^n come gruppo di Galois. In $\mathcal{Q}(\underline{\alpha})$ sia γ tale che $G_\gamma = G$. Allora il gruppo di Galois di $f(x)$ su $\mathcal{Q}(\gamma)$ è G. ♢

Se come mostra il corollario precedente è facile vedere che ogni gruppo finito è un gruppo di Galois su un certo campo K (in questo caso, un ampliamento di $\mathcal{Q}$), è invece estremamente difficile stabilire se un gruppo finito è un gruppo di Galois su $\mathcal{Q}$ è a tutt'oggi irrisolto. Oltre al gruppo simmetrico, la risposta è positiva anche per i gruppi abeliani come ora vedremo (e anche per i gruppi risolubili, ma si tratta di un risultato molto più profondo). Vi sono campi per

i quali la risposta è positiva (ad esempio, il campo $\mathcal{C}(x)$ delle funzioni razionali a coefficienti complessi).

Il risultato sui gruppi abeliani si basa sui seguenti fatti:

i) il teorema di Dirichlet (v. dim. del Teor. 3.13), e anzi su una forma più debole ($r = 1$): per ogni n, la successione $kn + 1$ contiene infiniti numeri primi; in altri termini, dato n, esistono infiniti primi $p \equiv 1 \bmod n$;

ii) se ϵ è una radice primitiva $n-$esima dell'unità, il gruppo di Galois di $\mathcal{Q}(\epsilon)$ su $\mathcal{Q}$ è il gruppo $U(n)$ (Teor. 3.13), e dunque, se $n = p$, primo, è ciclico di ordine $p - 1$;

iii) un gruppo abeliano (finito) è prodotto diretto di gruppi ciclici (teorema fondamentale dei gruppi abeliani);

iv) un gruppo ciclico contiene un sottogruppo per ogni divisore dell'ordine;

v) se $\varphi(n)$ è la funzione di Eulero, e $p_1, p_2, \cdots, p_k$ sono primi distinti, allora $\varphi(p_1 p_2 \cdots p_k) = \varphi(p_1)\varphi(p_2)\cdots\varphi(p_k) = (p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$ e

$$U(p_1 p_2 \cdots p_k) \simeq U(p_1) \times U(p_2) \times \cdots \times U(p_k).$$

3.50 Lemma. *Sia G un gruppo ciclico. Allora G è un gruppo di Galois su $\mathcal{Q}$.*

Dim. Sia $|G| = n$, e sia p un primo, $p \equiv 1 \bmod n$, ϵ una radice primitiva $p-$esima dell'unità. Il gruppo di Galois di $\mathcal{Q}(\epsilon)$ su $\mathcal{Q}$ è il gruppo ciclico $U(p)$, di ordine $p - 1$. Poiché n divide $p - 1$, $U(p)$ ha un sottogruppo H di ordine $(p - 1)/n$, e quindi di indice n. Il quoziente $U(p)/H$ è ciclico di ordine n, e dunque è isomorfo a G. Sia $\gamma \in \mathcal{Q}(\epsilon)$ tale che $H = U(p)_\gamma$. Allora il gruppo di Galois di $\mathcal{Q}(\epsilon)$ su $\mathcal{Q}$ è $U(p)/H$ (Teor. 2.52), e pertanto è isomorfo a G. $\diamondsuit$

3.51 Teorema. *Sia G un gruppo abeliano finito. Allora G è un gruppo di Galois su $\mathcal{Q}$.*

Dim. Se $G = \{1\}$, G è il gruppo di Galois di $\mathcal{Q}$ su $\mathcal{Q}$. Sia $|G| > 1$; analogamente al caso di un gruppo ciclico dimostriamo che G è isomorfo a un quoziente di $U(n)$ per un certo n. Si ha, per certi n_i, $G \simeq \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$. Per il teorema di Dirichlet esistono primi p_i distinti tali che $p_i \equiv 1 \bmod n_i$, $i = 1, 2, \ldots, k$. Come nel lemma precedente, $U(p_i)$ contiene un sottogruppo H_i di indice n_i, e il quoziente $U(p_i)/H_i$ è isomorfo a $\mathbf{Z}_{n_i}$. Sia $H = H_1 \times H_2 \times \cdots \times H_k$; si ha

$$\begin{aligned} G &\simeq \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k} \simeq \frac{U(p_1)}{H_1} \times \frac{U(p_2)}{H_2} \times \cdots \times \frac{U(p_k)}{H_k} \\ &\simeq \frac{U(p_1) \times U(p_2) \times \cdots \times U(p_k)}{H} \simeq \frac{U(p_1 p_2 \cdots p_k)}{H} \end{aligned}$$

dove l'ultimo isomorfismo segue dal fatto che i p_i sono distinti. Posto $n = p_1 p_2 \cdots p_k$ abbiamo allora $G \simeq U(n)/H$. Se ϵ è una radice $n-$esima dell'unità,

il gruppo di Galois di $\mathcal{Q}(\epsilon)$ su $\mathcal{Q}$ è $U(n)$, e se γ è tale che $U(n)_\gamma \simeq H$, il gruppo di Galois di $\mathcal{Q}(\gamma)$ su $\mathcal{Q}$ è $U(n)/H$, isomorfo a G.

Visto come gruppo di Galois di un polinomio, G è il gruppo di Galois di $J(x)$, il polinomio minimo di γ (Teor. 2.52). $\diamondsuit$

3.6 Complementi

3.6.1 Teoremi di Hilbert e Schur

Nella dimostrazione del teorema di Ruffini–Abel (Teor. 3.26) abbiamo visto che il gruppo di Galois su $Q(a_1, a_2, \ldots, a_n)$ dell'equazione generale di grado n (Def. 3.24) è il gruppo simmetrico S^n. In particolare, ciò dimostra che S^n è il gruppo di Galois di un polinomio su un opportuno campo. Abbiamo anche visto (Teor. 3.47) che S^n è gruppo di Galois di polinomi sui razionali. Quest'ultimo fatto si può dedurre dal precedente grazie al seguente teorema di Hilbert (che non dimostriamo):

3.52 Teorema (HILBERT, 1892). *Sia:*

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1} + b_n$$

un polinomio a coefficienti $b_i = b_i(a_1, a_2, \ldots, a_n)$ nel campo $Q(a_1, a_2, \ldots, a_n)$ delle funzioni razionali nelle indeterminate a_i. Allora, se G è il gruppo di Galois di $f(x)$ su questo campo, si possono scegliere in infiniti modi numeri razionali r_i tali che il polinomio :

$$f^*(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1} + c_n, \tag{3.13}$$

che ha come coefficienti i numeri $c_i = b_i(r_1, r_2, \ldots r_n)$ del campo Q così ottenuti ha gruppo di Galois G.

L'equazione generale su Q si ottiene per $b_i = a_i,\ i = 1, 2, \ldots, n$, e poiché essa ha come gruppo di Galois su $Q(a_1, a_2, \ldots, a_n)$ il gruppo S^n, esistono infinite $n-$ple di numeri razionali che sostituiti agli a_i danno equazioni con gruppo di Galois S^n.

Il teorema ora enunciato è un teorema di esistenza: non viene infatti fornito alcun procedimento per trovare i numeri razionali in questione.

Sia ora m un intero, e sia $a(m)$ il numero dei polinomi di grado n a coefficienti interi di valore assoluto minore o uguale a m. Sia inoltre $s(m)$ il numero di quelli tra questi che hanno S^n come gruppo di Galois su Q; si ha certamente $s(m) < a(m)$. Sussiste a questo proposito il seguente:

3.53 Teorema (SCHUR, 1933). *Si ha*:

$$\lim_{m\to\infty} \frac{s(m)}{a(m)} = 1.$$

Questo risultato si può interpretare nel senso che "quasi tutti" i polinomi a coefficienti interi su Q hanno come gruppo di Galois il gruppo simmetrico.

Sussiste un analogo risultato per le $n-$ple di razionali che forniscono polinomi con gruppo di Galois S^n (Teor. 3.52): le $n-$ple di razionali r_i per i quali il polinomio (3.13) non ha S^n come gruppo di Galois sono "rare" (Doerge, 1926).

3.6.2 Costruzioni con riga e compasso e divisione del cerchio

È noto che un numero algebrico è costruibile con riga e compasso (o semplicemente *costruibili*) se e solo se si ottiene risolvendo una catena di equazioni al più quadratiche su Q. In termini di gruppo di Galois abbiamo:

3.54 Teorema. *Le radici di un polinomio irriducibile sono costruibili con riga e compasso se, e solo se, l'ordine del gruppo di Galois del polinomio è una potenza di* 2.

Dim. La condizione è necessaria. Se le radici sono costruibili, si tratta di soluzioni di una catena di equazioni quadratiche, e dunque il gruppo di Galois si riduce all'identità per aggiunzioni successive di irrazionali quadratici. Gli indici di una serie di composizione del gruppo sono dunque uguali a 2, e il loro prodotto è l'ordine del gruppo.

La condizione è sufficiente. È noto che un gruppo di ordine una potenza di un primo è risolubile, e che quindi gli indici di una serie di composizione sono numeri primi; nel nostro caso sono tutti uguali a 2. Per ogni radice abbiamo allora una catena di ampliamenti quadratici (v. (3.3)), e quindi di equazioni quadratiche, e pertanto essa risulta costruibile. ♢

L'equivalente algebrico del problema della divisione del cerchio in n parti uguali, e cioè della costruzione del poligono regolare con n lati è la risoluzione dell'equazione ciclotomica $\Phi_n(x) = 0$, che sappiamo avere gruppo di Galois abeliano e di ordine $\varphi(n)$ (Teor. 3.13). Per il teorema ora dimostrato abbiamo allora:

3.55 Corollario. *Il poligono regolare con n lati è costruibile con riga e compasso se e solo se* $\varphi(n)$ *è una potenza di* 2. ♢

Sia $n = 2^k p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, con i p_i primi distinti dispari. Allora:

$$\varphi(n) = 2^{k-1} p_1^{m_1-1}(p_1 - 1) p_2^{m_2-1}(p_2 - 1) \cdots p_t^{m_t-1}(p_t - 1).$$

Se $\varphi(n)$ deve essere una potenza di 2, i fattori $p_i^{m_i-1}$ devono essere tutti uguali a 1, e i fattori $p_i - 1$ potenze di 2. Ne segue $m_i = 1$ per ogni i, e $p_i - 1 = 2^{s_i}$, ovvero:

3.56 Corollario. *Il poligono regolare con n lati è costruibile se e solo se n è una potenza di 2, oppure della forma:*

$$n = 2^k p_1 p_2 \cdots p_t,$$

dove i primi p_i sono distinti e della forma $p = 2^s + 1$ (primi di Fermat). $\diamondsuit$

Così ad esempio, il pentagono regolare è costruibile, come pure il poligono con 17 lati (Gauss).

Nota. Un numero della forma $2^s + 1$ è primo solo se s è una potenza di 2. Se infatti $s = qr$, con q primo dispari, si avrebbe la seguente decomposizione:

$$2^{qr} + 1 = (2^r + 1)(2^{r(q-1)} - 2^{r(q-2)} + \cdots - 2^r + 1).$$

Per $s = 0, 1, 2, 3, 4$ si hanno i numeri primi $3, 5, 17, 257, 65537$. Ma il successivo $2^{2^5} + 1$ non è più primo: è divisibile per 641 (Eulero). Quelli detti sono i soli numeri primi di Fermat conosciuti. Non è noto se ne esistono altri, o se ve ne sono in numero finito o infinito.