Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

RISOLUBILITÀ PER RADICALI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Mariagiulia De Maria

Sessione II
Anno Accademico 2012/2013

La felicità non è fare tutto ciò che si vuole,
ma volere tutto ciò che si fa.
Friedrich Nietzsche

Indice

Introduzione

Il titolo di questo elaborato *Risolubilità per Radicali* fa riferimento ad una parte della Teoria di Galois. Questa teoria, le cui fondamenta furono date dal matematico francese Évariste Galois (1811-1832), risolve il problema risalente agli arabi del IX secolo di trovare formule risolutive per le equazioni polinomiali. Un'equazione polinomiale di grado n un un campo K è un'equazione che si ottiene uguagliando a zero un polinomio di grado n a coefficienti in K, come la seguente

$$f(x) := a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

dove x, detta indeterminata, è un valore incognito. Risolvere un'equazione polinomiale significa trovarne le radici, ovvero quei valori α che stanno in un opportuno campo contente il campo di partenza K e tali che

$$f(\alpha) := a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0$$

I matematici si sono sempre chiesti se esistono delle formule generali per risolvere queste equazioni polinomiali. Per il grado $n = 2$, esiste la nota formula quadratica, per il grado $n = 3$ esistono le formule di Cardano, sviluppate nel XVI secolo ed infine per il grado $n = 4$ esistono le formule di Ferrari, sviluppate sempre nel XVI secolo. La particolarità di queste formule è che usano solamente somme, prodotti e radici. Per gradi più alti, non si trovarono mai delle soluzioni generali, solo delle soluzioni particolari. Fu solamente con gli scritti di Galois, che la teoria prese una svolta.
Galois riprese gli studi dei matematici precedenti e li sviluppò associando ad ogni equazione polinomiale un gruppo di permutazioni sulle radici, il futuro Gruppo di Galois. Galois riusci a ricondurre la risolubilità delle equazioni polinomiali ad alcune proprietà fondamentali di questo gruppo. Tramite questa corrispondenza, Galois fu in grado di mostrare che dal quinto grado in poi, non esistono delle formule risolutive per l'equazione polinomiale generale.
Inoltre Galois gettò le basi della moderna Algebra, dal momento che tramite i suoi trattati si svilupparono le teorie dei Gruppi e dei Campi.

Lo scopo di questa tesi è di esporre il cuore centrale della Teoria di Galois, la risolubilità per radicali delle equazioni polinomiali nel caso in cui il campo di partenza abbia carateristica 0. L'operato è articolato in tre capitoli.
Nel primo capitolo vengono introdotte le nozioni fondamentali della Teoria dei campi e della teoria di Galois, utili per comprendere i capitoli successivi.
Nel secondo capitolo, si sviluppa il problema della risolubilità per radicali. Vengono prima introdotti i gruppi risolubili e alcune loro particolarità. Poi vengono introdotte le nozioni di estensioni radicali e risolubili e relativi teoremi. Nel paragrafo 2.3 viene dimostrato il teorema principale della teoria, il Teorema di Galois, che identifica la risolubilità del gruppo di Galois con la risolubilità dell'estensione. Infine l'ultimo paragrafo si occupa della risolubilità dei polinomi, sfruttando il loro campo di spezzamento.
Nel terzo ed ultimo capitolo, viene discussa la risolubilità dell'equazione polinomiale generale di grado n. Vengono inoltre riportati diversi esempi ed infine viene presentato un esempio di estensione di Galois di grado primo p non risolubile in caratteristica p.

Simboli e Notazioni

$\mathbb{N}$	insieme dei numeri naturali
$\mathbb{Z}$	insieme dei numeri interi
$\mathbb{Z}/m\mathbb{Z}$	insieme delle classi di resto modulo m
$\mathbb{Q}$	insieme dei numeri razionali
$\in$	appartiene a
$\notin$	non appartiene a
$A \subseteq B$	A è sottoinsieme di B
$A \times B$	prodotto cartesiano tra gli insieme A e B
$f : A \to B$	f è una funzione da A a B
$g \circ f$	funzione composta da f e g
$\mathrm{Im} f$	immagine della funzione f
$\ker f$	nucleo della funzione f
$\simeq$	è isomorfo a
$a\|b$	a divide b
$\mathrm{MCD}(a, b)$	massimo comun divisore tra a e b
$\mathrm{mcm}(a, b)$	minimo comune multiplo tra a e b
$\|A\|$	ordine del gruppo A
$\|a\|$	ordine dell'elemento A
$\langle a \rangle$	(sotto)gruppo ciclico generato da a
$A \trianglelefteq B$	A è sottogruppo normale di B
B/A	gruppo quoziente di B su A
S_n	gruppo delle permutazioni su n elementi, detto gruppo simmetrico
A_n	gruppo alterno su n elementi
$\mathrm{Aut}\, R$	automorfismi dell'anello R in sè stesso
$R[x]$	insieme dei polinomi a coefficienti nell'anello R
$\deg f$	grado del polinomio f
$\mathrm{char}\, F$	caratteristica del campo F
$[L : F]$	grado dell'estensione $F \subseteq L$
$\mathrm{Gal}(L/F)$	gruppo di Galois dell'estensione di campi $F \subseteq L$

Capitolo 1

Nozioni preliminari della Teoria di Galois

In questo capitolo verranno riportati gli enunciati di alcuni risolutati fondamentali della Teoria di Galois, prerequisiti per il secondo capitolo. Per le dimostrazioni si veda [1], capitolo 7.

1.1 Gruppo di Galois

Definizione 1.1. Sia G un gruppo e R un anello. Si dice che G *agisce su* R se esiste un omomorfismo di gruppi $\varphi : G \longrightarrow \mathrm{Aut}(R)$ tale che $g \longmapsto \eta_g$. Allora per ogni $x \in R$ si pone $gx = \eta_g(x)$.
Sia

$$R^G := \{x \in R \,|\, gx = x \quad \forall g \in G\} \,.$$

È facile mostrare che R^G è un sottoanello di R, detto *sottoanello degli invarianti*.

Definizione 1.2. Sia K un campo e S un sottoinisieme di $\mathrm{Aut}(K)$. Si ha che K^S è un sottocampo di K, detto *campo fisso* di S in K.

Definizione 1.3. Sia $F \subseteq L$ un'estensione di campi. Definiamo *gruppo di Galois di* L/F il seguente gruppo:

$$\mathrm{Gal}(L/F) := \{\sigma \in \mathrm{Aut}(L) \,|\, \sigma(a) = a \quad \forall a \in F\}$$

dove $\mathrm{Aut}(L) = \{f : L \longrightarrow L \,|\, \text{f è isomorfismo}\}$ è un gruppo con l'operazione di composizione.

Osservazione 1. Il gruppo $\mathrm{Gal}(L/F)$ contiene gli automorfismi di L che lasciano fisso il campo F.

Osservazione 2. Si considerino le estensioni di campi $F \subseteq L \subseteq K$, allora risulta che $\mathrm{Gal}(K/L) \subseteq \mathrm{Gal}(K/F)$, infatti se un automorfismo fissa ogni elemento di L, allora fissa ogni elemento di $F \subseteq L$.

Esempio 1.1. Il gruppo di Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ha esattamente due elementi: l'identità e il coniugio. Inoltre risulta evidente che $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \subseteq \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$.

Esempio 1.2. Data l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$, si vuole calcolare il suo gruppo di Galois e il suo campo fisso. Il polinomio minimo di $\sqrt[3]{2}$ è $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, che ha come radici $\sqrt[3]{2}, \sqrt[3]{2}\mu, \sqrt[3]{2}\mu^2$, dove μ è radice cubica dell'unità. Allora $\mathbb{Q}(\sqrt[3]{2})$ contiene un sola radice di f. Quindi $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$.

1.2 Estensioni di campi

Si ricordino le seguenti definizioni e risultati fondamentali.

Definizione 1.4. Sia F un campo. Si consideri il seguente morfismo di anelli:

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow F \\ 1 &\longmapsto 1_F \\ n &\longmapsto n1_f = 1_F + \ldots + 1_F \end{aligned}$$

Se $\ker\varphi = 0$, si dice che il campo F ha *caratteristica* 0 e si indica con $\mathrm{char}\, F = 0$. Se $\ker\varphi = p\mathbb{Z}$, dove p è un primo, si dice che il campo F ha *caratteristica* p e si indica con $\mathrm{char}\, F = p$.

Osservazione 3. La definizione è ben posta, perché $\ker\varphi$ è un ideale primo. Infatti $\mathbb{Z}/\ker\varphi \simeq \mathrm{Im}\varphi$ e $\mathrm{Im}\varphi$ è un sottoanello del campo F, quindi in particolare è un dominio.

Definizione 1.5. Siano F ed L due campi. Si dice che L è *estensione di campi* di F se $F \subseteq L$, ovvero se F è sottocampo di L. Il *grado dell'estensione* si indica con $[L : F]$ ed è la dimensione di L come spazio vettoriale su F.

Definizione 1.6. Un'estensione di campi $F \subseteq L$ si dice *finita* se $[L : F] < \infty$.

Lemma 1.1 (della Torre)**.** *Siano $F \subseteq L \subseteq K$ delle estensioni di campi. Allora $F \subseteq K$ è un'estensione finita se e solo se $F \subseteq L$ e $L \subseteq K$ sono estensioni finite. In tal caso vale che:*

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

Definizione 1.7. Sia F un campo e sia $F \subseteq L$ un'estensione di campi. Preso $\xi \in L$, si definisce *valutazione in* ξ il seguente omomorfismo di anelli:

$$\begin{aligned} v_\xi : F[x] &\longrightarrow L \\ f(x) &\longmapsto f(\xi) \end{aligned}$$

Inoltre se $\ker v_\xi = 0$, l'elemento ξ è detto *trascendente* su F. Se $\ker v_\xi = I \neq 0$, dove I è un ideale, allora l'elemento ξ è detto *algebrico* su F.

Definizione 1.8. Un'estensione di campi $F \subseteq L$ è detta *algebrica* se ogni elemento di L è algebrico su F.

Osservazione 4. Se un'estensione è finita allora è algebrica, ma non vale il viceversa.

Proposizione 1.2. *Si consideri l'estensione $F \subseteq F(\alpha)$ con α algebrico su F e sia f il polinomio minimo di α su F. Allora $\beta \in F(\alpha)$ è radice di f se e solo se esiste $\sigma \in \mathrm{Gal}(F(\alpha)/F)$ tale che $\sigma(\alpha) = \beta$.*
Inoltre $|\operatorname{Gal}(F(\alpha)/F)| \Big| [F(\alpha) : F]$.

Esempio 1.3. Si consideri l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. Per la proposizione precedente, si ha che $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ è univocamente determinata da $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Perciò $|\operatorname{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| \leq 2$. Ma se $\sigma(\sqrt{2}) = \sqrt{2}$, allora $\sigma = id$, mentre se $\sigma(\sqrt{2}) = -\sqrt{2}$, σ è un automorfismo di $\mathbb{Q}(\sqrt{2})$. Allora $|\operatorname{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$, ovvero $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Per le dimostrazioni delle seguenti proposizioni si veda [4], capitolo 2.

Proposizione 1.3. *Siano F, Ω due campi e sia $F \subseteq F(\alpha)$ un'estensione semplice. Sia $\varphi : F \to \Omega$ un omomorfismo. Se α è algebrico su F con polinomio minimo $f \in F[x]$, allora la seguente mappa è una biezione:*

$$\begin{aligned} \{\text{omomorfismi } \tilde{\varphi} : F(\alpha) \to \Omega | \quad \tilde{\varphi}_{|F} = \varphi\} &\longleftrightarrow \{\text{radici di } \varphi(f) \text{ in } \Omega\} \\ \tilde{\varphi} &\longmapsto \tilde{\varphi}(\alpha) \end{aligned} \quad .$$

Proposizione 1.4. *Siano F, Ω due campi e $f \in F[x]$ un polinomio. Sia $E = F(\alpha_1, \ldots, \alpha_m)$ dove $f(\alpha_i) = 0$ per ogni $i = 1, \ldots, m$. Sia $\varphi_0 : F \to \Omega$ un omomorfismo di campi. Se $\varphi_0(f)$ si spezza linearmente in $\Omega[x]$, allora esiste almeno un omomorfismo $\varphi : E \to \Omega$ che estende φ_0.*

Proposizione 1.5. *Siano $K_1 \subseteq L_1$ e $K_2 \subseteq L_2$ due estensioni di campi. Sia $\varphi_0 : K_1 \to K_2$ un isomorfismo di campi. Presi $\alpha_1 \in L_1$ con polinomio minimo f su K_1 e $\alpha_2 \in L_2$ con polinomio minimo $\varphi_0(f)$ su K_2. Allora esiste $\varphi : K_1(\alpha_1) \to K_2(\alpha_2) \in L_2$ tale che $\varphi_{|K_1} = \varphi_0$ e $\varphi(\alpha_1) = \alpha_2$.*

Questa proposizione si può generalizzare nel modo seguente.

Proposizione 1.6. *Sia $\varphi : F_1 \to F_2$ un isomorfismo di campi. Sia $f_1 \in F_1[x]$ un polinomio e sia $f_2 = \varphi(f_1) \in F_2[x]$. Sia L_1 il campo di spezzamento di f_1 su F_1 e sia L_2 il campo di spezzamento di f_2 su F_2. Allora esiste un isomorfismo $\overline{\varphi} : L_1 \to L_2$ tale che $\overline{\varphi}_{|F_1} = \varphi$.*

1.2.1 Estensioni Normali e Separabili

Definizione 1.9. Un'estensione algebrica $F \subseteq L$ si dice *estensione normale* se ogni polinomio irriducibile con una radice in L si spezza linearmente in L.

Proposizione 1.7. *$F \subseteq L$ è un'estensione normale se e solo se L è il campo di spezzamente di qualche polinomio $f \in F[x]$.*

Esempio 1.4. Si consideri l'esempio 1.2. L'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ non è un'estensione normale perché il polinomio $x^3 - 2 \in \mathbb{Q}[x]$ non si spezza linearmente in $\mathbb{Q}(\sqrt[3]{2})$, perché non contiene le due radici complesse coniugate $\sqrt[3]{2}\mu, \sqrt[3]{2}\mu^2$. Mentre l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ dell'esercizio 1.3 è normale, perché $\mathbb{Q}(\sqrt{2})$ è il campo di spezzamento del polinomio $x^2 - 2 \in \mathbb{Q}[x]$.

Definizione 1.10. Sia $f \in F[x]$. Il polinomio f si dice *polinomio separabile* se nel suo campo di spezzamento non ha radici multiple.

Proposizione 1.8. *Un polinomio $f \in F[x]$ è separabile se e solo se risulta che $MCD(f, f') = 1$, ove f' indica la derivata prima di f.*

Proposizione 1.9. *Sia $f \in F[x]$ irriducibile. Allora f è separabile se e solo se $f' \neq 0$.*

Proposizione 1.10. *Se F è un campo con caratteristica 0, allora ogni polinomio irriducibile di $F[x]$ è separabile.*

Definizione 1.11. Sia $F \subseteq L$ un'estensione di campi. Un elemento $\alpha \in L$ è detto *elemento separabile* se il suo polinomio minimo è separabile.

Definizione 1.12. L'estensione $F \subseteq L$ si dice *estensione separabile* se ogni elemento di L è separabile su F.

Teorema 1.11 (dell'Elemento Primitivo)**.**
Sia $F \subseteq L = F(\alpha_1, ..., \alpha_n)$ un'estensione finita, dove gli α_i sono algebrici e separabili per ogni $i = 1, .., n$. Allora esiste un elemento $\alpha \in L$ separabile su F tale che $L = F(\alpha)$.

1.2.2 Estensioni di Galois

Definizione 1.13. Un'estensione $F \subseteq L$ si dice *estensione di Galois* se è normale e separabile.

Teorema 1.12. *Sia $F \subseteq L$ un'estensione finita. Allora sono equivalenti:*

1. *L è il campo di spezzamento di un polinomio separabile in $F[x]$;*
2. *F è il campo fisso di $\mathrm{Gal}(L/F)$, ovvero $L^{\mathrm{Gal}(L/F)} = F$;*
3. *$F \subseteq L$ è un'estensione di Galois;*
4. *$|\mathrm{Gal}(L/F)| = [L : F]$.*

Osservazione 5. Se $F \subseteq L$ è di Galois e K è un campo intermedio $F \subset K \subseteq L$, allora $K \subseteq L$ è ancora di Galois, per la parte 1 del teorema precedente.

Osservazione 6. Sia F un campo e sia $f \in F[x]$ un polinomio separabile con campo di spezzamento L su F. Siano $\alpha_1, ...\alpha_n$ le radici di f in L; allora σ induce una permutazione $\tilde{\sigma}$ sulle radici $\{\alpha_1, ...\alpha_n\}$ e l'applicazione

$$\begin{aligned} \varphi : \mathrm{Gal}(L/F) &\longrightarrow S_n \\ \sigma &\longmapsto \tilde{\sigma} \end{aligned}$$

è un omomorfismo iniettivo di gruppi.
In particolare $\mathrm{Gal}(L/F)$ è isomorfo a un sottogruppo di S_n.

Definizione 1.14. Sia F un campo e $f \in F[x]$ un polinomio. Siano $\alpha_1, \ldots, \alpha_n$ le radici di f in qualche estensione K di F. Si definisce *discriminante di f* il seguente

$$\Delta(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

Proposizione 1.13. *Sia F un campo e $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in F[x]$, con $n \geq 2$. Allora $\Delta(f) = h(a_{n-1}, \ldots, a_0)$ per qualche polinomio $h(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$ ed in particolare $\Delta(f) \in F$.*

Definizione 1.15. Si definisce *radice del discriminante* di un polinomio $f \in F[x]$, con radici $\alpha_1, \ldots, \alpha_n$ il seguente

$$\sqrt{\Delta(f)} := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

Proposizione 1.14. *Sia F un campo e sia $f \in F[x]$ un polinomio con discriminante $\Delta(f)$. Sia L il campo di spezzamento di f su F, allora si ha che $\mathrm{Gal}(L/F) \subseteq A_n$ se e solo se $\sqrt{\Delta(f)} \in F$.*

Definizione 1.16. Siano $F \subseteq K \subseteq L$ estensioni di campi finite. Sia $\sigma \in \mathrm{Gal}(L/F)$. Si chiama *campo coniugato di* K il seguente:

$$\sigma K = \{\sigma(\alpha) \mid \quad \alpha \in K\}$$

Teorema 1.15. *Sia $F \subseteq L$ un'estensione di Galois e sia K tale che $F \subseteq K \subseteq L$. Allora sono equivalenti:*

1. *$K = \sigma K$, per ogni $\sigma \in \mathrm{Gal}(L/F)$;*
2. *$\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$, ovvero $\mathrm{Gal}(L/K)$ è normale in $\mathrm{Gal}(L/F)$;*
3. *$F \subseteq K$ è un'estensione di Galois;*
4. *$F \subseteq K$ è un'estensione normale.*

Teorema 1.16. *Siano $F \subseteq K \subseteq L$ estensioni di campi finite tali che $F \subseteq L$ e $F \subseteq K$ sono estensioni di Galois. Allora si ha che:*

$$\mathrm{Gal}(K/F) \simeq \mathrm{Gal}(L/F)\big/ \mathrm{Gal}(L/K)$$

1.3 Corrispondenza di Galois

La corrispondenza di Galois vuole mettere in relazione i campi intermendi di un'estensione di Galois con i sottogruppi del rispettivo gruppo di Galois.

Teorema 1.17 (della corrispondenza di Galois)**.**
Sia $F \subset L$ un'estensione di Galois. Le mappe

$$\{\textit{campi } K | F \subseteq K \subseteq L\} \longleftrightarrow \{\textit{sottogruppi di } \mathrm{Gal}(L/F)\}$$
$$K \xrightarrow{\varphi} \mathrm{Gal}(L/K)$$
$$L^H \xleftarrow{\psi} H$$

sono biezioni e φ e ψ sono una l'inverso dell'altra.
In particolare a sottogruppi normali corrsipondono estensioni normali. Viceversa se l'estensione $F \subseteq K$ è normale allora $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$.

Proposizione 1.18. *Sia $F \subseteq L$ un'estensione finita e separabile. Allora esiste un'estensione $L \subseteq M$ tale che :*

1. *$F \subseteq M$ è estensione di Galois;*
2. *Data un'altra estensione $L \subseteq N$ tale che $F \subseteq N$ è di Galois, allora esiste un omomorfismo di campi $\varphi : M \to N$, che è l'identità su L.*

Il campo M è univocamente determinato a meno di isomorfismi.

Definizione 1.17. Data un'estensione $F \subseteq L$, il campo M con le proprietà della proposizione sopra è detto *chiusura di Galois di L su F.*

Proposizione 1.19. *Sia $F \subseteq L$ un'estensione finita e separabile. Allora esiste un numero finito di campi intermedi K, con $F \subseteq K \subseteq L$.*

Capitolo 2

Risolubilità Per Radicali

2.1 Elementi di Teoria dei Gruppi

2.1.1 Gruppi Risolubili

Definizione 2.1. Un gruppo G si dice *risolubile* se esiste una catena di sottogruppi

$$\{e\} = G_n \subseteq G_{n-1} \subseteq ... \subseteq G_1 \subseteq G_0 = G$$

tali che per $i = 1, .., n$ si ha:

1. $G_i \trianglelefteq G_{i-1}$;

2. G_{i-1}/G_i è abeliano.

Una catena con queste proprietà è detta *serie subnormale abeliana*. Se la seconda condizione non è soddisfatta la serie è detta *serie subnormale*.

Osservazione 7. Osserviamo subito che secondo questa definizione ogni gruppo abeliano non banale è risolubile, infatti un esempio di serie normale abeliana è : $\{e\} \subset G$.

Proposizione 2.1. *Ogni sottogruppo di un gruppo risolubile finito è risolubile.*

Dimostrazione. Sia G un gruppo finito risolubile con serie subnormale abeliana $\{e\} = G_n \subseteq G_{n-1} \subseteq ... \subseteq G_1 \subseteq G_0 = G$ e sia H un sottogruppo di G. Posto $H_i = G_i \cap H$ per ogni $i = 0, ..., n$, si osservi che

$$H_0 = G_0 \cap H = G \cap H = H \quad \text{e} \quad H_n = G_n \cap H = \{e\} \cap H = \{e\} \ .$$

Per ogni $i = 1, \ldots, n$, si consideri l'omomorfismo di gruppi

$$\pi : H_{i-1} \to G_{i-1}/G_i$$
$$h \mapsto hG_i$$

Un elemento $h \in \ker \pi$ se e solo se $hG_i = G_i$, cioè se e solo se $h \in H_{i-1} \cap G_i = (G_{i-1} \cap H) \cap G_i = H \cap G_i = H_i$. Quindi $\ker \pi = H_i$. Per il teorema fondamentale di omomorfismo per gruppi si ha allora che $H_i \trianglelefteq H_{i-1}$. Rimane da mostrare che i quozienti H_{i-1}/H_i sono abeliani. Per il teorema fondamentale di omomorfismo per gruppi si ha che $H_{i-1}/H_i \simeq \mathrm{Im}\pi \subset G_{i-1}/G_i$, ma $\mathrm{Im}\pi$ è abeliano perché sottogruppo di gruppo abeliano. Allora la serie $\{e\} = H_n \subseteq H_{n-1} \subseteq ... \subseteq H_1 \subseteq H_0 = H$ è una seria subnormale abeliana e quindi H è un gruppo risolubile. □

Teorema 2.2. *Sia G un gruppo finito e sia H un sottogruppo normale di G. Allora G è risolubile se e solo se H e G/H sono risolubili.*

Dimostrazione. Sia G un gruppo finito risolubile. Per la proposizione precedente anche H è risolubile. Si deve allora mostrare che il quoziente G/H è risolubile. Sia $\{e\} = G_n \subseteq G_{n-1} \subseteq ... \subseteq G_1 \subseteq G_0 = G$ una serie subnormale abeliana per G e sia $\pi : G \to G/H$ la proiezione canonica che ad ogni $g \in G$ associa $gH \in G/H$. Siano $\widetilde{G}_{i-1} = \pi(G_i)$ per ogni $i = 0, \ldots, n$, allora si ha che:

(*i*) $\widetilde{G}_0 = G/H$, perché π è un omomorfismo suriettivo di gruppi;

(*ii*) $\widetilde{G}_n = \{eH\}$, che è l'identità di G/H, per definizione di omomorfismo di gruppi.

(*iii*) $\widetilde{G}_i \trianglelefteq \widetilde{G}_{i-1}$, poiché $G_i \trianglelefteq G_{i-1}$.

Per mostrare che i quozienti sono abeliani, si consideri l'omomorfismo di gruppi suriettivo

$$\varphi : G_{i-1}/G_i \to \widetilde{G}_{i-1}/\widetilde{G}_i$$
$$gG_i \mapsto \pi(g)\pi(G_i) = \pi(g)\widetilde{G}_i$$

Si ha perciò che $\widetilde{G}_{i-1}/\widetilde{G}_i$ è isomorfo a un gruppo quoziente del gruppo abeliano G_{i-1}/G_i, che è ancora abeliano. Perciò la serie $\{eH\} = \widetilde{G}_n \subseteq \widetilde{G}_{n-1} \subseteq ... \subseteq \widetilde{G}_1 \subseteq \widetilde{G}_0 = G/H$ è una serie subnormale abeliana e quindi G/H è un gruppo risolubile.
Viceversa, siano H e G/H due gruppi risolubili. Esistono allora due serie subnormali abeliane:

$$\{e\} = H_n \subseteq H_{n-1} \subseteq \ldots \subseteq H_1 \subseteq H_0 = H$$

e

$$\{H\} = K_m/H \subseteq K_{m-1}/H \subseteq \ldots \subseteq K_1/H \subseteq G/H.$$

Si consideri allora la catena

$$\{e\} = H_n \subseteq H_{n-1} \subseteq \ldots \subseteq H_1 \subseteq H_0 = H = K_m \subseteq K_{m-1} \subseteq \ldots \subseteq K_1 \subseteq G.$$

Per $j = 0, \ldots, n$ i sottogruppi H_j sono già tali che H_j è normale in H_{j-1} e che H_{j-1}/H_j è abeliano, si deve mostrare che sono tali anche i sottogruppi K_i per $i = 1, \ldots, m$. Dato che $K_i/H \trianglelefteq K_{i-1}/H$, $K_i \trianglelefteq K_{i-1}$, per $i = 1, \ldots, m$ per il secondo teorema di omomorfismo per gruppi. Infine, sempre per il secondo teorema di omomorfismo per gruppi, si ha che i quozienti $K_{i-1}/K_i \simeq (K_{i-1}/H)/(K_i/H)$ sono abeliani per $i = 1, \ldots, m$. Dunque G è risolubile. □

Proposizione 2.3. *I gruppi S_n e A_n sono risolubili per $n \leq 4$.*

Dimostrazione. I casi $n = 1, 2$ sono banali. Una serie subnormale abeliana per S_3 è

$$\{id\} \subset A_3 \subset S_3 \ .$$

Infatti A_3 è ciclico di ordine 3 ed è tale che $A_3 \trianglelefteq S_3$. Inoltre $S_3/A_3 \simeq \mathbb{Z}_2$.
Si indichi con $K = \{id, (12)(34), (13)(24), (14)(23)\}$ il sottogruppo di Klein. Una serie subnormale abeliana per S_4 è

$$\{id\} \subset K \subset A_4 \subset S_4 \ .$$

Infatti $S_4/A_4 \simeq \mathbb{Z}_2$ e $A_4/K \simeq \mathbb{Z}_3$ sono gruppi abeliani. □

Teorema 2.4. *I gruppi S_n e A_n non sono risolubili per $n \geqslant 5$.*

Dimostrazione. Sia $n \geq 5$. Si supponga che $G := S_n$ oppure $G := A_n$ e si consideri un catena di sottogruppi

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n \supseteq \ldots$$

dove per ogni $i \geq 1$, $H_i \trianglelefteq H_{i-1}$ e H_{i-1}/H_i è ciclico. Si vuole allora mostrare, per induzione su i, che ogni H_i contiene tutti i 3-cicli di S_n, così che la catena sia necessariamente infinita. Se $i = 0$, è banalmente vero, perché $H_0 = G$. Si supponga valga l'ipotesi induttiva per H_{i-1}. Si vuole mostrare che il generico 3-ciclo $(cbe) \in H_{i-1}$ sta anche in H_i. Dal momento che $n \geq 5$, esistono altri due elementi $a, d \in H_{i-1}$ tali che $|\{a, b, c, d, e\}| = 5$. Si considerino allora i 3-cicli $x := (abc)$, $y := (cde) \in H_{i-1}$. Sia $\pi : H_{i-1} \to H_{i-1}/H_i$ la proiezione canonica. Per ipotesi H_{i-1}/H_i è abeliano, risulta allora che

$$\pi(x^{-1}y^{-1}xy) = \pi(x)^{-1}\pi(y)^{-1}\pi(x)\pi(y) = \{id\} \ .$$

Allora $x^{-1}y^{-1}xy \in \ker \pi = H_i$, ma $x^{-1}y^{-1}xy = (cba)(edc)(abc)(cde) = (cbe)$ e (cbe) è un generico 3-ciclo, quindi H_i contiene tutti i 3-cicli. □

2.1.2 Gruppi Semplici

Definizione 2.2. Un gruppo G si dice *semplice* se è non banale e i suoi unici sottogruppi normali sono $\{e\}$ e G.

Osservazione 8. Segue subito dalla definizione che un gruppo semplice non abeliano non può essere risolubile.

Proposizione 2.5. *Sia G un gruppo finito. Allora sono equivalenti:*

(i) *G è abeliano e semplice;*

(ii) *G è ciclico di ordine primo.*

Dimostrazione. Sia G un gruppo abeliano e semplice. Poichè ogni sottogruppo di un gruppo abeliano è normale, il gruppo G, essendo anche semplice, è privo di sottogruppi propri non banali. Allora G deve essere generato da ogni suo elemento diverso dall'elemento neutro, perciò è ciclico. Se il suo ordine non fosse primo, allora G avrebbe dei sottogruppi propri non banali e non sarebbe semplice. Viceversa, sia G un gruppo ciclico di ordine primo. Allora è abeliano e per il teorema di Lagrange esso non ha sottogruppi propri non banali. □

Definizione 2.3. Una serie subnormale di un gruppo G i cui fattori sono tutti gruppi semplici è detta *serie di composizione.*

Teorema 2.6. *Sia G un gruppo finito non banale. Allora G ha una serie di composizione.*
In particolare se G è risolubile, ogni sua serie subnormale abeliana si può raffinare a una serie di composizione.

Dimostrazione. Sia G un gruppo finito. Se G è semplice, una serie di composizione per G è $\{e\} \subset G$. Si vuole procedere per induzione sull'ordine di G. Se $|G| = 2$, G è semplice. Sia $|G| \geq 3$. Se G non è semplice, esso ha un sottogruppo normale proprio N, che possiamo scegliere con ordine massimo. Per ipotesi induttiva, N ammette una serie di composizione

$$\{e\} = N_m \subseteq N_{m-1} \subseteq \ldots \subseteq N_1 \subseteq N_0 = N$$

Inoltre G/N è semplice perché N ha ordine massimo. Quindi la serie

$$\{e\} = N_m \subseteq N_{m-1} \subseteq \ldots \subseteq N_1 \subseteq N_0 = N \subseteq G$$

è serie di composizione per G.
Sia ora G un gruppo risolubile con serie subnormale abeliana

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_1 \subseteq G_0 = G\ .$$

Poichè G_{i-1}/G_i è abeliano, ogni suo sottogruppo proprio è normale e abeliano. Se G_{i-1}/G_i non è semplice, si consideri un sottogruppo proprio non banale $\overline{H}$ di G_{i-1}/G_i. Si ha che $\overline{H} = H/G_i$, con H sottogruppo di G contenente G_i. Inoltre si ha che $G_i \subset H \subset G_{i-1}$, con $H \trianglelefteq G_{i-1}$ e $G_i \trianglelefteq H$ per il secondo teorema di omomorfismo di gruppi. Per di più i quozienti $G_{i-1}/H \simeq (G_{i-1}/G_i)/\overline{H}$ e $\overline{H} = H/G_i$ sono abeliani. Dal momento che G è un gruppo finito, si può ripetere il ragionamento per un numero finito di passi fino ad ottenere una catena

$$\{e\} = H_r \subset H_{r-1} \subset \ldots \subset H_1 \subset H_0 = G$$

di sottogruppi tali che $H_j \trianglelefteq H_{j-1}$ e i gruppi quoziente H_{i-1}/H_i non abbiano sottogruppi propri non banali, ovvero siano semplici. □

Proposizione 2.7. *Un gruppo finito è risolubile se e solo se ha una serie normale ciclica i cui fattori hanno tutti ordine primo.*

Dimostrazione. Sia G un gruppo finito risolubile. Allora ogni sua serie subnormale abeliana si può raffinare a una serie di compozione per il teorema appena visto, i cui fattori, essendo semplici e abeliani, sono per la proposizione 2.5 ciclici di ordine primo. Il viceversa è ovvio. □

Osservazione 9. Risulta allora che un gruppo finito G è risolubile se esiste una catena di sottogruppi

$$\{e\} = G_n \subseteq G_{n-1} \subseteq ... \subseteq G_1 \subseteq G_0 = G$$

tali che per $i = 1, .., n$ si ha:

1. $G_i \trianglelefteq G_{i-1}$;
2. G_{i-1}/G_i è gruppo ciclico di ordine p.

2.2 Estensioni radicali e risolubili

Definizione 2.4. Un'estensione di campi $F \subseteq L$ si dice *estensione radicale* se esiste una catena di campi

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_{n-1} \subseteq F_n = L$$

dove per ogni $i = 1, ..., n$ esistono $\gamma_i \in F_i$ e degli interi positivi m_i tali che $F_i = F_{i-1}(\gamma_i)$ e $\gamma_i^{m_i} \in F_{i-1}$.

Osservazione 10. Si osservi che un'estensione di campi $F \subseteq L$ è radicale se e solo se $L = F(\gamma_1, ..., \gamma_n)$, dove $\gamma_1^{m_1} \in F$ e $\gamma_i^{m_i} \in F(\gamma_1, ..., \gamma_{i-1})$ con $m_i \in \mathbb{N}$.

Osservazione 11. Se $\gamma_i^{m_i} \in F(\gamma_1, ..., \gamma_{i-1})$ allora γ_i è radice di

$$x^{m_i} - \gamma_i^{m_i} \in F(\gamma_1, ..., \gamma_{i-1})[x] \ .$$

Quindi l'estensione $F(\gamma_1, ..., \gamma_i)$ è finita e algebrica su $F(\gamma_1, ..., \gamma_{i-1})$. Si ha allora che le estensioni radicali sono finite e algebriche.

Esempio 2.1. Si consideri l'estensione di campi $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5+\sqrt{5}})$ e siano $\gamma_1 = \sqrt{5}$ e $\gamma_2 = \sqrt{5+\sqrt{5}}$. Si ha allora la seguente catena di estensioni:

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma_1) \subseteq \mathbb{Q}(\gamma_1)(\gamma_2)$$

dove $\gamma_1^2 = (\sqrt{5})^2 = 5 \in \mathbb{Q}$ e $\gamma_2^2 = \left(\sqrt{5+\sqrt{5}}\right)^2 = 5 + \sqrt{5} \in \mathbb{Q}(\gamma_1) = \mathbb{Q}(\sqrt{5})$. Basta allora mostrare che $\mathbb{Q}(\gamma_1)(\gamma_2) = \mathbb{Q}(\gamma_2)$, per avere un'estensione radicale. Per mostrare ciò, si deve mostrare che $\gamma_1 \in \mathbb{Q}(\gamma_2)$, il viceversa è banale. Risulta che

$$\gamma_2^2 = \left(\sqrt{5+\sqrt{5}}\right)^2 = 5 + \sqrt{5} = 5 + \gamma_1 \ .$$

Allora $\gamma_1 = \gamma_2^2 - 5 \in \mathbb{Q}(\gamma_2)$. Quindi l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5+\sqrt{5}})$ è radicale.

Osservazione 12. Se $F \subseteq L$ e $L \subseteq M$ sono estensioni radicali, allora lo è anche $F \subseteq M$. Infatti possiamo scrivere $L = F(\alpha_1, ..., \alpha_n)$, dove per ogni $i = 1, \ldots, n$ esistono degli interi m_i tali che $\alpha_i \notin F(\alpha_1, \ldots, \alpha_{i-1})$ ma $\alpha_i^{m_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$ e $M = L(\beta_1, ..., \beta_m)$, dove per ogni $i = 1, \ldots, m$ esistono degli interi n_i tali che $\beta_i \notin F(\beta_1, \ldots, \beta_{i-1})$, ma $\beta_i^{n_i} \in F(\beta_1, \ldots, \beta_{i-1})$ perciò risulta che:

$$M = L(\beta_1, ..., \beta_m) = F(\alpha_1, ..., \alpha_n)(\beta_1, ..., \beta_m) = F(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m) \ .$$

Definizione 2.5. Un'estensione $F \subseteq L$ è detta *estensione risolubile* se esiste un'estensione di L, $L \subseteq M$, tale che $F \subseteq M$ sia un'estensione radicale.

Osservazione 13. Si osservi che le definizioni di estensione radicale e risolubile sono diverse. Infatti esistono delle estensioni risolubili, che non sono radicali. Un esempio verrà riportato nel capitolo 3.

Definizione 2.6. Siano dati un campo L e due suoi sottocampi $K_1, K_2 \subseteq L$. Si chiama *campo composto* di K_1 e K_2 il sottocampo di L generato da $K_1 \bigcup K_2$ e si indica con K_1K_2.

Osservazione 14. Il composto è per definizione il più piccolo sottocampo di L che contiene K_1 e K_2.

Osservazione 15. Sia $F \subseteq L$ un'estensione di campi. Se $K_1 = F(\alpha_1, ..., \alpha_n)$ e $K_2 = F(\beta_1, ..., \beta_m)$ sono due estensioni finitamente generate di F, allora si ha che il composto è l'estensione finitamente generata

$$K_1K_2 = F(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m) \ .$$

Proposizione 2.8. *Siano date le estensioni $F \subseteq L \subseteq M$, tali che $F \subseteq M$ è di Galois. Allora il campo composto di tutti i campi coniugati di L in M è la chiusura di Galois di $F \subseteq L$.*

Dimostrazione. Per il Teorema dell'Elemento Primitivo (1.11), $L = F(\alpha)$ per qualche $\alpha \in L$. Dato che l'estensione $F \subseteq M$ è di Galois, il polinomio minimo h di α su F è separabile e si spezza linearmente su M. Supponiamo che in M si abbia che $h(x) = (x-\alpha_1)\dots(x-\alpha_r)$, dove $\alpha_1 = \alpha$. Allora risulta che l'estensione $F \subseteq K = F(\alpha_1, \dots, \alpha_r)$ è di Galois, contenente L. Ma K è proprio la chiusura di Galois di $F \subseteq L$, infatti:

- $F \subseteq K$ è un'estensione di Galois tale che $L \subseteq K$;
- Sia K' un altro campo contenente L e tale che l'estensione $F \subseteq K'$ è di Galois. Si consideri ora l'omomorfismo di inclusione φ_0 di F in K'. L'immagine tramite φ_0 di h si spezza linearmente su K', perché l'estensione $F \subseteq K'$ è di Galois per ipotesi, ed in particolare è normale, quindi dal momento che K' contiene la radice α di h, quest'ultimo si deve spezzare linearmente in K'. Allora per la proposizione 1.4 esiste almeno un omomorfismo $\varphi : K \to K'$ che estende φ_0. Ovvero K' contiene una copia isomorfa di K.

Si vuole ora mostrare che per ogni α_i esiste $\sigma \in \mathrm{Gal}(M/F)$ tale che $\sigma L = F(\alpha_i)$. Fissato $i \in \{1, \dots, r\}$ si consideri l' estensione $F \subseteq M$. Si noti che gli elementi $\alpha_1, \alpha_i \in M$ hanno entrambi polinomio minimo $h \in F[x]$. Allora per la proposizione 1.5, ove l'identità su F ha ruolo di φ_0, esiste un isomorfismo $\varphi : F(\alpha_1) \to F(\alpha_i)$, che è l'identità su F ed associa α_1 ad α_i. Dato che l'estensione $F \subseteq M$ è di Galois, M è il campo di spezzamento di un polinomio separabile $f \in F[x]$. Si osservi che $\varphi(f) = f$, perché φ è l'identità su F. Allora si può applicare la proposizione 1.6 all'isomorfismo φ tra i campi $F(\alpha_1)$ e $F(\alpha_i)$ rispetto al polinomio f con campo di spezzamento M su entrambe le estensioni. Perciò si è mostrato che esiste un automorfismo di $\mathrm{Gal}(M/F)$ che manda α_1 in α_i. Per l'arbitrarietà di i, si può trovare un

automorfismo che manda α_1 in una qualsiasi altra radice α_i. Perciò $F(\alpha_i)$ è campo coniugato di $F(\alpha_1) = L$. Allora per l'osservazione 15:

$$K = F(\alpha_1 \dots \alpha_r) = F(\alpha_1) \dots F(\alpha_r)$$

è il composto dei campi coniugati di L in M. □

Lemma 2.9. *Siano $F \subseteq K_1 \subseteq L$ e $F \subseteq K_2 \subseteq L$ estensioni di campi.*

(i) *Se $F \subseteq K_1$ è radicale, allora $K_2 \subseteq K_1K_2$ è radicale.*

(ii) *Se $F \subseteq K_1$ e $F \subseteq K_2$ sono radicali, allora $F \subseteq K_1K_2$ è ancora radicale.*

Dimostrazione.

(i) Dato che $F \subseteq K_1$ è un'estensione radicale, c'è una catena di campi $F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K_1$ dove $F_i = F_{i-1}(\gamma_i)$ con $\gamma_i^{m_i} \in F_{i-1}$ per ogni $i = 1, \dots, n$. Definendo $F_0' = K_2$ e $F_i' = F_{i-1}'(\gamma_i)$ per ogni $i = 1, \dots, n$, si vuole mostrare che $F_i \subseteq F_i'$. Infatti per $i = 0$ si ha $F_0 = F \subseteq K_2 = F_0'$, per ipotesi. Si può allora supporre per ipotesi induttiva che $F_{i-1} \subseteq F_{i-1}'$, ma segue che $F_i = F_{i-1}(\gamma_i) \subset F_{i-1}'(\gamma_i) = F_i'$. Si ha allora che $\gamma_i^{m_i} \in F_{i-1} \subseteq F_{i-1}'$, perciò $K_2 = F_0' \subseteq \dots \subseteq F_n'$ è estensione radicale. Resta da mostrare che F_n' è il composto K_1K_2. Ma $K_1 = F_n = F(\gamma_1, \dots, \gamma_n)$ e $F_n' = K_2(\gamma_1, \dots, \gamma_n)$, quindi F_n' contiene sia K_1 che K_2 ed è il più piccolo campo che li contiene entrambi.

(ii) Si ha che $K_2 \subseteq K_1K_2$ è un'estensione radicale, ma anche $F \subseteq K_2$ è radicale, perciò per l'osservazione 12 si ha che $F \subseteq K_1K_2$ è un'estensione radicale.

□

Teorema 2.10. *Se $F \subseteq L$ è un'estensione separabile e radicale, allora la sua chiusura di Galois è radicale.*

Dimostrazione. Per la proposizione 1.18, esiste un'estensione $L \subseteq M$ tale che $F \subseteq M$ è di Galois. Preso $\sigma \in \mathrm{Gal}(M/F)$ si hanno le estensioni$F \subseteq \sigma L \subseteq M$. Si vuole ora mostrare che l'estensione $F \subseteq \sigma L$ è radicale. Dato che per ipotesi l'estensione $F \subseteq L$ è radicale, si ha che $L = F(\gamma_1, \dots, \gamma_n)$, dove $\gamma_1^{m_1} \in F$ e $\gamma_i^{m_i} \in F(\gamma_1, ..., \gamma_{i-1})$ con $m_i \in \mathbb{N}$; σ per definizione lascia fisso F e posto $\beta_i = \sigma(\gamma_i)$ per ogni $i = 1, \dots, n$, si ha allora che $\sigma L = F(\beta_1, \dots, \beta_n)$, dove $\beta^{m_i} = \sigma^{m_i}(\gamma_i) = \sigma(\gamma_i^{m_i}) \in F(\beta_1, \dots, \beta_{i-1})$, perché $\gamma_i^{m_i} \in F(\gamma_1, \dots, \gamma_{i-1})$ per ogni $i = 1, \dots, n$. Ovvero l'estensione $F \subseteq L$ è radicale. Questo ragionamento vale per qualsiasi $\sigma \in \mathrm{Gal}(M/F)$, perciò si ha che il loro composto è radicale per la parte (ii) del lemma precedente. Inoltre per la proposizione 2.8 il composto di tutti i σL è una chiusura di Galois di $F \subseteq L$. □

Corollario 2.10.1. *Sia F un campo con* $\operatorname{char} F = 0$. *Se $F \subseteq L$ è un estensione risolubile, allora la sua chiusura di Galois è risolubile.*

Dimostrazione. Sia $F \subseteq L$ un'estensione risolubile, allora esiste $F \subseteq L \subseteq L'$ tale che $F \subseteq L'$ è radicale. Inoltre $F \subseteq L'$ è separabile (perché la caratteristica dei campi è 0) e quindi ha chiusura di Galois $F \subseteq L' \subseteq M$ e per il teorema precedente risulta che $F \subseteq M$ è radicale. Si considerino ora le estensioni $F \subseteq L \subseteq M$. Dato che $F \subseteq M$ è di Galois, per la proposizione 2.8 contiene la chiusura di Galois di $F \subseteq L$. Ovvero la chiusura di Galois sta in un'estensione radicale $F \subseteq M$ e per definizione è risolubile. □

2.3 Teorema di Galois

Verranno considerati da qui in poi solo campi ed estensioni di campi con caratteristica 0. Dato che si sta trattando di estensioni radicali e quindi di radici si deve introdurre il concetto di radici primitive m-esime dell'unità in un campo con caratteristica 0 qualsiasi, per rendere il risultato finale il più generale possibile.

Sia $m \in \mathbb{N}$ e sia L un campo con caratteristica 0. Si consideri il campo di spezzamento del polinomio $f(x) = x^m - 1 \in L[x]$. Questo polinomio è separabile per la proposizione 1.8, infatti $f'(x) = mx^{m-1}$ e quindi $MCD(f, f') = 1$. Per definizione di polinomio separabile, f ha m radici distinte nel suo campo di spezzamento. L'insieme G delle m radici è un gruppo:

- $1 \in G$, perché 1 è radice di f;
- Date due radici ξ, η di f, allora $\xi\eta$ è ancora radice di f:
  $(\xi\eta)^m - 1 = \xi^m\eta^m - 1 = 1 \cdot 1 - 1 = 0$
- Data $\xi \in G$, allora anche $\xi^{-1} \in G$, ovvero è ancora radice:
  per definizione $\xi^m = 1$, allora $(\xi^{-1})^m = (\xi^m)^{-1} = 1$ quindi $\xi^{-1} \in G$.

Così G è un gruppo, ovviamente è un gruppo finito perché contiene esattamente m elementi. Infine per la proposizione A.2 dimostrata nell'appendice, si ha che G è un gruppo ciclico. Sia ora ξ un generatore di G, allora esso ha le seguenti proprietà:

- Le m radici distinte di f sono 1, $\xi, \xi^2, ..., \xi^{m-1}$;
- Il campo di spezzamento di f è $L(\xi, \xi^2, ..., \xi^{m-1}) = L(\xi)$.

Definizione 2.7. Si definisce *radice primitiva m-esima dell'unità* un generatore ξ del gruppo ciclico G visto sopra.

Proposizione 2.11. *Sia ξ una radice primitiva m-esima dell'unità, allora $L \subseteq L(\xi)$ è estensione di Galois e* $\mathrm{Gal}(L(\xi)/L)$ *è abeliano.*

Dimostrazione. Per quanto appena visto $L(\xi)$ è un campo di spezzamento di un polinomio a coefficienti in L e inoltre l'estensione $L \subseteq L(\xi)$ è separabile, allora per definizione è una estensione di Galois. Si deve ora mostrare che il gruppo di Galois è abeliano. Siano $\sigma, \tau \in \mathrm{Gal}(L(\xi)/L)$. Si ha che σ,τ sono determinati dal valore che assumono su ξ che può essere solamente una radice del polinomio $x^m - 1$, ovvero $1, \xi, \ldots, \xi^{m-1}$. Si può allora suppore che $\sigma(\xi) = \xi^i$ e $\tau(\xi) = \xi^j$ per $i, j < m$. Si ha allora che

$$(\sigma\tau)(\xi) = \sigma(\xi^j) = (\xi^j)^i = \xi^{ij} = (\xi^i)^j = \tau(\xi^i) = (\tau\sigma)(\xi) \ .$$

Perciò $\mathrm{Gal}(L(\xi)/L)$ è abeliano. □

Data $F \subseteq L$ estensione di Galois si ha allora il seguente diagramma di estensioni:

$$\begin{array}{ccc} F(\xi) & \longrightarrow & L(\xi) \\ \uparrow & & \uparrow \\ F & \longrightarrow & L \end{array}$$

Si vuole ora mostrare che sono tutte estensioni di Galois.

Lemma 2.12. *Sia $F \subseteq L$ un estensione di Galois e sia ξ una radice primitiva m-esima dell'unità . Allora le estensioni $F \subseteq L(\xi)$ e $F(\xi) \subseteq L(\xi)$ sono di Galois. Inoltre:*

$$\begin{aligned} \mathrm{Gal}(L/F) \text{ è } \textit{risolubile} &\iff \mathrm{Gal}(L(\xi)/F) \text{ è } \textit{risolubile} \\ &\iff \mathrm{Gal}(L(\xi)/F(\xi)) \text{ è } \textit{risolubile} \ . \end{aligned}$$

Dimostrazione. Si considerino le estensioni $F \subseteq L \subseteq L(\xi)$, si ha che $F \subseteq L$ è di Galois, ma anche $L \subseteq L(\xi)$ è di Galois per la proposizione precedente. In particolare $L(\xi)$ è campo di spezzamento del polinomio $(x^m - 1) \in L[x]$, che appartiene anche a $F[x]$; mentre L è il campo di spezzamento di un polinomio $g \in F[x]$. Allora $L(\xi)$ è il campo di spezzamento del polinomio $(x^m - 1)g(x) \in F[x]$, perché contiene tutte le radici di g dal momento che è estensione di L e contiene tutte le radici m-esime dell'unità. Allora l'estensione $F \subseteq L(\xi)$ è normale, quindi di Galois. Si considerino poi le estensioni $F \subseteq F(\xi) \subseteq L(\xi)$, si ha allora che $F \subseteq L(\xi)$ è di Galois per quanto appena visto, allora anche $F(\xi) \subseteq L(\xi)$ è di Galois, perché $F(\xi)$ è un campo intermedio. Dal momento che le estensioni $F \subseteq L \subseteq L(\xi)$ sono di Galois per il teorema 1.16 si ha che $\mathrm{Gal}(L(\xi)/L)$ è un sottogruppo normale di $\mathrm{Gal}(L(\xi)/F)$ tale che

$$\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(L(\xi)/F)/\,\mathrm{Gal}(L(\xi)/L)$$

ma $\mathrm{Gal}(L(\xi)/L)$ è abeliano per la proposizione precedente e quindi è risolubile. Allora per il teorema 2.2 si ha che:

$$\mathrm{Gal}(L/F) \text{ è risolubile} \iff \mathrm{Gal}(L(\xi)/F) \text{ è risolubile} .$$

Si considerino ora le estensioni di Galois $F \subseteq F(\xi) \subseteq L(\xi)$. Con un ragionamento analogo a quello appena visto si ha che

$$\mathrm{Gal}(F(\xi)/F) \simeq \mathrm{Gal}(L(\xi)/F)/\,\mathrm{Gal}(L(\xi)/F(\xi) .$$

Ma $\mathrm{Gal}(F(\xi)/F)$ è abeliano e quindi risolubile per la proposizione precedente. Allora per il teorema 2.2 si ha che:

$$\mathrm{Gal}(L(\xi)/F) \text{ è risolubile} \iff \mathrm{Gal}(L(\xi)/F(\xi)) \text{ è risolubile} .$$

□

Lo strumento fondamentale utilizzato nel seguente lemma è quello delle risolventi di Lagrange.

Lemma 2.13. *Sia $K \subseteq M$ un'estensione di Galois tale che $\mathrm{Gal}(M/K)$ è un gruppo ciclico di ordine p, dove p è primo. Se K contiene una radice p-esima dell'unità ξ allora esiste $\alpha \in M$ tale che $M = K(\alpha)$ e $\alpha^p \in K$.*

Dimostrazione. Per ipotesi, il gruppo di Galois $\mathrm{Gal}(M/K)$ è un gruppo ciclico di ordine p. Sia σ un generatore di tale gruppo. Fissato $\beta \in M \setminus K$, si consideri per ogni $i = 0, \ldots, p-1$ la risolvente di Lagrange, definita da:

$$\alpha_i = \beta + \xi^{-i}\sigma(\beta) + \xi^{-2i}\sigma^2(\beta) + \ldots + \xi^{-i(p-1)}\sigma^{(p-1)}(\beta) . \tag{2.1}$$

Si ha allora che:

$$\xi^{-i}\sigma(\alpha_i) = \xi^{-i}\sigma(\beta) + \xi^{-2i}\sigma^2(\beta) + \ldots + \xi^{-i(p-1)}\sigma^{(p-1)}(\beta) + \xi^{-ip}\sigma^i(\beta) .$$

Ma $\xi^{-ip} = 1$, perché ξ è radice p-esima dell'unità, e $\sigma^i(\beta) = \beta$ perché σ è generatore di un gruppo ciclico di ordine p. Allora l'espressione sopra diventa:

$$\xi^{-i}\sigma(\alpha_i) = \xi^{-i}\sigma(\beta) + \xi^{-2i}\sigma^2(\beta) + \ldots + \xi^{-i(p-1)}\sigma^{(p-1)}(\beta) + \beta = \alpha_i$$

$$\xi^{-i}\sigma(\alpha_i) = \alpha_i .$$

Si ha ovvero che :

$$\sigma(\alpha_i) = \xi^i \alpha_i .$$

Dato che $\xi^{ip} = 1$, elevando tutto alla p si ottiene:

$$\sigma(\alpha_i^p) = \alpha_i^p$$

ovvero σ fissa α_i^p. Ma σ genera $\mathrm{Gal}(M/K)$, quindi α_i^p è fissato da $\mathrm{Gal}(M/K)$, allora appartiene a K. Si ha allora che $\alpha_i^p \in K$ per ogni $i = 0, \ldots, p-1$. Inoltre per $i = 0$ si ottiene che: $\sigma(\alpha_0) = \xi^0 \alpha_0 = \alpha_0$, ovvero $\alpha_0 \in K$.
Si supponga ora che esista $j \in \{1, \ldots, p-1\}$ tale che $\alpha_j \neq 0$, così risulta che $\xi^j \neq 1$ e $\xi^j \alpha_j \neq \alpha_j$. Si ha allora che $\sigma(\alpha_j) = \xi^j \alpha_j \neq \alpha_j$, ovvero $\alpha_j \notin K$ e quindi $M = K(\alpha_j)$, perché l'ordine dell'estensione è $[M : K] = p$. Posto $\alpha = \alpha_j$ si ottiene la tesi dal momento che $\alpha_j^p \in K$.
Si vuole ora mostrare che il caso in cui $\alpha_i = 0$ per ogni $i \in \{1, \ldots, p-i\}$ porta ad una contraddizione. Si scriva:

$$\alpha_0 = \alpha_0 + \alpha_1 + \ldots + \alpha_{p-1} \, .$$

Questo risulta vero perché $\alpha_i = 0$ per ogni $i \in \{1, \ldots, p-i\}$. Si applichi ora l'equazione 3.1 per ottenere:

$$\begin{aligned}
\alpha_0 = \quad & \big(\beta + \sigma(\beta) + \ldots + \sigma^{p-1}(\beta)\big) \\
& + \big(\beta + \xi^{-1}\sigma(\beta) + \xi^{-2}\sigma^2(\beta) + \ldots + \xi^{-(p-1)}\sigma^{p-1}(\beta)\big) + \ldots \\
& + \big(\beta + \xi^{-(p-1)}\sigma(\beta) + \xi^{-2(p-1)}\sigma^2(\beta) + \ldots + \xi^{-(p-1)(p-1)}\sigma^{p-1}(\beta)\big) \\
= \quad & p\beta + \big(1 + \xi^{-1} + \xi^{-2} + \ldots + \xi^{-(p-1)}\big)\sigma(\beta) \\
& + \big(1 + \xi^{-2} + \xi^{-4} + \ldots + \xi^{-2(p-1)}\big)\sigma^2(\beta) + \ldots \\
& + \big(1 + \xi^{-(p-1)} + \xi^{-2(p-1)} + \ldots + \xi^{-(p-1)(p-1)}\big)\sigma^{p-1}(\beta) \, .
\end{aligned}$$

Si vuole ora mostrare che $\gamma_i = 1 + \xi^{-i} + \ldots + \xi^{-i(p-1)} = 0$, per ogni $i \in \{1, \ldots, p-1\}$. Dal momento che ξ è radice p-esima dell'unità, si può scrivere $1 = (\xi^p)^{-i}$, perciò risulta che

$$\begin{aligned}
\gamma_i &= 1 + \xi^{-i} + \ldots + \xi^{-i(p-1)} \\
&= (\xi^p)^{-i} + \xi^{-i} + \ldots + \xi^{-i(p-1)} \\
&= \xi^{-i} + \xi^{-2i} \ldots + \xi^{-i(p-1)} + \xi^{-ip} \\
&= \xi^{-i}(1 + \xi^{-i} + \ldots + \xi^{-i(p-1)}) \\
&= \xi^{-i}\gamma_i \, .
\end{aligned}$$

Risulta allora che $0 = \gamma_i - \xi^{-i}\gamma_i = \gamma_i(1 - \xi^{-i})$. Ma in un campo vale la legge dell'annullamento del prodotto, allora uno dei due fattori deve essere nullo. Ma ξ è radice p-esima dell'unità, quindi $1 - \xi^{-i} \neq 0$ per ogni $i \neq p$. Si ha allora che necessariamente $\gamma_i = 0$ per ogni $i \in \{1, \ldots, p-1\}$. Si ha allora che $\alpha_0 = p\beta$, quindi $\beta = \alpha_0/p$ e risulta così che $\beta \in K$, perché $\alpha_0 \in K$, ma per ipotesi $\beta \in M \setminus K$, allora si ha una contraddizione, perciò esiste almeno un $j \in \{1, \ldots, p-1\}$ tale che $\alpha_j \neq 0$. □

Teorema 2.14 (di Galois)**.**
Sia F un campo di caratteristica zero. Sia $F \subseteq L$ un estensione di Galois. Allora sono equivalenti:

1. *$F \subseteq L$ è risolubile;*
2. *$\mathrm{Gal}(L/F)$ è un gruppo risolubile.*

Dimostrazione. La dimostrazione di questo teorema è molto articolata, perciò verrà spezzata in vari passaggi.

$1 \Rightarrow 2$ Questa implicazione è articolata in tre passi:

A. *Riduzione al caso Radicale*:
Per ipotesi $F \subseteq L$ è un'estensione risolubile, allora per definizione esiste un campo $L' \supseteq L$ tale che $F \subseteq L'$ è estensione radicale. Per il teorema 2.10, la chiusura di Galois $F \subseteq M$ di $F \subseteq L'$ è radicale, allora si possono considerare le estensioni $F \subseteq L \subseteq M$, dove $F \subseteq M$ è di Galois e radicale. Dato che $F \subseteq L$ è di Galois per ipotesi, se $\mathrm{Gal}(M/F)$ fosse risolubile si avrebbe che

$$\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(M/F)/\,\mathrm{Gal}(M/L)$$

e per il teorema 2.2 risulterebbe che anche $\mathrm{Gal}(L/F)$ è risolubile. Allora è sufficiente mostrare che $\mathrm{Gal}(L/F)$ è risolubile se $F \subseteq L$ è una estensione di Galois radicale.

B. *Aggiunta di Radici dell'unità*:
Sia $F \subseteq L$ un'estensione di Galois radicale. Se si aggiunge una radice primitiva m-esima dell'unità ξ sia ad F che ad L, per il lemma 2.9 parte (i) si ha che $F(\xi) \subseteq L(\xi)$ è ancora radicale, ma anche di Galois per il lemma 2.12. Sempre per il lemma 2.12 basta mostrare che $\mathrm{Gal}(L(\xi)/F(\xi)$ è risolubile, perché così risulta risolubile anche $\mathrm{Gal}(L/F)$. Si può allora assumere che F contenga tutte le radici primitive m-esime necessarie, per m opportuno.

C. *Verifica della Risolubilità*:
Dal momento che $F \subseteq L$ è radicale, c'è una catena di campi $F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = L$, dove $F_i = F_{i-1}(\gamma_i)$, $\gamma_i^{m_i} \in F_{i-1}$, per degli interi $m_i > 0$. Si vuole mostrare che $F_i \subseteq F_{i-1}$ è estensione di Galois con gruppo di Galois ciclico. Sia ξ_i una radice primitiva m_i-esima dell'unità, si osservi allora che $1, \xi_i, \ldots, \xi_i^{m_i-1}$ sono tutte le radici m_i-esime dell'unità e sono tutte distinte. Allora gli elementi $\gamma_i, \gamma_i\xi, \ldots, \gamma_i\xi^{m_i-1}$ sono radici distinte del polinomio $x^{m_i} - \gamma_i^{m_i} \in$

$F_{i-1}[x]$. Per il punto B di questa dimostrazione, si può assumere che $\xi_i \in F \subseteq F_{i-1}$, si ha allora che:

$$F_{i-1}(\gamma_i, \gamma_i\xi_i, \ldots, \gamma_i\xi_i^{m_i-1}) = F_{i-1}(\gamma_i) = F_i \ .$$

Allora $F_{i-1} \subseteq F_i$ è di Galois perché F_i è campo di spezzamento di un polinomio separabile a coefficienti in F_{i-1}.
Si deve ora mostrare che il gruppo di Galois è ciclico. Sia $\sigma \in \mathrm{Gal}(F_i/F_{i-1}) = \mathrm{Gal}(F_{i-1}(\gamma_i)/F_{i-1})$. L'automorfismo σ è determinato dal valore che assume su γ_i, perché F_{i-1} è campo fisso, ma deve anche risultare che $\sigma(\gamma_i)$ è radice del polinomio $x^{m_i} - \gamma_i^{m_i} \in F_{i-1}[x]$, le cui radici sono gli elementi $\gamma_i, \gamma_i\xi_i, \ldots, \gamma_i\xi_i^{m_i-1}$, che quindi possono essere immagine mediante σ di γ_i ovvero $\sigma(\gamma_i) = \xi_i^k\gamma_i$ per $k \in \{0, \ldots, m_i - 1\}$. Si consideri ora l'applicazione

$$\begin{aligned} \varphi : \mathrm{Gal}(F_i/F_{i-1}) &\longrightarrow \mathbb{Z}/m_i\mathbb{Z} \\ \sigma &\longmapsto k \end{aligned}$$

Questo è un isomorfismo di gruppi. Infatti è un omomorfismo perché presi $\sigma \mapsto k$ e $\tau \mapsto h$ si ha che

$$(\sigma\tau)(\gamma_i) = \sigma(\tau(\gamma_i)) = \sigma(\gamma_i\xi_i^h) = \gamma_i\xi_i^h\xi_i^k = \gamma_i\xi_i^{k+h} \ .$$

ovvero $\sigma\tau \mapsto k+h$. Inoltre è iniettivo perché presi $\sigma \mapsto k$ e $\tau \mapsto k$ si ha che

$$\sigma(\gamma_i) = \gamma_i\xi_i^k = \tau(\gamma_i) \ .$$

Quindi σ e τ assumono lo stesso valore su γ_i, allora poichè un automorfismo è determinato dal valore che assume sulle radici, si ha che $\sigma = \tau$. Infine è un omomorfismo suriettivo: preso $k \in \mathbb{Z}/m_i\mathbb{Z}$, utilizzando la proposizione 1.5 si può costruire un automorfismo $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$ tale che $\sigma(\gamma_i) = \xi_i^k\gamma_i$, così che $\sigma(F_{i-1}) = F_{i-1}$ e $\sigma \mapsto k$. Si è allora mostrato che $\mathrm{Gal}(F_i/F_{i-1})$ è ciclico, perché isomorfo ad un gruppo ciclico. Si può allora supporre che $\mathrm{Gal}(F_i/F_{i-1}) = \langle\sigma\rangle$, dove $\sigma(\gamma_i) = \xi_i\gamma_i$.
Si considerino ora i sottogruppi $G_i = \mathrm{Gal}(L/F_i) \subseteq \mathrm{Gal}(L/F)$. Poichè $F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = L$ e l'estensione $F_{i-1} \subseteq F_i$ è di Galois per ogni $i = 1, \ldots, n$, si ha la seguente catena di sottogruppi:

$$\{id_L\} = \mathrm{Gal}(L/F_n) = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_1 \subseteq G_0 = \mathrm{Gal}(L/F) \ .$$

Ma dal momento che $F \subseteq L$ è di Galois e F_{i-1} è un campo intermedio, anche $F_{i-1} \subseteq L$ è estensione di Galois. Allora per il

teorema 1.16 si ha che $G_i \trianglelefteq G_{i-1}$ con

$$G_{i-1}/G_i = \mathrm{Gal}(L/F_{i-1})/\mathrm{Gal}(L(F_i)) \simeq \mathrm{Gal}(F_i/F_{i-1})$$

che è ciclico e quindi abeliano. Allora la serie

$$\{id_L\} = \mathrm{Gal}(L/F_n) = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_1 \subseteq G_0 = \mathrm{Gal}(L/F)$$

è subnormale abeliana, quindi $G_0 = \mathrm{Gal}(L/F)$ è risolubile.

$2 \Rightarrow 1$ Il vicerversa è diviso in due passaggi:

A. *Un Caso Particolare*:
Sia $F \subseteq L$ un'estensione di Galois con gruppo di Galois risolubile. Si consideri la seguente condizione:

($*$) F ha una radice primitiva p-esima dell'unità per ogni p primo tale che $p \big| |\mathrm{Gal}(L/F)|$.

Si vuole ora mostrare che se F soddisfa la condizione ($*$), allora l'estensione $F \subseteq L$ è radicale. Per ipotesi $\mathrm{Gal}(L/F)$ è un gruppo risolubile, allora esiste una catena subnormale ciclica con quozienti di ordine primo:

$$\{1_L\} = G_n \subseteq \ldots, \subseteq G_0 = \mathrm{Gal}(L/F)\ .$$

Si considerino ora i campi fissi $F_i = L^{G_i} \subseteq L$, mediante la corrispondenza di Galois si ha che

$$F = L^{\mathrm{Gal}(L/F)} = L^{G_0} \subseteq G_1 \subseteq \ldots \subseteq F_n = L\ .$$

Inoltre dal momento che $G_i \trianglelefteq G_{i-1}$, per il teorema 1.16 si ha che l'estensione $F_{i-1} \subseteq F_i$ è una estensione di Galois e

$$G_{i-1}/G_i \simeq \mathrm{Gal}(F_i/F_{i-1})\ .$$

Dato che $[G_{i-1} : G_i]$ è primo, allora $G_{i-1}/G_i \simeq \mathbb{Z}/p\mathbb{Z}$, con p primo. Si vuole ora mostrare che $p = |\mathrm{Gal}(F_i/F_{i-1})| \big| |\mathrm{Gal}(L/F)|$, ovvero per il teorema 1.12 che $p = [F_i : F_{i-1}] \big| [L : F]$. Si considerino le estensioni $F \subseteq F_{i-1} \subseteq F_i \subseteq L$, per il lemma della torre si ha che:

$$[L : F_{i-1}] = [L : F_i][F_i : F_{i-1}]$$

perciò

$$[L : F] = [L : F_{i-1}][F_{i-1} : F] = [L : F_i][F_i : F_{i-1}][F_{i-1} : F]\ .$$

Ma $[F_i : F_{i-1}] = p$, perciò $p \big| [F : L]$. Per l'ipotesi $(*)$, F e quindi anche F_{i-1} contiene una radice primitiva p-esima dell'unità, allora l'estensione $F_{i-1} \subseteq F_i$ soddisfa le condizioni del lemma 2.13, così si ottiene che $F_i = F_{i-1}(\gamma_i)$, dove $\gamma_i^p \in F_{i-1}$ per ogni i. Si è così mostrato che l'estensione $F \subseteq L$ è radicale.

B. *Il Caso Generale*:
Si consideri ora il caso generale in cui $F \subseteq L$ è un'estensione di Galois con gruppo di Galois risolubile. Sia ξ radice primitiva m-esima dell'unità, dove $m = |\operatorname{Gal}(L/F)| = [L : F]$. Per il lemma 2.12 si ha che $\operatorname{Gal}(L(\xi)/F(\xi))$ è risolubile e per il teorema 1.16 si ha anche l'isomorfismo seguente:

$$\operatorname{Gal}(L/F) \simeq \operatorname{Gal}(L(\xi)/F)/\operatorname{Gal}(L(\xi)/L) \ .$$

Dal momento che $\operatorname{Gal}(L(\xi)/F(\xi))$ è un sottogruppo di $\operatorname{Gal}(L(\xi)/F)$, si ha l'omomorfismo

$$\varphi : \operatorname{Gal}(L(\xi)/F(\xi)) \to \operatorname{Gal}(L/F)$$

ottenuto restringendo ad L tutti gli automorfismi di $L(\xi)$. Inoltre risulta che $\ker\varphi = \{id\}$, perché gli elementi di $\ker\varphi$ devono essere l'identità sia su L che su $F(\xi)$. Allora φ è iniettiva e per il teorema di Lagrange si ha che m è multiplo di $|\operatorname{Gal}(L(\xi)/F(\xi))|$. Sia p un primo tale che $p \big| |\operatorname{Gal}(L(\xi)/F(\xi))|$; allora $p|m$. Dato che ξ è radice primitiva m-esima dell'unità, $\xi^{m/p}$ è radice primitiva p-esima dell'unità e $\xi^{m/p} \in F(\xi)$. Allora l'estensione $F(\xi) \subseteq L(\xi)$ soddisfa la condizione $(*)$ del caso particolare, quindi è una estensione radicale. Ma anche $F \subseteq F(\xi)$ è banalmente radicale, allora anche $F \subseteq L(\xi)$ è un'estensione radicale per l'osservazione 12. Si è allora mostrato che $F \subseteq L$ è risolubile, perché $F \subseteq L(\xi)$ è radicale e $L(\xi)$ è estensione di L.

□

Corollario 2.14.1. *Sia $F \subseteq L$ un'estensione di Galois risolubile e sia ξ una radice primitiva m-esima dell'unità, dove $m = [L : F]$. Allora $F \subseteq L(\xi)$ è una estensione radicale.*

Dimostrazione. É una conseguenza dell'implicazione $2 \Rightarrow 1$ del teorema precedente. □

2.4 Polinomi risolubili per radicali

Applichiamo quanto visto fino ad ora al caso concreto dei polinomi.

Definizione 2.8. Sia $f \in F[x]$, $f \notin F$, con campo di spezzamento L.

- Una radice $\alpha \in L$ di f si dice *esprimibile mediante radicali su* F se α appartiene ad una estensione radicale di F.
- Il polinomio f è detto *risolubile per radicali su* F se $F \subseteq L$ è una estensione risolubile.

Osservazione 16. La definizione precedente è ben posta, ovvero non dipende dal campo di spezzamento L, perché questo è unico a meno di isomorfismi.

Osservazione 17. Se f è risolubile per radicali su F allora tutte le sue radici sono esprimibili mediante radicali.

Definizione 2.9. Sia $f \in F[x]$, $f \notin F$, con campo di spezzamento L. Si pone allora $\mathrm{Gal}(f, F) = \mathrm{Gal}(L/F)$.

Proposizione 2.15. *Sia F un campo con caratteristica zero e sia $f \in F[x]$ un polinomio irriducibile. Allora f è risolubile per radicali se e solo se f ha una radice esprimibile per radicali.*

Dimostrazione. Sia f irriducibile e risolubile per radicali, allora banalmente f ha una radice esprimibile per radicali. Viceversa, sia f un polinomio irriducibile con una radice α in qualche estensione radicale di F. Questo significa che l'estensione $F \subseteq F(\alpha)$ è risolubile. Allora per il corollario 2.10.1 la sua chiusura di Galois M è risolubile, ove $F \subseteq F(\alpha) \subseteq M$ e $F \subseteq M$ è una estensione di Galois per definizione. In particolare l'estensione $F \subseteq M$ è normale e $\alpha \in M$ è una radice di f. Segue allora che f si spezza linearmente in M, perciò M contiene il campo di spezzamento di f; allora f è risolubile per radicali, perché l'estensione $F \subseteq M$ è risolubile. □

Teorema 2.16. *Un polinomio $f \in F[x]$ è risolubile per radicali su F se e solo se il suo gruppo di Galois* $\mathrm{Gal}(f, F)$ *è un gruppo risolubile.*

Dimostrazione. Segue direttamente dal teorema di Galois (teorema 2.14). □

Proposizione 2.17. *Sia $f \in F[x]$, $deg f \leq 4$. Allora f è risolubile per radicali.*

Dimostrazione. Il gruppo di Galois di un polinomio di grado n è isomorfo a un sottogruppo di S_n, che è risolubile per $n \leq 4$ per la proposizione 2.3. □

Capitolo 3

Applicazioni

In questo capitolo verrà studiata la risolubilità del polinomio universale. Verranno inoltre discussi diversi esempi, tra cui un esempio di estensione risolubile ma non radicale. Infine verrà presentato un esempio di non risolubilità in caratteristica p.

3.1 Il Polinomio Universale

Definizione 3.1. Sia F un campo e $n \in \mathbb{N}$ un intero positivo. Date $t_1, \ldots, t_n$ n indeterminate, si definisce *polinomio universale di grado n* il seguente polinomio in $F(t_1, \ldots, t_n)[x]$:

$$\tilde{f} = x^n - t_1 x^{n-1} + \ldots + (-1)^{n-1} t_{n-1} x + (-1)^n t_n$$

Allora l'equazione $\tilde{f} = 0$ è detta *equazione generale di grado n*.

Per la dimostrazione della seguente proposizione di veda [1] teorema 6.4.1.

Proposizione 3.1. *Posto $K = F(t_1, \ldots, t_n)$, se $x_1, \ldots, x_n$ sono le radici di $\tilde{f}$, il suo campo di spezzamento è*

$$L = F(x_1, \ldots, x_n)$$

e il gruppo di Galois $\mathrm{Gal}(L/K)$ *è isomorfo a S_n.*

Nel caso in cui $n = 2$ il polinomio universale è detto *polinomio quadratico generale*. Verrà ora studiato questo caso.

Definizione 3.2. Sia F un campo con caratteristica 0. Se t_1, t_2 sono due indeterminate, allora l'equazione

$$x^2 - t_1 x + t_2 = 0$$

sul campo $F(t_1, t_2)$ è detta *equazione quadratica generale su F*.

Osservazione 18. Si osservi che ogni equazione quadratica (monica) su F può essere ottenuta dall'equazione quadratica generale sostituendo a t_1, t_2 degli opportuni elementi di F.

Proposizione 3.2. *Sia Δ un elemento tale che $\Delta^2 = t_1^2 - 4t_2$. Allora le soluzioni dell'equazione quadratica generale sono*

$$x_{1,2} = \frac{t_1 \pm \Delta}{2}$$

e appartengono all'estensione radicale $F(t_1, t_2)(\Delta)$.

Dimostrazione. Per mostrare che $x_{1,2}$ sono soluzioni, è sufficiente sostituirle all'indeterminata x nell'equazione generale. Sia $x_1 = \frac{t_1+\Delta}{2}$, allora:

$$\begin{aligned} x_1^2 - t_1 x_1 + t_2 &= \left(\frac{t_1+\Delta}{2}\right)^2 - t_1\left(\frac{t_1+\Delta}{2}\right) + t_2 \\ &= \frac{1}{4}\big(t_1^2 + 2t_1\Delta + \Delta^2\big) - \frac{1}{2}\big(t_1^2 + t_1\Delta\big) + t_2 \\ &= \frac{1}{4}\big(t_1^2 + 2t_1\Delta + (t_1^2 - 4t_2)\big) - \frac{1}{2}\big(t_1^2 + t_1\Delta\big) + t_2 \\ &= \frac{1}{2}t_1^2 + \frac{1}{2}(t_1\Delta) - t_2 - \frac{1}{2}t_1^2 - \frac{1}{2}(t_1\Delta) + t_2 = 0\ . \end{aligned}$$

Perciò x_1 è radice dell'equazione quadratica generale. Per il secondo valore x_2 il ragionamento è analogo. Allora $x_{1,2}$ sono radici dell'equazione quadratica generale. Inoltre per come sono state definite nella proposizione risulta evidente che appartengono all'estensione $F(t_1, t_2)(\Delta)$. □

Definizione 3.3. L'equazione

$$x_{1,2} = \frac{t_1 \pm \Delta}{2}$$

è detta *formula quadratica*.

Quindi per il grado $n = 2$, esiste una formula risolutiva. Si analizzeranno ora gli altri casi.

Proposizione 3.3. *Sia $n \leq 4$. Il polinomio universale di grado n è risolubile per radicali.*

Dimostrazione. Poichè il gruppo di Galois del polinomio universale è isomorfo ad S_n, si ha che per $n \leq 4$ il gruppo S_n è risolubile per la proposizione 2.3. □

Osservazione 19. Si osservi che per $n \leq 4$, un polinomio di grado n è sempre risolubile per la proposizione 2.17. Questo implica l'esistenza di formule risolutive. Infatti per il grado $n = 3$ esistono le cosiddete formule di Cardano e per il grado $n = 4$ esistono le formule di Ferrari.

Teorema 3.4. *Se $n \geq 5$, allora il polinomio universale $\tilde{f} \in K[x]$ di grado n non è risolubile per radicali su K, e nessuna radice di $\tilde{f}$ è esprimibile mediante radicali su K.*

Dimostrazione. Per l'osservazione precedente, si ha che il gruppo di Galois $\mathrm{Gal}(\tilde{f}, K)$ è isomorfo a S_n e S_n per $n \geq 5$ non è risolubile per il teorema 2.4. La seconda parte segue dalla proposizione 2.15. □

Osservazione 20. Questo teorema non esclude però la possibilità che alcuni polinomi di grado $n \geq 5$ siano risolubili. Non esiste però una formula risolutiva, quindi lo studio del polinomio è di volta in volta differente.

3.2 Esempi

In questa sezione verranno riportati diversi esempi. Verranno studiati i gruppi di Galois di alcuni polinomi ed infine verrà presentato un esempio di estensione risolubile non radicale. Prima di ciò, è necessario però ricordare due criteri di irriducibilità di polinomi molto importanti.

Proposizione 3.5 (Criterio di Eisenstein)**.** *Sia $f(x) = a_m x^m + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. Se esiste un primo p tale che:*

$$\text{(i) } p \nmid a_m; \quad \text{(ii) } p | a_{m-1}, \ldots, a_0; \quad \text{(iii) } p^2 \nmid a_0;$$

allora f è irriducibile in $\mathbb{Z}[x]$

Lemma 3.6 (Lemma di Gauss)**.** *Sia $f \in \mathbb{Z}[x]$. Se f si fattorizza in modo non banale su $\mathbb{Q}[x]$, allora f si fattorizza in $\mathbb{Z}[x]$.*

Definizione 3.4. Un sottogruppo G di S_n si dice *transitivo* se dati $i \neq j$ con $1 \leq i, j \leq n$ esiste $\sigma \in G$ tale che $\sigma(i) = j$.

Teorema 3.7. *Sia F un campo e sia $f \in F[x]$ un polinomio separabile con gruppo di Galois associato G. Se f è irriducibile di grado n, allora $n \big| |G|$ e G è isomorfo a un sottogruppo transitivo di S_n.*

Dimostrazione. Sia K il campo di spezzamento del polinomio $f \in F[x]$, allora l'estensione $F \subseteq K$ è di Galois, perché è il campo di spezzamento di un polinomio separabile in $F[x]$ (teorema 1.12). Siano $\alpha_1, \ldots, \alpha_n$ le radici distinte di f in K, allora $K = F(\alpha_1, \ldots, \alpha_n)$. Risulta anche che $[F(\alpha_1) : F] = \deg f = n$, perché α_1 è elemento algebrico su F con polinomio minimo f. Allora G ha un sottogruppo di ordine n per il teorema sulla corrispondenza di Galois 1.17 e quindi $n \big| |G|$. Inoltre per ogni $i \neq j$ esiste un isomorfismo $\sigma : F(\alpha_i) \to F(\alpha_j)$ che lascia fisso F e tale che $\sigma(\alpha_i) = \alpha_j$, che si può estendere ad un automorfismo di K (proposizione 1.3). Così G è isomorfo ad un sottogruppo transitivo di S_n. □

Verranno ora riportati alcuni esempi per il grado 4.

Esempio 3.1. Si consideri il polinomio biquadratico $f(x) = x^4 + 30x + 45 \in \mathbb{Q}[x]$. Applicando due volte la formula quadratica si ottiene che le radici sono:

$$\alpha := \sqrt{-15 + 6\sqrt{5}}, \quad -\alpha, \quad \beta := \sqrt{-15 - 6\sqrt{5}}, \quad -\beta$$

Il campo di spezzamento di f è in realtà $\mathbb{Q}(\alpha)$, perché risulta che

$$\begin{aligned} \alpha\beta &= \sqrt{-15 + 6\sqrt{5}}\sqrt{-15 - 6\sqrt{5}} \\ &= \sqrt{(15 - 6\sqrt{5})(15 + 6\sqrt{5})} \\ &= \sqrt{15^2 - 36 \cdot 5} = \sqrt{45} = 3\sqrt{5}\ . \end{aligned}$$

Ma si osservi che $\sqrt{5} \in \mathbb{Q}(\alpha)$, perché $\alpha^2 = -15 + 6\sqrt{5}$ allora

$$\sqrt{5} = \frac{15 + \alpha^2}{6}\ .$$

Si può allora scrivere

$$\beta = \frac{3\sqrt{5}}{\alpha} = \frac{3(15 + \alpha^2)}{6\alpha}\ .$$

Si è così dimostrato che $\mathbb{Q}(\alpha)$ è campo di spezzamento di un polinomio separabile ed è quindi un estensione di Galois. Allora $|\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 4$ e si vuole ora mostrare che in particolare $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, quindi è risolubile. Basta mostrare che l'automorfismo $\sigma(\alpha) = \beta$ ha ordine 4 e induce sulle

radici la permutazione (1234). Sicuramente $\sigma(\alpha^2) = \beta^2$, allora risulta che

$$\begin{aligned}\sigma^2(\alpha) = \sigma(\beta) &= \sigma\left(\frac{3(15+\alpha^2)}{6\alpha}\right) \\ &= \frac{3(15+\beta^2)}{6\beta} = \frac{3(15-15-6\sqrt{5})}{6\beta} \\ &= \frac{-3\sqrt{5}}{\beta} = -\alpha\end{aligned}$$

e di conseguenza $\sigma^3(\alpha) = \sigma(-\alpha) = -\beta$.

Esempio 3.2. Si consideri ora il polinomio $f(x) = x^4 - 4x^2 + 5 \in \mathbb{Q}[x]$. Applicando anche in questo caso due volte la formula quadratica si ottiene che le radici sono:

$$\alpha_1 := \sqrt{2+i}, \quad \alpha_2 := \sqrt{2-i}, \quad \alpha_3 := -\alpha_1, \quad \alpha_4 := -\alpha_2$$

Il campo di spezzamento è allora $\mathbb{Q}(\alpha_1, \alpha_2)$. Si vuole ora mostrare che il polinomio f è irriducibile su $\mathbb{Q}[x]$. Sicuramente non si può scrivere come il prodotto di un polinomio di grado 1 ed uno di grado 3, perché nessuna radice sta in $\mathbb{Q}$. Si supponga che f si possa scrivere come prodotto di due polinomi di grado 2, allora deve risultare che:

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 - 4x^2 + 5$$

$$x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd = x^4 - 4x^2 + 5\ .$$

Si ottiene allora il seguente sistema a quattro incognite:

$$\begin{cases} c + a = 0 \\ d + ac + b = -4 \\ ad + bc = 0 \\ bd = 5 \end{cases}$$

Risolvendo il sistema si ottengono due sistemi di soluzioni non accettabili. Il primo è

$$\begin{cases} a = 0 \\ c = 0 \\ b + d = -4 \\ bd = 5 \end{cases}$$

che da l'equazione di secondo grado $b^2 - 4b + 5 = 0$, che ha come soluzioni $b_{1,2} = 2 \pm i$, che non stanno in $\mathbb{Q}$. Il secondo sistema è

$$\begin{cases} b = d \\ c = -a \\ b^2 = 5 \\ b + d - a^2 = -4 \end{cases}$$

ma questo è chiaramente impossibile, perché in $\mathbb{Q}$ non esiste una radice quadrata di 5.
L'estensione di campi $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1, \alpha_2)$ è di Galois. Si vuole ora calcolare l'ordine di $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$. Si osservi che sul campo $\mathbb{Q}(i)$ il polinomio f si spezza in due polinomi irriducibili primi fra loro:

$$f(x) = (x^2 - \alpha_1^2)(x^2 - \alpha_2^2) \ .$$

Si noti che $\mathbb{Q}(i) \subseteq \mathbb{Q}(\alpha_1)$, perché $i = \alpha_1^2 - 2$. Ci sono allora i seguenti campi intermedi:

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_1, \alpha_2) \ .$$

Si osservi che ogni estensione ha grado 2 sulla precedente. Applicando il Lemma della Torre si ha che

$$\begin{aligned}[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] &= [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] \\ &= 2 \cdot 2 \cdot 2 = 8\end{aligned}$$

A meno di isomorfismi, l'unico sottogruppo transitivo di S_4 di ordine 8 è il gruppo diedrale D_4, generato dalle permutazioni $(1234), (12)(34)$. Si devono allora cercare due elementi del gruppo di Galois che hanno associate le permutazioni $(1234), (12)(34)$. Si osservi che i campi $\mathbb{Q}(\alpha_1)$ e $\mathbb{Q}(\alpha_2)$ sono isomorfi con isomorfismo

$$\begin{aligned}\varphi : \mathbb{Q}(\alpha_1) &\longrightarrow \mathbb{Q}(\alpha_2) \\ \alpha_1 &\longmapsto \alpha_2\end{aligned}$$

Inoltre il campo $\mathbb{Q}(\alpha_1, \alpha_2)$ è il campo di spezzamento del polinomio $g_2(x) = x^2 - (2 - i) \in \mathbb{Q}(\alpha_1)$, perché contiene le due radici $\alpha_2, -\alpha_2$; ma è anche campo di spezzamento del polinomio $g_1(x) = x^2 - (2 + i) \in \mathbb{Q}(\alpha_2)$, perché contiene le due radici $\alpha_1, -\alpha_1$. Si ha inoltre che $\varphi(g_2) = g_1$. Allora per la proposizione 1.5, possiamo estendere φ ad un automorfismo τ di $\mathbb{Q}(\alpha_1, \alpha_2)$ che manda α_2 in α_1. Inoltre τ manda α_1 in α_2 perché estensione di φ. Si ha allora che τ agisce nel modo seguente:

$$\alpha_1 \mapsto \alpha_2 \mapsto \alpha_1; \quad \alpha_2 \mapsto \alpha_1 \mapsto \alpha_2; \quad \alpha_3 \mapsto \alpha_4 \mapsto \alpha_3; \quad \alpha_4 \mapsto \alpha_3 \mapsto \alpha_4 \ .$$

Ovvero τ è associato alla permutazione $(12)(34)$. Dal momento che $-\alpha_1$ appartiene a $\mathbb{Q}(\alpha_1, \alpha_2)$ con stesso polinomio minimo $g_1 = \varphi(g_2)$, si può estendere il morfismo φ ad un automorfismo σ di $\mathbb{Q}(\alpha_1, \alpha_2)$ che manda α_2 in $-\alpha_1$. Inoltre σ manda α_1 in α_2 perché estensione di φ. Si ha così che l'automorfismo σ agisce nel modo seguente:

$$\alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_4$$

Ovvero σ è associato alla permutazione (1234).

Verrà ora riportato un teorema utile per gradi primi.

Teorema 3.8. *Sia p un primo. Se $f \in \mathbb{Q}[x]$ è un polinomio irriducibile di grado p con esattamente due radici non reali complesse coniugate, allora*

$$\mathrm{Gal}(f, \mathbb{Q}) \simeq S_p \ .$$

Per dimostrare questo teorema è necessario un risultato sui gruppi simmetrici, dimostrato nell'appendice B.

Osservazione 21. Si osservi che se $p \geq 5$, allora i polinomi che soddisfano le ipotesi del teorema sopra non sono risolubili per radicali, perché il gruppo S_n non è risolubile per $n \geq 5$, teorema 2.4.

Dimostrazione. Sicuramente $\mathrm{Gal}(f, \mathbb{Q}) \subseteq S_p$. Inoltre per il teorema 3.7 $p \big| |\mathrm{Gal}(f, \mathbb{Q})|$, allora per il teorema di Cauchy $\mathrm{Gal}(f, \mathbb{Q})$ contiene un elemento σ di ordine p, che si può identificare con un ciclo σ di ordine p. Si consideri ora l'automorfismo di coniugio $\alpha + i\beta \mapsto \alpha - i\beta$, che ha come campo fisso $\mathbb{R}$. Questo lascia fisse tutte le radici di f tranne le due che per ipotesi sono complesse coniugate, e che quindi vengono scambiate tra loro. Questo implica che il gruppo di Galois $\mathrm{Gal}(f, \mathbb{Q})$ contiene una trasposizione $\tau = (ab)$. Dal momento che si può sempre scrivere $\sigma = (aj_2 \dots j_p)$, si ha che qualche potenza di σ è della forma $\sigma^k = (abi_3 \dots i_p) \in \mathrm{Gal}(f, \mathbb{Q})$. Cambiando notazione, se necessario, si può assumere che $\tau = (12)$ e $\sigma = (123 \dots p)$. Per il teorema B.2, questi due elementi, che stanno in $\mathrm{Gal}(f, \mathbb{Q})$, generano tutto S_p, allora $\mathrm{Gal}(f, \mathbb{Q}) = S_p$. □

Esempio 3.3. Il polinomio $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ è irriducibile per il criterio di Eisenstein. Indagando sul suo grafico si vede che ha solo tre radici reali, allora per il teorema precedente il suo gruppo di Galois è S_5, che non è risolubile.

Esempio 3.4. Il polinomio $f(x) = 15x^7 - 84x^5 - 35x^3 + 420x + 7 \in \mathbb{Q}[x]$ è irriducibile per il criterio di Eisenstein (per $p = 7$). Per capire se ha due radici complesse coniugate si può calcolare la sua derivata:

$$\begin{aligned} f'(x) &= 105x^6 - 420x^4 - 105x^2 + 420 \\ &= 105(x^6 - 4x^4 - x^2 + 4) \\ &= 105(x^2 + 1)(x^2 - 1)(x^2 - 4) \\ &= 105(x^2 + 1)(x - 1)(x + 1)(x - 2)(x + 2) \ . \end{aligned}$$

La derivata ha quattro radici reali distinte e due complesse coniugate. Valutando il polinomio nella radici reali si ottengono i punti di massimo e di minimo, che sono:

$$f(-2) = 215; \quad f(-1) = -309; \quad f(1) = 323; \quad f(2) = -201 \ .$$

Ovvero il polinomio ha due minimi relativi negativi e due massimi relativi positivi, allora ha esattamente cinque radici reali, perché cambia pendenza cinque volte. Allora per il teorema precedente, il polinomio f ha come gruppo di Galois S_7 che non è risolubile per il teorema 2.4.

Si può ora comprendere l'esempio di estensione risolubile non radicale, riportato di seguito.

Esempio 3.5. Si consideri il polinomio $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. Si vuole ora mostrare che è un polinomio irriducibile. Per il lemma di Gauss, basta mostrare che è irriducibile in $\mathbb{Z}[x]$. Poichè il polinomio ha grado 3, è sufficiente mostrare che non ha radici in $\mathbb{Z}[x]$ e ciò segue dal fatto che le eventuali radici di f in $\mathbb{Z}[x]$ devono essere divisori del termine noto -1, quindi le possibili radici sono $1, -1$. Ma $f(1) \neq 0$ e anche $f(-1) \neq 0$. Allora il polinomio f non ha radici in $\mathbb{Z}[x]$. Per studiare il gruppo di Galois di f è utile calcolare il discriminante di f utilizzando i suoi coefficienti. Il discriminante di un generico polinomio monico di terzo grado $g(x) = x^3+ax^2+bx+c \in \mathbb{Q}[x]$ è dato dalla seguente formula (si veda [2] esempio 2.7.18):

$$\Delta(g) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \, .$$

Calcolandolo per il polinomio f si ottiene che $\Delta(f) = 49$, che è un quadrato in $\mathbb{Q}$, ovvero $\sqrt{\Delta(f)} = 7 \in \mathbb{Q}$. Allora per la proposizione 1.14, il gruppo di Galois di f è $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$.
Operando un indagine analitica sul suo grafico, si vede facilmente che f ha tre radici reali distinte. Sia L il suo campo di spezzamento, allora l'estensione $\mathbb{Q} \subset L$ è di Galois risolubile, perché campo di spezzamento di un polinomio separabile e risulta che $L \subset \mathbb{R}$.
Si vuole ora mostrare che l'estensione $\mathbb{Q} \subset L$ non è radicale. Si supponga per assurdo che $\mathbb{Q} \subset L$ sia un'estensione radicale. Dal momento che $[L : \mathbb{Q}] = |\operatorname{Gal}(L/\mathbb{Q})| = 3$, si ha che $L = \mathbb{Q}(\gamma)$, dove $\gamma^m \in \mathbb{Q}$ per qualche $m \geq 3$. Allora il polinomio minimo f di γ deve dividere $x^m - \gamma^m$ in $\mathbb{Q}[x]$. Poichè L è il campo di spezzamento di f, f si spezza completamente su $\mathbb{Q}(\gamma)$, ma così tre elementi tra $\gamma, \xi\gamma, \xi^2\gamma, \ldots, \xi^{m-1}\gamma$, dove ξ è una radice primitiva m-esima dell'unità, devono appartenere ad L. Ma questo è assurdo, dal momento che $L \subset \mathbb{R}$. Perciò l'estensione non è radicale.

3.3 Un esempio di estensione non risolubile

Per prima cosa verrà illustrato un utile risultato per capire se un polinomio di grado p è irriducibile su un campo.

Proposizione 3.9. *Sia F un campo e sia p un primo. Allora il polinomio $f(x) = x^p - a \in F[x]$ è irriducibile su F se e solo se f non ha radici in F.*

Dimostrazione. Si supponga che f sia irriducibile e si supponga per assurdo che abbia una radice $\alpha \in F$, allora risulta che $(x - \alpha)$ è un fattore lineare di f in $F[x]$, ma questo è assurdo perché per ipotesi f è irriducibile.
Per il viceversa, si supponga che per assurdo f sia riducibile, si vuole allora mostrare che f ha una radice in F. Sia L il campo di spezzamento di f su F, allora su L risulta che :

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_p)$$

dove $\alpha_i \in L$ sono radici di f per $i = 1, \dots, p$. Se $\alpha_1 = 0$, si ha che f ha una radice in f, allora si può supporre $\alpha_1 \neq 0$. Si ponga ora

$$\xi_i = \frac{\alpha_i}{\alpha_1}, \qquad \text{per} \quad 1 \leq i \leq p \, .$$

Poichè $\alpha_i^p = a$ per ogni i, si ha che:

$$\xi_i^p = \frac{\alpha_i^p}{\alpha_1^p} = \frac{a}{a} = 1$$

ovvero ξ_i è una radice p-esima dell'unità. Inoltre si può scrivere $\alpha_i = \xi_i \alpha_1$ per ogni $1 \leq i \leq p$. Su L si ha quindi che:

$$f(x) = (x - \xi_1\alpha_1)(x - \xi_2\alpha_1) \dots (x - \xi_p\alpha_1) \, . \tag{3.1}$$

Dal momento che f è riducibile per ipotesi, si può supporre che $f = gh$, con $g, h \in F[x]$ di grado rispettivamente $r, s < p$. É possibile assumerli monici, moltiplicandoli per delle costanti se necessario. Poichè la fattorizzazione è unica, g deve essere prodotto di r fattori di 3.1. Eventualmente rinominandoli, si ottiene allora che:

$$g(x) = (x - \xi_1\alpha_1)(x - \xi_2\alpha_1) \dots (x - \xi_r\alpha_1) \, .$$

Dato che $g \in F[x]$, allora il suo termine nota appartiene a F e il termine noto di g è $\xi\alpha_1^r$, dove $\xi = \xi_1 \dots \xi_r$. Si osservi che $\xi^p = 1$. Per il teorema cinese dei resti, dal momento che p è primo e $1 < r < p$, esistono $m, n \in \mathbb{Z}$ tali che $mr + np = 1$. Allora si ha che

$$\xi^m\alpha_1 = \xi^m\alpha^{mr+np} = (\xi\alpha_1^r)^m(\alpha_1^p)^n$$

ma $\alpha_1^p = a \in F$ e $\xi\alpha_1^r \in F$, allora necessariamente anche $\xi^m\alpha_1 \in F$. Ma $\xi^m\alpha_1$ è proprio una radice del polinomio f dal momento che $(\xi^m\alpha_1)^p = (\xi^p)^m\alpha_1^p = 1 \cdot a = a$. Allora si ha una contraddizione perché $\xi^m\alpha_1$ è una radice di f che sta in F, ma f per ipotesi non ha radici in F, allora si è raggiunto l'assurdo. □

Definizione 3.5. Si dice che un campo F *contiene tutte le radici dell'unità* se $x^m - 1$ si spezza linearmente du F per ogni intero $m \geq 1$.

Lemma 3.10. *Sia F un campo contenente tutte le radici dell'unità. Sia γ un elemento tale che $\gamma \notin F$ e $\gamma^m \in F$ per qualche primo m. Allora il polinomio $g(x) = x^m - \gamma^m \in F[x]$ è irriducibile su F e $[F(\gamma) : F] = m$.*

Dimostrazione. Si supponga per assurdo che g abbia una radice $\beta \in F$, allora si ha che $\beta^m = \gamma^m$, ovvero $\beta = \xi\gamma$, dove ξ è una radice m-esima dell'unità. Poichè per ipotesi F contiene tutte le radici dell'unità, si ha che $\beta, \xi \in F$, allora $\gamma = \xi^{-1}\beta \in F$, ma questo è assurdo perché per ipotesi $\gamma \notin F$. Quindi poichè il polinomio g non ha radici in F, per la proposizione 3.9 è irriducibile su F. La seconda parte del lemma è banalmente vera, perché g è il polinomio minimo di γ essendo irriducibile, e perciò $[F(\gamma) : F] = \deg g = m$. □

Teorema 3.11. *Sia M un campo di caratteristica prima p che contiene tutte le radici dell'unità. Allora ogni estensione di Galois $M \subseteq L$ di grado p non è risolubile per radicali.*

Dimostrazione. Per mostrare che l'estensione $M \subseteq L$ non è risolubile, si deve mostrare che L non è contenuto in nessuna estensione radicale di M. Si consideri l'estensione $M \subseteq M(\gamma)$, dove $\gamma \notin M$, ma $\gamma^m \in M$, per qualche primo m. Per il lemma precedente si ha allora che il polinomio $g(x) = x^m - \gamma^m \in M[x]$ è irriducibile e che $[M(\gamma) : M] = m$. Si ha allora il seguente diagramma di estensioni:

$$\begin{array}{ccc} M(\gamma) & \longrightarrow & L(\gamma) \\ \uparrow & & \uparrow \\ M & \longrightarrow & L \end{array}$$

Si vuole ora mostrare che $\gamma \notin L$. Si supponga per assurdo che $\gamma \in L$, allora si ha che $L = M(\gamma)$, perché $[L : M] = p$, primo. Allora si ha che $m = [M(\gamma) : M] = [L : M] = p$, ovvero il polinomio minimo di γ su M è $g(x) = x^p - \gamma^p$. Poichè l'estensione $M \subseteq L$ è di Galois per ipotesi ed in particolare è separabile, γ deve essere separabile su M, ma invece risulta che $g(x) = x^p - \gamma^p = (x - \gamma)^p$ (M ha caratteristica p), che è chiaramente non separabile. Allora si è raggiunto un assurdo, perciò $\gamma \notin L$.
Applicando nuovamante il lemma 3.10 si ha che $[L(\gamma) : L] = m$, perciò applicando il Lemma della Torre (1.1) si ha che :

$$[L(\gamma) : L][L : M] = [L(\gamma) : M] = [L(\gamma) : M(\gamma)][M(\gamma) : M]$$

$$m \cdot [L : M] = [L(\gamma) : M(\gamma)] \cdot m$$

ovvero $[L : M] = [L(\gamma) : M(\gamma)]$. Quindi aggiungere radicali primi non cambia il grado dell'estensione. Inoltre l'estensione $M(\gamma) \subseteq L(\gamma)$ è ancora di Galois, infatti L è il campo di spezzamento di un polinomio separabile $f \in M[x]$, allora $L(\gamma)$ è ancora campo di spezzamento del polinomio separabile $f \in M(\gamma)[x]$. Infine, dal momento che M per ipotesi contiene tutte le radici dell'unità, $M(\gamma)$ contiene ancora tutte le radici dell'unità.
Si supponga per assurdo che esista un'estensione radicale di M contentenente L. È facile verificare che, inserendo opportuni campi intermedi, si può supporre che tale estensione radicale sia della forma $M(\gamma_1, \ldots, \gamma_s)$, dove $\gamma_1 = \gamma$, $\gamma_i \notin M(\gamma_1, \ldots, \gamma_{i-1})$, ma $\gamma_i^{m_i} \in M(\gamma_1, \ldots, \gamma_{i-1})$ per qualche primo m_i. Si consideri l'estensione $M(\gamma_1) \subseteq M(\gamma_1, \gamma_2)$, dove $\gamma_2 \notin M(\gamma_1)$, ma $\gamma_2^{m_2} \in M(\gamma_1)$ per qualche primo m_2. Si ottiene allora il seguente diagramma:

$$\begin{array}{ccc} M(\gamma_1, \gamma_2) & \longrightarrow & L(\gamma_1, \gamma_2) \\ \uparrow & & \uparrow \\ M(\gamma_1) & \longrightarrow & L(\gamma_1) \\ \uparrow & & \uparrow \\ M & \longrightarrow & L \end{array}$$

Utilizzando quanto dimostrato nella prima parte con $M(\gamma_1)$ nel ruolo di M e $M(\gamma_1, \gamma_2)$ nel ruolo di $M(\gamma)$, si ottiene che l'estensione $M(\gamma_1, \gamma_2) \subseteq L(\gamma_1, \gamma_2)$ è di Galois di grado p; in particolare $L(\gamma_1, \gamma_2) \nsubseteq M(\gamma_1, \gamma_2)$. Ripetendo iterativamente il ragionamento appena visto, si ottiene il diagramma seguente:

$$\begin{array}{ccc} M(\gamma_1, \ldots, \gamma_s) & \longrightarrow & L(\gamma_1, \ldots, \gamma_s) \\ \uparrow & & \uparrow \\ M(\gamma_1, \ldots, \gamma_{s-1}) & \longrightarrow & L(\gamma_1, \ldots, \gamma_{s-1}) \\ \uparrow & & \uparrow \\ \vdots & \longrightarrow & \vdots \\ \uparrow & & \uparrow \\ M(\gamma_1, \gamma_2) & \longrightarrow & L(\gamma_1, \gamma_2) \\ \uparrow & & \uparrow \\ M(\gamma_1) & \longrightarrow & L(\gamma_1) \\ \uparrow & & \uparrow \\ M & \longrightarrow & L \end{array}$$

dove risulta che $L(\gamma_1, \ldots, \gamma_s) \nsubseteq M(\gamma_1, \ldots, \gamma_s)$. Ma questo è assurdo, perché per ipotesi $M(\gamma_1, \ldots, \gamma_s)$ è un'estensione radicale di M contenente L, allora in particolare contiene L e $\gamma_1, \ldots, \gamma_s$. Quindi non esiste un'estensione radicale di M contenente L. □

Si vuole ora presentare un'applicazione di questo risultato. È però prima necessario dimostrare un ulteriore lemma.

Lemma 3.12. *Sia K un campo e sia $M = K(t)$, dove t è un'ideterminata. Sia $n > 1$, allora non esiste un elemento $\beta \in M$ tale che $\beta^p - \beta + t = 0$.*

Dimostrazione. Per definizione, ogni elemento $\beta \in M$ può essere scritto come $\beta = \frac{f(t)}{g(t)}$ dove $f(t), g(t) \in K[t]$ sono relativamente primi tra loro e $g(t) \neq 0$. Si vuole mostrare che se $\beta = \frac{f(t)}{g(t)}$ è tale che $\beta^n - \beta + t = 0$, deve risultare che g è un polinomio costante. Se $\beta = \frac{f(t)}{g(t)}$ e $\beta^n - \beta + t = 0$, si ha che

$$\frac{f(t)^n}{g(t)^n} - \frac{f(t)}{g(t)} + t = 0$$
$$f(t)^n - f(t)g(t)^{n-1} + tg(t)^n = 0$$

ovvero

$$f(t)^n = f(t)g(t)^{n-1} - tg(t)^n \ .$$

Dal momento che $g(t)$ divide il secondo membro dell'equazione sopra, $g(t)$ deve dividere $f(t)^n$. Si scomponga il polinomio $g(t)$ nel prodotto dei suoi fattori irriducibili

$$g(t) = p_1(t) \cdots p_k(t) \ .$$

Sia $p_i(t)$ un fattore irriducibile di $g(t)$. Allora $p_i(t)$ divide $g(t)$ e quindi deve dividere $f(t)^n$. Poichè $p_i(t)$ è primo, segue che deve dividere $f(t)$. Allora si ha che

$$p_i(t)|g(t) \quad \text{e} \quad p_i(t)|f(t)$$

ma $f(t)$ e $g(t)$ sono relativamente primi. Allora $p_i(t)$ è una costante. Questo ragionamento vale per tutti i fattori irriducibili di $g(t)$, allora $g(t)$ è una costante, come si voleva dimostrare. Per dimostrare allora che non esiste un elemento β tale che $\beta^n - \beta + t = 0$, basta mostrare che $f(t)^n - f(t) + t \neq 0$ per ogni $f \in F[t]$. Si supponga che $\deg f = s$, allora si ha che il coefficiente direttore del polinomio $f(t)^n - f(t) + t$ ha grado sn e dal momento che $n > 1$, il polinomio non si può annullare, perché ha grado sempre strettamente maggiore di 1.

□

Esempio 3.6. Sia K un campo algebricamente chiuso di caratteristica p e sia $M = K(t)$, dove t è una indeterminata. Dal momento che $x^m - 1$ si spezza linearmente su K per ogni intero positivo m, segue che M contiene tutte le radici dell'unità. Si consideri allora il polinomio:

$$f(x) = x^p - x + t \in M[x] \ .$$

Sia L il campo di spezzamento di f su M. Il polinomio f risulta separabile, perché

$$f'(x) = px^{p-1} - 1 = -1 \ ,$$

poichè la caratteristica di M è p. Quindi risulta che $(f, f') = 1$, allora per la proposizione 1.8 è separabile. Quindi L è il campo di spezzamento di un polinomio separabile f su M, allora l'estensione $M \subseteq L$ è un'estensione di Galois.
Sia ora α una radice di f, si vuole mostrare che le radici di f sono esattamente $\alpha, \alpha + 1, \ldots, \alpha + (p-1)$. Infatti sia $i < p$, dal momento che $\alpha - \alpha^p = t$ e $n^p \equiv n \mod p$ per ogni $0 \leq n \leq p-1$, risulta che

$$\begin{aligned} f(\alpha + i) &= (\alpha + i)^p - (\alpha + i) + t \\ &= \alpha^p + i^p - \alpha - i + t \\ &= (\alpha^p - \alpha) + (i^p - i) + t \\ &= -t + t = 0 \ . \end{aligned}$$

Allora preso $\sigma \in \mathrm{Gal}(L/M)$ risulta che $\sigma(\alpha) = \alpha + i$. Si consideri ora l'omomorfismo iniettivo di gruppi:

$$\begin{aligned} \varphi : \mathrm{Gal}(L/M) &\longrightarrow \mathbb{Z}/p\mathbb{Z} \\ \sigma &\longmapsto [i] \end{aligned}$$

Questo è un omomorfismo perché presi $\sigma, \tau \in \mathrm{Gal}(L/M)$, con $\sigma \mapsto [i]$, $\tau \mapsto [j]$, si ha che

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha + j) = \alpha + (i + j)$$

ovvero $\sigma\tau \mapsto [i + j]$, perché $\mathrm{char}\, M = p$. L'omomorsifmo φ è anche iniettivo, perché presi $\sigma, \tau \in \mathrm{Gal}(L/M)$ tali che $\tau, \sigma \mapsto [i]$, si ha che per ogni $j = 1, \ldots, p-1$

$$\sigma(\alpha + j) = \sigma(\alpha) + j = \alpha + i + j = \tau(\alpha) + j = \tau(\alpha + j)$$

ovvero i due automorfismi assumono lo stesso valore su ogni radice di f, ma un automorfismo è determinato dal valore che assume sulle radici di f, allora

$\sigma = \tau$. In particolare si ha che $|\operatorname{Gal}(L/M)| = 1$ o p. Dal momento che $[L : M] = |\operatorname{Gal}(L/F)|$ si ha che $[L : M] = 1$ o p. Se $[L : M] = 1$, si ha che $L = M$, ovvero il polinomio f si spezza linearmente su M, ma per il lemma precedente f non ha radici in M, di conseguenza $[L : M] = p$. Segue allora che l'estensione $M \subseteq L$ è di Galois di grado p, allora per il teorema 3.11 l'estensione $M \subseteq L$ non è risolubile.

Appendice A

Teorema di Struttura dei Gruppi Abeliani

Verrà dimostrato un enunciato, utilizzato nel capitolo 2, conseguenza del teorema di struttura per gruppi abeliani, risultato fondamentale nella teoria dei moduli.

Teorema A.1. *Sia V un gruppo abeliano finitamente generato. Allora esistono unici $d_1, \ldots, d_k, r \in \mathbb{N}$ tali che $d_1|d_2|\ldots|d_k$ e*

$$V \simeq C_{d_1} \times \ldots \times C_{d_k} \times L$$

dove i C_{d_i} sono gruppi ciclici di ordine d_i ed L è un gruppo abeliano libero di rango r.

Osservazione 22. Se V è un gruppo abeliano finito, allora è finitamente generato ma il gruppo libero L risulta essere il gruppo nullo.

Proposizione A.2. *Sia $G \subseteq F^*$ un sottogruppo finito del gruppo moltiplicativo di un campo F. Allora G è ciclico.*

Dimostrazione. Si osservi che G è abeliano perché F è un campo. Per il teorema A.1 di struttura dei gruppi abeliani si ha che G è isomorfo al prodotto diretto di gruppi ciclici, ad esempio

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$$

dove m_i sono interi maggiori di 1 tali che $m_1|m_2|\ldots|m_k$. Perciò $|G| = m_1 \cdot \ldots \cdot m_k$. Sia $m = \text{mcm}(m_1, \ldots, m_k)$ il minimo comune multiplo di $m_1, \ldots, m_k$. Si osservi che $m = m_k$. Si vuole ora mostrare che $g^m = 1$ per ogni $g \in G$, infatti un generico elemento di g è associato ad un elemento della

forma $([a_1]_{m_1}, \ldots, [a_k]_{m_k})$ e per ogni $i = 1, \ldots, k$ si ha che $m[a_i]_{m_i} = [0]_{m_i}$, per definizione di minimo comune multiplo e quindi $m([a_1]_{m_1}, \ldots, [a_k]_{m_k})$ è l'elemento nullo e dunque $g^m = 1$. Dato che G è un sottogruppo di F^*, segue che ogni $g \in G$ è radice del polinomio $x^m - 1 \in F[x]$, che ha al più m radici in F. Perciò risulta che

$$m_k = m \geq m_1 \cdot \ldots \cdot m_k \ ,$$

quindi $k = 1$, ovvero G è ciclico. □

Appendice B

Gruppo Simmetrico

Nel capitolo 3 è necessario un teorema sul gruppo simmetrico la cui dimostrazione è qui riportata. Verrano prima citati alcuni risultati fondamentali, per la cui dimostrazione si veda [3], capitolo 1, sezione 6.

Definizione B.1. Sia G un gruppo moltiplicativo, due elementi $x, y \in G$ sono detti *coniugati* se esiste un elemento $a \in G$ tale che $axa^{-1} = y$.

Lemma B.1. *Siano $\sigma, \gamma \in S_n$, dove σ è una permutazione qualsiasi e $\gamma = (i_1 \dots i_l)$ è un ciclo di lunghezza l. Allora il coniugato di γ tramite σ è*

$$\sigma\gamma\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_l)) \ .$$

In particolare è ancora un ciclo di lunghezza l.

Teorema B.2. *Il gruppo S_n è generato dalle permutazioni $\tau = (12)$ e $\sigma = (123 \dots n)$.*

Dimostrazione. Questa dimostrazione è articolata in tre passi:

1. S_n è generato dalle $n-1$ trasposizioni $(12), (13), (14), \dots, (1n)$.
   Infatti ogni ciclo di S_n può essere scritto come prodotto di trasposizioni e la generica trasposizione (ij) può essere scomposta nel modo seguente:

   $$(ij) = (1i)(1j)(1i) \ .$$

2. S_n è generato dalle $n-1$ trasposizioni $(12), (23), (34), \dots (n-1n)$.
   Si vuole mostrare ciò per induzione su n. Sia $n = 2$, allora per il punto 1, S_n è generato da (12). Si supponga valga l'ipotesi induttiva per $j-1$, allora il ciclo $(1j)$ si può scrivere nel modo seguente:

   $$(1j) = (1\ j-1)(j-1\ j)(1\ j-1)$$

e per ipotesi induttiva il ciclo $(1\ j-1)$ si può scrivere come prodotto delle trasposizioni $(12), (23), \dots (j-2\ j-1)$. Allora il ciclo $(1j)$ si può scrivere come prodotto della trasposizioni $(12), (23), \dots (j-1\ j)$. Quindi per induzione S_n è generato dalle $n-1$ trasposizioni $(12), (23), (34), \dots, (n-1\ n)$.

3. S_n è generato da (12) e $(12\dots n)$: Posto $\tau = (12)$ e $\sigma = (123\dots n)$, si possono considerare le seguenti traposizioni:

$$\tau_1 = \tau = (12), \tau_2 = \sigma\tau_1\sigma^{-1}, \dots, \tau_{n-1} = \sigma\tau_{n-2}\sigma^{-1}\ .$$

Per il lemma precedente queste sono trasposizioni perché ognuna è coniugata con quella precedente e la prima è una trasposizione. Ma risulta che:

$$\tau_1 = (12), \tau_2 = (23), \dots, \tau_{n-1} = (n-1n)$$

che generano S_n. Allora τ e σ generano S_n.

□

Bibliografia

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

[2] S. Gabelli, *Teoria delle Equazioni e Teoria di Galois*, Springer, 2008

[3] T. Hungerford, *Algebra*, Springer, 1974

[4] J.Milne, *Fields and Galois Theory*, J.S.Milne, 2012

[5] J.Milne, *Group Theory*, J.S.Milne, 2013

Ringraziamenti

Per prima cosa vorrei ringraziare la mia relatrice, la professorressa Marta Morigi per la sua disponibilità, per la sua pazienza e per il suo aiuto.
Vorrei ringraziare mio padre, che mi sprona sempre, nelle direzioni e nei modi meno convenzionali che conosco, ma che sa sempre come farmi sorridere. Ringrazio anche mia madre, per cui ogni occasione è buona per fare shopping, perchè è sempre stata presente e partecipe nel mio percorso di studi. Un ringraziamento va anche a mio fratello, che, anche se odio sei giorni su sette, ce n'è sempre uno in cui gli voglio bene. Un grazie particolare va ai miei nonni, che nonostante tutto sono sempre stati con me e mi hanno aiutato finché hanno potuto.
Vorrei poi ringraziare la mia enorme famiglia, che nel giorno della mia laurea si è riunita da tutta l'Italia per celebrare con me. Siete e sarete sempre tutti parte di me.
Vorrei ringraziare i miei compagni di corso o meglio di avventura, con cui ho condiviso questi ultimi tre anni, con cui ho superato i momenti e gli esami più difficili e con cui mi sono sempre divertita. Grazie Alex, Angelica, Bertoz, Gianlu, Greta, Marta Roxy, Marta Sacco, Palma, Sara e Stefano.
Vorrei ringraziare la Lolla, che nei momenti più tristi e difficili, rideva di me, facendomi tornare sempre il sorriso, che mi ha sempre sopportato nonostante tutte le mie stranezze e soprattutto che ha saputo accetarmi anche quando non era più io, ma ero una pesona nuova.
Infine un grande grazie va a Yuri, che è sempre stato con me negli ultimi due anni, nei momenti difficili come in quelli felici, che è stato capace di capirmi e di aiutarmi, che mi prende sempre in giro, ma che crede in me e che mi sprona, anche se il mio futuro mi porterà lontano da lui. Grazie a te che sei la persona più importante per me.
The last but not the least person I want to thank is Luisa, who came to my graduation after five years of being separated one from the other. She made this day much more bright and happy than I could ever immagine. Thank you for being here with me and for making this day the best of all.