ALGEBRA 2 — CAMPI E TEORIA DI GALOIS

ALESSANDRO D'ANDREA

INDICE

1. RICHIAMI SUGLI ANELLI

1.1. **Anelli, sottoanelli, ideali.** Un anello $(A, +, \cdot)$ è un insieme A, dotato di operazioni associative $+$ di *somma* e $\cdot$ di *prodotto* o *moltiplicazione*, tale che $(A, +)$ è un gruppo abeliano, e $\cdot$ distribuisce rispetto alla somma. Un anello A è *commutativo* se l'operazione $\cdot$ è commutativa, ed è un *anello con unità* se esiste un elemento $1 \in A, 1 \neq 0$, tale che $1 \cdot a = a \cdot 1 = a$ per ogni $a \in A$. Gli anelli che utilizzeremo saranno tutti commutativi

con unità, e in seguito per anello intenderemo **sempre** anello commutativo con unità a meno che non sia esplicitamente detto.

Un anello è un *dominio di integrità*, o semplicemente un dominio, se il prodotto di elementi diversi non nulli è diverso da 0; è un campo se ogni elemento non nullo possiede un inverso moltiplicativo. Ogni campo è chiaramente un dominio. L'anello $\mathbb{Z}$ dei numeri interi è, ad esempio, un dominio ma non un campo, in quanto i suoi soli elementi invertibili sono ± 1.

Se A è un anello, un sottoinsieme $B \subset A$ è un *sottoanello* se contiene 1, è un sottogruppo additivo di A, ed è chiuso rispetto al prodotto; ad esempio, l'unico sottoanello di $\mathbb{Z}$ è $\mathbb{Z}$ stesso. Un sottoanello di un campo che sia esso stesso un campo è un *sottocampo*: ad esempio, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono sottocampi, e quindi anche sottoanelli, di $\mathbb{C}$; anche $\mathbb{Z}$ è un sottoanello di $\mathbb{C}$, ma non ne è un sottocampo.

Un *ideale* di A è un sottogruppo additivo $I \subset A$ tale che $ai \in I$ non appena $a \in A, i \in I$. $\{0\}$ e A sono sempre ideali di A, e sono detti *ideali banali*; gli unici ideali di un campo sono quelli banali. Se $d \in A$, il sottoinsieme $(d) = dA = \{dk \,|\, k \in A\}$ è sempre un ideale di A, ed è detto *ideale principale* generato da d; gli unici ideali di $\mathbb{Z}$ sono principali.

1.2. **Omomorfismi di anelli ed anelli quoziente.** Se A, B sono anelli, un'applicazione $\phi : A \to B$ si dice *omomorfismo di anelli* o più semplicemente *omomorfismo* se $\phi(1) = 1$ e $\phi(a + a') = \phi(a) + \phi(a'), \phi(aa') = \phi(a)\phi(a')$ per ogni scelta di $a, a' \in A$. In tal caso, l'immagine di ϕ è un sottoanello di B, e se J è un ideale di B, allora $\phi^{-1}(J)$ è un ideale di A. In particolare, il nucleo $\ker \phi = \{a \in A \,|\, \phi(a) = 0\} = \phi^{-1}\{0\}$ è un ideale di A: non coincide con A in quando $\phi(1) = 1 \neq 0$. Inoltre ϕ è iniettivo se e solo se $\ker \phi = \{0\}$. Come conseguenza, ogni omomorfismo da un campo in un anello è necessariamente iniettivo.

Se $I \subsetneq A$ è un ideale, allora $a \sim_I a' \Leftrightarrow a' - a \in I$ definisce una relazione di equivalenza su A, e quindi un insieme quoziente $A/I = A/\sim_I$. Esiste un'unica struttura di anello su A/I che renda la proiezione canonica $\pi_I : A \to A/I$ un omomorfismo; il nucleo $\ker \pi_I$ coincide con I.

1.3. **Ideali primi e massimali. Domini e campi.** Un ideale $I \subsetneq A$ si dice *primo* se il prodotto di elementi che non stanno in I non appartiene ad I; si dice *massimale* se da $I \subsetneq J$ segue $J = A$. Equivalentemente, $I \subset A$ è primo quando A/I è un dominio, ed è massimale quando A/I è un campo. Pertanto, $\{0\}$ è un ideale primo di A se e solo se A è un dominio, e ogni ideale massimale è anche primo. Gli ideali massimali di $\mathbb{Z}$ sono tutti e soli quelli generati da numeri primi; l'unico ideale primo non massimale di $\mathbb{Z}$ è $\{0\}$.

Ogni omomorfismo $\phi : A \to B$ determina un isomorfismo — cioè un omomorfismo invertibile — tra $A/\ker \phi$ e l'immagine di B. In particolare, se J è un ideale di B, il nucleo di $\pi_J \circ \phi : A \to B/J$ coincide con $\phi^{-1}(J)$, ed il quoziente $A/\phi^{-1}(J)$ è allora isomorfo ad un sottoanello di B/J; di conseguenza, se J è un ideale primo di B, e quindi B/J è un dominio, allora anche $A/\phi^{-1}(J)$ è un dominio, e perciò $\phi^{-1}(J)$ è un ideale primo di A. In altre parole, la controimmagine di un ideale primo attraverso un omomorfismo è ancora un ideale primo.

1.4. **Caratteristica di un dominio.** Comunque sia scelto l'anello A, esiste un solo omomorfismo η_A da $\mathbb{Z}$ in A, che manda 0 in 0, 1 in 1, ogni numero positivo n nella somma di n copie di 1 ed ogni numero negativo $-n$ nell'inverso additivo di tale somma: si dice talvolta che $\mathbb{Z}$ è un *oggetto iniziale* nella categoria degli anelli commutativi con unità. Quando A è un dominio d'integrità, il nucleo di tale omomorfismo è controimmagine dell'ideale primo $\{0\}$, ed è pertanto un ideale primo $(d), d > 0$, di $\mathbb{Z}$: d è la *caratteristica* del dominio A, e si scrive $\operatorname{char} A = d$. Si noti che se $d \neq 0$, allora d è necessariamente un numero primo. L'immagine di $\eta_A : \mathbb{Z} \to A$ è un sottoanello di A isomorfo a $\mathbb{Z}$ quando $\operatorname{char} A = 0$ e a $\mathbb{F}_p = \mathbb{Z}/(p)$ quando $\operatorname{char} A = p \neq 0$.

1.5. **Campo delle frazioni e omomorfismi tra campi.** Da ciascun dominio d'integrità D si può costruire il corrispondente *campo delle frazioni* $F(D)$, i cui elementi sono della forma a/d, dove $a, d \in D$ e $d \neq 0$. Il dominio D si immerge nel suo campo delle frazioni,

nel senso che esiste un omomorfismo iniettivo $D \to F(D)$ dato da $d \mapsto d/1$. Ogni omomorfismo $\phi : D \to B$, tale che $\phi(d)$ sia invertibile per ogni $d \neq 0$, si estende ad un omomorfismo $\Phi : F(D) \to B$ ponendo $\Phi(a/d) = \phi(a)\phi(d)^{-1}$. In particolare, se D è contenuto in un campo K, anche il suo campo delle frazioni si immerge in K. In altre parole, $F(D)$ è il più piccolo campo nel quale D si immerga, e tutti questi campi sono isomorfi tra loro; quindi, se D è un campo, allora $F(D)$ è isomorfo a D.

Il campo delle frazioni di $\mathbb{Z}$ è $\mathbb{Q}$. Se K è un campo, il sottocampo generato da 1, cioè l'intersezione di tutti i sottocampi di K, è detto *campo primo* di K, ed è isomorfo a $\mathbb{Q}$ se $\operatorname{char} K = 0$ e a $\mathbb{F}_p$ se $\operatorname{char} K = p \neq 0$. Abbiamo già visto che un omomorfismo $\phi : K \to F$ tra campi è sempre iniettivo; poiché l'omomorfismo $\eta_F : \mathbb{Z} \to F$ deve coincidere con $\phi \circ \eta_K$, allora η_F e η_K hanno lo stesso nucleo. In altre parole, $\operatorname{char} K = \operatorname{char} F$ e ϕ identifica le immagini di $\mathbb{Z}$ in K ed F, e passando al campo delle frazioni, anche i campi primi di K ed F.

1.6. **Anelli di polinomi.** L'anello dei polinomi nelle indeterminate $x_1, \dots, x_n$ a coefficienti nell'anello A si indica con $A[x_1, \dots, x_n]$: contiene un sottoanello isomorfo ad A dato dai polinomi costanti, che identificheremo con A. Per ogni scelta di un omomorfismo $\phi : A \to B$ e di elementi $\gamma_1, \dots, \gamma_n \in B$ esiste un unico omomorfismo $\Phi : A[x_1, \dots, x_n] \to B$ tale che $\Phi(a) = \phi(a)$ e $\Phi(x_i) = \gamma_i$. Quando $B = A$ e $\phi = \mathrm{id}_A$, l'omomorfismo Φ è detto *omomorfismo di valutazione*, ed il suo nucleo è l'ideale $(x_1 - \gamma_1, \dots, x_n - \gamma_n)$.

1.7. **Domini a ideali principali e fattorizzazione unica.** Un elemento non invertibile $p \neq 0$ di un dominio D si dice *primo* se $p|ab \Rightarrow p|a$ oppure $p|b$ ed *irriducibile* se, quando $p = ab$, uno tra a e b è invertibile. Quando d è un elemento primo, l'ideale (d) è un ideale primo; inoltre $(d), d \neq 0$, è un ideale primo solo se d è primo. Tuttavia, un anello può contenere ideali primi non principali — e quindi non generati da un elemento primo.

Un dominio è un *dominio a fattorizzazione unica* (UFD) se ogni suo elemento non nullo si scrive (a meno di invertibili) come prodotto di elementi primi, e se due tali fattorizzazioni coincidono (a meno di invertibili) dopo averne permutati gli elementi. In un dominio a fattorizzazione unica, ogni elemento primo è anche irriducibile, e viceversa. Inoltre, due elementi possiedono sempre un massimo comun divisore, che è unico a meno di invertibili.

Un dominio è un *dominio a ideali principali* (PID) se ogni suo ideale è principale. Ogni dominio a ideali principali è anche un dominio a fattorizzazione unica. I suoi ideali massimali sono tutti e soli quelli generati da elementi primi; il suo unico ideale primo non massimale è (0). In un dominio a ideali principali D vale l'identità di Bézout: se $a, b \in D$, e $d = \mathrm{MCD}(a, b)$, allora esistono $h, k \in D$ tali che $d = ha + kb$.

Sono domini a ideali principali: $\mathbb{Z}, \mathbb{Z}[i]$, e anche $\mathbb{K}, \mathbb{K}[x], \mathbb{K}[[x]]$ quando $\mathbb{K}$ è un campo. Sono domini a fattorizzazione unica, ma non a ideali principali: $\mathbb{Z}[x_1, \dots, x_n]$ e in generale $D[x_1, \dots, x_n]$ quando $n > 1$ o D è un dominio a fattorizzazione unica ma non un campo.

1.8. **Sottoanelli e sottocampi.** L'intersezione di una famiglia di sottoanelli di un anello è ancora un sottoanello; allo stesso modo, l'intersezione di una famiglia di sottocampo di un campo è ancora un sottocampo. Pertanto, fissato un sottoinsieme X di un anello R (rispettivamente, di un campo K), esiste un più piccolo sottoanello di R (risp. sottocampo di K) contenente X, detto sottoanello generato (risp. sottocampo generato) da X.

Se A è un sottoanello dell'anello B e $\gamma_1, \dots, \gamma_n \in B$, allora $A[\gamma_1, \dots, \gamma_n]$ indica il sottoanello di B generato da $A \cup \{\gamma_1, \dots, \gamma_n\}$. In modo simile, se K è un sottocampo del campo F, e $\gamma_1, \dots, \gamma_n \in F$, allora $K(\gamma_1, \dots, \gamma_n)$ indica il sottocampo di F generato da $K \cup \{\gamma_1, \dots, \gamma_n\}$. Ad esempio, come sottoanelli di $\mathbb{C}$, abbiamo $\mathbb{Q}[i] = \mathbb{Q}(i)$, mentre $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi)$.

2. Estensioni di campi

Siano F, L due campi contenuti uno nell'altro: $F \subset L$. Questa è chiamata una *estensione di campi* e sarà l'oggetto principale del nostro interesse nel resto del corso. Facciamo subito alcune ovvie osservazioni preliminari.

Lemma 2.1. *Sia $F \subset L$ un'estensione di campi. Allora L è uno spazio vettoriale su F. Se $[L : F]$ è la dimensione di L come F-spazio vettoriale, allora $[L : F] = [L : K][K : F]$ per ogni estensione intermedia $F \subset K \subset L$.*

Dimostrazione. Se $\alpha_1, ..., \alpha_m$ è una base di L su K e $\beta_1, ..., \beta_n$ è una base di K su F, si dimostra facilmente che gli mn prodotti $\alpha_i\beta_j$ formano una base di L su F. La dimostrazione data a lezione ricalca quella sull'Herstein. Questo mostra che se $[L : K] = m$ e $[K : F] = n$, allora $[L : F] = mn$. □

Corollario 2.2. *Siano $F \subset L$ campi finiti, $[L : F] = n$. Allora se $|F| = q$, si avrà $|L| = q^n$.*

Dimostrazione. L è isomorfo, come spazio vettoriale, a F^n, e il numero di n.uple a coefficienti in F è pari a q^n. □

Se F è un campo, può essere sempre considerato come estensione del sottocampo generato da 1. Questo sottocampo conterrà tutti gli elementi ottenuti sommando 1 a se stesso più volte, nonché tutti i loro inversi, ed è detto *campo primo* di F.

Proposizione 2.3. *Il sottocampo di F generato da 1 è isomorfo a $\mathbb{Q}$ se la caratteristica di F è 0, e ad $\mathbb{F}_p$ se la caratteristica di F è uguale a p.*

Dimostrazione. Se la caratteristica di F è 0, allora gli elementi ottenuti sommando 1 a se stesso più volte, ed i loro inversi additivi, sono tutti distinti, e formano perciò un sottoanello isomorfo a $\mathbb{Z}$. Ma allora il sottocampo generato da 1 contiene tutti i rapporti tra tali elementi, ed è quindi isomorfo a $\mathbb{Q}$.

Se la caratteristica di F è p, gli elementi ottenuti sommando 1 a se stesso sono esattamente p, e le operazioni di somma e prodotto tra di essi sono come nell'anello $\mathbb{Z}/(p)$. Ma tale anello è un campo, e quindi il sottocampo generato da 1 è isomorfo a $\mathbb{F}_p$. □

Corollario 2.4. *Ogni campo di caratteristica 0 è infinito. Il numero di elementi in un campo finito è p^n, dove p è la caratteristica del campo.*

2.1. Estensioni finite ed elementi algebrici.

Sia ora $F \subset L$ un'estensione finita, cioè una in cui $[L : F] = n < \infty$. Se α è un elemento di L, allora le potenze $1, \alpha, \alpha^2, ..., \alpha^n$ saranno necessariamente linearmente dipendenti su F. Questo vuol dire che, per un'opportuna scelta di $c_i \in F$, avremo

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + ... + c_2\alpha^2 + c_1\alpha + c_0 = 0,$$

o in altre parole che α soddisfa un polinomio $c(x) = c_nx^n + ...c_1x + c_0$ a coefficienti in F. Un tale elemento si dice *algebrico su F*. Abbiamo quindi mostrato

Lemma 2.5. *Ogni elemento di un'estensione finita di F è algebrico su F.*

E' vero anche il viceversa.

Lemma 2.6. *Sia $F \subset L$ un'estensione di campi. Se $\alpha \in L$ è algebrico su F, allora α appartiene ad una sottoestensione finita di F.*

Dimostrazione. Sia $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ un polinomio a coefficienti in F che annulli α. Allora

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0). \tag{2.1}$$

Dimostriamo per induzione che ogni potenza di α si esprime come combinazione lineare degli elementi $1, \alpha, \alpha^2, ..., \alpha^{n-1}$. In effetti $\alpha^{N+1} = \alpha(\alpha^N)$. Per ipotesi induttiva sappiamo che $\alpha^N = c_01 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}$ per un'opportuna scelta di elementi $c_i \in F$. Ma allora $\alpha^{N+1} = c_0\alpha + c_1\alpha^2 + ... + c_{n-2}\alpha^{n-1} + c_{n-1}\alpha^n$ e possiamo sostituire in α^n l'espressione (2.1).

Essendo $1, \alpha, ..., \alpha^{n-1}$, generatori lineari di L su F, la dimensione di L come F-spazio vettoriale è limitata da n. □

Prima di procedere, un po' di notazioni. Sia $F \subset L$ un'estensione di campi, e prendiamo $\alpha \in L$. L'intersezione di tutti i sottoanelli di L che contengono sia F che α si indica con $F[\alpha]$, mentre l'intersezione di tutti i sottocampi di L con la stessa proprietà è indicato con $F(\alpha)$.

Lemma 2.7. *Gli elementi contenuti $F[\alpha]$ sono tutte e sole le combinazioni F-lineari di potenze di α.*

Dimostrazione. Sia R un sottoanello di L che contenga α. Allora contiene $\alpha^2 = \alpha \cdot \alpha$, ed ogni altra potenza di α. Se R contiene anche F, dovrà allora contenere anche i prodotti di elementi di F con potenze di α, nonché tutte le loro somme. In conclusione, un sottoanello R di L che contenga sia F che α deve contenere tutte le combinazioni lineari a coefficienti in F di potenze di α. Questo mostra che l'intersezione $F[\alpha]$ di tutti i sottoanelli di L che contengono F e α contiene tutte le espressioni polinomiali in α a coefficienti in α.

Per mostrare che questi sono i soli elementi di $F[\alpha]$, basta mostrare che formano un sottoanello di F. Ma moltiplicando due polinomi in α a coefficienti in F si ottiene ancora un polinomio in α a coefficienti in F. La dimostrazione è allora conclusa. □

Lemma 2.8. *Gli elementi di $F(\alpha)$ sono del tipo $p(\alpha)q(\alpha)^{-1}$, con $p(x), q(x) \in F[x]$, e $q(\alpha) \neq 0$.*

Dimostrazione. Come nel lemma precedente, si mostra che un sottocampo di L che contenga F e α deve contenere anche il sottoanello $F[\alpha]$. Essendo tuttavia un campo dovrà contenere anche i rapporti tra gli elementi di $F[\alpha]$.

E' semplice mostrare, a questo punto, che i rapporti di espressioni polinomiali in α a coefficienti in F formano un sottocampo di L. □

Chiaramente $F[\alpha]$ è contenuto in $F(\alpha)$. Vi sono tuttavia casi in cui i due concetti coincidono.

Un elemento α è algebrico su F quando annulla almeno un polinomio $0 \neq p(x) \in F[x]$. E' chiaro che l'insieme dei polinomi $p(x) \in F[x]$ tali che $p(\alpha) = 0$ è un ideale di $F[x]$. Sappiamo che gli ideali di $F[x]$ sono principali, ed esiste quindi un generatore di tale ideale, ovvero un polinomio di grado minimo di cui α sia soluzione. Questo polinomio è detto *polinomio minimo* di α, e può essere scelto monico, a meno di moltiplicarlo per un elemento di F.

Lemma 2.9. *Sia $F \subset L$ un'estensione di campi, $\alpha \in L$ un elemento algebrico su F. Allora il polinomio minimo $p(x)$ di α su F è irriducibile su F e $F(\alpha)$ è isomorfo al quoziente $F[x]/(p(x))$.*

Dimostrazione. Se $p(x) = a(x)b(x)$, allora $a(\alpha)b(\alpha) = p(\alpha) = 0$. Ma allora $a(\alpha) = 0$ oppure $b(\alpha) = 0$. In ogni caso, esistono polinomi che annullano α di grado minore di quello di $p(x)$, e quindi $p(x)$ non è il polinomio minimo.

Costruiamo ora l'applicazione $\phi : F[x] \to L$ tale che $\phi(p(x)) = p(\alpha)$. ϕ è chiaramente un omomorfismo, e la sua immagine coincide con $F[\alpha]$. Il nucleo di ϕ è l'ideale $(p(x))$ generato dal polinomio minimo di α. Sappiamo che $p(x)$ è irriducibile, quindi $(p(x))$ è un ideale massimale, ed il quoziente $F[x]/(p(x))$ è un campo. Per il teorema di omomorfismo, l'immagine $F[\alpha]$ di ϕ è isomorfa al campo $F[x]/(p(x))$ ed è quindi essa stessa un campo. Concludiamo che $F[\alpha] = F(\alpha)$ e che questo sottocampo di L è isomorfo a $F[x]/(p(x))$. □

Teorema 2.10. *Sia $F \subset L$ un'estensione di campi, α un elemento di L. Le seguenti affermazioni sono equivalenti.*

(1) *α è algebrico su F.*
(2) *$F[\alpha] = F(\alpha)$.*
(3) *$F[\alpha]$ è un campo.*
(4) *$F(\alpha)$ è un'estensione finita di F.*

Dimostrazione. (1) $\Rightarrow$ (2). Abbiamo già visto che se α è algebrico, allora $F[\alpha] = F(\alpha)$.

(2) $\Rightarrow$ (3). Se $F[\alpha] = F(\alpha)$ allora chiaramente $F[\alpha]$ è un campo.

$(3) \Rightarrow (1)$. Se $F[\alpha]$ è un campo, l'omomorfismo $\phi : F[x] \to F[\alpha]$ definito sopra non può essere iniettivo. Se così fosse, $F[\alpha]$ sarebbe isomorfo a $F[x]$, che non è un campo. Allora α è algebrico su F.

$(1) \Rightarrow (4)$. Se α è algebrico, allora $F(\alpha)$ è isomorfo a $F[x]/(p(x))$ dove $p(x)$ è il polinomio minimo di α. Se $p(x)$ ha grado n, ogni classe di equivalenza in $F[x]/(p(x))$ contiene uno e un solo polinomio di grado minore di n. Perciò $[1], [x], ..., [x^{n-1}]$ costituiscono una base di $F[x]/(p(x))$. Quindi $F(\alpha)$ è un F-spazio vettoriale di dimensione n.

$(4) \Rightarrow (1)$. Abbiamo già mostrato che gli elementi contenuti in un'estensione finita di F sono algebrici. □

Esempi.

- Il campo $\mathbb{Q}(\sqrt{2})$ è un'estensione di $\mathbb{Q}$. L'elemento $\sqrt{2}$ soddisfa il polinomio $x^2 - 2$, ma non soddisfa nessun polinomio di grado 1 a coefficienti in $\mathbb{Q}$, in quanto $\sqrt{2}$ non è razionale. Quindi $x^2 - 2$ è il suo polinomio minimo.

  Avremmo potuto mostrare questo fatto direttamente verificando che $x^2 - 2$ è irriducibile, il che segue dal criterio di Eisenstein. Il grado $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ è uguale al grado del polinomio minimo dell'algebrico che aggiungiamo, ed è quindi 2.
- π non è un numero algebrico – ma è un risultato troppo complesso per mostrarlo qui. In ogni caso, $\mathbb{Q}(\pi)$ non può essere un'estensione finita di $\mathbb{Q}$, perché in quel caso ogni suo elemento sarebbe algebrico. In altre parole $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Esercizi.

(a) Calcolare il grado dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{5})$.
(b) Calcolare il grado dell'estensione $\mathbb{R} \subset \mathbb{C}$.
(c) Qual è il polinomio minimo di $\sqrt{3} + i$? E di $\sqrt{3 + i}$?

2.2. **Costruzioni con riga e compasso.**

2.3. **Campi di spezzamento.**

Il quoziente $F[x]/(p(x))$ fornisce anche una costruzione utile per creare artificialmente un'estensione di F contenente radici di $p(x)$.

Proposizione 2.11. *Sia F un campo, $p(x) \in F[x]$ un polinomio irriducibile. Allora $L = F[x]/(p(x))$ è una estensione di F in cui $p(x)$ ammette almeno una radice.*

Dimostrazione. Indichiamo con $\alpha \in L$ la classe di congruenza del polinomio x. In altre parole $\alpha = [x]$. Allora $\alpha^2 = [x][x] = [x^2]$. Alla stessa maniera otteniamo che $\alpha^n = [x^n]$. Segue abbastanza facilmente che $f(\alpha) = f([x]) = [f(x)]$, qualunque sia il polinomio $f(x)$. Ma allora $p(\alpha) = [p(x)] = [0]$. Questo mostra che l'elemento $\alpha \in L$ è radice di $p(x)$. □

Corollario 2.12. *Sia F un campo, $0 \neq f(x) \in F[x]$. Allora esiste una estensione finita L di F in cui $f(x)$ si fattorizza nel prodotto di polinomi lineari.*

Dimostrazione. Possiamo esprimere $f(x)$ come prodotto di polinomi irriducibili in $F[x]$. Se tali polinomi sono tutti di primo grado, allora $f(x)$ si fattorizza in F come prodotto di polinomi lineari.

Supponiamo che così non sia, e scegliamo un fattore irriducibile non lineare $q(x)$ nella fattorizzazione di $f(x)$. Allora $F' = F[x]/(q(x))$ è un campo in cui $q(x)$ ammette una radice, e quindi la fattorizzazione di $f(x)$ in $F'[x]$ è un raffinamento di quella in $F[x]$. Reiterando questo procedimento, otteniamo dopo un numero finito di passi un'estensione L in cui $f(x)$ si spezza completamente. □

Un'estensione finita L di F si dice campo di spezzamento di $f(x) \in F[x]$ se $f(x)$ si spezza in fattori lineari su L, ma su nessun suo sottocampo proprio. E' chiaro che se $f(x)$ si spezza su L come $f(x) = (x - \alpha_1)...(x - \alpha_n)$, allora $F(\alpha_1, ..., \alpha_n) \subset L$ è un campo di spezzamento di $f(x)$.

Corollario 2.13. *Ogni polinomio $0 \neq f(x) \in F[x]$ ammette un campo di spezzamento.*

Se $\phi : F \to \overline{F}$ è un omomorfismo, possiamo definire un'applicazione $F[x] \to \overline{F}$ semplicemente calcolando ϕ sui coefficienti dei polinomi. In questa modo si ottiene un omomorfismo di anelli, che indicheremo ancora con ϕ per non appesantire la notazione. Essenziale per i nostri interessi è il seguente fatto:

Proposizione 2.14. *Siano $F, \overline{F}$ campi, e $\phi : F \to \overline{F}$ un isomorfismo. Se $f(x) \in F[x]$ e $\overline{f}(x) \in \overline{F}[x]$ sono tali che $\phi(f(x)) = \overline{f}(x)$, e $L, \overline{L}$ sono campi di spezzamento di $f(x)$ e $\overline{f}(x)$ rispettivamente, allora esiste un isomorfismo $\Phi : L \to \overline{L}$ tale che $\Phi|F \equiv \phi$.*

Dimostrazione. Per induzione su $[L : F]$. Se $[L : F] = 1$, allora $L = F$, e quindi $f(x)$ si spezza completamente in F. Applicando ϕ alla fattorizzazione di $f(x)$ in fattori lineari, otteniamo una simile fattorizzazione per $\overline{f}(x)$. Questo mostra che $\overline{L} = \overline{F}$. Ma allora l'estensione cercata è ϕ stessa.

Sia ora $[L : F] = n > 1$, e supponiamo che l'enunciato sia vero per tutte le estensioni di grado inferiore. Scegliamo una radice α di un fattore irriducibile non lineare $q(x)$ di $f(x)$ e una radice β del fattore irriducibile $\overline{q}(x) = \phi(q(x))$ di $\overline{f}(x)$. Abbiamo gli isomorfismi $F(\alpha) \simeq F[x]/(q(x))$ e $\overline{F}(\beta) \simeq \overline{F}[x]/(\overline{q}(x))$.

Consideriamo ora la composizione

$$F[x] \xrightarrow{\phi} \overline{F}[x] \xrightarrow{\pi} \overline{F}[x]/(\overline{q}(x)),$$

dove π è la proiezione al quoziente. Il nucleo di questa composizione è l'ideale $(q(x))$, mentre la composizione è suriettiva, e per il teorema di omomorfismo abbiamo un isomorfismo $F[x]/(q(x)) \simeq \overline{F}[x]/(\overline{q}(x))$.

Allora la composizione di isomorfismi

$$F(\alpha) \simeq F[x]/(q(x)) \simeq \overline{F}[x]/(\overline{q}(x)) \simeq \overline{F}(\beta)$$

estende l'isomorfismo $\phi : F \to \overline{F}$. Dal momento che $[L : F(\alpha)] < [L : F]$, per ipotesi induttiva questo isomorfismo si estende ad un isomorfismo di L con $\overline{L}$. □

Corollario 2.15. *Due campi di spezzamento $L, \overline{L}$ di uno stesso polinomio sono isomorfi.*

Dimostrazione. Applichiamo la proposizione precedente a $\mathrm{id} : F \to F$. □

2.4. **Costruzione della chiusura algebrica di un campo.**

3. Campi finiti

Diamo ora un'applicazione dei risultati appena dimostrati a proposito dei campi di spezzamento. Prima di procedere, dimostro due risultati tecnici che mi serviranno in seguito.

3.1. **Massimo comun divisore di polinomi e radici multiple.**

Lemma 3.1. *Sia $F \subset L$ campi, $p(x), q(x) \in F[x]$. Allora il massimo comun divisore di $p(x)$ e $q(x)$ in $F[x]$ è uguale a quello in $L[x]$.*

Dimostrazione. Il massimo comun divisore $d(x)$ tra $p(x)$ e $q(x)$ in $F[x]$ può essere espresso come $d(x) = a(x)p(x) + b(x)q(x)$, per opportuni polinomi $a(x), b(x) \in F[x]$.

Consideriamo ora gli ideali di $L[x]$: $I = (d(x))$, $J = (a(x), b(x))$. Sappiamo che $d(x)$ divide sia $a(x)$ che $b(x)$ in $F[x]$, quindi la stessa cosa è vera in $L[x]$. Allora $a(x), b(x) \in I \Rightarrow J \subset I$. Ma $d(x) = a(x)p(x) + b(x)q(x)$, quindi $d(x) \in J \Rightarrow I \subset J$. Perciò $I = J$.

Possiamo concludere che gli ideali $(d(x))$ e $(a(x), b(x))$ dell'anello $L[x]$ coincidono, e quindi che il massimo comun divisore in $L[x]$ tra $a(x)$ e $b(x)$ è ancora $d(x)$. □

Il prossimo lemma parla di radici multiple. α è una radice multipla di $p(x)$ se $(x-\alpha)^2$ divide $p(x)$. La derivata di un polinomio $p(x) = p_n x^n + ... + p_1 x + p_0$ è come sempre $np_n x^{n-1} + ... + 2p_2 x + p_1$.

Lemma 3.2. *Sia F un campo, $p(x) \in F[x]$. Se $(p(x), p'(x)) = 1$, allora $p(x)$ non ha radici multiple in F.*

Dimostrazione. Se $\alpha \in F$ è una radice multipla di $p(x)$, allora $p(x) = (x-\alpha)^2 h(x)$. Ma allora $p'(x) = 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x) = (x-\alpha)(2h(x) + (x-\alpha)h'(x))$. Questo mostra che $x - \alpha$ divide sia $p(x)$ che la sua derivata $p'(x)$. Di conseguenza questi due polinomi non possono essere primi tra loro. □

Corollario 3.3. *Sia F un campo, $p(x) \in F[x]$, e supponiamo che $p(x)$ si spezzi in F nel prodotto di fattori lineari. Le radici di $p(x)$ sono semplici (cioè non multiple) se e solo se $(p(x), p'(x)) = 1$.*

Dimostrazione. Sappiamo già che se $p(x)$ è primo con la sua derivata, le radici di $p(x)$ sono semplici. Supponiamo ora che $p(x)$ non sia primo con la sua derivata. Se $x - \alpha$ divide sia $p(x)$ che $p'(x)$, scriviamo $p(x) = (x - \alpha)h(x)$. Allora $p'(x) = (x - \alpha)h'(x) + h(x)$. Poiché $x - \alpha$ divide sia $p'(x)$ che $(x - \alpha)h'(x)$, deve dividere anche la loro differenza $h(x)$, e quindi $p(x) = (x - \alpha)h(x)$ è divisibile per $(x - \alpha)^2$. □

Corollario 3.4. *Sia $q(x)$ un polinomio irriducibile a coefficienti nel campo F di caratteristica 0. Allora $(q(x), q'(x)) = 1$.*

Dimostrazione. Dal momento che $\operatorname{char} K = 0$, la derivata $q'(x)$ è un polinomio non nullo. Il massimo comun divisore $(q(x), q'(x))$ divide $q'(x)$, che ha grado inferiore a quello di $q(x)$. Essendo un divisore del polinomio irriducibile $q(x)$ dovrà essere uguale a 1. □

Osservazione. Un controesempio nel caso di caratteristica finita è istruttivo. Sia $F = \mathbb{F}_p(t)$ il campo delle frazioni dell'anello $\mathbb{F}_p[t]$. Il polinomio $q(x) = x^p - t \in F[x]$ ha derivata 0, e quindi $(q(x), q'(x)) = q(x)$. Nel campo $L = \mathbb{F}_p(t^{1/p})$, il polinomio $q(x)$ si spezza in fattori lineari, però $q(x) = (x - t^{1/p})^p$ e quindi l'unica radice $t^{1/p}$ è multipla.

Questo non succede nel caso in cui F sia un campo finito : se $q(x) \in F[x]$ ha derivata nulla, allora $q(x) = a_n x^{np} + a_{n-1}x^{(n-1)p} + ... + a_1 x^p + a_0$ in quanto gli unici monomi di derivata nulla hanno grado multiplo di p. Vedremo in seguito che in un campo finito ogni elemento è una potenza p-esima. Ma allora se $a_i = (b_i)^p$ si ha $q(x) = (b_n x^n + ... + b_1 x + b_0)^p$ e quindi $q(x)$ non può essere irriducibile. I campi in cui i polinomi irriducibili non hanno radici multiple si dicono *perfetti*. Un'estensione algebrica $F(\alpha)$ per cui il polinomio minimo di α non ammette radici multiple è detta *separabile*. Evidentemente le estensioni algebriche di campi perfetti sono tutte separabili! Gli unici campi di caratteristica non nulla che considereremo sono quelli finiti, e quindi tutte le nostre estensioni algebriche saranno separabili.

3.2. **Classificazione dei campi finiti.** Sia L un campo finito. Allora la caratteristica di L è un numero primo p, e l'ordine di L è p^n dove $n = [L : \mathbb{F}_p]$. Mostreremo che per ogni scelta di p e di $n \geq 1$ esiste un solo campo di ordine p^n a meno di isomorfismo. Per fare ciò mostreremo che ogni campo di un fissato ordine è campo di spezzamento dello stesso polinomio.

Lemma 3.5. *Sia L un campo con p^n elementi. Allora $x^{p^n} = x$ per ogni $x \in L$.*

Dimostrazione. Il gruppo moltiplicativo L^* possiede $p^n - 1$ elementi. Pertanto $x^{p^n - 1} = 1$ per ogni $x \in L^*$, da cui $x^{p^n} = x$. Ma questa equazione è soddisfatta anche per $x = 0$, ed è quindi valida per ogni elemento di L. □

Lemma 3.6. *Sia L un campo con p^n elementi. Allora L è campo di spezzamento del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$.*

Dimostrazione. Il polinomio $x^{p^n} - x$ possiede p^n radici in L, e quindi necessariamente si spezza nel prodotto di fattori lineari. Questo non accade in nessun sottocampo di L, in quanto i sottocampi di L hanno meno di p^n elementi, e non possono quindi contenere tutte le radici di $x^{p^n} - x$. □

Corollario 3.7. *Due campi finiti con lo stesso numero di elementi sono isomorfi.*

Dimostrazione. Sono entrambi campi di spezzamento del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$. Ma campi di spezzamento dello stesso polinomio sono isomorfi. □

L'unico tassello mancante alla completa descrizione dei campi finiti è un risultato che ci garantisca l'esistenza di almeno un campo di ordine p^n. Prima di fare questo, abbiamo bisogno di fare conoscenza con l'automorfismo di Frobenius.

Lemma 3.8. *Sia L un campo finito di caratteristica p, $F : L \to L$ l'applicazione definita da $F(x) = x^p$. Allora F è un automorfismo di L.*

Dimostrazione. Se a, b sono elementi di un dominio di caratteristica p, allora $(a+b)^p = a^p + b^p$. Infatti tutti i coefficienti binomiali $\binom{p}{i}, i \neq 0, p$ sono divisibili per p, e quindi tutti i termini intermedi si annullano. Allora abbiamo $F(x+y) = (x+y)^p = x^p + y^p = F(x) + F(y)$ e chiaramente $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. Iniettività e suriettività sono facili. Notate che, per la suriettività di F, ogni elemento di L è una p-esima potenza, come promesso nell'osservazione della pagina precedente. □

Corollario 3.9. *Ogni potenza di F è un automorfismo di L. $F^i = \mathrm{id}$ solo se i è un multiplo di $n = [L : \mathbb{F}_p]$.*

Dimostrazione. La composizione di automorfismi è un automorfismo, quindi F^i è un automorfismo. Supponiamo che $F^i = \mathrm{id}$ con $i < n$. Allora ogni elemento di L soddisfa $x^{p^i} - x = 0$, ma questo è impossibile, in quanto L possiede $p^n > p^i$ elementi, mentre un polinomio di grado p^i a coefficienti in un campo può avere al più p^i radici. Questo mostra che F ha ordine n nel gruppo degli automorfismi di L. □

Lemma 3.10. *Sia L il campo di spezzamento di $q(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Allora L possiede esattamente p^n elementi.*

Dimostrazione. Consideriamo in L il sottoinsieme $F = \{\alpha \in L | \alpha \text{ è radice di } q(x)\}$. Gli elementi di F sono quelli fissati dall'automorfismo F^n, ed è facile mostrare che formano un sottocampo di L. Inoltre la derivata di $q(x)$ è $p^n x^{p^n - 1} - 1 = -1$, quindi $(q(x), q'(x)) = 1$. Ma allora le radici di $q(x)$ in L sono tutte semplici, e $q(x)$ ammette p^n radici. Questo mostra che F è un campo con p^n elementi, e quindi che $q(x)$ si spezza su F, da cui $L = F$. □

3.3. **Automorfismi di un campo finito.**

Lemma 3.11. *Sia L un campo finito di caratteristica p. Allora $x^p = x$ se e solo se $x \in \mathbb{F}_p$.*

Dimostrazione. Abbiamo già visto, all'inizio del corso, che $a^p \equiv a \mod p$, quindi $x^p = x$ per ogni $x \in \mathbb{F}_p$. Tuttavia $x^p = x$ ha al più p soluzioni in L, e quindi non ci sono altre soluzioni. □

Lemma 3.12. *Sia $p(x) \in \mathbb{F}_p[x]$ un polinomio irriducibile di grado d, e sia L un'estensione di F_p in cui $p(x)$ possieda una radice α. Allora $p(x)$ si spezza in L, e le sue radici sono $\alpha, \alpha^p, ..., \alpha^{p^{d-1}}$.*

Dimostrazione. Sappiamo che $0 = p(\alpha) = a_d \alpha^d + ... + a_1 \alpha + a_0$. Applicando ad entrambi i membri l'automorfismo di Frobenius, otteniamo $a_d F(\alpha)^d + ... + a_1 F(\alpha) + a_0 = 0$, quindi anche $F(\alpha)$ è una radice di $p(x)$. Ripetendo il procedimento, si mostra che $F^i(\alpha)$ è soluzione di $p(x) = 0$ per ogni i. Chiaramente $F^d = \mathrm{id}$ nel campo $\mathbb{F}_p(\alpha)$, in quanto $\mathbb{F}_p(\alpha)$ possiede p^d elementi.

Consideriamo ora il polinomio di grado d

$$q(x) = (x - \alpha)(x - F(\alpha))...(x - F^{d-1}(\alpha)). \tag{3.1}$$

Per calcolare il polinomio $F(q(x))$ i cui coefficienti si ottengono da quelli di $q(x)$ applicando F, possiamo calcolare direttamente F sulla fattorizzazione (3.1) e poi moltiplicare. Ma si vede che l'applicazione di F a tale prodotto permuta semplicemente i fattori, quindi $F(q(x)) = q(x)$. Abbiamo trovato un polinomio i cui coefficienti non cambiano dopo l'applicazione di F. Per il lemma precedente, i coefficienti appartengono a $\mathbb{F}_p$. I polinomi $p(x)$ e $q(x)$ hanno lo stesso grado, ed hanno entrambi α come radice. Dal momento che $p(x)$ è il polinomio minimo di α, concludiamo che $p(x) = q(x)$. Abbiamo osservato in precedenza che un polinomio irriducibile a coefficienti in un campo finito non può avere radici multiple in un'estensione. Ne deduciamo in particolare che gli elementi $\alpha, F(\alpha), ..., F^{d-1}(\alpha)$ sono tutti distinti. □

Mostriamo ora, nel caso dei campi finiti, un risultato importante che dimostreremo in seguito per campi di caratteristica zero.

Teorema 3.13. *Sia L un campo finito di caratteristica p. E' sempre possibile trovare $\gamma \in L$ in modo che $L = \mathbb{F}_p(\gamma)$.*

Dimostrazione. L^* è un gruppo ciclico. Se γ ne è un generatore, ogni elemento di L^* è potenza di γ, e quindi appartiene a $\mathbb{F}_p(\gamma)$. Ma allora $\mathbb{F}_p(\gamma)$ contiene tutti gli elementi di L, in quanto ogni campo contiene 0. □

Teorema 3.14. *Gli unici automorfismi di un campo finito L sono le potenze dell'automorfismo di Frobenius.*

Dimostrazione. Scegliamo $\gamma \in L$ in modo che $L = \mathbb{F}_p(\gamma)$. Se $[L : \mathbb{F}_p] = n$, il polinomio minimo di γ deve avere grado n, e quindi $1, \gamma, ..., \gamma^{n-1}$ formano una $\mathbb{F}_p$-base di L.

Sia ϕ un automorfismo di L. $\phi(\gamma)$ deve essere una radice del polinomio minimo di γ. Dal momento che ogni polinomio minimo è irriducibile, per quanto detto precedentemente avremo $\phi(\gamma) = F^i(\gamma)$ per qualche i. Ma allora $\phi(\gamma^m) = \phi(\gamma)^m = F(\gamma)^m = F(\gamma^m)$. Ogni elemento si scrive come combinazione lineare delle potenze di γ a coefficienti in $\mathbb{F}_p$. Ma allora $\phi(c_0 + c_1\gamma + ... + c_{n-1}\gamma^{n-1}) = c_0 + c_1\phi(\gamma) + ... + c_{n-1}\phi(\gamma^{n-1}) = c_0 + c_1F^i(\gamma) + ... + c_{n-1}F^i(\gamma^{n-1}) = F^i(c_0 + ...c_{n-1}\gamma^{n-1})$. Quindi $\phi \equiv F^i$. □

4. Estensioni ciclotomiche e reciprocità quadratica

4.1. **Estensioni ciclotomiche.**

4.2. **Reciprocità quadratica.**

4.3. **Un algoritmo non deterministico per il controllo di primalità.**

5. Teoria di Galois

5.1. **Estensioni di Galois.** Abbiamo visto in alcuni esempi che ci sono estensioni (finite) di campi che si comportano in maniera più regolare di altre:

Esempio 5.1. Consideriamo l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. Poiché $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$, ogni automorfismo di $\mathbb{Q}(\sqrt{2})$ — che deve necessariamente fissare il campo primo $\mathbb{Q}$ elemento per elemento — si ottiene scegliendo l'immagine di $\sqrt{2}$ tra le due radici del suo polinomio minimo $x^2 - 2$. Pertanto gli unici due automorfismi di $\mathbb{Q}(\sqrt{2})$ sono l'identità e la *coniugazione* $\phi : a + b\sqrt{2} \mapsto a - b\sqrt{2}$, dove $a, b \in \mathbb{Q}$. Si ha $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \phi\} \simeq \mathrm{C}_2$, e quindi:

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = |\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})|$;
- $\mathbb{Q}(\sqrt{2})^{\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})} = \mathbb{Q}$;
- $\mathbb{Q}(\sqrt{2})$ è il campo di spezzamento di $x^2 - 2$ su $\mathbb{Q}$.

Esempio 5.2. Consideriamo l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$. Poiché $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[x]/(x^3 - 2)$, ogni automorfismo di $\mathbb{Q}(\sqrt[3]{2})$ — che fissa il campo primo $\mathbb{Q}$ elemento per elemento — si ottiene scegliendo l'immagine di $\sqrt[3]{2}$ tra le radici del suo polinomio minimo $x^3 - 2$ contenute in $\mathbb{Q}(\sqrt[3]{2})$. Tuttavia, tutti gli elementi di $\mathbb{Q}(\sqrt[3]{2})$ sono reali, e l'unico numero reale il cui cubo sia 2 è $\sqrt[3]{2}$. Questo mostra che l'unico automorfismo di $\mathbb{Q}(\sqrt[3]{2})$ è l'identità. Si ha $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}\}$, e quindi:

- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 1 = |\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|$;
- $\mathbb{Q}(\sqrt[3]{2})^{\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$;
- $\mathbb{Q}(\sqrt[3]{2})$ non è il campo di spezzamento di $x^3 - 2$ su $\mathbb{Q}$.

Esempio 5.3. Sia $F \subset \mathbb{C}$ il campo di spezzamento su $\mathbb{Q}$ del polinomio $x^3 - 2$. Allora F è generato su $\mathbb{Q}$ dalle tre radici complesse di $x^3 - 2$:

$$\alpha = \sqrt[3]{2}, \qquad \beta = \sqrt[3]{2}(-1 + \sqrt{-3})/2, \qquad \overline{\beta} = \sqrt[3]{2}(-1 - \sqrt{-3})/2,$$

e quindi $F = \mathbb{Q}(\alpha, \beta, \overline{\beta})$. Ogni elemento di $\mathrm{Gal}(F/\mathbb{Q})$ permuta le tre radici di $x^3 - 2$, e la sua azione su F è determinata da tale permutazione. Il gruppo $\mathrm{Gal}(F/\mathbb{Q})$ contiene quindi al più 6 elementi.

Si osserva subito che $\sqrt{-3} = 2\beta/\alpha + 1$ è un elemento di F, e quindi $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \subset F$. D'altronde, l'inclusione opposta è evidente, e si ha $F = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. Si vede quindi che il grado di F su $\mathbb{Q}$ è 6: in effetti, se $K = \mathbb{Q}(\sqrt[3]{2})$, abbiamo già visto come $[K : \mathbb{Q}] = 3$;

inoltre $\sqrt{-3} \notin K \subset \mathbb{R}$, e quindi il suo grado su K non può essere 1. Tuttavia, il polinomio x^2+3 annulla $\sqrt{-3}$, e ne è quindi il polinomio minimo. In conclusione, $[F:K]=2, [K:\mathbb{Q}]=3$ e quindi $[F:\mathbb{Q}]=6$. Se $\gamma=\sqrt{-3}$, una $\mathbb{Q}$-base di F è data da $\{1,\alpha,\alpha^2,\gamma,\alpha\gamma,\alpha^2\gamma\}$.

Le prime sei potenze di $\delta=\alpha\gamma=\sqrt[6]{-108}$ si calcolano facilmente ricordando che $\alpha^3=2$ e che $\gamma^2=-3$. Sono $\delta^0=1, \delta^1=\alpha\gamma, \delta^2=-3\alpha^2, \delta^3=-6\gamma, \delta^4=18\alpha, \delta^5=18\alpha^2\gamma$ e sono pertanto linearmente indipendenti. Il polinomio x^6+108 annulla δ, e ne è quindi il polinomio minimo. Le sei radici di x^6+108 in $\mathbb{C}$ giacciono tutte in F, e sono $\pm\delta, \delta(\pm 1 \pm \sqrt{-3})/2$, e gli omomorfismi da F in F si ottengono tutti scegliendo l'immagine di δ tra tali sei valori. In conclusione, $G=\mathrm{Gal}(F/\mathbb{Q})$ contiene 6 elementi ed è quindi isomorfo a S_3. Se il campo fisso F^G non si limitasse a $\mathbb{Q}$, il grado $[F:F^G]$ sarebbe 2 o 3, e per i ragionamenti precedentemente fatti avrebbe in ogni caso al più 3 elementi.

- $[F:\mathbb{Q}]=6=|\mathrm{Gal}(F/\mathbb{Q})|$;
- $F^{\mathrm{Gal}(F/\mathbb{Q})}=\mathbb{Q}$;
- $\mathbb{Q}(\sqrt[3]{2})$ è il campo di spezzamento di x^3-2 (ma anche di x^6+108) su $\mathbb{Q}$.

Esempio 5.4. Consideriamo l'estensione $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, dove p è un numero primo e $n>1$. Abbiamo già incontrato l'omomorfismo di Frobenius $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ definito da $F(\alpha)=\alpha^p$: è necessariamente iniettivo, essendo un omomorfismo tra campi, ed è allora anche suriettivo poiché $\mathbb{F}_{p^n}$ è un insieme finito. F fissa inoltre $\mathbb{F}_p$ elemento per elemento, come si può ad esempio osservare utilizzando il piccolo Teorema di Fermat. Quindi $F\in\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Sappiamo già che $F^n(\alpha)=\alpha^{p^n}=\alpha$ per ogni $\alpha\in\mathbb{F}_{p^n}$ e quindi $F^n=\mathrm{id}$. Inoltre se $0<h<n$, allora $F^h(x)=x$ ha al più p^h soluzioni, e quindi $F^h\neq\mathrm{id}$. In altre parole, F ha ordine n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, e $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ possiede almeno n elementi.

Sia ora γ un generatore ciclico del gruppo $\mathbb{F}_{p^n}^\times$. Allora $\mathbb{F}_p(\gamma)=\mathbb{F}_{p^n}$ e quindi il polinomio minimo di γ su $\mathbb{F}_p$ ha grado $[\mathbb{F}_{p^n}:\mathbb{F}_p]=n$. Allora ogni elemento di $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ si ottiene scegliendo l'immagine di γ tra una delle al più n radici di tale polinomio: in altre parole l'ordine del gruppo di Galois è al più n. Le due maggiorazioni ci informano che $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|=n$ e quindi che $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)=\langle F\rangle$.

Il campo fisso di $\mathbb{F}_{p^n}$ per l'azione del gruppo di Galois concide allora con l'insieme degli elementi fissati da F: questi sono le soluzioni di $x^p=x$ e sono quindi al più p; contengono inoltre tutti gli elementi di $\mathbb{F}_p$, come abbiamo visto prima. In conclusione:

- $[\mathbb{F}_{p^n}:\mathbb{F}_p]=n=|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$;
- $\mathbb{F}_{p^n}^{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}=\mathbb{F}_p$;
- $\mathbb{F}_{p^n}$ è il campo di spezzamento su $\mathbb{F}_p$ del polinomio $x^{p^n}-x$ che è primo con la sua derivata.

Esempio 5.5. Consideriamo l'estensione $\mathbb{F}_2(t)\subset\mathbb{F}_2(t^{1/2})$. L'elemento $t^{1/2}$ soddisfa chiaramente il polinomio $f(x)=x^2-t\in\mathbb{F}_2(t)[x]$, che è irriducibile poiché non ha radici in $\mathbb{F}_2(t)$. $f(x)$ si spezza su $\mathbb{F}_2(t^{1/2})$ in fattori lineari, dal momento che $x^2-t=(x-t^{1/2})^2$ — non dimenticate che siamo in caratteristica 2!!! Si tratta quindi di un'estensione di grado 2.

Gli elementi del suo gruppo di Galois sono determinati dall'immagine di $t^{1/2}$, che deve essere una delle radici del suo polinomio minimo. Ad ogni modo, vi è una sola radice in $\mathbb{F}_2(t^{1/2})$ di tale polinomio, poiché i due fattori lineari coincidono. Pertanto $\mathrm{Gal}(\mathbb{F}_2(t^{1/2})/\mathbb{F}_2(t))=\{\mathrm{id}\}$.

- $[\mathbb{F}_2(t^{1/2}):\mathbb{F}_2(t)]=2\neq 1=|\mathrm{Gal}(\mathbb{F}_2(t^{1/2})/\mathbb{F}_2(t))|$;
- $\mathbb{F}_2(t^{1/2})^{\mathrm{Gal}(\mathbb{F}_2(t^{1/2})/\mathbb{F}_2(t))}=\mathbb{F}_2(t^{1/2})\neq\mathbb{F}_2(t)$;
- $\mathbb{F}_2(t^{1/2})$ è il campo di spezzamento su $\mathbb{F}_2(t)$ del polinomio irriducibile x^2-t che non è primo con la sua derivata.

Il nostro obiettivo è ora quello di mostrare che le proprietà che abbiamo osservato negli esempi sono tutte più o meno equivalenti. Prima di dare l'enunciato da dimostrare, ho bisogno di un paio di definizioni.

Definizione 5.6. Un polinomio irriducibile $q(x) \in \mathbb{K}[x]$ si dice *separabile* se $q(x)$ e la sua derivata $q'(x)$ sono coprimi o, equivalentemente, se $q'(x) \neq 0$. Un polinomio $f(x)$ si dice *separabile* se tutti i suoi fattori irriducibili sono separabili.

Se $\mathbb{K} \subset \mathbb{F}$ è un'estensione di campi, un elemento $\alpha \in \mathbb{F}$, algebrico su $\mathbb{K}$, si dice *separabile su* $\mathbb{K}$ se il suo polinomio minimo su $\mathbb{K}$ è separabile. Un'estensione algebrica $\mathbb{K} \subset \mathbb{F}$ è *separabile* se ogni elemento di $\mathbb{F}$ è separabile su $\mathbb{K}$.

Si noti che, in caratteristica 0, ogni polinomio ed ogni estensione sono separabili. Le estensioni finite di campi finiti, e di campi perfetti in generale, sono sempre separabili.

Definizione 5.7. Un'estensione algebrica $\mathbb{K} \subset \mathbb{F}$ è *normale* se ogni polinomio irriducibile a coefficienti in $\mathbb{K}$, che ha una radice in $\mathbb{F}$, si spezza su $\mathbb{F}$.

Esempio 5.8. $\mathbb{C}$ è un'estensione normale di $\mathbb{R}$. I polinomi irriducibili a coefficienti reali hanno grado 1 o 2, e possiedono sempre una radice complessa; ma allora si spezzano completamente su $\mathbb{C}$.

Allo stesso modo, se $[\mathbb{F} : \mathbb{K}] = 2$, $\mathbb{F}$ è sempre un'estensione normale di $\mathbb{K}$. Un polinomio irriducibile in $\mathbb{K}[x]$ che abbia una radice γ in $\mathbb{F}$ è il polinomio minimo di γ su $\mathbb{K}$ ed ha quindi grado 1 o 2. Ma allora si spezza completamente su $\mathbb{F}$.

Teorema 5.9. *Sia $\mathbb{K} \subset \mathbb{F}$ un'estensione finita di campi. Allora le seguenti proprietà sono equivalenti:*

(1) *$\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ di un polinomio separabile;*
(2) *$|\operatorname{Gal}(\mathbb{F}/\mathbb{K})| = [\mathbb{F} : \mathbb{K}]$;*
(3) *$\mathbb{F}^{\operatorname{Gal}(\mathbb{F}/\mathbb{K})} = \mathbb{K}$;*
(4) *$\mathbb{F}$ è un'estensione normale e separabile di $\mathbb{K}$.*

La dimostrazione del teorema seguirà da una serie di affermazioni che andiamo a dimostrare, che ci daranno informazioni sempre più precise sulla relazione che sussiste tra il grado di un'estensione e l'ordine del gruppo di Galois corrispondente.

Lemma 5.10. *Sia $\mathbb{E} \subset \mathbb{F}$ un'estensione finita di campi. Allora un omomorfismo $\phi : \mathbb{E} \to \mathbb{F}$ si estende ad un omomorfismo $\Phi : \mathbb{F} \to \mathbb{F}$ in al più $[\mathbb{F} : \mathbb{E}]$ modi distinti.*

Dimostrazione. Indichiamo con $\mathbb{E}^\phi$ il sottocampo di $\mathbb{F}$ che è immagine di ϕ; allora $\phi : \mathbb{E} \to \mathbb{E}^\phi$ è chiaramente un isomorfismo, che induce un corrispondente isomorfismo $\mathbb{E}[x] \to \mathbb{E}^\phi[x]$ — che indicheremo con $f(x) \mapsto f^\phi(x)$ — ottenuto applicando ϕ ai coefficienti di $f(x)$. E' immediato osservare come $q(x) \in \mathbb{E}[x]$ sia irriducibile se e solo se $q^\phi(x) \in \mathbb{E}^\phi[x]$ è irriducibile. Inoltre il grado di $q(x)$ coincide con quello di $q^\phi(x)$.

Dimostriamo l'enunciato per induzione su $[\mathbb{F} : \mathbb{E}]$, la base dell'induzione $[\mathbb{F} : \mathbb{E}] = 1$ essendo ovvia. Scegliamo $\alpha \in \mathbb{F}$, $\alpha \notin \mathbb{E}$. Se $q(x)$ è il polinomio minimo di α su $\mathbb{E}$, allora $q(x)$ è irriducibile, diciamo di grado d. Ogni omomorfismo $\Phi : \mathbb{F} \to \mathbb{F}$ che estende ϕ deve soddisfare

$$0 = \Phi(0) = \Phi(q(\alpha)) = q^\phi(\Phi(\alpha))$$

e quindi applica α in una delle al più d radici del polinomio irriducibile $q^\phi(x)$. Per ogni radice $\beta \in \mathbb{F}$ di $q^\phi(x)$, abbiamo un unico omomorfismo

$$\mathbb{E}(\alpha) \simeq \mathbb{E}[x]/(q(x)) \simeq \mathbb{E}^\phi[x]/(q^\phi(x)) \simeq \mathbb{E}^\phi(\beta) \hookrightarrow \mathbb{F}$$

che manda α in β ed estende $\phi : \mathbb{E} \to \mathbb{E}^\phi \subset \mathbb{F}$.

Pertanto $\phi : \mathbb{E} \to \mathbb{F}$ si estende ad un omomorfismo $\mathbb{E}(\alpha) \to \mathbb{F}$ in al più $d = [\mathbb{E}(\alpha) : \mathbb{E}]$ modi diversi. Per ipotesi induttiva, poiché $[\mathbb{F} : \mathbb{E}(\alpha)] < [\mathbb{F} : \mathbb{E}]$, ciascuno di tali omomorfismi si estende a tutto $\mathbb{F}$ in al più $[\mathbb{F} : \mathbb{E}(\alpha)]$ modi distinti. In conclusione ϕ si estende a tutto $\mathbb{F}$ in al più $[\mathbb{F} : \mathbb{E}(\alpha)][\mathbb{E}(\alpha) : \mathbb{E}] = [\mathbb{F} : \mathbb{E}]$ modi diversi. □

Osservazione 5.11. E' possibile che un omomorfismo $\phi : \mathbb{E} \to \mathbb{F}$ non possieda alcuna estensione ad $\mathbb{F}$.

Osservazione 5.12. Gli omomorfismi ϕ e Φ sono sempre iniettivi, dal momento che l'anello di partenza è un campo. Se $\phi : \mathbb{E} \to \mathbb{F}$ è l'omomorfismo di inclusione — cioè quello che manda ogni elemento di $\mathbb{E}$ in se stesso — allora ogni estensione Φ :

$\mathbb{F} \to \mathbb{F}$ è $\mathbb{E}$-lineare (dimostratelo!). In questo caso, se $\mathbb{F}$ è un'estensione finita di $\mathbb{E}$, allora dall'iniettività di Φ segue anche la sua suriettività, e Φ è necessariamente un automorfismo.

Corollario 5.13. *Se $\mathbb{K} \subset \mathbb{F}$ è un'estensione finita di campi, allora $|\operatorname{Gal}(\mathbb{F}/\mathbb{K})| \leq [\mathbb{K} : \mathbb{F}]$.*

Dimostrazione. L'inclusione di $\mathbb{E}$ in $\mathbb{F}$ si estende a tutto $\mathbb{F}$ in al più $[\mathbb{F} : \mathbb{E}]$ modi diversi. □

L'enunciato che segue è una variante del Lemma 5.10, e si dimostra in maniera simile.

Proposizione 5.14. *Siano $\mathbb{K} \subset \mathbb{E} \subset \mathbb{F}$ campi, e sia $\mathbb{F}$ il campo di spezzamento su $\mathbb{K}$ di un polinomio separabile $f(x) \in \mathbb{K}[x]$. Allora ogni omomorfismo $\phi : \mathbb{E} \to \mathbb{F}$ tale che $\phi|_{\mathbb{K}} = \mathrm{id}$ si estende ad un omomorfismo $\Phi : \mathbb{F} \to \mathbb{F}$ in esattamente $[\mathbb{F} : \mathbb{E}]$ modi distinti.*

Dimostrazione. Sempre per induzione su $[\mathbb{F} : \mathbb{E}]$, la base dell'induzione $[\mathbb{F} : \mathbb{E}]$ essendo anche in questo caso banale.

Osserviamo innanzitutto che se $[\mathbb{F} : \mathbb{E}] > 1$, allora $\mathbb{E} \neq \mathbb{F}$. Per la minimalità del campo di spezzamento, $\mathbb{E}$ non contiene allora tutte le radici di $f(x)$. Sia allora $\alpha \in \mathbb{F}$ una tale radice non contenuta in $\mathbb{E}$, e $q(x)$ il suo polinomio minimo — di grado $d = [\mathbb{E}(\alpha) : \mathbb{E}]$ — su $\mathbb{E}$. Allora $q(x)$ è irriducibile in $\mathbb{E}[x]$ e $q(x)|f(x)$. Come prima, un omomorfismo $\Phi : \mathbb{F} \to \mathbb{F}$ che estenda ϕ deve soddisfare

$$0 = \Phi(0) = \Phi(q(\alpha)) = q^{\phi}(\Phi(\alpha))$$

e quindi applica α in una delle radici del polinomio irriducibile $q^{\phi}(x)$. Ma dal fatto che $q(x)$ divide $f(x)$ segue che $q^{\phi}(x)$ divide $f^{\phi}(x) = f(x)$, ed in particolare ne divide uno dei fattori irriducibili — su $\mathbb{K}$! — $q_i(x)$. Poiché il polinomio $q_i(x)$ si spezza in $\mathbb{F}$ nel prodotto di fattori lineari distinti, anche $q^{\phi}(x)$ si spezza in $\mathbb{F}$ e non ha radici multiple. Quindi ci sono esattamente d radici distinte di $q^{\phi}(x)$ in $\mathbb{F}$. Per ogni radice $\beta \in \mathbb{F}$ di $q^{\phi}(x)$, abbiamo, come prima, un unico omomorfismo

$$\mathbb{E}(\alpha) \simeq \mathbb{E}[x]/(q(x)) \simeq \mathbb{E}^{\phi}[x]/(q^{\phi}(x)) \simeq \mathbb{E}^{\phi}(\beta) \hookrightarrow \mathbb{F}$$

che manda α in β ed estende $\phi : \mathbb{E} \to \mathbb{E}^{\phi} \subset \mathbb{F}$. Pertanto ϕ si estende a $\mathbb{E}(\alpha)$ in $d = [\mathbb{E}(\alpha) : \mathbb{E}]$ maniere distinte e ciascuno di questi omomorfismi si estende a $\mathbb{F}$ in $[\mathbb{F} : \mathbb{E}(\alpha)]$ modi diversi per ipotesi induttiva. Di conseguenza, ϕ ammette $[\mathbb{F} : \mathbb{E}(\alpha)][\mathbb{E}(\alpha) : \mathbb{E}] = [\mathbb{F} : \mathbb{E}]$ estensioni a tutto $\mathbb{F}$. □

Corollario 5.15. *Se $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ di un polinomio separabile, allora $|\operatorname{Gal}(\mathbb{F}/\mathbb{K})| = [\mathbb{F} : \mathbb{K}]$.*

Dimostrazione. L'inclusione $\mathrm{id} : \mathbb{K} \to \mathbb{F}$ si estende a tutto $\mathbb{F}$ in $[\mathbb{F} : \mathbb{K}]$. Queste estensioni sono tutte $\mathbb{K}$-lineari. Se $\mathbb{F}$ è il campo di spezzamento di un polinomio $f(x)$ di grado n, allora $[\mathbb{F} : \mathbb{K}] \leq n!$, e quindi $\mathbb{F}$ è un'estensione finita di $\mathbb{K}$. Ma allora, per l'Osservazione 5.12, le $[\mathbb{F} : \mathbb{K}]$ estensioni ottenute sono tutte automorfismi di $\mathbb{F}$. □

Lemma 5.16. *Sia $\mathbb{F}$ un campo, G un gruppo finito di automorfismi di $\mathbb{F}$, $\mathbb{K} = \mathbb{F}^G$. Allora $\mathbb{F}$ è un'estensione finita di $\mathbb{K}$ e $[\mathbb{F} : \mathbb{K}] \leq |G|$.*

Dimostrazione. Sia $|G| = n$. Mi basta far vedere che comunque si prendano $m > n$ elementi $\alpha_1, \ldots, \alpha_m$ in $\mathbb{F}$, questi sono $\mathbb{K}$-linearmente dipendenti, perché in tal caso $\dim_{\mathbb{K}} \mathbb{F} \leq n$. Sia

$$S = \{(c_1, c_2, \ldots, c_m) \in \mathbb{F}^m \mid c_1\sigma(\alpha_1) + \cdots + c_m\sigma(\alpha_m) = 0 \text{ per ogni } \sigma \in G\}.$$

S è l'insieme delle soluzioni di un sistema di n equazioni lineari (una per ogni $\sigma \in G$) nelle $m > n$ incognite $c_1, \ldots, c_m$. Pertanto ho sicuramente soluzioni in $\mathbb{F}^m$ non banali (cioè non nulle) del sistema. Il mio obiettivo è quello di mostrare che S possiede anche elementi non nulli tutti a coefficienti in $\mathbb{K}$. Innanzitutto osserviamo che:

- S è un $\mathbb{F}$-sottospazio vettoriale di $\mathbb{F}^n$. In particolare, se $c = (c_1, \ldots, c_m) \in S$ e $c_1 \neq 0$, posso riscalare c in modo che il suo i-esimo coefficiente sia 1.

- Se $\alpha \in \mathbb{F}$, allora $\alpha \in \mathbb{K}$ se e solo se $\sigma(\alpha) = \alpha$ per ogni $\sigma \in G$, cioè quando $\sigma(\alpha) - \alpha = 0$ per ogni σ.
- Se $c = (c_1, \dots, c_m) \in S$, e $\tau \in G$, allora anche $\tau(c) = (\tau(c_1), \dots, \tau(c_n)) \in S$. In effetti da $c_1\sigma(\alpha_1) + \cdots + c_m\sigma(\alpha_m) = 0$ segue, applicando τ ad entrambi i membri, $\tau(c_1)\tau\sigma(\alpha_1) + \cdots + \tau(c_m)\tau\sigma(\alpha_m) = 0$, e quindi $\tau(c)$ soddisfa tutte le equazioni lineari che definiscono S, opportunamente permutate dall'azione di τ.

A meno di permutare gli elementi α_i, possiamo allora supporre che $c = (1, c_2, \dots, c_m)$ sia un elemento di S con un numero di coefficienti nulli massimo tra gli elementi non nulli di S. Allora anche $\tau(c) = (1, \tau(c_2), \dots, \tau(c_m)) \in S$ e quindi anche $\tau(c) - c = (0, \tau(c_2) - c_2, \dots, \tau(c_m) - c_m) \in S$. Si osserva subito che $\tau(c) - c$ ha almeno un coefficiente nullo in più rispetto a c, e per la scelta di c si ha allora che $\tau(c_i) - c_i = 0$ per $i = 2, \dots, m$. In altre parole $c_i \in \mathbb{K}$ per ogni $i = 2, \dots, m$ e quindi c è un elemento non nullo di S con coefficienti tutti in $\mathbb{K}$. □

Proposizione 5.17. *Se G è un gruppo finito di automorfismi del campo $\mathbb{F}$, e $\mathbb{K} = \mathbb{F}^G$, allora $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) = G$ e $[\mathbb{F} : \mathbb{K}] = |G|$.*

Dimostrazione. Gli elementi di G fissano il sottocampo $\mathbb{F}^G$ elemento per elemento, e quindi $G \subset \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Per il lemma appena dimostrato, abbiamo $[\mathbb{F} : \mathbb{K}] \leq |G| \leq |\mathrm{Gal}(\mathbb{F}/\mathbb{K})|$. Ma per il Corollario 5.13, sappiamo che $|\mathrm{Gal}(\mathbb{F}/\mathbb{K})| \leq [\mathbb{F} : \mathbb{K}]$ e quindi tutte le maggiorazioni sono uguaglianze. In particolare $|G| = |\mathrm{Gal}(\mathbb{F}/\mathbb{K})|$, da cui $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. □

Corollario 5.18. *Se $\mathbb{K} \subset \mathbb{F}$ è un'estensione di campi, e $|\mathrm{Gal}(\mathbb{F}/\mathbb{K})| = [\mathbb{F} : \mathbb{K}]$, allora $\mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K})} = \mathbb{K}$.*

Dimostrazione. Sia $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Allora $[\mathbb{F} : \mathbb{F}^G] = |G|$ per la proposizione precedente, e $|G| = [\mathbb{F} : \mathbb{K}]$ per ipotesi, pertanto $[\mathbb{F} : \mathbb{F}^G] = [\mathbb{F} : \mathbb{K}]$. Poiché $\mathbb{K} \subset \mathbb{F}^G$, concludiamo che $\mathbb{K} = \mathbb{F}^G$. □

Corollario 5.19. *Se $\mathbb{K} \subset \mathbb{F}$ è un'estensione di campi, allora $|\mathrm{Gal}(\mathbb{F}/\mathbb{K})|$ divide $[\mathbb{F} : \mathbb{K}]$.*

Dimostrazione. Se $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, abbiamo $\mathbb{K} \subset \mathbb{F}^G \subset \mathbb{F}$, e $[\mathbb{F} : \mathbb{F}^G] = |G|$. Pertanto, $[\mathbb{F} : \mathbb{K}]$ è un multiplo di $|G|$. □

Lemma 5.20. *Sia G un gruppo finito di automorfismi di un campo $\mathbb{F}$, $\mathbb{K} = \mathbb{F}^G$, $\alpha \in \mathbb{F}$, $q(x) \in \mathbb{K}$ il polinomio minimo di α su $\mathbb{K}$. Allora $q(x)$ si spezza in $\mathbb{F}$ ed è separabile.*

Dimostrazione. Se $\alpha \in \mathbb{F}$, l'orbita $G.\alpha = \{\sigma(\alpha) \,|\, \sigma \in G\}$ è un sottoinsieme finito di $\mathbb{F}$ — sappiamo addirittura che la sua cardinalità divide $|G|$. Il polinomio $f(x) = \prod_{\beta \in G.\alpha}(x - \beta)$ è invariante per l'azione degli elementi di G sui suoi coefficienti, poiché l'azione di G non fa altro che permutare i fattori $x - \beta$ tra loro. Pertanto $f(x)$ ha i suoi coefficienti in $\mathbb{F}^G = \mathbb{K}$, e di conseguenza $f(x)$ si spezza in $\mathbb{F}$ con radici tutte distinte. Il polinomio minimo $q(x)$ di α su $\mathbb{K}$ deve allora dividere $f(x)$: ne segue che anche $q(x)$ si spezza in $\mathbb{F}$, con radici tutte distinte, ed è quindi separabile. □

Proposizione 5.21. *Se G è un gruppo finito di automorfismi del campo $\mathbb{F}$, allora $\mathbb{F}$ è un'estensione finita, normale e separabile di $\mathbb{F}^G$.*

Dimostrazione. Sappiamo già che $[\mathbb{F} : \mathbb{K}] = |G|$ e quindi $\mathbb{F}$ è un'estensione finita di $\mathbb{K}$. Per il lemma precedente, ogni elemento di $\mathbb{F}$ ha un polinomio minimo su $\mathbb{K}$ che si spezza in $\mathbb{F}$. Ma ogni polinomio irriducibile $q(x) \in \mathbb{K}$ che ha una radice in $\mathbb{F}$ ne è il polinomio minimo, e si spezza quindi in $\mathbb{F}$. □

Dimostrazione del Teorema 5.9: Il Corollario 5.15 mostra che (1) ⇒ (2). Il Corollario 5.18 mostra che (2) ⇒ (3). Se $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, e $\mathbb{K} = \mathbb{F}^G$, la Proposizione 5.21 mostra che $\mathbb{F}$ è un'estensione normale e separabile di $\mathbb{K}$. Basta quindi mostrare che ogni estensione finita normale e separabile $\mathbb{K} \subset \mathbb{F}$ si ottiene come campo di spezzamento su $\mathbb{K}$ di un polinomio separabile.

Se $\mathbb{K} \subset \mathbb{F}$ è un estensione finita, possiamo trovare $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ in modo che $\mathbb{F} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Se l'estensione è separabile, ogni α_i soddisfa un polinomio separabile

$q_i(x) \in \mathbb{K}$. Poiché l'estensione è normale, tutti i $q_i(x)$ si spezzano in $\mathbb{F}$, e quindi $\mathbb{F}$ è il campo di spezzamento del prodotto $q_1(x) \dots q_n(x) \in \mathbb{K}[x]$, che è ancora separabile. □

Un'estensione (finita) $\mathbb{K} \subset \mathbb{F}$ si dice *di Galois* se è normale e separabile. Chiaramente, per verificare che un'estensione finita sia di Galois, è sufficiente controllare una delle quattro proprietà equivalenti elencate nel Teorema 5.9.

Esercizi:

(1) Mostrare che il prodotto di polinomi separabili è separabile.
(2) Mostrare che un polinomio irriducibile è separabile se e solo se non ha radici multiple nel suo campo di spezzamento.
(3) Mostrare che un divisore di un polinomio separabile è separabile.
(4) Mostrare che se un polinomio $f(x) \in \mathbb{K}[x]$ è separabile su $\mathbb{K}$, allora è separabile in ogni estensione di $\mathbb{K}$.
(5) Mostrare che un polinomio $f(x) \in \mathbb{K}[x]$ separabile su $\mathbb{K}$ può non essere separabile su un sottocampo di $\mathbb{K}$.
(6) Mostrare che il polinomio $f(x)$ costruito nel Lemma 5.20 è il polinomio irriducibile di α.
(7) Mostrare che l'estensione ciclotomica $\mathbb{Q} \subset \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/n}$ è di Galois, e calcolarne il gruppo di Galois.
(8) Mostrare che l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ è di Galois, e calcolarne il gruppo di Galois.
(9) Mostrare che un'estensione $\mathbb{K} \subset \mathbb{F}$ di campi finiti è sempre di Galois, e descriverne il gruppo di Galois.
(10) Siano $\mathbb{K} \subset \mathbb{E} \subset \mathbb{F}$ campi. Mostrare che se $\mathbb{F}$ è un'estensione di Galois di $\mathbb{K}$, allora è anche un'estensione di Galois di $\mathbb{E}$, mentre il viceversa non è vero in generale. Mostrare inoltre che se $\mathbb{E}$ è un'estensione di Galois di $\mathbb{K}$ e $\mathbb{F}$ è un'estensione di Galois di $\mathbb{E}$, non è detto che $\mathbb{F}$ sia un'estensione di Galois di $\mathbb{K}$.

5.2. **La corrispondenza di Galois.** Il fatto che, per un'estensione (finita) di Galois $\mathbb{K} \subset \mathbb{F}$, si abbia $\mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K})} = \mathbb{K}$ è solo la punta di un'iceberg, che permette di mettere in corrispondenza sottoestensioni di $\mathbb{F}$ con sottogruppi di $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Enuncio subito il cosiddetto Teorema fondamentale della Teoria di Galois.

Teorema 5.22. *Sia $\mathbb{K} \subset \mathbb{F}$ un'estensione finita di Galois. Allora esiste una corrispondenza biunivoca tra estensioni intermedie $\mathbb{K} \subset \mathbb{E} \subset \mathbb{F}$ e sottogruppi $H < \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ data da $\mathbb{E} \mapsto \mathrm{Gal}(\mathbb{F}/\mathbb{E})$, $H \mapsto \mathbb{F}^H$. Inoltre, $\mathbb{E}$ è un'estensione normale di $\mathbb{K}$ se e solo se il gruppo corrispondente H è un sottogruppo normale di $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$, ed in tal caso $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \simeq \mathrm{Gal}(\mathbb{F}/\mathbb{K})/\mathrm{Gal}(\mathbb{F}/\mathbb{E})$.*

Dimostrazione. Innanzitutto, $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ è un sottogruppo di $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$, poiché è costituito da automorfismi di $\mathbb{F}$ che fissano $\mathbb{E}$, e quindi anche $\mathbb{K} \subset \mathbb{E}$, elemento per elemento, ed è un sottoinsieme chiaramente chiuso rispetto alle operazioni di gruppo. Inoltre, se $H < \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, allora gli elementi di H fissano $\mathbb{K}$ elemento per elemento, e quindi $\mathbb{F}^H$ è un sottocampo di $\mathbb{F}$ che contiene $\mathbb{K}$.

Dobbiamo quindi far vedere che le due applicazioni sono una l'inversa dell'altra. $\mathrm{Gal}(\mathbb{F}/\mathbb{F}^H) = H$ è già stato mostrato nella Proposizione 5.17. Rimane da mostrare che $\mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{E})} = \mathbb{E}$: questo è falso in generale, ma segue dal Teorema 5.9 se $\mathbb{F}$ è un'estensione di Galois di $\mathbb{E}$. Ad ogni modo, poiché $\mathbb{F}$ è un'estensione di Galois di $\mathbb{K}$, $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ di un polinomio separabile $f(x) \in \mathbb{K}$; ma allora ne è il campo di spezzamento di $f(x)$ — che rimane separabile come elemento di $\mathbb{E}[x]$ — anche su $\mathbb{E}$.

Rimane da dimostrare solo l'affermazione sulla normalità. Prima di farlo, abbiamo bisogno di una descrizione diversa della normalità di un'estensione:

Lemma 5.23. *Se $\mathbb{K} \subset \mathbb{E} \subset \mathbb{F}$ campi, e $\mathbb{F}$ è un'estensione di Galois di $\mathbb{K}$, allora $\mathbb{E}$ è un'estensione normale di $\mathbb{K} \Leftrightarrow \sigma(E) \subset E$ per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \Leftrightarrow \sigma(E) \subset E$ per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$.*

Dimostrazione. Se $\sigma(E) = E$ per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, allora $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è un gruppo di automorfismi del campo $\mathbb{E}$ che fissa $\mathbb{K}$ elemento per elemento. Ma allora l'estensione $\mathbb{E}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K})} \subset \mathbb{E}$ è un'estensione di Galois. Ad ogni modo, $\mathbb{K} \subset \mathbb{E}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K})} \subset \mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K})} = \mathbb{K}$.

Viceversa, supponiamo che $\mathbb{E}$ sia un'estensione normale di $\mathbb{K}$, e sia $\alpha \in \mathbb{E}$. Allora ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ deve mandare α in un'altra radice del suo polinomio minimo su $\mathbb{K}$. Poiché $\mathbb{E}$ è un'estensione normale di $\mathbb{K}$, ogni altra radice di tale polinomio deve giacere in $\mathbb{E}$, e quindi $\sigma(\alpha) \in \mathbb{E}$ per ogni $\alpha \in \mathbb{E}$, cioè $\sigma(\mathbb{E}) \subset \mathbb{E}$ per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$.

L'equivalenza di $\sigma(E) \subset E$ con $\sigma(E) = E$ segue dall'Osservazione 5.12 e dal fatto che le estensioni sono tutte finite. □

Possiamo adesso concludere la dimostrazione del teorema. Dire che $\sigma(\alpha) = \alpha$ è la stessa cosa che dire che $\tau\sigma\tau^{-1}(\tau(\alpha)) = \tau(\alpha)$. Pertanto $\tau(\mathbb{F}^H) = \mathbb{F}^{\tau H \tau^{-1}}$. Ma allora $H \lhd \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \Rightarrow \tau(\mathbb{F}^H) = \mathbb{F}^H$ e quindi $\mathbb{F}^H$ è conservato da ogni elemento $\tau \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ ed è pertanto un'estensione normale di $\mathbb{K}$. Viceversa, se $\mathbb{F}^H$ è un'estensione normale di $\mathbb{K}$, allora $\mathbb{F}^H = \tau(\mathbb{F}^H) = F^{\tau H \tau^{-1}}$ e quindi per la corrispondenza di Galois, $H = \tau H \tau^{-1}$ per ogni $\tau \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. In altre parole, $H \lhd \mathrm{Gal}(\mathbb{F}/\mathbb{K})$.

Una volta che sappiamo che $\sigma(\mathbb{E}) = \mathbb{E}$ per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, l'applicazione $R : \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ che associa a σ la sua restrizione $\sigma|_{\mathbb{E}}$ risulta ben definita, ed è chiaramente un omomorfismo di gruppi (la restrizione della composizione coincide con la composizione delle restrizioni!), che è suriettivo per la Proposizione 5.14. Il nucleo di questo omomorfismo è dato dalle σ che fissano $\mathbb{E}$ elemento per elemento, e quindi applicando il teorema di isomorfismo ad R si ottiene $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \simeq \mathrm{Gal}(\mathbb{F}/\mathbb{K})/\mathrm{Gal}(\mathbb{F}/\mathbb{E})$. □

Osservazione 5.24. La corrispondenza di Galois traduce il grado di un'estensione nell'indice del sottogruppo corrispondente. Effettivamente, poiché $\mathrm{Gal}(\mathbb{F}/\mathbb{F}^H) = H$, si ha che se la sottoestensione $\mathbb{E}$ è in corrispondenza con il sottogruppo $H \subset G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, allora $[\mathbb{F} : \mathbb{E}] = |H|$ e di conseguenza $[\mathbb{E} : \mathbb{K}] = [G : H]$. Utilizzando queste informazioni, è facile mostrare che se $\mathbb{K} \subset \mathbb{E}_1 \subset \mathbb{E}_2 \subset \mathbb{F}$ corrispondono ai gruppi $G > H_1 > H_2 > \{\mathrm{id}\}$ rispettivamente, allora $[\mathbb{E}_2 : \mathbb{E}_1] = [H_1 : H_2]$.

5.3. **Caratterizzazione degli algebrici costruibili con riga e compasso.** Le tecniche che abbiamo appena visto ci permettono di descrivere in dettaglio quali siano gli algebrici costruibili per riga e compasso.

Teorema 5.25. *Un algebrico $\alpha \in \mathbb{R}$ è costruibile per riga e compasso se e solo se è contenuto in un'estensione normale finita $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{C}$ tale che $[\mathbb{F} : \mathbb{Q}]$ è una potenza di 2.*

Dimostrazione. La coniugazione complessa è un elemento di $G = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ che coincide con l'identità quando $\mathbb{F} \subset \mathbb{R}$; genera un sottogruppo H_0 di ordine 1 o 2, e per mostrare che $\alpha \in \mathbb{F}$ è costruibile con riga e compasso è necessario trovare una catena di sottogruppi

$$H_0 \subset H_1 \subset \cdots \subset H_n = G,$$

tali che $[H_i : H_{i-1}] = 2$ per ogni $i = 1, \ldots, n$. Questo è comunque sempre possibile, dal momento che in un p-gruppo finito — e G è un 2-gruppo finito — il normalizzatore di ciascun sottogruppo proprio lo contiene propriamente.

Viceversa, supponiamo che $\alpha \in \mathbb{R}$ sia costruibile con riga e compasso. Allora è un algebrico, e il suo grado è una potenza di 2. Sia $\mathbb{F}$ il campo di spezzamento del suo polinomio minimo: ogni altra radice del suo polinomio minimo è esprimibile per radicali quadratici. Allora possiamo procedere come nella dimostrazione della Proposizione 7.8 e mostrare che $\mathbb{F}$ si ottiene da $\mathbb{Q}$ per estensioni successive di grado 2; il grado di $\mathbb{F}$ su $\mathbb{Q}$ è pertanto una potenza di 2. □

Esercizi:

(1) Utilizzare la corrispondenza di Galois per determinare tutti i sottocampi di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(2) Utilizzare la corrispondenza di Galois per mostrare che $\mathbb{Q}(\sqrt{-7})$ e $\mathbb{Q}(\cos(2\pi/7))$ sono gli unici sottocampi di $\mathbb{Q}(\zeta_7)$.

(3) Utilizzare la corrispondenza di Galois per determinare tutte le estensioni intermedie di $\mathbb{F}_p \subset \mathbb{F}_{p^6}$, dove p è un primo.
(4) Descrivere il gruppo di Galois dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ e mostrare che $\sqrt{2} + \sqrt{3} + \sqrt{5}$ non giace in nessuna estensione intermedia. Concludere che $\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
(5) Mostrate che un'estensione di Galois $\mathbb{K} \subset \mathbb{F}$ finita contiene solo un numero finito di estensioni intermedie, e che se $\alpha \in \mathbb{F}$ non appartiene all'unione di tali estensioni, allora $\mathbb{K}(\alpha) = \mathbb{F}$.
(6) Dimostrate il teorema dell'elemento primitivo: se $\mathbb{K} \subset \mathbb{F}$ è un'estensione finita separabile (attenti: nessuno vi ha detto che sia di Galois!) allora esiste $\gamma \in \mathbb{F}$ tale che $\mathbb{F} = \mathbb{K}(\gamma)$. — effettivamente nessuno vi ha detto neppure che i campi $\mathbb{K}, \mathbb{F}$ siano infiniti...

6. Costruibilità per radicali

6.1. **Estensioni di Kummer.** Il nostro prossimo obiettivo è quello di studiare la risolubilità per radicali delle equazioni algebriche in una incognita. Per motivi tecnici, è conveniente utilizzare come campo base un campo che, di volta in volta, contenga tutte le radici dell'unità che possano servire. In quello che segue, quindi, il campo base $\mathbb{K}_0$ ha caratteristica 0 e tipicamente NON è il campo dei numeri razionali.

Proposizione 6.1. *Sia $a \in \mathbb{K}_0$, p un numero primo, e supponiamo che $\mathbb{K}_0$ contenga tutte le radici p-esime dell'unità. Allora l'estensione $\mathbb{K}_0 \subset \mathbb{K}_0(\sqrt[p]{a})$ è normale, e quando $\mathbb{K}_0(\sqrt[p]{a}) \neq \mathbb{K}_0$, allora $[\mathbb{K}_0(\sqrt[p]{a}) : \mathbb{K}_0] = p$ e $\mathrm{Gal}(\mathbb{K}_0(\sqrt[p]{a})/\mathbb{K}_0) \simeq \mathrm{C}_p$.*

Dimostrazione. Sia $\zeta \in \mathbb{K}_0$ una radice p-esima primitiva dell'unità. Le radici del polinomio $x^p - a$ sono $\sqrt[p]{a}$, $\zeta\sqrt[p]{a}$, $\dots$, $\zeta^{p-1}\sqrt[p]{a}$ e sono tutte contenute in $\mathbb{K}_0(\sqrt[p]{a})$, che è pertanto il campo di spezzamento di $x^p - a$ su $\mathbb{K}_0$. L'estensione $\mathbb{K}_0 \subset \mathbb{K}_0(\sqrt[p]{a})$ è quindi di Galois di grado $\leq p$ — non sappiamo se il polinomio $x^p - a$ sia o meno irriducibile!

Se $\mathbb{K}_0 \neq \mathbb{K}_0(\sqrt[p]{a})$, allora $\mathrm{Gal}(\mathbb{K}_0(\sqrt[p]{a})/\mathbb{K}_0)$ contiene almeno un elemento $\sigma \neq \mathrm{id}$. Allora $\sigma(\sqrt[p]{a}) \neq \sqrt[p]{a}$, e quindi $\sigma(\sqrt[p]{a}) = \zeta^i\sqrt[p]{a}$ per qualche $0 < i < p$. Si vede facilmente che σ deve avere ordine p e quindi $[\mathbb{K}_0(\sqrt[p]{a}) : \mathbb{K}_0] = |\mathrm{Gal}(\mathbb{K}_0(\sqrt[p]{a})/\mathbb{K}_0)| \geq p$. Il gruppo di Galois dell'estensione ha ordine primo, ed è quindi ciclico. □

Proposizione 6.2. *Sia $\mathbb{K}_0 \subset \mathbb{F}$ un'estensione di Galois di grado primo p, e supponiamo che $\mathbb{K}_0$ contenga tutte le radici p-esime dell'unità. Allora esiste $a \in \mathbb{K}_0$ tale che $\mathbb{F} = \mathbb{K}_0(\sqrt[p]{a})$.*

Dimostrazione. Scegliamo $\alpha \in \mathbb{F}$, $\alpha \notin \mathbb{K}_0$, e poniamo $\beta_i = \sum_{j=0}^{p-1} \zeta^{ij}\sigma^j(\alpha), i = 0, \dots, p-1$. Applicando σ a β_i si vede che $\sigma(\beta_i) = \zeta^{-i}\beta_i$; vogliamo però scongiurare la possibilità che $\beta_i = 0$ per ogni $i \neq 0$. Il sistema

$$\begin{cases} x_0 + & x_1 + & x_2 + & \cdots + & x_{p-1} = & \beta_0 \\ x_0 + & \zeta\, x_1 + & \zeta^2\, x_2 + & \cdots + & \zeta^{p-1}\, x_{p-1} = & \beta_1 \\ x_0 + & \zeta^2\, x_1 + & \zeta^{2\cdot 2}\, x_2 + & \cdots + & \zeta^{2(p-1)}\, x_{p-1} = & \beta_2 \\ \vdots & & & \vdots & & \vdots \\ x_0 + & \zeta^{p-1} x_1 + & \zeta^{(p-1)\cdot 2} x_2 + & \cdots + & \zeta^{(p-1)^2} x_{p-1} = & \beta_{p-1} \end{cases}$$

ammette $x_j = \sigma^j(\alpha)$ come soluzione. Tale soluzione è unica, perché il determinante della matrice dei coefficienti è un determinante di Vandermonde, che è diverso da zero perché $1, \zeta, \dots, \zeta^{p-1}$ sono tutti distinti. Si vede immediatamente che $\beta_0 \in \mathbb{F}^\sigma = \mathbb{K}_0$. Se $\beta_i \in \mathbb{K}_0$ per ogni altro i, il sistema avrebbe tutti i coefficienti in $\mathbb{K}_0$ e sarebbe in $\mathbb{K}_0$ anche la sua soluzione: un assurdo con la scelta di $\alpha \notin \mathbb{K}_0$. Di conseguenza, almeno un $\beta_i, i \neq 0$, non appartiene a $\mathbb{K}_0$ ed è in particolare non nullo.

Ma allora, da $\sigma(\beta_i) = \zeta^{-i}\beta_i$ segue $\sigma(\beta_i^p) = (\zeta^{-i}\beta_i)^p = \beta_i^p$ e quindi β_i^p appartiene al campo fisso $\mathbb{K}_0$ di σ. In altre parole, $\beta_i^p = a$ è un elemento di $\mathbb{K}_0$ e $\beta_i \notin \mathbb{K}_0$ è la sua radice p-esima. Poiché $\mathbb{K}_0 \subsetneq \mathbb{K}_0(\beta_i)$, e $[\mathbb{F} : \mathbb{K}_0] = p$ è primo, allora $\mathbb{F} = \mathbb{K}_0(\beta_i) = \mathbb{K}_0(\sqrt[p]{a})$. □

In conclusione, le estensioni normali di $\mathbb{K}_0$ di grado p primo sono tutte e sole quelle che si ottengono aggiungendo una radice p-esima di un elemento di $\mathbb{K}_0$ — a patto che tale elemento non sia una potenza p-esima di qualcosa.

6.2. **Costruibilità per radicali.** Iniziamo con una definizione che illustra cosa intendiamo per "esprimere un numero per radicali" .

Definizione 6.3. Sia $\mathbb{K}_0 \subset \mathbb{F}$ un'estensione di campi. Un elemento $\alpha \in \mathbb{F}$ si *esprime per radicali* se esiste una catena di sottoestensioni di $\mathbb{F}$

$$\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_{n-1} \subset \mathbb{K}_n,$$

con la proprietà che $\alpha \in \mathbb{K}_n$ e $\mathbb{K}_{i+1} = \mathbb{K}_i(\sqrt[n_i]{a_i})$ per un'opportuna scelta di $a_i \in \mathbb{K}_i, n_i \in \mathbb{N}$.

In pratica, ad ogni passaggio, stiamo prendendo una radice n-esima di qualche espressione razionale in radicali precedenti. Chiaramente, $\mathbb{K}_n$ è un'estensione finita di $\mathbb{K}_0$ e quindi solo elementi di $\mathbb{F}$ che siano algebrici su $\mathbb{K}_0$ possono essere espressi per radicali.

Proposizione 6.4. *Sia $\mathbb{K}_0 \subset \mathbb{F}$ un'estensione di campi, e supponiamo che $\mathbb{K}_0$ contenga tutte le radici p-esime dell'unità, per ogni primo p che divida $[\mathbb{F} : \mathbb{K}_0]$. Allora $\alpha \in \mathbb{F}$ è esprimibile per radicali se e solo se esiste una catena di estensioni*

$$\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_{n-1} \subset \mathbb{K}_n \subset \mathbb{F},$$

tali che $\mathbb{K}_i \subset \mathbb{K}_{i+1}$ è un'estensione normale di grado p_i primo per ogni i.

Dimostrazione. Non perdiamo di generalità se ipotizziamo che ad ogni passo sia aggiunta una radice di ordine primo di un elemento del campo precedente, in quanto se $N = p_1 \cdot \ldots \cdot p_r$ è una fattorizzazione in primi di N possiamo ottenere $a^{1/N}$ come $(\ldots(a^{1/p_1})^{\cdots})^{1/p_r}$. L'affermazione segue allora dalle Proposizioni 6.1 e 6.2. □

Il passo successivo è quello di utilizzare la corrispondenza di Galois per controllare l'esistenza di una tale catena di estensioni. Dal momento che il numero che vogliamo esprimere per radicali è algebrico, possiamo trasferire il problema sul campo di spezzamento del suo polinomio minimo.

7. Risolubilità di un'equazione per radicali

7.1. **Polinomi simmetrici.** Se A è un anello (commutativo, con unità) possiamo definire, sull'anello $A[x_1, \ldots, x_n]$, un'azione[1] del gruppo simmetrico S_n per permutazione delle n indeterminate. Infatti, se poniamo

$$f^\sigma(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

si ottiene immediatamente

$$(f^\sigma)^\tau(x_1, \ldots, x_n) = f^\sigma(x_{\tau(1)}, \ldots, x_{\tau(n)}) = f(x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(n))}) = f^{\sigma\tau}(x_1, \ldots, x_n).$$

Un polinomio $f(x) \in A[x_1, \ldots, x_n]$ si dice allora *simmetrico* se è stabile per l'azione di S_n, cioè se $f^\sigma = f$ per ogni $\sigma \in \mathrm{S}_n$. Sono, ad esempio, elementi simmetrici di $\mathbb{Z}[x_1, x_2, x_3]$ i polinomi $x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1x_2 + x_1x_3 + x_2x_3$, come anche tutte le costanti. L'insieme degli polinomi simmetrici a coefficienti in A in n indeterminate si indica con $A[x_1, \ldots, x_n]^{\mathrm{S}_n}$.

Definizione 7.1. I coefficienti del prodotto

$$(X+x_1)(X+x_2)\ldots(X+x_n) = X^n + \sigma_1^n(x_1, \ldots, x_n)X^{n-1} + \cdots + \sigma_{n-1}^n(x_1, \ldots, x_n)X + \sigma_n^n(x_1, \ldots, x_n)$$

sono polinomi simmetrici in n indeterminate, e sono detti *polinomi simmetrici elementari*. Si ha: $\sigma_1^n = x_1 + x_2 + \cdots + x_n$, e più in generale

$$\sigma_k^n = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

[1] Si tratta effettivamente di un'azione destra, e non sinistra, di S_n. Se si vuole trasformarla in un'azione sinistra, bisogna comporla con un antiautomorfismo di S_n, come ad esempio l'applicazione che manda ogni elemento nel suo inverso

Ogni volta che il numero delle indeterminate sia evidente dal contesto, sopprimeremo il relativo indice, e scriveremo σ_k invece di σ_k^n.

Il nostro obiettivo è quello di mostrare come ogni polinomio simmetrico possa esprimersi per mezzo dei polinomi simmetrici elementari.

Teorema 7.2. *Se $f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]^{\mathrm{S}_n}$, allora esiste un unico polinomio $q(t_1, \dots, t_n) \in A[t_1, \dots, t_n]$ tale che $f(x_1, \dots, x_n) = q(\sigma_1, \dots, \sigma_n)$.*

Prima di procedere con la dimostrazione, introduciamo un ordinamento $\prec$ sui monomi nelle n indeterminate $x_1, \dots, x_n$: monomi di grado diverso sono ordinati per grado, mentre I monomi dello stesso grado sono invece ordinati lessicograficamente. In altre parole:

$$x_1^{a_1} \dots x_n^{a_n} \prec x_1^{b_1} \dots x_n^{b_n}$$

se $a_1 + \dots + a_n < b_1 + \dots + b_n$, oppure se $a_1 + \dots + a_n = b_1 + \dots + b_n$, ma esiste k tale che $a_k < b_k$ e $a_i = b_i$ per ogni $i < k$. Questo è evidentemente un ordinamento totale sull'insieme dei monomi, ed inoltre ogni monomio ha soltanto un numero finito di predecessori, in quanto i monomi di grado $< N$ sono in numero finito per ogni $N \in \mathbb{N}$. Il monomio minimo è quello di grado 0, cioè 1.

Un'altra proprietà importante di questo ordinamento è che ogni polinomio possiede, nella sua espressione, un unico monomio massimo rispetto a $\prec$. Per quanto riguarda i polinomi simmetrici elementari, che sono omogenei, il monomio massimo di σ_i è $x_1 x_2 \dots x_i$, e quindi il monomio di grado massimo di $(\sigma_1)^{h_1} \dots (\sigma_n)^{h_n}$ è

$$(x_1)^{h_1} (x_1 x_1)^{h_2} \dots (x_1 x_2 \dots x_n)^{h_n} = x_1^{h_1 + \dots + h_n} x_2^{h_2 + \dots + h_n} \dots x_{n-1}^{h_{n-1} + h_n} x_n^{h_n}.$$

Dimostrazione. Dimostriamo l'enunciato per induzione sul massimo monomio presente con coefficiente non nullo in $f(x_1, \dots, x_n)$. La base dell'induzione si ha quando il massimo monomio è 1, e quindi quando f è un polinomio costante: in tale situazione basta prendere $q = f$, e non c'è nulla da dimostrare.

Per quanto riguarda il passo induttivo, dal momento che $f(x_1, \dots, x_n)$ è un polinomio simmetrico, il massimo monomio che appare nella sua espressione deve essere della forma $a \cdot x_1^{k_1} \dots x_n^{k_n}$, con $k_1 \geq k_2 \geq \dots \geq k_n$, in quanto se un monomio compare in f, compaiono anche tutti i monomi che si ottengono permutandone gli esponenti. Questo è anche il monomio massimo del polinomio simmetrico

$$p(\sigma_1, \dots, \sigma_n) = a \cdot (\sigma_1)^{k_1 - k_2} (\sigma_2)^{k_2 - k_3} \dots (\sigma_{n-1})^{k_{n-1} - k_n} (\sigma_n)^{k_n}.$$

Il polinomio $f(x_1, \dots, x_n) - p(\sigma_1, \dots, \sigma_n$ ha monomio massimo inferiore a quello di f, e si esprime come polinomio in $\sigma_1, \dots, \sigma_n$ per ipotesi induttiva.

Rimane solo da mostrare che il polinomio q è unico: per fare questo è sufficiente mostrare che se $q(\sigma_1, \dots, \sigma_n) = 0$, allora q è il polinomio nullo. Abbiamo già visto che il polinomio simmetrico $\sigma_1^{h_1} \dots \sigma_n^{h_n}$ ha monomio di grado massimo

$$(x_1)^{h_1} (x_1 x_1)^{h_2} \dots (x_1 x_2 \dots x_n)^{h_n} = x_1^{h_1 + \dots + h_n} x_2^{h_2 + \dots + h_n} \dots x_{n-1}^{h_{n-1} + h_n} x_n^{h_n}.$$

Pertanto, se $t_1^{h_1} \dots t_n^{h_n}$ è il monomio di grado massimo in $q(t_1, \dots, t_n) \neq 0$, allora il monomio

$$(x_1)^{h_1} (x_1 x_1)^{h_2} \dots (x_1 x_2 \dots x_n)^{h_n} = x_1^{h_1 + \dots + h_n} x_2^{h_2 + \dots + h_n} \dots x_{n-1}^{h_{n-1} + h_n} x_n^{h_n}$$

non può avere coefficiente nullo in $q(\sigma_1, \dots, \sigma_n)$, che è pertanto non nullo. □

7.2. **Risolubilità di gruppi finiti.** In questo paragrafo richiamiamo alcune definizioni e proprietà che riguardano i gruppi risolubili finiti.

Definizione 7.3. Il *sottogruppo derivato* G' di un gruppo G è il sottogruppo generato da tutti gli elementi della forma $ghg^{-1}h^{-1}$, al variare di $g, h \in G$.

Abbiamo fatto vedere nella prima parte del corso che G' è il più piccolo sottogruppo normale di G a quoziente abeliano. In particolare, G è abeliano se e soltanto se $G' = \{\mathrm{id}\}$.

Definizione 7.4. Se G è un gruppo, definiamo $G^{(0)} = G$, $G^{(n+1)} = (G^{(n)})'$ se $n \geq 0$. Allora G si dice *risolubile* se $G^{(N)} = \{\mathrm{id}\}$ per valori sufficientemente grandi di N.

Proposizione 7.5. *Ogni gruppo abeliano è risolubile. Sottogruppi e quozienti di un gruppo risolubile sono anch'essi risolubili. In particolare, se $N \lhd G$, allora G è risolubile se e solo se N, G/N sono entrambi risolubili.*

Forniremo ora una caratterizzazione dei gruppi risolubili che sarà essenziale al momento di considerare l'esprimibilità dei numeri algebrici per radicali.

Teorema 7.6. *Un gruppo G è risolubile se e solo se è possibile trovare una catena di sottogruppi*

$$\{\mathrm{id}\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{r-1} \lhd H_r = G$$

in modo che ciascun H_i abbia indice primo in H_{i+1} per ogni $i = 0, \ldots, r-1$.

Dimostrazione. Supponiamo esista una tale catena, e mostriamo che H_n è risolubile per induzione su n. H_0 è il gruppo banale, che è banalmente risolubile. Per mostrare la risolubilità di $H_n, n > 0$ basta osservare che $H_{n-1} \lhd H_n$ è risolubile per ipotesi induttiva, mentre il quoziente H_n/H_{n-1} ha ordine primo, ed è quindi ciclico e di conseguenza abeliano. Poiché $H_r = G$, concludiamo che G è risolubile.

Per mostrare il viceversa, osserviamo innanzitutto che se G è abeliano, allora una tale catena di sottogruppi esiste. Questo si può dimostrare per induzione su $|G|$, scegliendo un elemento $g \in G$ di ordine primo — che esiste per il Teorema di Cauchy — ed applicando l'ipotesi induttiva al gruppo $G/(g)$, utilizzando la corrispondenza tra sottogruppi di $G/(g)$ e sottogruppi di G che contengono (g). La normalità di ciascun sottogruppo nel successivo è ovvia, in quanto G è abeliano, e di conseguenza lo sono tutti i sottogruppi H_i.

Per quanto riguarda il caso di un gruppo risolubile qualsiasi G, possiamo procedere per induzione su $|G|$ in maniera simile. Poiché G/G' è abeliano, otteniamo una catena di sottogruppi

$$G' = H_k \lhd H_{k+1} \lhd \cdots \lhd H_n = G$$

ciascuno normale nel successivo e di indice primo. L'ipotesi induttiva applicata al gruppo risolubile G' ci fornisce invece la parte iniziale della catena $\{\mathrm{id}\} = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G'$ con le medesime proprietà. □

7.3. **Risolubilità per radicali di un'equazione algebrica in una incognita.** Come al solito, $\mathbb{K}_0$ è un campo di caratteristica 0 che contiene tutte le radici dell'unità che possano servire.

Lemma 7.7. *Sia $\mathbb{F}$ il campo di spezzamento su $\mathbb{K}_0$ del polinomio irriducibile $q(x)$, e $\alpha \in \mathbb{F}$ una radice di $q(x)$. Allora α si esprime per radicali se e solo se ogni altra radice di $q(x)$ si esprime per radicali.*

Dimostrazione. Abbiamo già visto che l'azione di $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_0)$ sulle radici di $q(x)$ è transitiva. Allora se β è un'altra radice di $q(x)$, possiamo trovare $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K}_0)$ tale che $\sigma(\alpha) = \beta$. Se $\mathbb{K}_0 \subset \mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$ e $\mathbb{F} = \mathbb{K}(a)$ con $a^n \in \mathbb{K}, a \notin \mathbb{K}$, allora $\sigma(\mathbb{K}) \subset \sigma(\mathbb{F})$, $\sigma(\mathbb{F}) = \sigma(\mathbb{K})(\sigma(a))$, e $\sigma(a)^n = \sigma(a^n) \in \sigma(\mathbb{K})$, mentre $\sigma(a) \notin \mathbb{K}$. Pertanto, applicando σ ad una una catena di estensioni

$$\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_{n-1} \subset \mathbb{K}_n \ni \alpha,$$

come nella Definizione 6.3, si ottiene un'analoga catena

$$\mathbb{K}_0 = \sigma(\mathbb{K}_0) \subset \sigma(\mathbb{K}_1) \subset \cdots \subset \sigma(\mathbb{K}_{n-1}) \subset \sigma(\mathbb{K}_n) \ni \sigma(\alpha) = \beta.$$

□

Proposizione 7.8. *Sia $\mathbb{F}$ il campo di spezzamento su $\mathbb{K}_0$ del polinomio irriducibile $q(x)$ di grado d, e supponiamo che $\mathbb{F}$ contenga tutte le radici p-esime dell'unità, per ogni primo $p \leq d$. Allora una radice $\alpha \in \mathbb{F}$ di $q(x)$ si esprime per radicali se e solo se esiste una catena di campi*

$$\mathbb{K}_0 = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_N = \mathbb{F}$$

tali che $\mathbb{L}_i \subset \mathbb{L}_{i+1}$ è un estensione normale di grado primo per ogni $i = 0, \ldots, N-1$.

Dimostrazione. Innanzitutto, poiché $[\mathbb{F} : \mathbb{K}_0]$ divide $d!$, $\mathbb{K}_0$ contiene tutte le radici p-esime dell'unità per ogni p che divide $d!$. Sappiamo già che se α si esprime per radicali, ogni altra radice di $q(x)$ si esprime per radicali. Inoltre, se $\alpha = \alpha_0, \alpha_1, \dots, \alpha_r$ sono le radici di $q(x)$, allora $\mathbb{F} = \mathbb{K}_0(\alpha_1, \dots, \alpha_r)$. Sappiamo che ogni radice α_i appartiene ad un'estensione di $\mathbb{K}_0$ che si raggiunge aggiungendo progressivamente radici p-esime di elementi già nel campo: possiamo quindi trovare campi $\mathbb{K}_{i,j} \subset \mathbb{F},$, elementi $a_{i,j} \in \mathbb{K}_{i,j}$ e numeri primi $p_j, i = 0, \dots, r$, $j = 1, \dots, n$ in modo che

$$\mathbb{K}_0 = \mathbb{K}_{i,0} \subset \mathbb{K}_{i,1} \subset \cdots \subset \mathbb{K}_{i,n} \ni \alpha_i,$$

dove $\mathbb{K}_{i,j} = \mathbb{K}_{i,j-1}(a_{i,j})$ è un'estensione normale di $\mathbb{K}_{i,j-1}$ di grado p_j, e $a_{i,j}^{p_j} \in \mathbb{K}_{i,j-1}$.

Costruiamo ora una nuova catena di estensioni di campi, ponendo $\mathbb{L}_0 = \mathbb{K}_0$, $\mathbb{L}_{in+j} = \mathbb{L}_{in+(j-1)}(a_{i,j})$ se $i = 0, \dots, r$, $j = 1, \dots, n$. Allora $\mathbb{K}_{(r+1)n}$ contiene $\alpha_0, \dots, \alpha_r$ e coincide quindi con $\mathbb{F}$. Inoltre ogni estensione $\mathbb{L}_{in+(j-1)} \subset \mathbb{L}_{in+j}$ ha grado p_j se $a_{i,j} \notin \mathbb{L}_{in+(j-1)}$, cioè se i due campi non coincidono, e si ottiene aggiungendo una radice p_j-esima, dal momento che $a_{i,j}^{p_j} \in \mathbb{K}_{i,j-1} \subset L_{in+(j-1)}$: è pertanto un'estensione normale. Eliminando le ripetizioni, si ottiene una catena di estensioni normali di campi di grado primo. L'implicazione contraria è invece ovvia. □

Proposizione 7.9. *Sia $\mathbb{F}$ il campo di spezzamento su $\mathbb{K}_0$ del polinomio irriducibile $q(x) \in \mathbb{K}_0[x]$ di grado d, e supponiamo che $\mathbb{K}_0$ contenga tutte le radici p-esime dell'unità, per ogni primo $p \leq d$. Una radice $\alpha \in \mathbb{F}$ di $q(x)$ si esprime per radicali se e solo se $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_0)$ è risolubile.*

Dimostrazione. $\mathbb{F}$ è un'estensione di Galois di $\mathbb{K}_0$ poiché è il campo di spezzamento del polinomio — separabile, poiché siamo in caratteristica 0 — $q(x)$. Allora l'esistenza di estensioni normali nidificate ciascuna di grado primo sulla precedente è equivalente, attraverso la corrispondenza di Galois, all'esistenza di una catena decrescente di sottogruppi di $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K}_0)$, ciascuno normale nel precedente e di indice primo. Ma una tale catena esiste se e solo se G è risolubile. □

Teorema 7.10. *Sia $\mathbb{K}_0 \subset \mathbb{F}$ un'estensione di campi, $\alpha \in \mathbb{F}$ un elemento algebrico su $\mathbb{K}_0$ di grado d, e supponiamo che $\mathbb{K}_0$ contenga tutte le radici p-esime dell'unità per ogni primo $p \leq d$. Allora α si esprime per radicali se e soltanto se appartiene ad una sottoestensione finita normale $\mathbb{K}_0 \subset \mathbb{E} \subset \mathbb{F}$, il cui gruppo di Galois $\mathrm{Gal}(\mathbb{E}/\mathbb{K}_0)$ sia risolubile.*

Dimostrazione. Se α è costruibile per radicali, il campo di spezzamento del suo polinomio minimo è l'estensione normale cercata. Se invece α appartiene ad una sottoestensione normale $\mathbb{E}$ di $\mathbb{K}_0$, tale che $G = \mathrm{Gal}(\mathbb{E}/\mathbb{K}_0)$ sia risolubile, allora il campo di spezzamento del polinomio minimo di α è una sottoestensione di $\mathbb{E}$, sempre normale su $\mathbb{K}$, ed il suo gruppo di Galois è un quoziente di G, ed è pertanto anch'esso risolubile. □

7.4. **Il Teorema di Abel.** Possiamo finalmente dimostrare che il polinomio generale di grado ≥ 5 non ammette una formula risolutiva per radicali.

Teorema 7.11 (Abel)**.** *Sia $\mathbb{K}_0$ un campo di caratteristica 0, $\mathbb{K} = \mathbb{K}_0(a_1, \dots, a_n)$, dove $a_1, \dots, a_n$ sono indeterminate, e supponiamo che $\mathbb{K}_0$ contenga tutte le radici p-esime dell'unità per ogni primo $p \leq n$. Sia $\mathbb{F}$ un campo di spezzamento di $f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$ su $\mathbb{K}$; allora, se $n \geq 5$, le radici di $f(X)$ in $\mathbb{F}$ non si esprimono per radicali in termini dei coefficienti $a_1, \dots, a_n$.*

Dimostrazione. E' sufficiente mostrare che $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ non è risolubile.

Consideriamo il campo $\mathbb{F} = \mathbb{K}_0(x_1, \dots, x_n)$ delle funzioni razionali in n indeterminate a coefficienti in $\mathbb{K}_0$. Il gruppo simmetrico S_n agisce su $\mathbb{F}$ per permutazioni delle indeterminate, e per il Teorema fondamentale delle funzioni simmetriche sappiamo che $\mathbb{F}^{\mathrm{S}_n} = \mathbb{K}_0(\sigma_1, \dots, \sigma_n)$, dove $\sigma_i = \sigma_i(x_1, \dots, x_n)$ sono le funzioni simmetriche elementari. Abbiamo anche mostrato che gli elementi σ_i sono algebricamente indipendenti su $\mathbb{K}_0$, e quindi $\sigma_i \mapsto (-1)^i a_i$ fornisce un isomorfismo tra i campi $\mathbb{K}_0(\sigma_1, \dots, \sigma_n)$ e $\mathbb{K}_0(a_1, \dots, a_n)$.

Attraverso tale isomorfismo, si vede che $\mathbb{F}$ è un campo di spezzamento di $f(x)$ su $\mathbb{K}$; dal momento che il campo di spezzamento è unico a meno di isomorfismo, possiamo

dire che $\mathbb{F}$ è IL campo di spezzamento di $f(x)$ su $\mathbb{K}$. Allora $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) = \mathrm{Gal}(\mathbb{F}/\mathbb{F}^{\mathrm{S}_n}) = \mathrm{S}_n$, che non è risolubile se $n \geq 5$. □

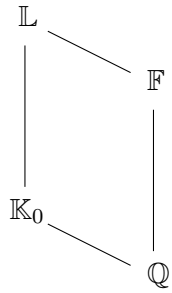
Rimane aperta la possibilità che ciascun polinomio a coefficienti in $\mathbb{K}_0$ abbia radici esprimibili per radicali, sebbene manchi una formula generale. Il calcolo del gruppo di Galois di un polinomio è spesso più agevole su $\mathbb{Q}$ che su $\mathbb{K}_0$, ed avremo quindi bisogno di un'equivalenza più raffinata tra la risolubilità di un'equazione e quella del suo gruppo di Galois.

7.5. **Un esempio esplicito di equazione non risolubile per radicali.** Sia $f(x) \in \mathbb{Q}[x]$ un polinomio del cui campo di spezzamento su $\mathbb{Q}$ siamo in grado di calcolare il gruppo di Galois G. Se $\mathbb{K}_0$ è un'estensione (finita) di $\mathbb{Q}$ che contiene tutte le radici dell'unità necessarie per la validità delle nostre dimostrazioni, possiamo anche vedere $f(x)$ come polinomio a coefficienti in $\mathbb{K}_0$. Il gruppo di Galois del campo di spezzamento corrispondente non sarà generalmente isomorfo a G.

Il nostro obiettivo è quello di mostrare che la risolubilità dei due gruppi è legata, in modo da poter studiare la risolubilità per radicali di un polinomio attraverso il suo gruppo di Galois su $\mathbb{Q}$, o su qualsiasi estensione sia più conveniente.

Proposizione 7.12. *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio di grado n, $N \in \mathbb{N}$ tale che $\mathbb{K}_0 = \mathbb{Q}(\zeta_N)$ contenga tutte le radici p-esime dell'unità per ogni primo $p \leq n$, ed indichiamo con $\mathbb{F}$ (rispettivamente $\mathbb{L}$) il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ (rispettivamente $\mathbb{K}_0$). Allora $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ è risolubile se e solo se $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_0)$ è risolubile.*

Dimostrazione. Innanzitutto, $\mathbb{K}_0$ è il campo di spezzamento su $\mathbb{Q}$ dell'N-esimo polinomio ciclotomico $\Phi_N(x)$. Pertanto, $\mathbb{L}$ è il campo di spezzamento su $\mathbb{Q}$ di $f(x)\Phi_N(x)$ e su $\mathbb{F}$ di $\Phi_N(x)$. Ciascuno dei campi in considerazione è quindi un'estensione di Galois dei campi che contiene.



Abbiamo già mostrato che $\mathrm{Gal}(\mathbb{K}_0/\mathbb{Q}) \simeq (\mathbb{Z}/(N))^\times$ è un gruppo abeliano. In maniera analoga si mostra che $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) \simeq \Gamma \subset (\mathbb{Z}/(N))^\times$. In effetti, essendo $\mathbb{L}$ il campo di spezzamento di $\Phi_N(x)$ su $\mathbb{F}$, gli elementi del gruppo di Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ sono determinati dall'immagine di ζ_N, che può essere soltanto un'altra radice primitiva N-esima dell'unità. Non possiamo concludere che $\Gamma = (\mathbb{Z}/(N))^\times$ a meno che $\Phi_N(x)$ non sia irriducibile anche su $\mathbb{F}$.

Utilizziamo ora le notazioni: $G_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{F}/\mathbb{Q}), G_0 = \mathrm{Gal}(\mathbb{L}/\mathbb{K}_0), G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Applicando la corrispondenza di Galois all'estensione $\mathbb{Q} \subset \mathbb{L}$, si ottengono $G/G_0 \simeq \mathrm{Gal}(\mathbb{K}_0/\mathbb{Q}) \simeq (\mathbb{Z}/(N))^\times$ e $G/\Gamma \simeq G_{\mathbb{Q}}$. Dal momento che sia $(\mathbb{Z}/(N))^\times$ che il suo sottogruppo Γ sono abeliani, otteniamo che la risolubilità di G_0 è equivalente a quella di G che è a sua volta equivalente a quella di $G_{\mathbb{Q}}$. Pertanto $G_{\mathbb{Q}}$ è risolubile se e soltanto se G_0 è risolubile. □

Esempio 7.13. Il polinomio $f(x) = x^5 - 80x + 5 \in \mathbb{Q}[x]$ è irriducibile per il criterio di Eisenstein. La sua derivata $f'(x) = 5(x^4 - 16)$ ha le sole radici reali ± 2, ed il grafico di $f(x)$ ha quindi un massimo relativo in $(-2, 133)$ e un minimo relativo in $(2, -123)$: $f(x)$ ha quindi tre radici reali — una minore di -2, una compresa tra -2 e 2, e la terza maggiore di 2 — e due complesse coniugate.

Sia $\mathbb{F}$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$. Sappiamo già che $G = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ si identifica ad un sottogruppo del gruppo S_5 delle permutazioni delle radici di $f(x)$. Se α è una radice di $f(x)$ in $\mathbb{C}$, allora $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ per l'irriducibilità di $f(x)$, e quindi $[\mathbb{F} : \mathbb{Q}]$

è multiplo di 5. Inoltre, la coniugazione complessa è un elemento di $G \subset \mathrm{S}_5$, e agisce come una trasposizione sulle radici di $f(x)$.

In conclusione, G contiene una trasposizione, e sicuramente anche un 5-ciclo, poiché possiede un elemento di ordine 5 per il Teorema di Cauchy. A meno di rinumerare le radici, e di sostituire tale elemento di ordine 5 con una sua potenza, G contiene (12) e (12345). Coniugando (12) con le potenze di (12345) si ottengono le trasposizioni $(12), (23), (34), (45)$, che generano tutto S_5. Pertanto $G = \mathrm{S}_5$, che non è risolubile.

Per quanto appena dimostrato, neanche il gruppo di Galois su un'estensione che contenga tutte le radici dell'unità necessarie è risolubile, e quindi le radici di $f(x)$ non possono esprimersi per radicali.

E-mail address: dandrea@mat.uniroma1.it