ROMA TRE
UNIVERSITÀ DEGLI STUDI

**Università degli Studi di Roma Tre**

FACOLTÀ DI MATEMATICA

Appunti integrativi

# Istituzioni di Algebra superiore

AL310

Di:
**Edoardo Signorini**

**A.A. 2016–2017, Semestre I**

# INDICE

# 1 | DEFINIZIONI E RISULTATI DI BASE

## 1.1 ANELLI

**Definizione 1.1 – Anello**

Un *anello* è un insieme $A$ dotato di due operazioni $+$ e $\cdot$ tali che

1. $(A, +)$ è un gruppo commutativo;
2. $(A, \cdot)$ è un monoide commutativo;
3. la moltiplicazione è distributiva rispetto alla somma.

**Notazione.** In questo corso un anello, a meno di esplicitarlo altrimenti, si intende sempre unitario e commutativo.

**Definizione 1.2 – Sottoanello**

Sia $A$ un anello e $B \subseteq A$. $B$ si dice *sottoanello* di $A$ se

- $(B, +)$ è un sottogruppo di $(A, +)$;
- $B$ è chiuso rispetto al prodotto;
- $1_A$ appartiene a $B$.

*Osservazione.* In particolare un sottoanello costituisce un anello. D'altronde il viceversa è falso, infatti $A = \mathbb{Z} \times \mathbb{Z}$ è un anello rispetto alle operazioni canoniche la cui identità è $(1, 1)$. Se considero $S = \{ (x, 0) \mid x \in \mathbb{Z} \}$ avrò che $S$ è un anello e $S \subseteq A$, ma $S$ non è un sottoanello di $A$ in quanto $(1, 1) \notin S$, la cui identità è invece $(1, 0)$.

**Definizione 1.3 – Omomorfismo di anelli**

Siano $A, A'$ anelli. Un *omomorfismo di anelli* $\varphi \colon A \to A'$ è una mappa che mantiene le operazioni, ovvero tale che per ogni $a, b \in A$

$$\varphi(a + b) = \varphi(a) + \varphi(b), \qquad \varphi(a\,b) = \varphi(a)\varphi(b), \qquad \varphi(1_A) = 1_{A'}.$$

**Esempio.** Riprendendo l'esempio dell'osservazione precedente avremo che

$$\varphi \colon S \hookrightarrow A, (x, 0) \mapsto (x, 0),$$

non è un omomorfismo in quanto

$$\varphi(1_S) = \varphi((1, 0)) = (1, 0) \neq 1_A.$$

**Definizione 1.4 – Dominio di integrità**

Un anello $A$ si definisce *dominio di integrità* se il prodotto di elementi non nulli è sempre non nullo, ovvero

$$a\,b = 0 \implies a = 0 \text{ oppure } b = 0,\ \forall\ a, b \in A.$$

**Notazione.** Spesso la sola parola dominio viene utilizzata per i domini di integrità.

**Esempio.** $\mathbb{Z} \times \mathbb{Z}$ non è un dominio di integrità, infatti

$$(1,0)(0,1) = (0,0) \qquad \text{con} \qquad (1,0), (0,1) \neq (0,0).$$

**Definizione 1.5 – Ideale**

Sia $A$ un anello e sia $I \subseteq A$. $I$ si dice *ideale* di $A$ se

- $(I, +)$ è un sottogruppo di $(A, +)$;
- $I$ è chiuso rispetto alla moltiplicazioni di elementi in $A$, ovvero

$$a\,x \in I,\ \forall\ x \in I,\ \forall\ a \in A.$$

**Proprietà.** Se $A$ è un anello e $I \subseteq A$ è un ideale,

$$\frac{A}{I} = \{\, a + I : a \in A \,\} \qquad \text{con } a + I = \{\, a + x : x \in I \,\} \subseteq A,$$

è una partizione di $A$ e costituisce un anello con le operazioni indotte sulle classi laterali.

**Definizione 1.6 – Ideale generato**

Sia $A$ un anello e siano $\alpha_1, \ldots, \alpha_r \in A$. Definiamo

$$(\alpha_1, \ldots, \alpha_r) = \{\, x_1\alpha_1 + \ldots + x_r\alpha_r \mid x_1, \ldots, x_r \in A \,\},$$

come l'*ideale generato* da $\alpha_1, \ldots, \alpha_r$.

**Definizione 1.7 – Anello a ideali principali**

Un anello $A$ si dice *a ideali principali* se per ogni ideale $I \subseteq A$, si ha che $I$ è generato da un elemento di $A$, ovvero

$$\exists\ a \in A : I = (a).$$

## 1.2 CAMPI

**Definizione 1.8 – Campo**

Un anello $K$ si definisce *campo* se ogni suo elemento non nullo è invertibile, ovvero

$$\forall\ x \in K, x \neq 0\ \exists\ y \in K : x\,y = 1_K.$$

*Osservazione.* In altre parole un campo è un insieme $K$ costituito da due operazioni $+$ e $\cdot$ tali che

1. $(K, +)$ è un gruppo abeliano;
2. $(K \setminus \{0\}, \cdot)$ è un gruppo abeliano;
3. la moltiplicazione è distributiva rispetto alla somma.

**Esempio.** $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ sono alcuni esempi di campi.

*Osservazione.* Vi sono moltissimi campi che possono essere costruiti fra $\mathbb{Q}$ ed $\mathbb{R}$ od oltre $\mathbb{C}$. D'altronde non ve ne è nessuno fra $\mathbb{R}$ e $\mathbb{C}$.

**Esempio.** L'estensione algebrica $\mathbb{Q}(\sqrt{2})$ di $\mathbb{Q}$ definita come

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\},$$

è un campo. Si mostra facilmente che ogni suo elemento ha inverso, infatti

$$\frac{1}{a + \sqrt{2}b} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

**Esempio.** L'esensione trascendente $\mathbb{Q}(\pi)$ di $\mathbb{Q}$ definita come

$$\mathbb{Q}(\pi) = \left\{ \frac{a_0 + a_1\pi + \ldots + a_n\pi^n}{b_0 + b_1\pi + \ldots + b_m\pi^m} \;\middle|\; a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{Q} \right\},$$

è un campo.

## Definizione 1.9 – Sottocampo

Sia $K$ un campo e sia $L \subseteq K$. $L$ si dice *sottocampo* di $K$ se è un suo sottoanello ed inoltre costitutisce un campo.

*Osservazione.* Se $L$ è un sottocampo di $K$ allora $K$ è anche uno spazio vettoriale su $L$. Infatti se $\alpha \in L, k \in K$, allora $\alpha \cdot k = \alpha k$. su uno spazio vettoriale posso anche parlare di dimensione $\dim_L K$.

**Notazione.** Un'inclusione di campi $L \subseteq K$ si chiama *estensione di campi* e se ne definisce il *grado* come

$$[K : L] := \dim_L K.$$

**Esempio.** Rifacendoci a due esempi precedenti abbiamo

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \qquad \text{e} \qquad [\mathbb{Q}(\pi) : \mathbb{Q}] = +\infty.$$

**Proposizione 1.10 – Caratterizzazione dei campi tramite ideali**

Sia $A$ un anello. Allora $A$ è un campo se e soltanto se per ogni $I \subseteq A$ ideale risulta

$$I = (0) \qquad \text{oppure} \qquad I = A.$$

⇐) *Dimostrazione.* Sia $a \in A \setminus \{0\}$. Dobbiamo esibire un inverso di $a$. Consideriamo l'ideale da esso generato $(a)$, chiaramente

$$(a) \neq 0 \implies (a) = A \implies 1 \in (a).$$

Ovvero esiste $b \in A$ tale che $a\,b = 1$, quindi $a$ è invertibile.

⇒) Sia $I \subseteq A$ un ideale tale che $I \neq (0)$. Allora per ogni $a \in A$ possiamo fissare $x \in I, x \neq 0$ e scrivere

$$a = a\,x^{-1}x.$$

D'altronde $a\,x^{-1} \in A$ e $x \in I$, da cui

$$a\,x^{-1}x \in I \implies a \in I, \forall\, a \in A.$$

Ovvero $A \subseteq I$ che implica immediatamente $A = I$. □

**Proposizione 1.11 – Omomorfismi di campi**

Sia $\varphi\colon F_1 \to F_2$ un omomorfismo di campi. Allora $\varphi$ è iniettivo.

*Dimostrazione.* Sappiamo che $\operatorname{Ker}\varphi \subseteq F_1$ è un ideale. D'altronde $F_1$ è un campo, quindi, per la teorema 1.10,

$$\operatorname{Ker}\varphi = (0) \qquad \text{oppure} \qquad \operatorname{Ker}\varphi = F_1.$$

Ma $1_{F_1} \notin \operatorname{Ker}\varphi$ in quanto $\varphi(1_{F_1}) = 1_{F_2} \neq 0_{F_2}$. Quindi $\operatorname{Ker}\varphi = (0)$, ovvero $\varphi$ è iniettivo. □

## 1.3 CARATTERISTICA DI UN CAMPO

Sia $F$ un campo, si mostra facilmente che la mappa

$$\varphi\colon \mathbb{Z} \to F, n \mapsto \overbrace{1_F + 1_F + \ldots + 1_F}^{n\text{volte}} =: n\,1_F, -1 \mapsto -1_F,$$

è un omomorfismo di anelli. Pertanto il suo nucleo $\operatorname{Ker}\varphi$ è un ideale di $\mathbb{Z}$.

**Definizione 1.12 – Caratteristica**

Sia $A$ un anello, si definisce *caratteristica* di $A$ il più piccolo naturale $n \in \mathbb{N}$ tale che

$$\underbrace{1_A + 1_A + \ldots + 1_A}_{n\text{volte}} = 0_A.$$

**Notazione.** Se tale naturale non esiste si dice che $A$ ha caratteristica $0$ per definizione.

## Teorema 1.13 – Caratteristica di un campo

Sia $F$ un campo. Allora la caratteristica di $F$ è zero oppure un numero primo.

*Dimostrazione.* Consideriamo nuovamente l'omomorfismo $\varphi$ introdotto all'inizio del paragrafo e analizziamo due casi distinti:

- Se $\operatorname{Ker}\varphi = (0)$, allora
$$n\,1_F = 0 \implies n = 0.$$
Per cui gli elementi non nulli di $\mathbb{Z}$ vengono mappati in elementi invertibili di $F$, ne segue che $\varphi$ può essere esteso a $\mathbb{Q}$ tramite
$$\mathbb{Q} \to F, \frac{n}{m} \mapsto (n\,1_F)(m\,1_F)^{-1},$$
ovvero in questo caso $F$ contiene una copia isomorfa a $\mathbb{Q}$ ed ha caratteristica zero.
- Se $\operatorname{Ker}\varphi \neq (0)$ allora esiste $m \neq 0$ tale che $m\,1_F = 0_F$ e si avrebbe
$$p = \operatorname{Char} F = \min\{\, m \mid m\,1_F = 1_F + 1_F + \ldots + 1_F = 0 \,\},$$
è primo. Infatti se per assurdo $p = a\,b$ si avrebbe $p\,1_F = a\,b\,1_F = (a\,1_F)(b\,1_F)$. D'altronde $F$ è in particolare un dominio, per cui
$$p\,1_F = 0 \implies a\,1_F = 0 \qquad \text{oppure} \qquad b\,1_F = 0,$$
ma ciò è assurdo per la minimalità di $p$.
Inoltre in questo caso si ha $\operatorname{Ker}\varphi = (p) \subset \mathbb{Z}$, per cui il Teorema Fondamentale degli Omomorfismi definisce un'inclusione
$$\frac{\mathbb{Z}}{(p)} = \frac{\mathbb{Z}}{p\mathbb{Z}} \hookrightarrow F, n \pmod p \mapsto n\,1_F.$$
Ovvero $F$ contiene una copia isomorfa a $\mathbb{F}_p$ e ha caratteristica $p$.

□

**Notazione.** Quando $F$ ha caratteristica $p$ diciamo che $\mathbb{F}_p$ è il *sottocampo fondamentale* di $F$.

## Proposizione 1.14 – Binomio di Newton nei campi

Se $F$ è un campo di caratteristica $p$ allora
$$(a+b)^p = a^p + b^p, \forall\, a, b \in F.$$

*Dimostrazione.* Il binomio di Newton
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$
è valido in ogni anello commutativo. Ora se $n = p$ si ha $p \mid \binom{p}{k}$ per ogni $k = 1, \ldots, p-1$. Quindi se $F$ ha caratteristica $p$ avremo
$$p \mid \binom{p}{k} \implies \binom{p}{k} 1_F = m\,p\,1_F = m\,(p\,1_F) = 0_F,$$
da cui, sostituendo nell'espressione del binomio di Newton, si giunge alla tesi. □

*Osservazione.* In generale vale

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}, \ \forall\, n \geqslant 1.$$

Per cui la mappa $F \to F, x \mapsto x^p$ risulta essere un omomorfismo, detto *Endomorfismo di Frobenius*. Tale endomorfismo risulta essere un automorfismo quando $F$ è finito.

## 1.4 ANELLI DI POLINOMI

Se $F$ è un campo possiamo definire il seguente insieme

$$F[X] = \left\{ \sum_{j=0}^{k} a_j X^j \;\middle|\; a_j \in F \right\}.$$

Inoltre se consideriamo due elementi

$$f(X) = \sum_{j=0}^{n} a_j X^j \qquad \text{e} \qquad g(X) = \sum_{j=0}^{m} b_j X^j,$$

possiamo definire le operazioni di somma

$$(f+g) = \sum_{j=0}^{\max\{n,m\}} (a_j + b_j) X^j \qquad \text{con} \begin{cases} a_j = 0 & \text{se } j > n \\ b_j = 0 & \text{se } j > m \end{cases}$$

e di prodotto

$$(f\,g) = \sum_{j=0}^{m+n} c_j X^j \qquad \text{con } c_j = \sum_{\substack{h+k=j \\ 0 \leqslant h \leqslant n \\ 0 \leqslant k \leqslant m}} a_h + b_k.$$

**Definizione 1.15 – Anello di polinomi**

Sia $F$ un campo. L'insieme $F[X]$ si definisce *anello di polinomi* nell'indeterminata $X$ a coefficienti in $F$.

*Osservazione.* Si osservi che $F[X]$ è un anello rispetto alle operazioni definite sopra, inoltre risulta $F \subseteq F[X]$ e $F[X]$ un dominio.

**Proprietà 1.16** (Divisione di polinomi)**.** Siano $f, g \in F[X]$ con $g \neq 0$. Allora esistono unici $q(X), r(X) \in F[X]$ tali che

$$f(X) = q(X)g(X) + r(X) \qquad \text{con } r(X) = 0 \text{ oppure } \deg r < \deg g.$$

*Osservazione.* $F[X]$ è pertanto un dominio euclideo con il grado dei polinomi come norma. In particolare è anche un dominio a fattorizzazione unica ed esiste sempre il MCD di due elementi.

**Proprietà 1.17.** Siano $f(X) \in F[X]$ e $a \in F$. Allora esiste unico $q(X) \in F[X]$ tale che

$$f(X) = (X-a)q(X) + c \qquad \text{con } c = f(a).$$

*Osservazione.* Se $a$ è una radice di $f$, ovvero $f(a) = 0$, allora

$$(X - a) \mid f(X),$$

da ciò segue inoltre che $f$ ha al più $\deg f$ radici.

**Proprietà 1.18** (Algoritmo euclideo)**.** Siano $f, g \in F[X]$ e supponiamo che $d(X) = \big(f(X), g(X)\big)$. Tramite l'algoritmo euclideo delle divisioni è possibile costruire $a(X), b(X) \in F[X]$ tali che

$$a(X)f(X) + b(X)g(X) = d(X) \qquad \text{con } \deg a < \deg g \text{ e } \deg b < \deg f.$$

**Definizione 1.19 – Campo dei quozienti dei polinomi**

Dal momento che $F[X]$ è un dominio di integrità possiamo considerare il suo *campo dei quozienti* $F(X)$. Esso è costituito dai quozienti $f/g$, dove $f, g \in F[X]$ e $g \neq 0$.

## 1.5 FATTORIZZAZIONE DI POLINOMI

In questo paragrafo studieremo in quali casi è possibile determinare la riducibilità dei polinomi.

In questo corso quando diciamo che $f \in \mathbb{Z}[X]$ è irriducibile si intende che per ogni $g \mid f$ si ha $\deg g = 0$ oppure $\deg g = f$.

**Proposizione 1.20 – Radici razionali di un polinomio a coefficienti interi**

Sia $f(X) = a_0 + a_1X + \ldots + a_mX^m \in \mathbb{Z}[X]$ e supponiamo che $q = N/D, N, D \in \mathbb{Z}, (N, D) = 1$ sia una radice di $f$. Allora

$$N \mid a_0 \qquad \text{e} \qquad D \mid a_m.$$

*Dimostrazione.* Per ipotesi $f(q) = 0$. Se all'espressione di $f(q)$ semplifichiamo il denominatore, otteniamo

$$a_0D^m + a_1D^{m-1}N + \ldots + a_{m-1}DN^{m-1} + a_mN^m = 0 \implies D\,(a_0D^{m-1} + \ldots + a_{m-1}) = -a_mN^m,$$

da cui $D \mid a_mN^m$. D'altronde $(N, D) = 1 \implies D \mid a_m$.
Analogamente si mostra che $N \mid a_0$. □

**Esempio.** Consideriamo il polinomio $f(X) = X^3 + aX + 1, a \in \mathbb{Z}$. Per la proposizione le uniche possibili radici razionali di $f$ sono $x = \pm 1$, dove

$$f(1) = a + 2 \qquad \text{e} \qquad f(-1) = -a.$$

Per cui se $a \neq 0, -2$ allora $f$ è irriducibile.

**Proposizione 1.21 – Lemma di Gauss**

Sia $f(X) \in \mathbb{Z}[X]$ e supponiamo che $f$ si fattorizzi in modo non banale in $\mathbb{Q}[X]$. Allora $f$ si fattorizza in modo non banale anche in $\mathbb{Z}[X]$.

*Dimostrazione.* Per ipotesi $f = hg$ con $h, g \in \mathbb{Q}[X]$ divisori propri di $f$. Certamente esisteranno $m, n \in \mathbb{Z}$ tali che

$$m\,h(X) = h_1(X) \in \mathbb{Z}[X] \qquad \text{e} \qquad n\,g(X) = g_1(X) \in \mathbb{Z}[X],$$

da cui

$$m\,n\,f(X) = h_1(X)g_1(X). \tag{$\star$}$$

Vogliamo mostrare di poter assumere che $m\,n = 1$.
Se $p \mid n\,m$ leggiamo $(\star)$ in $\mathbb{F}_p[X]$, così da ottenere $\bar{h}_1\bar{g}_1 \equiv_p 0$. D'altronde $\mathbb{F}_p[X]$ è un dominio, per cui $\bar{h}_1(X) \equiv_p 0$ oppure $\bar{g}_1(X) \equiv_p 0$. Assumiamo $\bar{h}_1 \equiv_p 0$, ciò significa che tutti i coefficienti di $h_1$ sono divisibili per $p$. Quindi

$$m\,h(X) = h_1(X) = p\,h_2(X) \implies \frac{m\,n}{p}\,f(X) = h_2(X)g_1(X),$$

iterando il procedimento si giunge alla tesi. □

## Proposizione 1.22 – Fattori monici di un polinomio monico a fattori interi

Sia $f(X) \in \mathbb{Z}[X]$ un polinomio monico. Supponiamo che $g \mid f$ con $g \in \mathbb{Q}[X]$ monico. Allora $g(X) \in \mathbb{Z}[X]$.

*Dimostrazione.* Scriviamo $f = g\,h$ con $g, h \in \mathbb{Q}[X]$ monici. Sappiamo, tramite lo stesso argomento della che esistono $m, n \in \mathbb{Z}$ tali che $m\,g, n\,h \in \mathbb{Z}[X]$, consideriamo inoltre $m, n$ tali che abbiano un numeri di fattori primi minimi. Vogliamo ottenere una contraddizione mostrando che se $p \mid m\,n$ allora $m$, oppure $n$, non sarebbero minimali rispetto alla proprietà di avere un numero minimo di fattori.
Supponiamo quindi che $p \mid m\,n$ con $p$ primo, allora

$$m\,g \cdot n\,h = m\,n\,f \implies m\,g \cdot n\,h \equiv_p 0.$$

Siccome $\mathbb{F}_p[X]$ è un dominio, otteniamo $m\,g \equiv_p 0$ oppure $n\,h \equiv_p 0$. Assumiamo che $m\,g \equiv_p = 0$, in tal caso si avrebbe $p \mid m$ in quanto $g$ è monico per ipotesi, da cui

$$\frac{m}{p}g(X) \in \mathbb{Z}[X],$$

che è assurdo per la minimalità di $m$. □

## Proposizione 1.23 – Criterio di Eisenstein

Sia $f(X) = a_m X^m + a_{m-1}X^{m-a} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ e supponiamo che esista $p$ primo tale che

1. $p$ non divide $a_m$.
2. $p$ divide $a_j$ per ogni $j \in \{0, \ldots, m-1\}$.
3. $p^2$ non divide $a_0$.

Allora $f$ è irriducibile in $\mathbb{Q}[X]$.

*Dimostrazione.* Se per assurdo fosse

$$a_m X^m + \ldots + a_1 X + a_0 = (b_r X^r + \ldots + b_1 X + b_0)(c_s X^s + \ldots + c_1 X + c_0).$$

Dal momento che $p$, ma non $p^2$, divide $a_0 = b_0 c_0$, si avrebbe che $p$ deve dividere necessariamente $b_0$ oppure $c_0$, assumiamo $b_0$. Inoltre da

$$a_1 = b_0 c_1 + b_1 c_0,$$

deduciamo che $p \mid b_1$. Analogamente da

$$a_2 = b_0c_2 + b_1c_1 + b_2c_0,$$

deduciamo che $p \mid b_2$. Iterando tale procedimento otteniamo che $p$ divide $b_0, b_1, \ldots, b_r$ che è assurdo per l'ipotesi che $p \nmid a_m$. □

*Osservazione.* Le proposizioni che abbiamo dimostrato finora in questo paragrafo sono ancora valide se al posto di $\mathbb{Z}$ consideriamo un qualsiasi altro dominio a fattorizzazione unica.

**Proprietà 1.24.** Sia $f(X) \in \mathbb{Z}[X]$ e siano $a, b \in \mathbb{Q}, a \neq 0$. Allora $f(X)$ è irriducibile se e solo se $f(aX + b)$ è irriducibile.

*Dimostrazione.* Supponiamo che $f(aX + b)$ sia irriducibile, se per assurdo fosse $f(X) = g(X)h(X)$ si avrebbe

$$f(aX + b) = g(aX + b)h(aX + b),$$

che è chiaramente assurdo. Analogamente si mostra il viceversa, infatti

$$F(X) := f(aX + b) \implies f(X) = F\Big(\frac{1}{a}X - \frac{b}{a}\Big),$$

d'altronde abbiamo già mostrate che $F(X)$ irriducibile implica $F(1/aX - b/a)$ irriducibile. □

**Esempio.** Consideriamo il $p$-*esimo polinomio ciclotomico*

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \ldots + X^{p-1} = \prod_{j=1}^{p-1} \Big(X - e^{\frac{2\pi i j}{p}}\Big) \in \mathbb{Z}[X]$$

Per mostrare che $\phi_p(X)$ è irriducibile vogliamo sfruttare il criterio di Eisenstein. Scriviamo $\phi_p(X + 1)$:

$$\phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + pX^{p-2} + \binom{p}{2}X^{p-3} + \ldots + \binom{p}{p-2}X + \binom{p}{p-1},$$

*tramite il binomio di Newton*

otteniamo quindi che $\phi_p(X + 1)$ è un $p$-eisenstein, per cui $\phi_p(X + 1)$ è irriducibile e di conseguenza $\phi_p(X)$ è irriducibile.

## Teorema 1.25 – Irriducibilità in $\mathbb{Z}[X]$ è deterministico

Sia $f(X) \in \mathbb{Z}[X]$, allora esiste un algoritmo per fattorizzare $f$. Ovvero l'irriducibilità di un polinomio in $\mathbb{Z}[X]$ è un problema deterministico.

*Dimostrazione.* Possiamo assumere che $f$ sia monico a meno di moltiplicare per una costante, per cui

$$f(X) = X^m + a_1X^{m-1} + \ldots + a_m, \qquad \text{con } a_i \in \mathbb{Z}.$$

Dal Teorema Fondamentale dell'Algebra sappiamo che esistono $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ tali che

$$f(X) = \prod_{j=1}^{m}(X - \alpha_j).$$

Osserviamo che dall'identità

$$0 = f(\alpha_j) = \alpha_j^m + a_1\alpha_j^{m-1} + \ldots + a_m,$$

si deduce che $|\alpha_j|$ è limitata e può essere stimata in termini dei soli coefficienti di $f$. Infatti avremo

$$|\alpha_j| \leqslant \left|\frac{a_m}{\alpha_j^{m-1}}\right| + \left|\frac{a_{m-1}}{\alpha_j^{m-2}}\right| + \ldots + |a_1| \implies |\alpha_j| \leqslant \sum_{k=1}^{m} \frac{|a_k|}{|\alpha_j|^{k-1}}$$

Da cui

$$|\alpha_j| \geqslant 1 \implies |\alpha_j| \leqslant \sum_{k=1}^{m} |a_k|,$$

ovvero

$$|\alpha_j| \leqslant \max\left\{1, \sum_{k=1}^{m} |a_k|\right\}, \forall\, j = 1, \ldots, m.$$

Ora se $g(X)$ è un fattore monico di $f(X)$, allora le sue radici saranno un sottoinsieme di quelle di $f$ e i suoi coefficienti saranno polinomi simmetrici nelle sue radici. Per cui i moduli dei coefficienti di $g$ saranno limitati in termini dei coefficienti di $f$. Dal momento che essi sono anche interi, ne deduciamo che esistono solo un numero finito di possibilità per $g(X)$. Per cui, per trovare i fattori di $f(X)$, dobbiamo analizzare un numero finito di casi. □

*Osservazione.* Tale procedimento può essere esteso anche ai polinomi in $\mathbb{Q}[X]$. Infatti se $f \in \mathbb{Q}[X]$ possiamo renderlo monico tramite la moltiplicazione per un razionale e infine sostituirlo con

$$F_D(f) := D^{\deg f} f\left(\frac{X}{D}\right),$$

dove $D$ è il mcm dei denominatore dei coefficienti di $f$. Abbiamo così ottenuto un polinomio monico a coefficienti interi che ha le stesse radici di quello di partenza.

**Esempio.** Se $f(X) = X - 1/2$ possiamo scrivere

$$F_2(f) = 2^1\left(\frac{X}{2} - \frac{1}{2}\right) = X - 1.$$

## 1.6 ESTENSIONE DI CAMPI

### Definizione 1.26 – Estensione di campi

Se $E, F$ sono campi e $F \subseteq E$ è un sottocampo, diciamo che $E$ è un'*estensione* di $F$.

**Notazione.** Per denotare che $E$ è un'estensione di $F$ scriviamo $E/F$.

### Definizione 1.27 – Grado dell'estensione

Il *grado* di un'estensione $E/F$ è la dimensione di $E$ come $F$-spazio vettoriale:

$$[E : F] := \dim_F E.$$

**Notazione.** Diciamo che $E/F$ è un'estensione *finita* se $[E : F] < +\infty$.

**Esempio.**
- $\mathbb{C}/\mathbb{R}$ è un'estensione finita e $[\mathbb{C}:\mathbb{R}]=2$, infatti $\{1,i\}$ è una $\mathbb{R}$-base di $\mathbb{C}$.
- $\mathbb{R}/\mathbb{Q}$ è un'estensione infinita. Infatti se fosse $[\mathbb{R}:\mathbb{Q}]<+\infty$, allora esisterebbe $n$ tale che $\mathbb{R}\cong_{\mathbb{Q}}\mathbb{Q}^n$, il che è assurdo in quanto $\mathbb{Q}$ ha cardinalità numerabile ed $n-$copie di $\mathbb{Q}$ sarebbero ancora numerabili, mentre $\mathbb{R}$ ha la cardinalità del continuo.
- Il campo dei numeri di Gauss $\mathbb{Q}(i)=\{a+ib\mid a,b\in\mathbb{Q}\}$ ha dimensione 2 come estensione di $\mathbb{Q}$. Infatti $\{1,i\}$ è una $\mathbb{Q}$-base.
- Il campo dei quozienti di un campo $F$, definito come
$$F(X)=\left\{\frac{f}{g}\;\middle|\; f,g\in F[X],g\neq 0\right\},$$
è un'estensione infinita di $F$. Infatti $\{1,X,X^2,\dots,X^n,\dots\}$ è una famiglia infinita in $F(X)$ che è $F$-linearmente indipendente.

## Proposizione 1.28 – Formula del grado

Consideriamo $L,E,F$ campi tali che $L\supset E\supset F$. Allora $L/F$ ha grado finito se e soltanto se $L/E$ e $E/F$ hanno grado finito, nel qual caso vale
$$[L:F]=[L:E][E:F].$$

*Dimostrazione.* Supponiamo che $L/F$ sia finita, allora $E/F$ è finita poiché $E$ è un $F$-sottospazio di $L$. Inoltre anche $L/E$ è finita, infatti se $(\alpha_1,\dots,\alpha_r)$ sono generatori di $L/F$, ovvero ⇒)
$$L=\{a_1\alpha_1+\dots+a_r\alpha_r\mid a_i\in F\},$$
allora a maggior ragione
$$L=\{b_1\alpha_1+\dots+b_r\alpha_r\mid b_i\in E\}.$$
Supponiamo che $L/E$ e $E/F$ siano estensioni finite. Siano $(\alpha_1,\dots,\alpha_t)$ e $(\beta_1,\dots,\beta_s)$ rispettivamente una $F$-base di $E$ e una $E$-base di $L$. Vogliamo mostrare che ⇐)
$$(\alpha_i\beta_j)_{\substack{i=1,\dots,t\\ j=1,\dots,s}},$$
è una $F$-base di $L$. Da ciò seguirebbe $[L:F]=ts=[E:F][L:E]$.
Per prima cosa $(\alpha_i,\beta_j)_{i,j}$ genera $L$: se $x\in L$, allora $x=x_1\beta_1+\dots+x_s\beta_s$ con $x_1,\dots,x_s\in E$. Ora per ogni $j=1,\dots,s$ avremo $x_j=x_{1j}\alpha_1+\dots+x_{tj}\alpha_t$, in quanto $(\alpha_1,\dots,\alpha_t)$ è una base di $E$. Sostituendo otteniamo
$$x=\sum_{i=1}^{t}\sum_{j=1}^{s}x_{ij}\alpha_i\beta_j,$$
ovvero $(\alpha_i\beta_j)_{i,j}$ genera $L/F$.
Inoltre $(\alpha_i,\beta_j)_{i,j}$ sono linearmente indipendenti: supponiamo che esistano $y_{ij}\in F$ tali che
$$\sum_{i,j}y_{ij}\alpha_i\beta_j=0,$$
allora
$$\underbrace{(y_{11}\alpha_1+\dots+y_{t1}\alpha_t)}_{\in E}\beta_1+\underbrace{(y_{12}\alpha_1+\dots+y_{t2}\alpha_t)}_{\in E}\beta_2+\dots+\underbrace{(y_{1s}\alpha_1+\dots+y_{ts}\alpha_t)}_{\in E}\beta_s=0,$$
da cui $y_{1j}\alpha_1+\dots+y_{tj}\alpha_t=0$ per ogni $j$ per la lineare indipendenza di $(\beta_1,\dots,\beta_s)$. D'altronde poiché $(\alpha_1,\dots,\alpha_t)$ è una $F$-base di $E$ si ha
$$y_{1j}\alpha_1+\dots+y_{tj}\alpha_t=0\implies y_{1j},\dots,y_{tj}=0,\ \forall\, j.$$
□

## 1.7 SOTTOANELLI GENERATI DA SOTTOINSIEMI

**Definizione 1.29 – Sottoanello generato da un sottoinsieme**

Sia $F$ un sottocampo di un campo $E$ e sia $S \subset E$. Definisco il *sottoanello di* $E$ *generato da* $S$ *su* $F$ come il più piccolo sottoanello di $E$ che contiene $F$ e $S$:

$$F[S] := \bigcap_{\substack{R \subseteq E \text{ anello} \\ F \subseteq R, S \subseteq R}} R.$$

**Notazione.** Quando $S = \{\alpha_1, \dots, \alpha_n\}$ è finito scriviamo $F[\alpha_1, \dots, \alpha_n]$ per $F[S]$.

**Proprietà 1.30.** L'anello $F[S]$ consiste negli elementi di $E$ che possono essere scritti come somme finite della forma

$$\sum a_{i_1 \dots i_n} \alpha_1^{i_1} \cdot \ldots \cdot \alpha_n^{i_n}, \qquad \text{con } a_{i_1 \dots i_n} \in F, \quad \alpha_i \in S.$$

*Dimostrazione.* Supponiamo che $R$ sia l'insieme di tutti tali elementi. Chiaramente $R$ è un sottoanello che contiene $F, S$, per cui $F[S] \supseteq R$. Inoltre ogni altro sottoanello che contiene $F, S$ deve necessariamente contenere $R$ per le proprietà di un anello. Quindi $F[S] = R$. □

**Esempio.** L'anello $\mathbb{Q}[\pi]$ consiste in tutti i numeri complessi che possono essere espressi nella forma

$$a_0 + a_1\pi + a_2\pi^2 + \ldots + a_n\pi^n, \qquad \text{con } a_i \in \mathbb{Q}.$$

**Proprietà 1.31.** Sia $R$ un anello integro e sia $F \subseteq R$ un campo. Se $\dim_F R < \infty$ allora $R$ è un campo.

*Dimostrazione.* Per ogni $\beta \in R, \beta \neq 0$ consideriamo la mappa $f\colon R \to R, x \mapsto \beta x$. Tale mappa è un applicazione lineari di $F$-spazi vettoriali, infatti

$$f(a x + b y) = \beta (a x + b y) = \beta a x + \beta b y = a f(x) + b f(y).$$

Inoltre $f$ è iniettiva, infatti $\operatorname{Ker} f = \{ x \in R \mid \beta x = 0 \} = (0)$ in quanto $R$ è integro. Ricordando che un endomorfismo fra spazi finiti quando è iniettivo è anche suriettivo si avrà che

$$\exists\, \alpha \in R : \beta \alpha = 1 \implies \beta \text{ invertibile.}$$

□

## 1.8 SOTTOCAMPI GENERATI DA SOTTOINSIEMI

**Definizione 1.32 – Sottocampo generato da un sottoinsieme**

Sia $F$ un sottocampo di un campo $E$ e sia $S \subset E$. Definisco il *sottocampo di* $E$ *generato da* $S$ *su* $F$ come il più piccolo sottocampo di $E$ che contiene $F$ e $S$:

$$F(S) := \bigcap_{\substack{L \subseteq E \text{ sottocampo} \\ F \subseteq L, S \subseteq L}} L.$$

**Notazione.** Quando $S = \{\alpha_1, \dots, \alpha_n\}$ è finito scriviamo $F(\alpha_1, \dots, \alpha_n)$ per $F(S)$.

*Osservazione.* Dal momento che i sottocampi sono in particolare sottoanelli, avremo $F[S] \subseteq F(S)$.

**Proprietà 1.33.** $F(S)$ è il campo dei quozienti di $F[S]$, ovvero

$$f(S) = \left\{ \frac{x}{y} \;\middle|\; x, y \in F[S], y \neq 0 \right\}.$$

*Dimostrazione.* Segue dal fatto che $F(S)$ è un sottocampo che contiene $F$ e $S$ e che è contenuto in ogni altro sottocampo con questa proprietà. □

*Osservazione.* Dalla teorema 1.31 sappiamo che $F[S]$ è un campo se ha dimensione finita su $F$. In tal caso si avrebbe $F(S) = F[S]$.

**Definizione 1.34 – Estensione semplice**

Un'estensione $E/F$ si dice *semplice* se esiste $\alpha \in E$ tale che $F(\alpha) = E$.

**Esempio.** $\mathbb{Q}(\pi)$ e $\mathbb{Q}[i]$ sono estensioni semplici di $\mathbb{Q}$.

**Definizione 1.35 – Estensione finitamente generata**

Un'estensione $E/F$ si dice *finitamente generata* se esistono $\alpha_1, \dots, \alpha_k \in E$ tale che $F(\alpha_1, \dots, \alpha_k) = E$.

## 1.9 ANELLI COL GAMBO

Sia $f(X) \in F[X]$ un polinomio monico di grado $m$ e sia $(f)$ l'ideale generato da $f(X)$. Consideriamo l'anello quoziente $F[X]/(f)$ e denotiamo con $\alpha$ l'immagine di $X$ in tale anello, ovvero $\alpha$ sarà la classe laterale $X + (f(X))$. Ne segue:

- La mappa
$$F[X] \to F[\alpha], P(X) \mapsto P(\alpha),$$
è un omomorfismo suriettivo in cui $f(X)$ viene mappato in $0$, ovvero $f(\alpha) = 0$.
- Dall'algoritmo euclideo delle divisioni, sappiamo che ogni elemento $g(X) \in F[X]/(f)$ è rappresentato da un unico polinomio $r(X)$ con $\deg r < m$. Quindi ogni elemento di $F[X]/(f)$ può essere scritto come
$$a_0 + a_1\alpha_1 + \dots + a_{m-1}\alpha^{m-1}, \qquad \text{con } a_i \in F. \tag{$\star$}$$
- Per sommare due elementi nella forma $(\star)$ è sufficiente sommarne i coefficienti.
- Per moltiplicare due elementi nella forma $(\star)$ si deve moltiplicare nel modo usuale, sfruttando la relazione $f(\alpha) = 0$ per scrivere i termini di grado superiore a $m$ in termini di grado inferiore.

- Supponiamo che $f(X)$ sia irriducibile. Allora ogni elemento $\beta \in F[\alpha]$ ha un inverso. Tale inverso può essere trovato scrivendo $\beta = g(\alpha)$ con $g(X)$ un polinomio di grado inferiore a $m$, per poi applicare l'algoritmo euclideo per ottenere $a(X)$ e $b(X)$ tali che

$$a(X)f(X) + b(X)g(X) = d(X), \qquad \text{con } d(X) = \big(f(X), g(X)\big).$$

  Nel nostro caso $f$ è irriducibile per cui $d(X) = 1$. Inoltre $\deg g < \deg f$, per cui sostituendo $\alpha$ si ottiene

$$b(\alpha)g(\alpha) = 1 \implies g(\alpha)^{-1} = b(\alpha).$$

**Definizione 1.36 – Anello col gambo**

Sia $F$ un campo e sia $f$ un polinomio monico in $F[X]$. Si definisce *anello col gambo* l'anello

$$R = \left\{ a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \;\middle|\; a_j \in F \right\},$$

con le operazioni definite sopra e tale che

$$F[\alpha] = R \qquad \text{e} \qquad f(\alpha) = 0.$$

*Osservazione.* Se $f \in F[X]$ è irriducibile $F[\alpha]$ è un campo, per cui $F[\alpha] = F(\alpha)$, e inoltre

$$\deg f = n = \big[F[\alpha] : F\big].$$

**Esempio.** Consideriamo $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$. Avremo che

$$\mathbb{Q}[\alpha] = \left\{ a + b\,\alpha + c\,\alpha^2 \;\middle|\; a, b, c \in \mathbb{Q} \right\}.$$

Inoltre $f$ è irriducibile in $\mathbb{Q}[X]$, per cui $\mathbb{Q}[\alpha]$ è un campo ed ha base $(1, \alpha, \alpha^2)$ come $\mathbb{Q}$-spazio vettoriale.
Consideriamo adesso $\beta = \alpha^4 + 2\alpha^3 + 3 \in \mathbb{Q}[\alpha]$. Sapendo che $\alpha^3 - 3\alpha - 1 = 0$ otteniamo

$$\beta = (3\alpha + 1)\,\alpha + 6\alpha + 2 + 3 = 3\alpha^2 + 7\alpha + 5.$$

Vogliamo calcolare l'inversa di $\beta$. Dal momento che $f(X)$ è irriducibile in $\mathbb{Q}[X]$ segue

$$(X^3 - 3X - 1, 3X^2 + 7X + 5) = 1.$$

Applicando l'algoritmo di Euclide otteniamo l'identità di Bezout

$$(X^3 - 3X - 1)\left(-\frac{7}{37}X + \frac{29}{111}\right) + (3X^2 + 7X + 5)\left(\frac{7}{111}X^2 + \frac{26}{111}X + \frac{28}{111}\right) = 1,$$

da cui segue immediatamente

$$\beta^{-1} = \frac{7}{111}\alpha^2 + \frac{26}{111}\alpha + \frac{28}{111}.$$

## 1.10 ELEMENTI ALGEBRICI E TRASCENDENTI

Sia $E/F$ un'estensione e sia $\alpha \in E$, avremo che

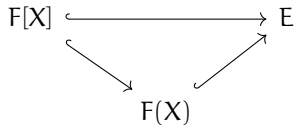
$$\varphi \colon F[X] \to E,\ h(X) \mapsto h(\alpha),$$

è un omomorfismo di anelli.

**Definizione 1.37 – Elemento trascendente**

Se $\operatorname{Ker}\varphi = (0)$ diciamo che $\alpha$ è *trascendente* su $F$.

*Osservazione.* Quando un elemento è trascendente significa che per ogni $h \in F[X], h \neq 0$ si ha $h(\alpha) \neq 0$. Ciò significa che l'immagine di $\varphi$ è isomorfa a $F[X]$, ovvero $F[\alpha] \cong F[X]$. Inoltre avremo




$$\text{con } F(X) \hookrightarrow E, \frac{h_1(X)}{h_2(X)} \mapsto \frac{h_1(\alpha)}{h_2(\alpha)}.$$

**Esempio.** Prendiamo $E = \mathbb{C}, F = \mathbb{Q}$ e $\alpha = \pi$. Siccome $\pi$ è trascendente si ha

$$\mathbb{Q}[X] \cong \mathbb{Q}[\pi] \subseteq \mathbb{C}.$$

Ciò significa che $\mathbb{Q}[\pi]$ è algebricamente indistinguibile da $\mathbb{Q}[X]$.

**Definizione 1.38 – Elemento algebrico**

Se $\operatorname{Ker}\varphi = (f_\alpha)$ diciamo che $\alpha$ è *algebrico* su $F$.

**Definizione 1.39 – Polinomio minimo**

I polinomi $g$ tali che $g(\alpha) = 0$ formano un ideale non banale in $F[X]$. Tale ideale è generato dal più piccolo polinomio monico $f_\alpha$ tale che $f_\alpha(\alpha) = 0$. Definiamo $f_\alpha$ come il *polinomio minimo di* $\alpha$ *su* $F$.

*Osservazione.* Il polinomio minimo è irriducibile poiché altrimenti vi sarebbero due elementi non nulli di $E$ che hanno come prodotto zero.

*Osservazione.* Siccome $F[X]/(f_\alpha) \cong F[\alpha]$, in $F[\alpha]$ possiamo assumere che tutte le espressioni polinomiali abbiano grado minore di $\deg f_\alpha$. Cioè l'immagine tramite $\varphi$ è il campo col gambo $F[\alpha]$ di gambo $f_\alpha$. In questo caso si ha che

$$F[\alpha] = F(\alpha).$$

Inoltre $\big[F[\alpha] : F\big] = \deg f_\alpha$ e $(1, \alpha, \ldots, \alpha^{\deg f_\alpha - 1})$ è una base.

**Proposizione 1.40 – Caratterizzazione del polinomio minimo**

Se $E/F$ è un'estensione e $\alpha \in E$ è algebrico su $F$, il polinomio minimo $f_\alpha$ è caratterizzato come polinomio di $F[X]$ da ognuna seguenti condizioni:

- L'unico polinomio monico e irriducibile in $F[X]$ che si annulla in $\alpha$.
- L'unico polinomio monico con la proprietà che se $g(X) \in F[X]$ e $g(\alpha) = 0$ allora $f_\alpha \mid g$.
- L'unico polinomio monico che si annulla in $\alpha$ e ha grado minimo.

**Esempio.** Su $(\mathbb{Q}[\alpha], \alpha^3 = 3\alpha + 1)$ prendiamo $\alpha^2 \in \mathbb{Q}[\alpha]$. Vogliamo stabilire se $\alpha^2$ è trascendete su $\mathbb{Q}$. Se non lo è vogliamo trovare il suo polinomio minimo.
Prendiamo un generico polinomio $X^3 + AX^2 + BX + C$. Se trovo $A, B, C \in \mathbb{Q}$ tali che una volta sostituito $\alpha^2$ nel polinomio ottengo zero, ho trovato il polinomio minimo:

$$\begin{aligned} \alpha^6 + A\alpha^4 + B\alpha^2 + C = 0 &\iff (3\alpha+1)^2 + A(3\alpha^2+\alpha) + B\alpha^2 + C = 0 \\ &\iff (9\alpha^2 + 6\alpha + 1) + A(3\alpha^2+\alpha) + B\alpha^2 + C = 0 \\ &\iff (3A + B + 9)\alpha^2 + (A+6)\alpha + (C+1) = 0, \end{aligned}$$

da cui

$$\begin{cases} 3A + B + 9 = 0 \\ A + 6 = 0 \\ C + 1 = 0 \end{cases} \implies \begin{cases} A = -6 \\ B = 9 \\ C = -1 \end{cases}$$

ovvero $f_{\alpha^2}(X) = X^3 - 6X^2 + 9X - 1$. Quindi

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}[\alpha] \cong \mathbb{Q}(\alpha).$$

Con $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg(\alpha^3 - 3\alpha - 1) = 3$ e ancora $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 3$, da cui

$$[\mathbb{Q}[\alpha] : \mathbb{Q}(\alpha^2)] = 1 \implies \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2).$$

### Definizione 1.41 – Estensione algebrica

Un'estensione $E/F$ si dice *algebrica* se ogni elemento $\alpha \in E$ è algebrico in $F$.

### Definizione 1.42 – Estensione trascendente

Un'estensione $E/F$ si dice *trascendente* se non è algebrica, ovvero se esiste un elemento $\beta \in E$ che è trascendente su $F$.

### Proposizione 1.43 – Caratterizzazione estensione finita

Sia $E/F$ un'estensione. Allora $E/F$ è finita se e soltanto se $E/F$ e algebrica e finitamente generata.

$\Rightarrow$) *Dimostrazione.* Supponiamo che $E/F$ sia un'estensione finita, allora

- $E/F$ algebrica: se per assurdo esistesse $\beta \in E$ trascendente su $F$, si avrebbe che $(1, \beta, \dots, \beta^n, \dots)$ sarebbero linearmente indipendenti su $F$. Ciò implicherebbe che $\dim_F E = \infty$ che è assurdo per la finitezza dell'estensione.
- $E/F$ finitamente generate: se $E = F$ allora $E = F(1)$; se invece $E \supset F$, preso $\alpha_1 \in E - F$ avremmo

  $$E \supseteq F[\alpha_1] \supset F.$$

  In particolare $F[\alpha_1]/F$ è finita per cui $F[\alpha_1] = F(\alpha_1)$. Ora se $E = F[\alpha_1]$ abbiamo mostrato la tesi, altrimenti se $E \supset F[\alpha_1]$ possiamo trovare $\alpha_2 \in E - F[\alpha_1]$ ottenendo

  $$E \supset F[\alpha_1, \alpha_2] \supset F[\alpha_1] \supset F,$$

  che sono tutte estensioni finite. Posso quindi iterare il processo scrivendo $E \supseteq F[\alpha_1, \dots, \alpha_k] = F(\alpha_1, \dots, \alpha_k)$. Tale processo deve terminare poiché

  $$n_1 n_2 \cdot \ldots \cdot n_k = [F[\alpha_1, \dots, \alpha_k] : F] = [F[\alpha_1, \dots, \alpha_k] : F[\alpha_1, \dots, \alpha_{k-1}]]\,[F[\alpha_1, \dots, \alpha_{k-1}] : F],$$

dove $n_j = [F[\alpha_1, \dots, \alpha_j] : F[\alpha_1, \dots, \alpha_{j-1}]] > 1$. D'altronde $n_1 \cdot \ldots \cdot n_k \mid [E : F] < \infty$, per cui deve esistere $k_0$ tale che

$$n_1 \cdot \ldots \cdot n_{k_0} = [E : F] \implies E = F[\alpha_1, \dots, \alpha_{k_0}].$$

Supponiamo che $E/F$ sia un'estensione finitamente generata, con $E = F[\alpha_1, \dots, \alpha_k]$, e algebrica. Dobbiamo mostrare che è finita. ⇐)

- Se $k = 1$ allora $E = F[\alpha]/F$ è finita di grado $\deg f_\alpha$ poichè $F[\alpha]$ risulta essere un campo col gambo.
- Se $k > 1$ possiamo scrivere $E = F[\alpha_1, \dots, \alpha_{k-1}][\alpha_k]$ che per induzione ci dice che $F[\alpha_1, \dots, \alpha_{k-1}]/F$ è finita. Inoltre $E/F[\alpha_1, \dots, \alpha_{k-1}]$ è finita perché è un campo col gambo, il cui gambo è il polinomio minimo $f_{\alpha_k}$ su $F[\alpha_1, \dots, \alpha_{k-1}][\alpha_k]$ e il suo grado è

$$[E : F] = \underbrace{[E : F[\alpha_1, \dots, \alpha_{k-1}]]}_{<\infty} \underbrace{[F[\alpha_1, \dots, \alpha_{k-1}] : F]}_{<\infty} < \infty. \qquad \square$$

**Corollario.** Siano $E/F$ un'estensione algebrica e $R$ un anello tale che $F \subset R \subset E$. Allora $R$ è un campo.

*Dimostrazione.* Preso $\alpha \in R \setminus \{0\}$ avremo che $\alpha$ è algebrico su $F$ in quanto elemento di $E$. Ora $F[\alpha]$ è algebrico e finitamente generato, quindi per la proposizione precedente $F[\alpha]$ è finito, ovvero $F[\alpha] = F(\alpha)$. Da cui segue

$$\frac{1}{\alpha} \in F[\alpha] \subset R,$$

poiché ciò vale per ogni elemento non nullo di $R$, segue che $R$ è un campo. $\square$

**Corollario.** Siano $E/F$ e $L/E$ due estensioni algebriche. Allora $L/F$ è un'estensione algebrica.

*Dimostrazione.* Sia $\alpha \in L$. Dal momento che $L/E$ è algebrica esisterà $f \in E[X]$ monico tale che $f(\alpha) = 0$. Dove

$$f(X) = X^m + a_1 X^{m-1} + \ldots + a_m, \qquad \text{con } a_j \in E.$$

Per ipotesi $E/F$ è algebrica, per cui $a_j \in E \implies F[a_1, \dots, a_m]$ è ancora algebrica su $F$, inoltre è finitamente generata. Quindi per la proposizione $F[a_1, \dots, a_m]/F$ è finita. Inoltre anche

$$F[a_1, \dots, a_m, \alpha]/F[a_1, \dots, a_m],$$

è finita poiché $F[a_1, \dots, a_m, \alpha] = F[a_1, \dots, a_m][\alpha]$ è l'anello col gambo su $F[a_1, \dots, a_m]$. Quindi per la la formula del grado avremo

$$[F[a_1, \dots, a_m, \alpha] : F] = [F[a_1, \dots, a_m, \alpha] : F[a_1, \dots, a_m]] [F[a_1, \dots, a_m] : F] < +\infty.$$

Ovvero $F[a_1, \dots, a_m, \alpha]$ è finito, e quindi algebrico, su $F$. $\square$

## 1.11 NUMERI TRASCENDENTI

Un numero complesso si dice *algebrico* o *trascendente* secondo che sia algebrico o trascendente su $\mathbb{Q}$. Per comodità definiamo l'insieme dei numeri algebrici

$$\mathbb{A} = \{ \alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q} \}.$$

Si può dimostrare che $\mathbb{A}$ è un campo e che ha cardinalità numerabile.

Ora riportiamo alcuni cenni storici:

**1844** Liouville dimostra l'esistenza di numeri trascendenti, ovvero che $\mathbb{C} - \mathbb{A} \neq \emptyset$.

**1873** Hermite dimostra che $e$ è un numero trascendente.

**1874** Cantor dimosta che l'insieme $\mathbb{A}$ è numerabile e che $\mathbb{R}$ non lo è. Ciò prova che la maggior parte dei reali sono trascendenti, anche se è molto difficile dimostrare che un numero specifico lo sia.

**1882** Lindemann dimostra che $\pi$ è trascendente.

**1934** Gel'fond dimostra che se $\alpha$ e $\beta$ sono algebrici con $\alpha, \beta \neq 0, 1$ e $\beta \notin \mathbb{Q}$, allora $\alpha^\beta$ è trascendente.

**2016** Non è stato ancora dimostrato se la costante di Eulero-Mascheroni

$$\gamma = \lim_{N \to +\infty} \left( \sum_{n=1}^{N} \frac{1}{n} - \ln N \right),$$

è trascendente o addirittura se è irrazionale.

**2016** Nonostante i numeri $\pi + e$ e $\pi - e$ siano certamente trascendenti non è stato ancora dimostrato se sono irrazionali.

**Proposizione 1.44 – Numerabilità dell'insieme dei numeri algebrici**

L'insieme $\mathbb{A}$ dei numeri algebrici è numerabile.

*Dimostrazione.* Definiamo l'altezza $H(r)$ di un razionale $r = n/m$, con $(n, m) = 1$ e $n \in \mathbb{Z}, m \in \mathbb{N}$, come

$$H(r) = \max |n|, m.$$

È è facile convincersi che vi sono solo un numero finito di razionali con la proprietà di avere l'altezza minore di un certo $N$ fissato. Definiamo inoltre l'altezza di un polinomio monico come

$$H(a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + X^n) = \max\{ H(a_0), \ldots, H(a_{n-1}) \}.$$

La strategia è mostrare che, definito $B_n = \{ \alpha \in \mathbb{A} \mid \deg f_\alpha \leqslant n, H(f_\alpha) \leqslant n \}$, si abbia

$$\mathbb{A} = \bigcup_{n \in \mathbb{N}} B_n \qquad \text{e} \qquad \#B_n < +\infty.$$

Da cui seguirebbe che $\#\mathbb{A}$ è numerabile in quanto unione numerabile di insiemi finiti. Anche in questo caso è facile convincersi che $\#B_n$ è finito. □

**Teorema 1.45 – Trascendenza di un numero di Liouville**

Il seguente numero di Liouville

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{2^{n!}}$$

è trascendente.

*Dimostrazione.* Supponiamo per assurdo che $\alpha$ sia algebrico. Scriviamo il polinomio minimo di $\alpha$:

$$f_\alpha(X) = X^d + a_1 X^{d-1} + \ldots + a_d, \qquad \text{con } a_j \in \mathbb{Q}.$$

Fissato $N \in \mathbb{N}$ definiamo

$$\Sigma_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}.$$

Chiaramente avremo che $\Sigma_N \in \mathbb{Q}$ e $\Sigma_N \to \alpha$ monotonicamente. Inoltre avremo che $X_N = f_\alpha(\Sigma_N) \in \mathbb{Q} - \{0\}$, in quanto $f_\alpha$ è un polinomio irriducibile in $\mathbb{Q}$ e pertanto non può avere radici razionali a meno che non sia di grado uno, ma in tal caso la sua unica radice sarebbe $\alpha$.
Sia $D \in \mathbb{Z}$ tale che $D\, f_\alpha(X) \in \mathbb{Z}[X]$, per cui avremo

$$(2^{N!})^d D\, X_n \in \mathbb{Z} - \{0\} \qquad \text{e} \qquad 1 \leqslant |(2^{N!})^d D\, X_N|.$$

Ora per il Teorema Fondamentale dell'Algebra

$$f_\alpha(X) = (X - \alpha)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_d),$$

da cui

$$|X_N| = |\Sigma_N - \alpha| \prod_{j=2}^{d} |\Sigma_N - \alpha_j|.$$

In particolare, da $k \geqslant N + 1 \implies k! - (N+1)! \geqslant k$, avremo

$$|\Sigma_N - \alpha| = \sum_{k=N+1}^{\infty} \frac{1}{2^{k!}} \leqslant \frac{1}{2^{(N+1)!}} \sum_{k=0}^{\infty} \frac{1}{2^k} \leqslant \frac{2}{2^{(N+1)!}}$$

Inoltre

$$|\Sigma_N - \alpha_j| \leqslant \Sigma_N + |\alpha_j| \leqslant \alpha + M, \qquad \text{con } M = \max\{|\alpha_2|, \ldots, |\alpha_d|\}.$$

Quindi

$$|X_N| \leqslant \frac{2}{2^{(N+1)!}} (\alpha + M)^{d-1},$$

ovvero

$$1 \leqslant |(2^{N!})^d D\, X_N| \leqslant \frac{(2^{N!})^d 2}{2^{(N+1)!}} (\alpha + M)^{d-1} = \left(\frac{2^d}{2^{N+1}}\right)^{N!} 2(\alpha + M)^{d-1},$$

che tende a zero, da cui l'assurdo. □

## 1.12 CAMPI ALGEBRICAMENTE CHIUSI

**Notazione.** Diciamo che un polinomio si *spezza* su un campo $F$ se può essere scritto come prodotto di polinomi di grado 1 in $F[X]$.

**Definizione 1.46 – Campo algebricamente chiuso**

Un campo $\Omega$ si dice *algebricamente chiuso* se ogni polinomio non costante in $\Omega[X]$ si spezza in $\Omega$.

*Osservazione.* $\mathbb{C}$ è algebricamente chiuso come immediata conseguenza del Teorema Fondamentale dell'Algebra.

**Proposizione 1.47 – Caratterizzazione di campi algebricamente chiusi**

Sia $\Omega$ un campo, allora le seguenti affermazioni sono equivalenti:

1. Ogni polinomio non costante in $\Omega[X]$ si spezza in $\Omega$.
2. Ogni polinomio non costante in $\Omega$ ha almeno una radice in $\Omega$.
3. Se un polinomio su $\Omega[X]$ è irriducibile allora ha grado 1.
4. Se $E/\Omega$ è un'estensione finita allora $E = \Omega$.

*Dimostrazione.* Le implicazioni $(1) \implies (2) \implies (3) \implies (1)$ sono ovvie.

$(3) \implies (4)$ Sia $E/\Omega$ un'estensione finita e sia $\alpha \in E$. Il polinomio minimo $f_\alpha(X) \in \Omega[X]$ è irriducibile, quindi, per ipotesi, $\deg f_\alpha = 1$. In particolare

$$f_\alpha(X) = X - \alpha \implies \alpha \in \Omega,$$

da cui $E \subseteq \Omega$.

$(4) \implies (3)$ Sia $f(X) \in \Omega[X]$ un polinomio irriducibile. Consideriamo $\Omega' = \Omega[X]/(f)$, avremo che $\Omega'/\Omega$ è un'estensione finita con

$$[\Omega' : \Omega] = \deg f.$$

D'altronde per ipotesi $\Omega' = \Omega$, quindi $1 = [\Omega' : \Omega] = \deg g$. □

*Osservazione.* $\mathbb{C}(X)/\mathbb{C}$ è un'estensione non banale di $\mathbb{C}$ ma è infinita.

**Definizione 1.48 – Chiusura algebrica**

Un'estensione $\Omega/F$ si definisce *chiusura algebrica* di $F$ se

- $\Omega/F$ è un'estensione algebrica.
- $\Omega$ è algebricamente chiuso.

**Esempio.** $\mathbb{C}/\mathbb{R}$ è una chiusura algebrica, d'altronde $\mathbb{C}/\mathbb{Q}$ non lo è in quanto non è un'estensione algebrica.

**Proprietà 1.49.** Sia $\Omega/F$ è un'estensione algebrica e supponiamo che per ogni $f \in F[X]$ si abbia che $f$ si spezza in $\Omega[X]$. Allora $\Omega$ è algebricamente chiuso.

*Dimostrazione.* Sia $f \in \Omega[X]$ con $\deg f \geqslant 1$. Vogliamo trovare una radice di $f$ in $\Omega$. Scriviamo il polinomio come

$$f(X) = a_n X^n + \ldots + a_1 X + a_0, \qquad \text{con } a_j \in \Omega.$$

Supponiamo per assurdo che $f$ sia irriducibile. Allora possiamo trovare un'estensione $L/\Omega$ tale che $f$ ha una radice in $L$. Infatti è sufficiente prendere $L = \Omega[X]/(f)$. In particolare avremo $L/\Omega$ finita e $f(\alpha) = 0$ per una certa $\alpha \in L$. Inoltre

$$F \subseteq F[a_0, \ldots, a_n] \subseteq F[a_0, \ldots, a_n, \alpha] \subseteq L = \Omega[\alpha].$$

Dove la prima estensione è finita in quanto algebrica e finitamente generata, mentre la seconda lo è poiché costruita con la radice di un polinomio nel campo di partenza. Quindi per la la formula del grado avremo che $F[a_0, \ldots, a_n, \alpha]/F$ è finita, e in particolare

$\alpha$ soddisfa un polinomio irriducibile in $F[X]$. Ovvero esiste $g \in F[X]$ tale che $g(\alpha) = 0$. Ora, per ipotesi, $g$ si spezza in $\Omega$, per cui $\alpha \in \Omega$. □

*Osservazione.* In particolare $\Omega$ è una chiusura algebrica di $F$.

**Proprietà 1.50.** Sia $E/F$ un'estensione, allora

$$\mathbb{A}_{E/F} = \{\, \alpha \in E \mid \alpha \text{ è algebrico su } F \,\}$$

è un campo.

*Dimostrazione.* Siano $\alpha, \beta$ elementi algebrici di $F$. Allora $F[\alpha, \beta]$ è un campo ed un'estensione finita di $F$, in quanto algebrico e finitamente generato. In particolare ogni elemento di $F[\alpha, \beta]$ sarà algebrico su $F$, compresi

$$\alpha + \beta; \qquad \alpha\,\beta; \qquad \frac{\alpha}{\beta}.$$

□

# 2 | CAMPI DI SPEZZAMENTO E RADICI MULTIPLE

## 2.1 OMOMORFISMI FRA ESTENSIONI

**Definizione 2.1 – Omomorfismo di campi**

Siano $E/F$ e $E'/F$ estensioni di $F$. Si definisce $F$-omomorfismo un omomorfismo

$$\varphi\colon E \to E',$$

tale che $\varphi(a) = a$ per ogni $a \in F$.

*Osservazione.* Un $F$-omomorfismo è iniettivo in quanto omomorfismo di campi.

*Osservazione.* Se $[E : F] = [E' : F] < +\infty$ allora $\varphi$ è un isomorfismo in quanto omomorfismo iniettivo fra spazi della stessa dimensione.

*Osservazione.* Se $\varphi$ è un $F$-omomorfismo e $g \in F[X]$ allora

$$g\big(\varphi(\beta)\big) = \varphi\big(g(\beta)\big) \;\forall\; \beta \in F[\alpha].$$

**Proprietà 2.2.** Sia $F(\alpha)$ un'estensione semplice di $F$ e sia $E/F$ un'altra estensione. Supponiamo che $\alpha$ sia trascendente su $F$. Allora per ogni $F$-omomorfismo $\varphi\colon F(\alpha) \to E$, si ha $\varphi(\alpha)$ trascendente su $F$. Inoltre vi è una corrispondenza biunivoca

$$\{\, \varphi\colon F(\alpha) \to E \mid \varphi \text{ } F\text{-omomorfismo} \,\} \longleftrightarrow \{\, x \in E \mid x \text{ trascendente su } F \,\}$$

tramite

$$\varphi \longmapsto \varphi(\alpha) \qquad \text{e} \qquad \left(\frac{f(\alpha)}{g(\alpha)} \mapsto \frac{f(x)}{g(x)}\right) \longmapfrom x.$$

↦ *Dimostrazione.* Supponiamo che $\varphi\colon F(\alpha) \to E$ sia un $F$-omomorfismo. La mappa $\varphi \mapsto \varphi(\alpha)$ è ben definita, infatti se per assurdo esistesse $g \in F[X]$ tale che $g\big(\varphi(\alpha)\big) = 0$, allora avremmo

$$0 = g\big(\varphi(\alpha)\big) = \varphi\big(g(\alpha)\big) \implies g(\alpha) = 0,$$

che è assurdo per la trascendenza di $\alpha$.

↤ Supponiamo che $x \in E$ sia trascendente su $F$. La mappa $x \longmapsto (\alpha \mapsto x)$ definisce l'omomorfismo $\varphi\colon F(\alpha) \to E, \alpha \mapsto x$, il quale si estende in modo unico a

$$F[\alpha] \to F[x] \subset E, h(\alpha) \mapsto h(x),$$

da cui

$$F(\alpha) \to F(x) \subset E, \frac{h_1(\alpha)}{h_2(\alpha)} \mapsto \frac{h_1(x)}{h_2(x)}.$$

Si mostra facilmente che una funzione è l'inversa dell'altra. □

**Proprietà 2.3.** Sia $F(\alpha)$ un'estensione semplice di $F$ e sia $E/F$ un'altra estensione. Supponiamo che $\alpha$ sia algebrico su $F$ e che $f_\alpha(X)$ sia il suo polinomio minimo. Allora per ogni $F$-omomorfismo $\varphi\colon F[\alpha] \to E$, si ha che $\varphi(\alpha)$ è una radice di $f_\alpha(X)$ in $E$. Inoltre vi è una corrispondenza biunivoca

$$\{\, \varphi\colon F[\alpha] \to E \mid \varphi \text{ } F\text{-omomorfismo} \,\} \longleftrightarrow \{\, \gamma \in E \mid \gamma \text{ radice di } f_\alpha \,\}$$

tramite

$$\varphi \longmapsto \varphi(\alpha) \qquad \text{e} \qquad (\alpha \mapsto \gamma) \longleftarrow\!\shortmid\, \gamma.$$

*Dimostrazione.* Scriviamo il polinomio minimo di $\alpha$: $\mapsto$

$$f_\alpha(X) = X^n + a_1 X^{n-1} + \ldots + a_n.$$

Supponiamo $\varphi\colon F[\alpha] \to E$ sia un $F$-omomorfismo, mostriamo che $\varphi(\alpha)$ è una radice di $f_\alpha$:

$$\begin{aligned} f\big(\varphi(\alpha)\big) &= \varphi(a)^n + a_1\varphi(\alpha)^{n-1} + \ldots + a_{n-1}\varphi(\alpha) + a_n \\ &= \varphi(\alpha^n) + \varphi(a_1)\varphi(\alpha^{n-1}) + \ldots + \varphi(a_{n-1})\varphi(\alpha) + \varphi(a_n) \\ &= \varphi(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n) \\ &= \varphi\big(f_\alpha(\alpha)\big) = \varphi(0) = 0. \end{aligned}$$

*sfruttiamo l'ipotesi che $\varphi$ è un $F$-omomorfismo*

Viceversa se $\gamma$ è una radice di $f_\alpha$, dobbiamo mostrare che $\gamma \longmapsto (\alpha \mapsto \gamma)$ individua un ben definito $F$-omomorfismo $F[\alpha] \to E, \alpha \mapsto \gamma$. Ciò è vero in quanto $\longleftarrow\!\shortmid$

$$F[X] \to E, X \mapsto \gamma,$$

ha $(f_\alpha)$ come nucleo, per cui viene indotto l'omomorfismo

$$F[\alpha] = \frac{F[X]}{(f_\alpha)} \to E, \alpha \mapsto \gamma. \qquad \square$$

*Osservazione.* Dalla proposizione segue che se $F[\alpha]/F$ è algebrica, allora

$$\#\{\, \varphi\colon F[\alpha] \to E \mid \varphi \text{ } F\text{-omomorfismo} \,\} \leqslant \deg f_\alpha.$$

**Esempio.** Supponiamo che $F = \mathbb{Q}, \alpha = \sqrt{2}$ e $E = \mathbb{C}$. Stiamo quindi considerando i $\mathbb{Q}$-omomorfismi del tipo $\varphi\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{C}$. Per la proposizione vi è una corrispondenza biunivoca

$$\left\{\, \varphi\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{C} \;\middle|\; \varphi \text{ } \mathbb{Q}\text{-omomorfismo} \,\right\} \longleftrightarrow \{\, \gamma \in \mathbb{C} \mid \gamma \text{ radice di } X^2 - 2 \,\} = \{\sqrt{2}, -\sqrt{2}\}.$$

Per cui i $\mathbb{Q}$-omomorfismi possibili sono quelli tali che

$$\sqrt{2} \mapsto \sqrt{2} \qquad \text{oppure} \qquad \sqrt{2} \mapsto -\sqrt{2}.$$

**Teorema 2.4 – Corrispondenza fra F-omomorfismi di estensioni semplici**

Sia $F(\alpha)$ un estensione semplice di $F$ e sia $\varphi_0 \colon F \to E$ un omomorfismo di campi. Allora vi è una corrispondenza biunivoca:

- Se $\alpha$ è trascendente

$$\{\, \varphi \colon F(\alpha) \to E \mid \varphi|_F = \varphi_0, \varphi \text{ omom.} \,\} \longleftrightarrow \{\, x \in E \mid x \text{ trascendente su } \varphi_0(F) \,\}.$$

- Se $\alpha$ è algebrico

$$\{\, \varphi \colon F(\alpha) \to E \mid \varphi|_F = \varphi_0, \varphi \text{ omom.} \,\} \longleftrightarrow \{\, \beta \in E \mid \beta \text{ radice di } f_\alpha \,\}.$$

*Dimostrazione.* Questo teorema è una generalizzazione delle due proprietà precedenti. Non forniremo un'ulteriore dimostrazione. □

**Proprietà 2.5.** Supponiamo che $E_1, E_2$ siano campi aventi la stessa caratteristica. Allora gli omomorfismi $E_1 \to E_2$ sono $F$-omomorfismi, dove $F$ è il sottocampo fondamentale di entrambi, ovvero

$$F = \mathbb{Q} \qquad \text{oppure} \qquad F = \mathbb{F}_p.$$

## 2.2 CAMPI DI SPEZZAMENTO

**Definizione 2.6 – Campo di spezzamento**

Un'estensione $E/F$ si definisce *campo di spezzamento* di $f \in F[X]$ se

- $f$ si spezza in $E$:

$$f(X) = a \prod_{j=1}^{n} (X - \alpha_j), \qquad \text{con } \alpha_j \in E, n = \deg f.$$

- $E = F[\alpha_1, \dots, \alpha_n]$.

**Esempio.** $\mathbb{Q}[\sqrt{2}]$ è un campo di spezzamento per $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ in $\mathbb{Q}$

**Proprietà 2.7.** Sia $f \in F[X]$ e supponiamo

$$f = a \prod_{j=1}^{n} (X - \alpha_j).$$

Se $E/F$ è un campo di spezzamento per $f$, allora

$$E = F[\alpha_1, \dots, \alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}].$$

*Dimostrazione.* L'inclusione $F[\alpha_1, \dots, \alpha_n] \supseteq F[\alpha_1, \dots, \alpha_{n-1}]$ è banalmente vera. Per

dimostrare l'uguaglianza è quindi sufficiente mostrare che $\alpha_n \in F[\alpha_1, \ldots, \alpha_{n-1}]$. Ora

$$a X^n + a_1 X^{n-1} + \ldots + a_n = f(X) = a \prod_{j=1}^{n} (X - \alpha_j),$$

da cui

$$\frac{a_1}{a} = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n) \implies \alpha_n = -\frac{a_1}{a} - \alpha_1 - \ldots - \alpha_{n-1}. \qquad \square$$

**Esempio.** Troviamo un campo di spezzamento per $X^3 - 2 \in \mathbb{Q}[X]$. Posto $w = e^{\frac{2\pi i}{3}}$ avremo

$$X^3 - 2 = \prod_{j=0}^{2} (X - w^j 2^{\frac{1}{3}}).$$

Quindi un campo di spezzamento è $\mathbb{Q}[2^{\frac{1}{3}}, w\,2^{\frac{1}{3}}, w^2 2^{\frac{1}{3}}]$. Per la proposizione precedente avremo

$$\mathbb{Q}[2^{\frac{1}{3}}, w\,2^{\frac{1}{3}}, w^2 2^{\frac{1}{3}}] = \mathbb{Q}[2^{\frac{1}{3}}, w\,2^{\frac{1}{3}}].$$

Inoltre $\mathbb{Q}[2^{\frac{1}{3}}, w\,2^{\frac{1}{3}}] = \mathbb{Q}[2^{\frac{1}{3}}, w]$. Infine si può dimostrare che

$$\mathbb{Q}[2^{\frac{1}{3}}, w] = \mathbb{Q}[2^{\frac{1}{3}} + w].$$

**Esempio.** Un campo di spezzamento di $X^4 - 2$ è

$$\mathbb{Q}[2^{\frac{1}{4}}, -2^{\frac{1}{4}}, i\,2^{\frac{1}{4}}, -i\,2^{\frac{1}{4}}] = \mathbb{Q}[2^{\frac{1}{4}}, i\,2^{\frac{1}{4}}] = \mathbb{Q}[2^{\frac{1}{4}}, i].$$

**Esempio** (p-esimo polinomio ciclotomico)**.** Consideriamo il p-esimo polinomio ciclotomico

$$\phi_p(X) = 1 + \ldots + X^{p-1} = \prod_{j=1}^{p-1} (X - e^{\frac{2\pi i j}{p}}) = \prod_{j=1}^{p-1} (X - \zeta_p^j).$$

Tale polinomio ha come campo di spezzamento

$$\mathbb{Q}[\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}] = \mathbb{Q}[\zeta_p].$$

**Esempio** (Polinomio di grado 2)**.** Consideriamo un generico polinomio di secondo grado irriducibile in $\mathbb{Q}$:

$$f(X) = X^2 + a\,X + b.$$

Se $D_f = a^2 - 4b$ è il discriminante di $f$, allora un campo di spezzamento di $f$ è il seguente:

$$\mathbb{Q}\left[-\frac{a}{2} + \frac{\sqrt{D_f}}{2}, -\frac{a}{2} - \frac{\sqrt{D_f}}{2}\right] = \mathbb{Q}[\sqrt{D_f}].$$

**Esempio** (Polinomio di grado 3)**.** Consideriamo un generico polinomio di terzo grado irriducibile in $\mathbb{Q}$:

$$f(X) = X^3 + X^2 + b\,X + c = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

Sappiamo che $\mathbb{Q}[\alpha_1, \alpha_2]$ è un suo campo di spezzamento. Ora per la formula del

grado

$$\big[\mathbb{Q}[\alpha_1,\alpha_2]:\mathbb{Q}\big] = \big[\mathbb{Q}[\alpha_1,\alpha_2]:\mathbb{Q}[\alpha_1]\big]\big[\mathbb{Q}[\alpha_1]:\mathbb{Q}\big],$$

dove $\big[\mathbb{Q}[\alpha_1]:\mathbb{Q}\big] = 3$, mentre rispetto a $\mathbb{Q}[\alpha_1]$ possiamo considerare $\mathbb{Q}[\alpha_1,\alpha_2]$ come il campo di spezzamento del polinomio

$$\frac{f(X)}{X-\alpha_1} \in \mathbb{Q}[\alpha_1][X],$$

che ha grado 2. Per cui il grado $\big[\mathbb{Q}[\alpha_1,\alpha_2]:\mathbb{Q}[\alpha_1]\big]$ può essere 1 oppure 2.
In conclusione un polinomio irriducibile di grado 3 ha un campo di spezzamento di grado 3 oppure 6. Vedremo in seguito che il grado è 3 se e soltanto se $D_f$ è un quadrato perfetto.

## Proposizione 2.8 – Stima della dimensione del campo di spezzamento

Sia $f \in F[X]$ un polinomio di grado $n$. Allora esiste un campo di spezzamento $E/F$ di $f$ e vale

$$[E:F] \leqslant n!$$

*Dimostrazione.* Sia $f \in F[X]$ e sia $F_1 = F[\alpha_1]$, dove $\alpha_1$ è una radice di un fattore irriducibile di $f$. In particolare $f_{\alpha_1} \mid f$, da cui

$$[F_1:F] = \deg f_{\alpha_1} \leqslant \deg f.$$

Prendiamo ora $F_2 = F_1[\alpha_2]$, dove $\alpha_2$ è una radice di un fattore irriducibile di $f(X)/(x-\alpha_1) \in F_1[X]$. Avremo

$f_{\alpha_2} \in F_1[X]$

$$[F_2:F_1] = \deg f_{\alpha_2} \leqslant (\deg f - 1)$$

Iterando per ogni $2 \leqslant k \leqslant n$ troviamo $F_k = F_{k-1}[\alpha_k]$, dove $\alpha_k$ è una radice di un fattore irriducibile di

$$\frac{f(X)}{(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_{k-1})} \in F_{k-1}[X],$$

dove $[F_k:F_{k-1}] = \deg f_{\alpha_k} \leqslant (\deg f - k + 1)$, con $f_{\alpha_k} \in F_{k-1}[X]$. Infine avremo

$$F_n = F_{n-1}[\alpha_n] = \ldots = F[\alpha_1,\ldots,\alpha_n]$$

il quale sarà un campo di spezzamento di $f$. In particolare, per la formula del grado, avremo

*abbiamo posto* $F_0 = F$

$$[F_n:F] = \prod_{j=1}^{n}[F_j:F_{j-1}] \leqslant n!$$ □

*Osservazione.* A priori $1 \leqslant [E:F]$, d'altronde se $f$ è irriducibile in $F[X]$ si ha $n \leqslant [E:F]$ in quanto

$$E \supseteq F[\alpha] \supseteq F,$$

dove $\alpha$ è una radice di $f$ e sappiamo che $\big[F[\alpha]:F\big] = n$ Inoltre in tal caso vale anche $n \mid [E:F]$.

**Esempio.** Tramite l'osservazione precedente si può dimostrare facilmente quale sia il possibile grado del campo di spezzamento di un polinomio irrducibile di grado 3. Infatti se $E$ è il campo di spezzamento di $f \in F[X]$ avremo

$$3 \leqslant [E:F] \leqslant 3! \qquad \text{e} \qquad 3 \mid [E:F],$$

da cui

$$[E : F] = 3 \qquad \text{oppure} \qquad [E : F] = 6.$$

**Esempio.** Se $f \in F[X]$ è un polinomio irriducibile di grado 4 e se $E/F$ è un suo campo di spezzamento, avremo

$$4 \leqslant [E : F] \leqslant 4! = 24 \qquad \text{e} \qquad 4 \mid [E : F],$$

quindi i possibili gradi di $E$ sono $4, 8, 12, 16, 20, 24$

## Proposizione 2.9

Sia $f \in F[X]$ e siano $E_1/F, E_2/F$ due estensioni tali che $E_1$ è generata su $F$ da alcune radici di $f$; $E_2$ è tale che $f$ si spezza al suo interno. Allora

$$\{\, \varphi \colon E_1 \to E_2 \mid \varphi \text{ F-omomorfismo} \,\} \neq \emptyset.$$

Inoltre tale insieme contiene al più $[E_1 : F]$ elementi.

*Dimostrazione.* Per ipotesi $E_1 = F[\alpha_1, \ldots, \alpha_m]$, dove $\alpha_j$ sono radici di $f$. Il polinomio minimo di $\alpha_1$ è un polinomio irriducibile $f_1$ che divide $f$ e tale che $\deg f_1 = \big[F[\alpha_1] : F\big]$. Per ipotesi $f$ si spezza in $E_2$, quindi anche $f_1$ deve spezzarsi in $E_2$, inoltre le sue radici saranno distinte se lo erano quelle di $f$. Per la teorema 2.3 esisteranno degli F-omomorfismi

$$\varphi_1 \colon F[\alpha_1] \to E_2,$$

e tali omomorfismi saranno in numero al più uguale a $\big[F[\alpha_1] : F\big]$, e saranno proprio uguali nel caso in cui $f$ abbia tutte radici distinte in $E_2$.
Ora, il polinomio minimo di $\alpha_2$ su $F[\alpha_1]$ è un polinomio irriducibile $f_2$ che divide $f$ in $F[\alpha_1][X]$. Avremo che $\varphi_1(f_2) \in F[\alpha_1][X]$ e $\varphi_1(f_2) \mid f$, per cui $\varphi_1(f_2)$ si spezza in $E_2$ e le sue radici sono distinte se lo sono quelle di $f$. Sfruttando l'enunciato più generale della proposizione usata poc'anzi, ogni $\varphi_1$ si estende ad un omomorfismo

$$\varphi_2 \colon F[\alpha_1, \alpha_2] \to E_2$$

e tali estensioni saranno in numero al più uguale a $\deg f_2 = \big[F[\alpha_1, \alpha_2] : F[\alpha_2]\big]$, e saranno proprio uguali quando $f$ ha tutte radici distinte in $E_2$.
Combinando le precedenti affermazioni, possiamo concludere che esiste un F-omomorfismo

$$\varphi \colon F[\alpha_1, \alpha_2] \to E_2$$

il cui numero è al più $\big[F[\alpha_1, \alpha_2] : F[\alpha_1]\big]\big[F[\alpha_1] : F\big] = \big[F[\alpha_1, \alpha_2] : F\big]$.
Iterando questo procedimento fino a $m$ si giunge alla tesi. □

*Osservazione.* Il numero di elementi nell'insieme degli F-omomorfismi è precisamente $[E_1 : F]$ se $f$ ha tutte le radici distinte in $E_2$.

**Corollario.** Se $E_1/F, E_2/F$ sono campi di spezzamento di $f \in F[X]$, allora

$$E_1 \cong_F E_2.$$

*Dimostrazione.* Applichiamo la proposizione nel caso in cui $E_1, E_2$ sono due campi di spezzamento di $f$ su $F$. Otteniamo che esiste $\varphi \colon E_1 \to E_2$ che in quanto F-omomorfismo

è iniettivo, da cui

$$[E_1 : F] \leqslant [E_2 : F].$$

Applicando nuovamente la proposizione scambiando il ruolo di $E_1$ con $E_2$, otteniamo che esiste un altro $F$-omomorfismo $\psi\colon E_2 \to E_1$, la cui iniettività implica

$$[E_2 : F] \leqslant [E_1 : F].$$

Da ciò segue che $E_1, E_2$ hanno le stesso grado su $F$, per cui $\varphi, \psi$ sono isomorfismi. Ovvero

$$E_1 \cong_F E_2.$$

□

**Corollario.** Sia $E/F$ un'estensione finita e $L/F$ un'estensione qualsiasi. Allora

$$\#\{\, \varphi\colon E \to L \mid \varphi \text{ } F\text{-omomorfismo} \,\} \leqslant [E : F].$$

*Dimostrazione.* Per ipotesi $E/F$ è finita, quindi $E = F[\alpha_1, \dots, \alpha_m]$. Prendiamo $f = f_{\alpha_1} \cdot \dots \cdot f_{\alpha_m} \in F[X]$ il prodotto dei polinomi minimi di $\alpha_1, \dots, \alpha_m$.
Ora $f \in F[X] \subseteq L[X]$, sia $\Omega$ un campo di spezzamento di $f$ su $L$; in particolare $\Omega$ è un'estensione di $L$ dove $f$ si spezza. Per la proposizione precedente

$$\#\{\, \varphi\colon E \to \Omega \mid \varphi \text{ } F\text{-omomorfismo} \,\} \leqslant [E : F].$$

D'altronde ogni omomorfismo $\tilde{\varphi}\colon E \to L$ può essere composto con l'inclusione $L \hookrightarrow \Omega$. In conclusione

$$\#\{\, \varphi\colon E \to L \mid \varphi \text{ } F\text{-omomorfismo} \,\} \leqslant \#\{\, \varphi\colon E \to \Omega \mid \varphi \text{ } F\text{-omomorfismo} \,\} \leqslant [E : F].$$ □

**Esempio.** Consideriamo $E = \mathbb{Q}[\sqrt[3]{2}]$ che sappiamo avere $[E : F] = 3$. Per il corollario precedente, ciò significa che $\mathbb{Q}[\sqrt[3]{2}]$ può essere immerso in al più 3 modi distinti in $\mathbb{C}$. Da alcuni esempi precedenti si capisce facilmente che tali omomorfismi sono del tipo:

$$\varphi_1\colon \sqrt[3]{2} \mapsto \sqrt[3]{2}; \qquad \varphi_2\colon \sqrt[3]{2} \mapsto w\sqrt[3]{2}; \qquad \varphi_3\colon \sqrt[3]{2} \mapsto w^2\sqrt[3]{2},$$

dove $w = e^{\frac{2\pi i}{3}}$.

**Corollario.** Supponiamo di avere una famiglia di estensioni finite $E_1/F, E_2/F, \dots, E_k/F$. Allora esiste un'estensione finita $\Omega/F$ tale che

$$\Omega \supseteq \tilde{E}_1, \dots \tilde{E}_k, \qquad \text{con } \tilde{E}_j \cong_F E_j.$$

*Dimostrazione.* DA FINIRE! □

## 2.3 RADICI MULTIPLE

Siano $f, g \in F[X]$. Anche quando $f, g$ non hanno divisori in comune in $F[X]$, ci si potrebbe aspettare che acquisiscano un fattore comune se ci si porta in un certo $\Omega[X]$ con $\Omega \supset F$. In realtà questo non accade, il massimo comun divisore non cambia quando si estende un campo.

**Proposizione 2.10 – Invarianza del MCD tramite estensione**

Siano $f, g \in F[X]$ e sia $\Omega/F$ un'estensione. Se $r(X)$ è il MCD di $f, g$ calcolato in $F[X]$, allora tale MCD non cambia quando lo si calcola in $\Omega[X]$.

*Dimostrazione.* Siano $r_F(X)$ e $r_\Omega(X)$ i MCD di $f, g$ calcolati rispettivamente in $F[X]$ e $\Omega[X]$.
$r_F(X) \in F[X] \subseteq \Omega[X]$, quindi per le proprietà del MCD si avrà

$$r_F(X) \mid r_\Omega(X).$$

D'altronde in $F[X]$ varrà l'identità di Bezout rispetto a $r_F(X)$, ovvero esisteranno $a, b \in F[X]$ tali che

$$a(X)f(X) + b(X)g(X) = r_F(X) \in F[X] \subseteq \Omega[X].$$

Ora $r_\Omega(X)$ in quanto MCD di $f, g$ in $\Omega[X]$ divide ogni combinazione dei due polinomi, in particolare

$$r_\Omega(X) \mid r_F(X),$$

da cui la tesi. □

*Osservazione.* In particolare, polinomi monici irriducibili in $F[X]$ non acquisiscono radici in comune in nessuna estensione di $F$.

**Definizione 2.11 – Insieme dei polinomi irriducibili**

SIa $F$ un campo, si definisce l'insieme $\mathrm{Irr}(F)$ dei polinomi irriducibili di $F[X]$ come l'insieme dei polinomi $f$ tali che

- $f$ monico;
- $\deg f \geqslant 1$;
- $f$ non ha fattori propri.

**Definizione 2.12 – Molteplicità di una radice**

Sia $f \in F[X]$ e sia $F_f$ un suo campo di spezzamento. Scritto

$$f(X) = a \prod_{j=1}^{k} (X - \alpha_j)^{m_j}, \qquad \text{con } \alpha_1, \dots, a_k \in F_f,$$

gli interi $m_1, \dots, m_k \in \mathbb{N}^{\geqslant 1}$ si definiscono *molteplicità* di $f$ su $F_f$.

**Notazione.** Una radice $\alpha_j$ si dice *semplice* se $m_j = 1$. Viceversa se $m_j \geqslant 2$, $a_j$ si dice *multipla*.

*Osservazione.* Per definizione si ha

$$\sum_{j=1}^{k} m_j = \deg f.$$

*Osservazione.* Come diretta conseguenza del teorema 2.2 La molteplicità di una radice è invariante rispetto alla scelta del campo di spezzamento.

**Esempio.** Sia $F = \mathbb{F}_p(T)$ e prendiamo $f(X) = X^p - T \in F[X]$. Mostriamo che $f$ è irriducibile e che ha una sola radice in qualsiasi campo di spezzamento $F_f$.
Sia $\alpha$ una radice di un fattore irriducibile di $f(X)$, consideriamo il campo col gambo $F[\alpha], \alpha^p = T$. Se adesso consideriamo $f(X) \in F[\alpha][X]$ avremo, per la "formula sbagliata",

$$X^p - T = (X - \alpha)^p,$$

da cui segue che la molteplicità di $\alpha$ è $p$.
Infine $X^p - T$ è irriducibile perché se $g \in F[X]$ fosse un divisore di $f$, si avrebbe

$$g(X) = (X - \alpha)^k \in F[X].$$

D'altronde

$$(X - \alpha)^k = X^k - k\,\alpha\,X^{k-1} + \ldots \implies k\,\alpha \in F \implies k = 0,$$

da cui $p \mid k$ ma $k \leqslant p$, quindi $k = p$. Per cui

$$g(X) = (X - \alpha)^p = f(X).$$

## Definizione 2.13 – Derivata formale

Sia $f \in F[X]$ un generico polinomio del tipo

$$f(X) = \sum_{j=0}^{n} a_j X^k, \qquad \text{con } a_j \in F.$$

Definiamo la *derivata formale* $f'(X)$ di $f(X)$ come

$$f'(X) = \sum_{j=0}^{n} j\,a_j X^{j-1}.$$

**Proprietà 2.14.** Siano $f, g \in F[X]$, allora valgono le seguenti identità:

$$(f+g)'(X) = f'(X) + g'(X) \qquad \text{e} \qquad (f \cdot g)'(X) = f'(X)g(X) + f(X)g'(X).$$

*Dimostrazione.* Basta verificarlo con la definizione. □

## Proposizione 2.15 – Caratterizzazione delle radici multiple

Sia $f \in F[X]$ con $\deg f \geqslant 1$ e $f$ irriducibile. Allora le seguenti affermazioni sono equivalenti:

1. $f$ ha una radice multipla.
2. $(f, f') \neq 1$.
3. $F$ ha caratteristica $p$ ed esiste $g \in F[X]$ tale che $f(X) = g(X^p)$.
4. Tutte le radici di $f$ sono multiple.

*Dimostrazione.* Supponiamo che $\alpha \in F_f$ sia una radice multipla di $f$. Allora esiste $g \in F_f[X]$ tale che (1) $\Longrightarrow$ (2)

$$f(X) = (X-\alpha)^2 g(X) \in F_f[X].$$

Passando alla derivata otteniamo

$$f'(X) = 2(X-\alpha)\, g(X) + (X-\alpha)^2 g'(X) = (X-\alpha)\, h(X) \in F_f[X],$$

da cui $(X-\alpha) \mid (f, f')$.
Supponiamo che $(f, f') \neq 1$. Allora, per l'irriducibilità di $f$, avremo (2) $\Longrightarrow$ (3)

$$(f, f') = f.$$

In particolare $f \mid f' \implies f' = 0$ in quanto $\deg f' < \deg f$. Ora

$$f(X) = a_0 + a_1 X + \ldots + a_{m-1} X^{m-1} + a_m X^m,$$

da cui

$$0 = f'(X) = a_1 + 2a_2 X + \ldots + (m-1) a_{m-1} X^{m-2} + m\, a_m X^{m-1},$$

quindi per ogni $j = 1, \ldots, m$ si ha $j \cdot a_j = 0$, ovvero $j = 0$ oppure $a_j = 0$. Da ciò segue immediatamente che $F$ ha caratteristica $p$, poiché altrimenti si avrebbe $a_j = 0 \,\forall\, j$, che contraddice l'ipotesi $\deg f \geqslant 1$.
In particolare se $p \nmid j$ si ha $a_j = 0$, da cui

$$f(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \ldots + a_{k\,p} X^{k\,p}, \qquad \text{con } k\,p = m.$$

Quindi se prendiamo $g(X) = a_0 + a_p X + \ldots a_{k\,p} X^k \in F[X]$ otteniamo

$$f(X) = g(X^p).$$

Supponiamo che $F$ abbia caratteristica $p$ e che esista $g \in F[X]$ tale che $f(X) = g(X^p)$. (3) $\Longrightarrow$ (4)
Fissato un campo di spezzamento $F_f$ di $f$, avremo

$$g(X) = \prod_{j=1}^{k} (X - \alpha_j)^{m_j}, \qquad \text{con } \alpha_j \in F_f,$$

da cui

$$f(X) = g(X^p) = \prod_{j=1}^{k} (X^p - \alpha_j)^{m_j}.$$

Ora da $\operatorname{Char} F = p$ segue $\alpha_j^p = \alpha_j$, quindi possiamo applicare la "formula sbagliata":

$$f(X) = \prod_{j=1}^{k} (X^p - \alpha_j)^{m_j} = \prod_{j=1}^{k} (X^p - \alpha_j^p)^{m_j} = \prod_{j=1}^{k} (X - \alpha_j)^{p\, m_j},$$

dove $m_j\, p > 1$.
Conseguenza ovvia. □ (4) $\Longrightarrow$ (1)

**Definizione 2.16 – Polinomio separabile**

Un polinomio $f \in F[X]$ si dice *separabile* se ha solo radici semplici.

**Proposizione 2.17 – Caratterizzazione dei polinomi separabili**

Sia $f \in F[X]$. Allora $f$ è separabile se e soltanto se $(f, f') = 1$.

⇒) *Dimostrazione.* Supponiamo che $f$ sia separabile. Se per assurdo esistesse $h \in F[X]$ tale che

$$h \mid f \qquad \text{e} \qquad h \mid f',$$

fissato un campo di spezzamento $F_f$, se $h(\alpha) = 0$, si avrebbe

$$(X-\alpha) \mid f(X) \qquad \text{e} \qquad (X-\alpha) \mid f'(X),$$

da cui $(X-\alpha)^2 \mid f(X)$, ovvero $\alpha$ ha molteplicità maggiore di uno, che è assurdo per ipotesi.

⇐) Supponiamo che $(f, f') = 1$. Se per assurdo $\alpha$ fosse una radice di $f$ con molteplicità maggiore di uno, si avrebbe

$$(X-\alpha)^2 \mid f \implies (X-\alpha) \mid f',$$

da cui $(X-\alpha) \mid (f, f')$ che è assurdo. □

*Osservazione.* In generale un polinomio $f \in F[X]$ può essere non separabile se

- $f(X) = f_1^{m_1} \cdot \ldots \cdot f_t^{m_t}$ dove $f_j \in F[X]$ ed esiste $j$ tale che $m_j \geqslant 2$.
- $f(X) = f_1 \cdot \ldots \cdot f_t$ con $f_j$ distinti, $F$ ha caratteristica $p$ ed esiste $j_0$ tale che $f_{j_0} = g(X^p)$.

## Definizione 2.18 – Campo perfetto

Un campo $F$ si dice *perfetto* se ogni polinomio $f \in \mathrm{Irr}(F)$ è separabile.

*Osservazione.* Tutti i campi di caratteristica zero sono perfetti.

## Proposizione 2.19 – Caratterizzazione dei campi perfetti di caratteristica $p$

Sia $F$ un campo di caratteristica $p$. Allora $F$ è perfetto se e soltanto se per ogni $\alpha \in F$, $\alpha$ è un $p$-esima potenza in $F$, ovvero

$$\exists\, \beta \in F : \alpha = \beta^p.$$

⇒) *Dimostrazione.* Sia $F$ perfetto. Supponiamo per assurdo che $a \in F$ non sia una $p$-esima potenza. Consideriamo $f(X) = X^p - a \in F[X]$, vogliamo mostrare che $f$ è irriducibile e non separabile, da cui seguirebbe l'assurdo. Sia $\alpha$ una radice di un fattore irriducibile di $f(X)$ e consideriamo il campo col gambo

$$F[\alpha], \qquad \alpha^p = a.$$

Quindi se consideriamo $f(X) \in F[\alpha][X]$ avremo

$$X^p - a = X^p - \alpha^p = (X-\alpha)^p$$

*ricordiamo che in un campo di caratteristica $p$ vale la "formula sbagliata".*

da cui segue che la molteplicità di $\alpha$ è $p$, per cui $f$ non è separabile.
Inoltre $f$ è irriducibile poiché se $g(X) \in F[X]$ fosse un divisore di $f(X)$, si avrebbe

$$g(X) = (X-\alpha)^k \in F[X].$$

D'altronde

$$(X-\alpha)^k = X^k - k\,\alpha\, X^{k-1} + \ldots \implies k\,\alpha \in F \implies k = 0,$$

da cui $p \mid k$ ma $k \leqslant p$, quindi $k = p$. Ovvero

$$g(X) = (X-\alpha)^p = f(X).$$

⇐) Supponiamo che ogni $a \in F$ sia una $p$-esima potenza. Se per assurdo $F$ non fosse perfetto, esisterebbe $f \in \mathrm{Irr}(F)$ non separabile. Per la teorema 2.15 esiste $g(X) \in F[X]$ tale che $f(X) = g(X^p)$. Inoltre per ipotesi

$$g(X) = a_0 + a_1X + \ldots + a_nX^n = b_0^p + b_1^pX + \ldots + b_n^pX^n,$$

da cui, applicando la "formula sbagliata",

$$f(X) = g(X^p) = (b_0 + b_1X + \ldots + b_nX^n)^p,$$

ovvero $f$ non è irriducibile. □

**Corollario.** Tutti i campi finiti sono perfetti.

*Dimostrazione.* Sia $F$ un campo finito e consideriamo $\varphi\colon F \to F, \alpha \mapsto \alpha^p$. $\varphi$ è l'*endomorfismo di Frobenius* che è un automorfismo quando $F$ è finito, per cui applicando la proposizione precedente si ha che $F$ è perfetto. □

**Corollario.** Se $F$ è un campo di caratteristica $p$ e $F/\mathbb{F}_p$ è algebrico, allora $F$ è perfetto.

*Dimostrazione.* Sia $\alpha \in F$, poiché $F/\mathbb{F}_p$ è algebrico, avremo che $\mathbb{F}_p[\alpha]$ è finito. In particolare $\alpha = \beta^p$, da cui la tesi. □

*Osservazione.* In conclusione i campi imperfetti sono i campi infiniti, trascendenti e di caratteristica $p$. Come ad esempio $\mathbb{F}_p(T)$.

# 3 IL TEOREMA FONDAMENTALE DI GALOIS

## 3.1 GRUPPI DI AUTOMORFISMI

**Definizione 3.1 – Gruppo degli automorfismi**

Sia $E/F$ un'estensione. Un $F$-isomorfismo $E \to E$ si dice $F$-*automorfismo* di $E$. Gli $F$-automorfismi di $E$ definiscono un gruppo

$$\mathrm{Aut}(E/F) = \{\, \varphi \colon E \to E \mid \varphi \text{ } F\text{-automorfismo} \,\}.$$

**Notazione.** In generale quando scriviamo $\mathrm{Aut}(E)$ faremo riferimento ad $E$ come estensione sul suo sottocampo fondamentale, che come sappiamo può essere $\mathbb{F}_p$ oppure $\mathbb{Q}$.

*Osservazione.* Con queste notazioni si ha

$$\mathrm{Aut}(E/F) \leqslant \mathrm{Aut}(E), \ \forall\, E/F.$$

Inoltre se $E \supseteq M \supseteq F$ vale

$$\mathrm{Aut}(E/M) \leqslant \mathrm{Aut}(E/F).$$

**Proposizione 3.2 – Dimensione del gruppo degli automorfismi di un campo di spezzamento**

Supponiamo che $E$ sia il campo di spezzamento di un polinomio separabile $f \in F[X]$. Allora

$$\#\,\mathrm{Aut}(E/F) = [E : F].$$

*Dimostrazione.* Applichiamo la proposizione teorema 2.9 ad $E_1 = E_2 = E$ che soddisfano le ipotesi, in quanto $E$ è il campo si spezzamento di un polinomio separabile. Quindi avremo

$$\#\{\, \varphi \colon E \to E \mid \varphi \text{ } F\text{-omomorfismo} \,\} = [E : F],$$

dove abbiamo messo l'uguaglianza al posto del minore uguale in quanto $f$, essendo separabile, ha tutte radici distinte in $E$. □

**Esempio.** Tramite la preposizione possiamo dedurre che $\mathbb{Q}[\sqrt[3]{2}]$ non è il campo di spezzamento di nessun $f \in \mathbb{Q}[X]$. Infatti sappiamo che

$$\mathrm{Aut}\left(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}\right) \longleftrightarrow \left\{ \gamma \in \mathbb{Q}[\sqrt[3]{2}] \;\middle|\; \gamma \text{ radice di } f_{\sqrt[3]{2}} = X^3 - 2 \right\}$$

e infatti

$$\#\,\mathrm{Aut}\left(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}\right) = 1 \neq 3 = \left[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}\right].$$

**Esempio.** $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-2})/\mathbb{Q}$ è il campo di spezzamento di $X^3 - 2 \in \mathbb{Q}[X]$. Quindi per la proposizione

$$\#\operatorname{Aut}\left(\mathbb{Q}(\sqrt[3]{2}, \sqrt{-2})/\mathbb{Q}\right) = \left[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-2}) : \mathbb{Q}\right] = 6.$$

Per la caratterizzazione dei gruppi di ordine 6, avremo che

$$\operatorname{Aut}\left(\mathbb{Q}(\sqrt[3]{2}, \sqrt{-2})/\mathbb{Q}\right) \in \{\mathbb{Z}/\mathbb{Z}_6, S_3\}.$$

Per determinare a quale gruppo sia effettivamente isomorfo dovremo stabilire se è abeliano o meno. Per prima cosa troviamo esplicitamente gli automorfismi

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt{-2}) \to \mathbb{Q}(\sqrt[3]{2}, \sqrt{-2}).$$

Osserviamo che $\sqrt[3]{2}$ e $\sqrt{-3}$ sono generatori del campo, quindi basta determinare le loro immagini per descrivere gli automorfismi. Inoltre

$$f_\alpha(\alpha) = 0 \implies f_\alpha\big(\sigma(\alpha)\big) = \sigma\big(f(\alpha)\big) = 0,$$

ovvero ogni radice di un polinomio minimo deve andare in un'altra radice, da cui

$$\sqrt[3]{2} \longmapsto \begin{cases} \sqrt[3]{2} \\ w\sqrt[3]{2} \\ w^2\sqrt[3]{2} \end{cases} \qquad \text{e} \qquad \sqrt{-3} \longmapsto \begin{cases} \sqrt{-3} \\ -\sqrt{-3} \end{cases}$$

Quindi

$$\sigma_1 : \begin{matrix} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \sqrt{-3} \longmapsto \sqrt{-3} \end{matrix} \qquad \sigma_2 : \begin{matrix} \sqrt[3]{2} \longmapsto w\sqrt[3]{2} \\ \sqrt{-3} \longmapsto \sqrt{-3} \end{matrix} \qquad \sigma_3 : \begin{matrix} \sqrt[3]{2} \longmapsto w^2\sqrt[3]{2} \\ \sqrt{-3} \longmapsto \sqrt{-3} \end{matrix}$$

$$\sigma_4 : \begin{matrix} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \sqrt{-3} \longmapsto -\sqrt{-3} \end{matrix} \qquad \sigma_5 : \begin{matrix} \sqrt[3]{2} \longmapsto w\sqrt[3]{2} \\ \sqrt{-3} \longmapsto -\sqrt{-3} \end{matrix} \qquad \sigma_6 : \begin{matrix} \sqrt[3]{2} \longmapsto w^2\sqrt[3]{2} \\ \sqrt{-3} \longmapsto -\sqrt{-3} \end{matrix}$$

Valutiamo la commutatività di $\sigma_2 \circ \sigma_6$:

$$\sigma_2 \circ \sigma_6(\sqrt{-3}) = \sigma_2(-\sqrt{-3}) = -\sqrt{-3};$$
$$\sigma_2 \circ \sigma_6(\sqrt[3]{2}) = \sigma_2(w^2\sqrt[3]{2}) = \sigma_2(w^2)\, w\sqrt[3]{2},$$

dove

$$\sigma_2(w) = \sigma_2\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = -\frac{1}{2} + \frac{1}{2}\sigma_2(\sqrt{-3}) = -\frac{1}{2} + \frac{\sqrt{-3}}{2} = w,$$

quindi

$$\sigma_2(w^2) w\sqrt[3]{2} = w^3\sqrt[3]{2} = \sqrt[3]{2}.$$

Segue che $\sigma_2 \circ \sigma_6 = \sigma_4$. Calcoliamo il viceversa:

$$\sigma_6 \circ \sigma_2(\sqrt{-3}) = \sigma_6(\sqrt{-3}) = -\sqrt{-3};$$
$$\sigma_6 \circ \sigma_2(\sqrt[3]{2}) = \sigma_6(w\sqrt[3]{2}) = \sigma_6(w)\, w^2\sqrt[3]{2},$$

dove

$$\sigma_6(w) = \sigma_6\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = -\frac{1}{2} + \frac{1}{2}\sigma_6(\sqrt{-3}) = -\frac{1}{2} - \frac{\sqrt{-3}}{2} = w^2,$$

quindi

$$\sigma_6(w) w^2\sqrt[3]{2} = w^4\sqrt[3]{2} = w\sqrt[3]{2}.$$

Segue che $\sigma_6 \circ \sigma_2 = \sigma_5$. Quindi

$$\operatorname{Aut}\left(\mathbb{Q}(\sqrt[3]{2}, \sqrt{-2})/\mathbb{Q}\right) \cong S_3,$$

poiché non è abeliano.

**Esempio.** $\mathbb{Q}(\sqrt[4]{2}, i)$ è il campo di spezzamento di $X^4 - 2 \in \mathbb{Q}[X]$. Per la proposizione

$$\#\operatorname{Aut}\left(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}\right) = \left[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}\right] = 8.$$

I gruppi di ordine 8 sono

$$\frac{\mathbb{Z}}{8\mathbb{Z}}; \qquad \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}; \qquad \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}; \qquad D_4; \qquad Q_8.$$

A quale di questi corrisponde $\operatorname{Aut}\left(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}\right)$ lo si determina in base al numero di elementi di ordine 2.

**Esempio** (Campo di spezzamento di un polinomio non separabile)**.** $\mathbb{F}_p(T, \alpha), \alpha^p = T$ è il campo di spezzamento di $X^p - T \in \mathbb{F}_p(T)$. Sappiamo che l'estensione $\mathbb{F}_p(T, \alpha)/\mathbb{F}_p(T)$ ha grado $p$, d'altronde

$$\operatorname{Aut}\left(\mathbb{F}_p(T, \alpha)/\mathbb{F}_p(T)\right) = \{id\}$$

in quanto

$$f_\alpha(X) = X^p - T = (X - \alpha)^p \implies \alpha \mapsto \alpha.$$

## Definizione 3.3 – Sottocampo invariante

Sia $E/F$ un estensione e sia $G \leqslant \operatorname{Aut}(E/F)$. Definiamo

$$E^G = \operatorname{Inv}(G) = \{\, \alpha \in E \mid \sigma\alpha = \alpha \,\forall\, \sigma \in G \,\}$$

un sottocampo di $E$, detto *sottocampo invariante di* $G$

*Osservazione.* Per ogni $G \leqslant \operatorname{Aut}(E/F)$, si ha che $F \subseteq E^G \subseteq E$ è un campo. Infatti per ogni $\alpha, \beta \in E^G$ e per ogni $\sigma \in G$, si ha

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta \qquad \text{e} \qquad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta.$$

**Proprietà 3.4.** Preso $E/F$ e $\operatorname{Aut}(E/F)$ vi è una relazione fra il reticolo dei sottocampi di $E/F$ e quello dei sottogruppi di $\operatorname{Aut}(E/F)$

$$\{\, M \text{ campo} \mid F \subseteq M \subseteq E \,\} \longleftrightarrow \{\, G \text{ gruppo} \mid G \leqslant \operatorname{Aut}(E/F) \,\}$$

tramite

$$M \longmapsto \operatorname{Aut}(E/M) \qquad \text{e} \qquad E^G \longmapsto G$$

*Osservazione.* Se $E$ è il campo di spezzamento di un polinomio separabile in $F[X]$ mostreremo che la corrispondenza è biunivoca. In altre parole

$$E^{\operatorname{Aut}(E/M)} = M \qquad \text{e} \qquad \operatorname{Aut}(E/E^G) = G.$$

**Teorema 3.5 – Lemma di Artin**

Sia $G$ un sottogruppo finito di $\mathrm{Aut}(E)$. Allora

$$[E : E^G] \leqslant \#G.$$

*Dimostrazione.* Sia $F = E^G$. Da $G$ finito avremo $G = \{\sigma_1, \dots, \sigma_m\}$ con $\sigma_1 = \mathrm{id}$. Presi $\alpha_1, \dots, \alpha_n \in E$, con $n > m$, mostreremo che $\alpha_1, \dots, \alpha_n$ sono $F$-linearmente dipendenti. Da ciò segue che $\dim_F E \leqslant m$.
Consideriamo il seguente sistema lineare:

$$\begin{cases} \sigma_1(\alpha_1)X_1 + \dots + \sigma_1(\alpha_n)X_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \sigma_m(\alpha_1)X_1 + \dots + \sigma_m(\alpha_n)X_n = 0 \end{cases}$$

che ha $m$ righe e $n$ colonne. Dal momento che $n > m$, vi sono più incognite che equazioni, per cui esiste una soluzione del sistema non banale.
Sia $(c_1, \dots, c_n) \in E^n$ una soluzione del sistema tale che abbia il minimo numero di componenti non nulle. A meno di riordinare le $\alpha_j$, possiamo supporre che $c_1 \neq 0$ e, siccome l'insieme delle soluzioni di un sistema omogeneo è invariante per moltiplicazione di scalari, possiamo assumere che $c_1 \in F$.
Se tutte le altre componenti $c_2, \dots, c_n$ appartengono a $F$, allora, dal momento che $\sigma_1 = \mathrm{id}$, sostituendo la soluzione alla prima riga del sistema si avrebbe

$$c_1\alpha_1 + \dots + c_n\alpha_n = 0,$$

ovvero $\alpha_1, \dots, \alpha_n$ sono $F$-linearmente dipendenti.
Supponiamo per assurdo che esista $j$ tale che $c_j \notin F = E^G$. Per la definizione di sottocampo invariante, segue che esiste $\sigma_k \in G$ tale che $\sigma_k c_j \neq c_j$. Se al sistema lineare sostituisco le soluzioni $c_j$ e applico ad ogni riga $\sigma_k$, ottengo:

$$\begin{cases} \sigma_k \circ \sigma_1(\alpha_1)\sigma_k(c_1) + \dots + \sigma_k \circ \sigma_1(\alpha_n)\sigma_k(c_n) = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \sigma_k \circ \sigma_m(\alpha_1)\sigma_k(c_1) + \dots + \sigma_k \circ \sigma_m(\alpha_n)\sigma_k(c_n) = 0 \end{cases}$$

D'altronde $G = \{\sigma_1, \dots, \sigma_m\} = \{\sigma_k\sigma_1, \dots, \sigma_k\sigma_m\}$, per cui abbiamo ottenuto uno scambio delle equazioni del sistema lineare. Inoltre $\big(\sigma_k(c_1), \dots, \sigma_k(c_n)\big)$ è ancora una soluzione e pertanto lo è anche

$$\big(\sigma_k(c_1) - c_1, \dots, \sigma_k(c_k) - c_k, \dots, \sigma_k(c_n) - c_n\big),$$

dove

$$\sigma_k(c_1) = c_1 \implies \sigma_k(c_1) - c_1 = 0 \qquad \text{e} \qquad \sigma_k(c_k) \neq c_k \implies \sigma_k(c_k) - c_k \neq 0.$$

Per cui abbiamo trovato un'altra soluzione del sistema che è non nulla ed ha uno zero in più della soluzione presa in ipotesi. Ciò è assurdo per la minimalità della soluzione $c_1, \dots, c_n$, da cui segue che $c_1, \dots, c_n \in F$ che implica la tesi. □

**Corollario.** Se $G$ è un sottogruppo finito di $\mathrm{Aut}(E)$ allora

$$\mathrm{Aut}(E/E^G) = G.$$

*Dimostrazione.* Dalle definizioni di sottocampo invariante e gruppo di automorfismi

$$E^G = \{\, \alpha \in E \mid \sigma\alpha = \alpha,\ \forall\ \sigma \in G \,\},$$
$$\mathrm{Aut}(E/E^G) = \left\{\, \sigma \in \mathrm{Aut}(E) \;\middle|\; \sigma\alpha = \alpha,\ \forall\ \alpha \in E^G \,\right\}.$$

Per cui è ovvio che $\mathrm{Aut}(E/E^G) \supseteq G$, da cui

$$\#G \leqslant \#\,\mathrm{Aut}(E/E^G).$$

Ora per il lemma di Artin $[E : E^G] \leqslant \#G$. Inoltre per un vecchio corollario avremo $\#\,\mathrm{Aut}(E/E^G) \leqslant [E : E^G]$. Quindi

$$[E : E^G] \leqslant \#G \leqslant \#\,\mathrm{Aut}(E/E^G) \leqslant [E : E^G],$$

da cui $\#G = \#\,\mathrm{Aut}(E/E^G)$ che implica la tesi. □

## 3.2 ESTENSIONI SEPARABILI, NORMALI E DI GALOIS

**Definizione 3.6 – Estensione separabile**

Un'estensione $E/F$ si dice *separabile* se il polinomio minimo $f_\alpha(X) \in F[X]$ di ogni elemento $\alpha \in E$ è separabile.

*Osservazione.* Quindi un'estensione $E/F$ è separabile se ogni polinomio irriducibile in $F[X]$, avente una radice in $E$, è separabile. Viceversa è non separabile se $F$ è non perfetto, in particolare ha caratteristica $p$, e vi è un elemento $\alpha \in E$ il cui polinomio minimo è della forma $g(X^p)$, con $g \in F[X]$.

**Esempio.** $\mathbb{F}_p(T)$ è un'estensione non separabile di $\mathbb{F}_p(T^p)$.

**Definizione 3.7 – Estensione normale**

Un'estensione $E/F$ si dice *normale* se il polinomio minimo $f_\alpha(X) \in F[X]$ di ogni elemento $\alpha \in E$ si spezza in $E[X]$.

*Osservazione.* Quindi un'estensione $E/F$ è normale se ogni polinomio irriducibile in $F[X]$, avente una radice in $E$, si spezza in $E[X]$.

*Osservazione.* Sia $f$ un polinomio irriducibile di grado $m$ in $F[X]$. Se $f$ ha una radice in $E$, allora

$$\left.\begin{array}{rcl} E/F \text{ separabile} & \Longrightarrow & \text{radici di } f \text{ distinte} \\ E/F \text{ normale} & \Longrightarrow & f \text{ si spezza in } E \end{array}\right\} \Longrightarrow\ f \text{ ha } m \text{ radici distinte in } E.$$

Quindi $E/F$ è normale e separabile se e soltanto se, per ogni $\alpha \in E$, il polinomio minimo di $\alpha$ ha $\deg f_\alpha$ radici distinte in $E$.

**Esempio.** $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ è un'estensione separabile ma non normale. Infatti $X^3 - 2$ non si spezza su $\mathbb{Q}[\sqrt[3]{2}]$.

**Esempio.** Il campo $\mathbb{F}_p(T)$ è normale ma non separabile su $\mathbb{F}_p(T^p)$. Infatti il polinomio minimo di $T$ è $X^p - T^p$ che non è separabile.

## Teorema 3.8 – Caratterizzazione delle estensioni Galois

Sia $E/F$ un'estensione qualsiasi. Allora le seguenti affermazioni sono equivalenti:

1. $E = F_f$ con $f \in F[X]$ separabile.
2. $F = E^G$ con $G \leqslant \mathrm{Aut}(E)$ finito.
3. $E/F$ è finita, normale e separabile.
4. $E/F$ è finita e $F = E^{\mathrm{Aut}(E/F)}$.

*Dimostrazione.* Se $E = F_f$ allora $E$ è algebrico e finitamente generato, in particolare $E$ è finito. Resta da dimostrare che $F = E^{\mathrm{Aut}(E/F)}$. $1 \implies 4$
Poniamo $F' = E^{\mathrm{Aut}(E/F)} \supseteq F$. Siccome $E = F_f$ posso pensare $f(X) \in F'[X]$, in particolare avremo $F'_f = E$. Per la teorema 3.2 avremo

$$[E : F'] = \#\,\mathrm{Aut}(E/F') \qquad \text{e} \qquad [E : F] = \#\,\mathrm{Aut}(E/F).$$

Ora $\mathrm{Aut}(E/F)$ è finito, quindi per il corollario di Artin

$$\mathrm{Aut}(E/F') = \mathrm{Aut}(E/E^{\mathrm{Aut}(E/F)}) = \mathrm{Aut}(E/F).$$

Per un corollario precedente sappiamo che $\#\,\mathrm{Aut}(E/F) \leqslant [E : F]$ che è finito per ipotesi. $4 \implies 2$
Quindi la tesi è un banale caso particolare.
Per ipotesi $F = E^G$, quindi dal lemma di Artin otteniamo che $2 \implies 3$

$$[E : F] \leqslant \#G < \infty.$$

Sia ora $\alpha \in E$, dobbiamo mostrare che $f_\alpha$ ha $\deg f_\alpha$ radici distinte in $E$. Consideriamo l'orbita di $\alpha$ sotto $G$:

$$\alpha^G = \{\, \sigma\alpha \mid \sigma \in G \,\} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$$

*possiamo supporre $\alpha_1 = \alpha$ poichè $\mathrm{id} \in G$*

dove $\alpha^G \subseteq E$ poiché $\sigma$ sono tutti automorfismi di $E$. Inoltre $m \leqslant \#G$. Definiamo

$$g(X) = \prod_{j=1}^{m}(X - \alpha_j) = \prod_{\beta \in \alpha^G}(X - \beta).$$

Dimostriamo che $g(X) = f_\alpha(X) \in F[X]$. Per definizione

$$g(X) = X^m + c_1 X^{m-1} + \ldots + c_m,$$

dove

$$c_1 = -(\alpha_1 + \ldots + \alpha_m) \qquad \text{e} \qquad c_m = (-1)^m \alpha_1 \cdot \ldots \cdot \alpha_m,$$

e, in generale, $c_j = (-1)^j \sigma_j(\alpha_1, \ldots, \alpha_m)$, dove $\sigma_j$ è la $j$-esima funzione simmetrica elementare. Osserviamo che, per ogni $\sigma \in G$, si ha

$$\sigma(c_1) = -\big(\sigma(\alpha_1) + \ldots + \sigma(\alpha_m)\big) = -(\alpha_1 + \ldots + \alpha_m) = c_1,$$

infatti $\alpha^G \to \alpha^G, \alpha_j \mapsto \sigma(\alpha_j)$ è una permutazione dell'orbita. In generale avremo $\sigma(c_j) = c_j$ per ogni $\sigma \in G$. Ciò significa che $c_1, \dots, c_m$ sono fissati da ogni elemento di $G$, ovvero $c_1, \dots, c_m \in E^G = F$. In particolare

$$g(X) \in F[X].$$

D'altronde $\alpha_1 = \alpha$ ci dice che $\alpha$ è una radice di $g$, pertanto $f_\alpha(X) \mid g(X)$. Inoltre, per ogni $\sigma \in G$,

$$f_\alpha(\alpha_j) = f_\alpha\big(\sigma(\alpha)\big) = \sigma\big(f_\alpha(\alpha)\big) = 0,$$

in quanto $\sigma \in \mathrm{Aut}(E/F)$. Per cui

$$g(X) \mid f_\alpha(X) \implies g(X) = f_\alpha(X).$$

$3 \implies 1$ $E/F$ è finita, quindi $E = F[\alpha_1, \dots, \alpha_m]$. Sia $f = \mathrm{mcm}(f_{\alpha_1}, \dots, f_{\alpha_m})$. Segue che $f$ è separabile e $E$ è il campo di spezzamento di $f$. Mostriamo che $F_f = F[\alpha_1, \dots, \alpha_m]$. Chiaramente $F_f \supseteq F[\alpha_1, \dots, \alpha_m]$. L'altra inclusione segue da $E/F$ normale e pertanto tutte le radici di $f$ sono in $E$. □

**Definizione 3.9 – Estensione Galois**

Un'estensione finita $E/F$ si dice *Galois* se soddisfa una delle condizioni equivalenti del teorema precedente.

**Notazione.** Se $E/F$ è Galois scriviamo

$$\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F).$$

**Proprietà 3.10.** Sia $E/F$ Galois. Se $G = \mathrm{Gal}(E/F)$ allora

$$f_\alpha(X) = \prod_{\beta \in \alpha^G} (X - \beta)$$

per ogni $\alpha \in E$.

*Dimostrazione.* Segue dal passo (2) $\implies$ (3) del teorema precedente. □

**Esempio.** $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ è Galois in quanto $E = \mathbb{Q}_f$ con $f(X) = (X^2 - 2)(X^2 - 3)$. In quanto campo di spezzamento $\mathrm{Gal}(E/\mathbb{Q})$ ha $[E : \mathbb{Q}] = 4$ elementi. Nello specifico:

$$\sigma_1 = \mathrm{id}; \quad \sigma_2 = \begin{pmatrix} \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{2} \mapsto \sqrt{2} \end{pmatrix}; \quad \sigma_3 = \begin{pmatrix} \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{2} \mapsto -\sqrt{2} \end{pmatrix}; \quad \sigma_4 = \begin{pmatrix} \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{2} \mapsto -\sqrt{2} \end{pmatrix}.$$

Avevamo infatti già osservato che $\mathrm{Gal}(E/\mathbb{Q}) \cong V$ il gruppo di Klein.
Vorremmo calcolare il polinomio minimo di $\sqrt{3}$ e $\sqrt{3} + \sqrt{2}$. Applichiamo la proprietà:

$$(\sqrt{3})^G = \{\sqrt{3}, -\sqrt{3}\} \implies f_{\sqrt{3}}(X) = (X - \sqrt{3})(X + \sqrt{3}) = X^2 - 3$$
$$(\sqrt{3} + \sqrt{2})^G = \{\pm\sqrt{3} \pm \sqrt{2}, \pm\sqrt{3} \mp \sqrt{2}\},$$

da cui

$$\begin{aligned} f_{\sqrt{3}+\sqrt{2}}(X) &= (X - \sqrt{3} - \sqrt{2})(X - \sqrt{3} + \sqrt{2})(X + \sqrt{3} - \sqrt{2})(X + \sqrt{3} + \sqrt{2}) \\ &= X^4 - 10X^2 + 1. \end{aligned}$$

**Definizione 3.11 – Orbita di un elemento**

Se $G$ è un gruppo che agisce sull'insieme $E$, per ogni $\alpha \in E$, si definisce *l'orbita di* $\alpha$ *sotto* $G$, come

$$\alpha^G = \{ \sigma\alpha \mid \sigma \in G \}$$

**Notazione.** Se $E/F$ è Galois e $\alpha \in E$. Posto $G = \mathrm{Gal}(E/F)$, gli elementi di $\alpha^G$ si definiscono *coniugati* di $\alpha$.

**Definizione 3.12 – Chiusura di Galois**

Sia $E/F$ un'estensione finita. $\overline{E}$ si definisce *chiusura di Galois* di $E$ se

- $\overline{E}/F$ è Galois;
- $\overline{E}$ è minimale, ovvero per ogni campo intermedio $\overline{E} \supset L \supseteq F$, $L/F$ non è Galois.

*Osservazione.* Se $E/F$ è finita e separabile, esiste sempre la chiusura di Galois $\overline{E}$ di $E$. Infatti se $E = F[\alpha_1, \dots, \alpha_m]$, è sufficiente prendere $f = \mathrm{mcm}(f_{\alpha_1}, \dots, f_{\alpha_m})$ che è separabile, così da avere $\overline{E} = F_f$. Infatti $F_f \supseteq E$ ed è Galois su $F$.

**Esempio.** $E = \mathbb{Q}[\sqrt[3]{2}]$ è finita e separabile su $\mathbb{Q}$. Per ottenere la chiusura di Galois di $E$, è sufficiente prendere il campo di spezzamento di $X^3 - 2$, ovvero $\mathbb{Q}[\sqrt[3]{2}, w]$.

**Proprietà 3.13.** La chiusura di Galois di $E/F$ è unica a meno di isomorfismi.

**Proprietà 3.14.** Se $E/F$ è Galois e $E \supseteq M \supseteq F$. Allora $E/M$ è Galois.

*Dimostrazione.* Supponiamo che $E/F$ sia Galois. Per la caratterizzazione, $E = F_f$ con $f \in F[X]$ separabile. In particolare, se consideriamo $f$ in $M[X]$, avremo $E = M_f$, dove $f \in M[X]$ rimane ancora separabile. Per cui $E/M$ è Galois. □

*Osservazione.* In generale non è però vero che $M/F$ è Galois. Ad esempio se consideriamo $\mathbb{Q}[\sqrt[3]{2}, w] \supseteq \mathbb{Q}[\sqrt[3]{2}] \supseteq \mathbb{Q}$, abbiamo che $\mathbb{Q}[\sqrt[3]{2}, w]$ è Galois su $\mathbb{Q}$ e $\mathbb{Q}[\sqrt[3]{2}]$. Ma $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ non lo è.

## 3.3 TEOREMA FONDAMENTALE DELLA CORRISPONDENZA DI GALOIS

In questo paragrafo tratteremo il teorema di Galois, andando poi a dimostrarne le principali conseguenze.

**Teorema 3.15 – fondamentale della corrispondenza di Galois**

Sia $E/F$ Galois e sia $G = \mathrm{Gal}(E/F)$. Allora le mappe

$$H \longmapsto E^H \qquad \text{e} \qquad M \longmapsto \mathrm{Gal}(E/M),$$

sono biezioni, l'una l'inversa dell'altra, tra l'insieme dei sottogruppi di $G$ e quello dei campi intermedi fra $E$ ed $F$:

$$\{ H \mid H \leqslant G \} \longleftrightarrow \{ M \mid F \subseteq M \subseteq E \}$$

*Dimostrazione.* É Sufficiente mostrare che la composizione delle mappa costituisce l'identità per i rispettivi insiemi. $H = \mathrm{Gal}(E/E^H)$ segue dal corollario di Artin in quanto $G$ è finito. Viceversa, $M = E^{\mathrm{Gal}(E/M)}$ segue da

$$E/F \text{ Galois} \implies E/M \text{ Galois},$$

quindi, per la quarta proprietà della caratterizzazione,

$$M = E^{\mathrm{Aut}(E/M)} = E^{\mathrm{Gal}(E/M)}.$$

□

**Proprietà 3.16** (Inversione dell'inclusione tramite la corrispondenza)**.** Se $H_1, H_2 \leqslant G$ allora

$$H_1 \subseteq H_2 \iff E^{H_1} \supseteq E^{H_2}.$$

*Dimostrazione.* Per definizione

$$E^{H_1} = \{ \alpha \in E \mid \sigma\alpha = \alpha, \forall\, \sigma \in H_1 \} \qquad \text{e} \qquad E^{H_2} = \{ \alpha \in E \mid \sigma\alpha = \alpha, \forall\, \sigma \in H_2 \}.$$

Quindi se $H_1 \subseteq H_2$, chiaramente $E^{H_1} \supseteq E^{H_2}$. Viceversa se $E^{H_1} \supseteq E^{H_2}$, segue immediatamente che $\mathrm{Gal}(E/E^{H_2}) \supseteq \mathrm{Gal}(E/E^{H_1})$. Per il corollario di Artin

$$\mathrm{Gal}(E/E^{H_2}) = H_2 \qquad \text{e} \qquad \mathrm{Gal}(E/E^{H_1}) = H_1.$$

Quindi $H_2 \supseteq H_1$. □

*Osservazione.* Chiaramente, per la corrispondenza, vale anche il viceversa. Ovvero se $F \subseteq M_1, M_2 \subseteq E$, allora

$$M_1 \subseteq M_2 \iff \mathrm{Gal}(E/M_1) \supseteq \mathrm{Gal}(E/M_2).$$

**Proprietà 3.17** (Conservazione degli indici)**.** Se $H_1, H_2 \leqslant G$ e $H_1 \subseteq H_2$, allora

$$[H_2 : H_1] = [E^{H_1} : E^{H_2}].$$

*Dimostrazione.* Per il corollario di Artin $H_2 = \mathrm{Gal}(E/E^{H_2})$, da cui

$$|H_2| = \#\,\mathrm{Gal}(E/E^{H_2}) = [E : E^{H_2}] = [E : E^{H_1}][E^{H_1} : E^{H_2}].$$

D'altronde, dal teorema di Lagrange della teoria dei gruppi

$$|H_2| = |H_1|[H_2 : H_1],$$

dove $|H_1| = [E : E^{H_1}]$ ancora per il corollario di Artin. Da ciò segue immediatamente

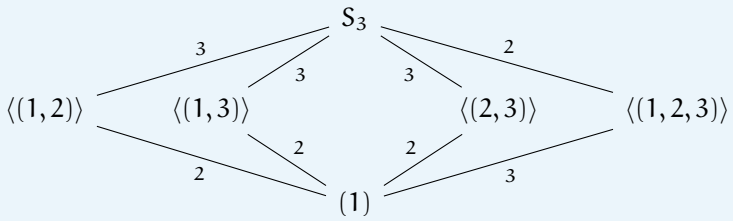
$$[E : E^{H_1}][E^{H_1} : E^{H_2}] = [E : E^{H_1}][H_2 : H_1] \implies [E^{H_1} : E^{H_2}] = [H_2 : H_1].$$

□

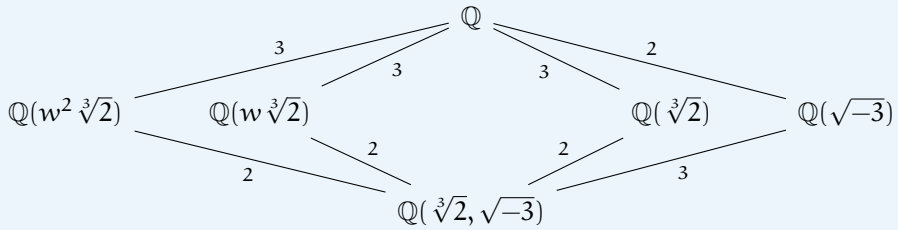
*Osservazione.* Anche in questo caso vale il viceversa. Se $F \subseteq M_1, M_2 \subseteq E$ e $M_1 \subseteq M_2$, allora

$$[M_2 : M_1] = \big[\mathrm{Gal}(E/M_1) : \mathrm{Gal}(E/M_2)\big].$$

**Esempio.** In esempi precedenti abbiamo mostrato che $\mathbb{Q}[\sqrt[3]{2}, w]/\mathbb{Q}$ è Galois e $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}, w]/Q) \cong S_3$. Sappiamo che il reticolo di $S_3$ è il seguente




il teorema di corrispondenza ci permette di dedurre




Infatti anche se in principio riconoscevamo solo $\mathbb{Q}[\sqrt[3]{2}]$, la teoria ci dice che vi sono altre due sottocampi di grado 3 su $\mathbb{Q}$. D'altronde sappiamo che se $\sigma \in G$ e $F \subseteq M \subseteq E$, allora

$$\sigma M = \{\, \sigma(\gamma) \mid \gamma \in M \,\},$$

che si chiama sottocampo coniugato a $M$. Ora $M$ è isomorfo $\sigma M$ tramite $\gamma \mapsto \sigma(\gamma)$. Quindi per trovare gli alti due sottocampi, ci basta studiare i coniugati di $\mathbb{Q}[\sqrt[3]{2}]$. Tali coniugati sono proprio definiti dai coniugati di $\sqrt[3]{2}$, per cui avremo

$$\mathbb{Q}[w\sqrt[3]{2}] \qquad \text{e} \qquad \mathbb{Q}[w^2\sqrt[3]{2}].$$

Osserviamo che non è possibile dire con precisione a chi corrisponde $\langle(1,2)\rangle$, poiché esso risente della rappresentazione scelta per $S_3$.
D'altra parte sappiamo con esattezza che $\langle(1,2,3)\rangle$ corrisponde a $\mathbb{Q}[w]$ e possiamo osservare una proprietà interessante:

$$\langle(1,2,3)\rangle = A_3 \trianglelefteq S_3$$

e infatti $\mathbb{Q}[w]$ è normale su $\mathbb{Q}$.

**Proprietà 3.18** (Invariante del coniugato)**.** Per ogni $\sigma \in G$ e per ogni $H \leqslant G$ vale

$$E^{\sigma H \sigma^{-1}} = \sigma E^H.$$

*Dimostrazione.* Per definizione

$$E^{\sigma H\sigma^{-1}} = \{\, \alpha \in E \mid \sigma\tau\sigma^{-1}(\alpha) = \alpha,\ \forall\, \tau \in H \,\},$$
$$\sigma E^H = \{\, \sigma\alpha \in E \mid \tau(\alpha) = \alpha,\ \forall\, \tau \in H \,\}.$$

Si mostra facilmente che

$$\tau\alpha = \alpha \iff (\sigma\tau\sigma^{-1})\big(\sigma(\alpha)\big) = \sigma(\alpha).$$

Quindi

$\sigma^{-1}(\beta) = \alpha$

$$\begin{aligned}\beta \in E^{\sigma H\sigma^{-1}} &\iff \sigma\tau\sigma^{-1}(\beta) = \beta \iff \tau\big(\sigma^{-1}(\beta)\big) = \sigma^{-1}(\beta)\\ &\iff \tau\alpha = \alpha \iff \alpha \in E^H\\ &\iff \beta = \sigma\alpha \in \sigma E^H.\end{aligned}$$

□

*Osservazione.* Chiaramente vale anche il viceversa. Se $\sigma \in G$ e $F \subseteq M \subseteq E$, allora

$$\sigma \operatorname{Gal}(E/M)\sigma^{-1} = \operatorname{Gal}(E/\sigma M).$$

**Proprietà 3.19** (Conservazione della normalità)**.** $N$ è normale in $G$ se e soltanto se $E^N/F$ è normale.

*Dimostrazione.* Per definizione

$$N \trianglelefteq G \iff \sigma n\sigma^{-1} \in N,\ \forall\, n \in N \forall\, \sigma \in G \iff \sigma N\sigma^{-1} = N.$$

Mentre $E^N/F$ è normale se il polinomio minimo $f_\alpha(X)$ di ogni $\alpha \in E^N$ si spezza in $E^N$. Quindi se

$$f_\alpha(X) = \prod_{j=1}^{\deg f_\alpha} (X - \alpha_j) \implies \alpha_1, \dots, \alpha_{\deg f_\alpha} \in E^N.$$

D'altronde esisterà $\sigma \in \operatorname{Gal}(E/F)$ tale che $\alpha_j = \sigma(\alpha)$. Quindi $E^N/F$ è normale se e soltanto se

$$\sigma\alpha \in E^N,\ \forall\, \alpha \in E^n \forall\, \sigma \in G \iff \sigma E^N = E^N.$$

DA FINIRE!!!

□

*Osservazione.* Se $E^N/F$ è normale è necessariamente Galois. In generale sappiamo che se $F \subseteq M \subseteq E$ e $E/F$ è Galois, non è necessariamente vero che $M/F$ lo sia. D'altronde se $E/F$ è separabile lo è anche $M/F$. Quindi $E^N/F$ è Galois per la caratterizzazione in quanto finito, normale e separabile.

*Osservazione.* Se $E^N/F$ è normale, e quindi Galois, vale

$$\operatorname{Gal}(E^N/F) \cong \frac{G}{N}.$$

L'identità fra gli ordine è facile da dedurre, infatti

$$\#G = \#\operatorname{Gal}(E/F) = [E : F] = [E : E^N][E^N : F] = \#N\#\operatorname{Gal}(E^N/F),$$

da cui

$$\#\operatorname{Gal}(E^N/F) = \frac{\#G}{\#N} = \#\frac{G}{N}.$$

**Proprietà 3.20** (Invariante dell'intersezione di sottogruppi)**.** Se $H_1, H_2 \leqslant G$, allora

$$E^{H_1 \cap H_2} = E^{H_1} E^{H_2}.$$

*Dimostrazione.* $H_1 \cap H_2$ è per definizione il più grande sottogruppo contenuto in $H_1$ e $H_2$. Il teorema ci dice che vi è un'anti-corrispondenza fra i sottogruppi di $G$ e i campi intermedi di $E/F$. Pertanto $E^{H_1 \cap H_2}$ deve essere il più piccolo sottocampo che contiene $E^{H_1}$ e $E^{H_2}$, ovvero $E^{H_1} E^{H_2}$. □

*Osservazione.* In generale vale

$$E^{H_1 \cap \ldots \cap H_n} = E^{H_1} \cdot \ldots \cdot E^{H_n}.$$

**Proprietà 3.21** (Corrispondenza del normalizzatore)**.** Sia $H \leqslant G$, allora

$$\bigcap_{\sigma \in G} \sigma H \sigma^{-1} \text{ corrisponde a } \prod_{\sigma \in G} \sigma E^H.$$

*Dimostrazione.* Per definizione il normalizzatore di $H$ in $G$

$$n_H G = \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$$

è il più grande sottogruppo normale di $G$ contenuto in $H$. Nuovamente, poiché il teorema inverte l'ordine nella corrispondenza, $n_H G$ dovrà corrispondenre alla più piccola estensione normale di $F$ che contiene $E^H$, ovvero

$$\prod_{\sigma \in G} \sigma E^H.$$ □

**Notazione.** La composizione

$$\prod_{\sigma \in G} \sigma E^H$$

viene detta *chiusura normale, o Galois*, di $E^H$ e si denota con $\overline{E^H}$.

# 4 CALCOLO DEI GRUPPI DI GALOIS

## 4.1 CAMPI CICLOTOMICI

In questo paragrafo studieremo il gruppo di Galois di $\mathbb{Q}[\zeta_m]$, dimostrando in particolare che

$$U(\mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Gal}(\mathbb{Q}[\zeta_m] : \mathbb{Q}) \qquad \text{tramite} \qquad a \mapsto \sigma_a(\zeta_m) = z_m^a.$$

Infine studieremo alcuni casi particolari.

Come prima cosa elenchiamo alcune proprietà, molte delle quali già note, riguardo a $\mathbb{Q}[\zeta_m]$ che saranno utili alla nostra tesi.

Da ora in avanti faremo uso di queste notazioni:

$$\zeta = \zeta_m = e^{i\frac{2\pi}{m}} \qquad \text{e} \qquad G = \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}).$$

**Proprietà 4.1.** $\mathbb{Q}[\zeta]/\mathbb{Q}$ è un'estensione di Galois.

*Dimostrazione.* Per la caratterizzazione delle estensioni di Galois, infatti $\mathbb{Q}[\zeta]$ è il campo di spezzamento di

$$X^m - 1 \in \mathbb{Q}[X].$$

□

**Proprietà 4.2.** $X^m - 1$ è separabile.

*Dimostrazione.* Sia $f(X) = X^m - 1$. Sappiamo dalla caratterizzazione delle radici multiple che se $f$ non fosse semplice si avrebbe

$$(f, f') \neq 1.$$

D'altronde $f'(X) = n X^{n-1}$ e $0$ non è una radice di $f$, quindi $(f, f') = 1$. □

**Proprietà 4.3.** La mappa

$$U(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}), k \longmapsto \sigma_k \colon \zeta \mapsto \zeta^k$$

è un omomorfismo iniettivo di gruppi.

*Dimostrazione.* Mostriamo che è un omomorfismo: siano $a, b \in U(\mathbb{Z}/m\mathbb{Z})$, avremo

$$\sigma_a \circ \sigma_b(\zeta) = \sigma_a(\zeta^b) = \zeta^{b\cdot a} = \sigma_{a\,b}(\zeta).$$

Quindi le operazioni vengono conservate. Per cui, dal momento che $k \mapsto \sigma_k$ è ben definito, abbiamo un omomorfismo di gruppi.
Per dimostrare che è iniettivo, mostriamo che il nucleo è banale:

$$\sigma_k(\zeta) = \zeta \iff \zeta^k = \zeta \iff k = 1$$

in quanto $k \in U(\mathbb{Z}/m\mathbb{Z})$ implica $(k, m) = 1$. Quindi l'omomorfismo è iniettivo. □

*Osservazione.* Per dimostrare che è suriettivo, ho bisogno di dimostrare che

$$\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) = \varphi(m).$$

**Proprietà 4.4.** Vale la seguente identità:

$$X^m - 1 = \prod_{d|m} \Phi_d(X) \qquad \text{dove} \qquad \Phi_d(X) = \prod_{\substack{k=1 \\ (k,d)=1}}^{d} (X - \zeta_d^m).$$

*Dimostrazione.* Sappiamo che le radici di $X^m - 1$ sono le $\zeta^k$ con $k = 1, \dots, m$. Quindi

$$X^m - 1 = \prod_{k=1}^{m} (X - \zeta^k) = \prod_{d|m} \prod_{\substack{k=1 \\ (k,m)=d}}^{m} (X - \zeta^k) = \prod_{d|m} \Phi_{\frac{m}{d}}(X),$$

dove

$$\Phi_{\frac{m}{d}}(X) = \prod_{\substack{k=1 \\ (k,m)=d}}^{m} (X - \zeta^k) = \prod_{\substack{k=1 \\ (\frac{k}{d},\frac{m}{d})=1}}^{m} (X - \zeta^k) = \prod_{\substack{j=1 \\ (j,m/d)=1}}^{m/d} (X - \zeta^{j\,d}). \qquad \textit{posto } j = k/d$$

Ora se

$$\zeta = \zeta_m = e^{i\frac{2\pi}{m}} \implies \zeta^d = e^{i\frac{2\pi}{m}d} = \zeta_{\frac{m}{d}}.$$

Quindi

$$\Phi_{\frac{n}{d}}(X) = \prod_{\substack{j=1 \\ (j,m/d)=1}}^{m/d} (X - \zeta_d^j).$$

Inoltre, poiché $d \mid m \implies m/d \mid m$, avremo

$$X^m - 1 = \prod_{d|m} \Phi_{\frac{m}{d}}(X) = \prod_{d|m} \Phi_d(X),$$

dove

$$\Phi_d(X) = \prod_{\substack{j=1 \\ (j,d)=1}}^{d} (X - \zeta_d^j). \qquad \square$$

**Proprietà 4.5.** Il polinomio $\Phi_m(X)$ è a coefficienti interi ed è irriducibile.

*Dimostrazione.* Per mostrare che $\Phi_m(X) \in \mathbb{Z}[X]$, è sufficiente mostrare che ha coefficienti razionali. Infatti, dalla proprietà precedente,

$$X^m - 1 = \prod_{d|m} \Phi_d(X),$$

dove $X^m - 1 \in \mathbb{Z}[X]$ monico, quindi per la teorema 1.22 ogni suo fattore a coefficienti razionali è a coefficienti interi. Mostriamolo per induzione:

- $\Phi_1(X) = X - 1$ ha coefficienti interi.
- Assumiamo che $\Phi_d(X) \in \mathbb{Q}[X]$ per ogni $d < n$, segue

$$\Phi_m(X) = \frac{X^m - 1}{\prod_{\substack{d|m \\ d<m}}^{m} \Phi_d(X)} \in \mathbb{Q}[X]$$

in quanto rapporto di polinomi a coefficienti razionali.

Mostriamo ora che è irriducibile. Per definizione

$$\Phi_m(X) = \prod_{\substack{k=1 \\ (k,m)=1}}^{m} (X - \zeta^m)$$

noi vorremmo dimostrare che $\Phi_m = f_\zeta$. Osserviamo che

$$f_\zeta(X) = \prod_{\sigma \in G} \big(X - \sigma(\zeta)\big).$$

D'altronde

$$\sigma(\zeta) = \zeta^k \qquad \text{e} \qquad \sigma^{-1}(\zeta) = z^{k'},$$

quindi $\zeta = \sigma \circ \sigma^{-1}(\zeta) = \zeta^{k\,k'}$, da cui $k\,k' \equiv_m 1$. Ovvero

$$(k, m) = 1.$$

Questo significa che le radici di $f_\zeta$ sono della forma $\zeta^k$ con $(k, m) = 1$, da cui

$$f_\zeta \mid \Phi_m.$$

Resta da mostrare il viceversa. Per farlo possiamo verificare che se $(k, m) = 1$ allora

$$f_\zeta(\alpha) = 0 \implies f_\zeta(\alpha^k) = 0.$$

In tal caso tutte le radici di $\Phi_m$ sarebbero radici di $f_\zeta$, che implicherebbe $\Phi_m \mid f_\zeta$. Noi dimostreremo che per ogni $p$ primo tale che $(p, m) = 1$ si ha

$$f_\zeta(\alpha) = 0 \implies f_\zeta(\alpha^p) = 0,$$

da cui, preso $k = p_1 \cdot \ldots \cdot p_s$, avremo

$$f_\zeta(\alpha) = 0 \implies f_\zeta(\alpha^{p_1}) = 0 \implies f_\zeta(\alpha^{p_1 p_2}) = 0 \implies \ldots \implies f(\alpha^k) = 0.$$

Sia $f_\zeta(\alpha) = 0$, supponiamo per assurdo che $p$ sia un primo tale che $f(\alpha^p) \neq 0$. Da $f_\zeta \mid \Phi_m$ segue $\Phi_m(X) = f_\zeta(X)g(X)$. Inoltre per la definizione di $\Phi_m$ si ha necessariamente

$$\Phi_m(\alpha) = 0 \implies \Phi_m(\alpha^p) = 0.$$

Quindi

$$0 = \Phi_m(\alpha^p) = f_\zeta(\alpha^p)g(\alpha^p) \implies g(\alpha^p) = 0.$$

Ciò significa che $f_\zeta$ ha una radice in comune con $g(X^p)$, da cui

$$\big(f_\zeta(X), g(X^p)\big) \neq 1.$$

Se prendiamo le classi di equivalenza modulo $p$, $\overline{f_\zeta(X)}, \overline{g(X^p)} \in \mathbb{F}_p[X]$, allora

$$\big(\overline{f_\zeta(X)}, \overline{g(X^p)}\big) \neq 1.$$

Ma, modulo $p$, $\overline{g(X^p)} = \big(\overline{g(X)}\big)^p$. Quindi $f_\zeta(X)$ e $g(X)$ hanno una radice in comune modulo $p$. Da

$$f_\zeta(X)g(X) = \Phi_m(X)$$

segue che $\Phi_m(X)$ ha una radice doppia modulo $p$. In particolare $\Phi_m(X)$ è un fattore di $X^m - 1$, quindi anche quest'ultimo avrà una radice doppia modulo $p$. Ciò è assurdo poiché abbiamo visto nella teorema 4.2 che $X^m - 1$ è separabile. Quindi $\Phi_m(X)$ è irriducibile □

**Proprietà 4.6.** Il grado di $\mathbb{Q}[\zeta]/\mathbb{Q}$ è $\varphi(m)$.

*Dimostrazione.* In quanto estensione algebrica semplice, avremo

$$\left[\mathbb{Q}[\zeta] : \mathbb{Q}\right] = \deg f_\zeta.$$

Nella proprietà precedente abbiamo dimostrato che $f_\zeta = \Phi_m$. Per definizione

$$\Phi_m(X) = \prod_{\substack{k=1 \\ (k,m)=1}}^{m} (X - \zeta^k).$$

Quindi è chiaro che $\deg \Phi_m = \varphi(m)$, da cui la tesi. □

## Teorema 4.7 – Gruppo di Galois dei campi ciclotomici

Il gruppo di Galois dei campi ciclotomici $\mathrm{Gal}\left(\mathbb{Q}[\zeta_m]/\mathbb{Q}\right)$ è isomorfo a $U(\mathbb{Z}/m\mathbb{Z})$, tramite

$$U(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}), k \longmapsto \sigma_k \colon \zeta \mapsto \zeta^k.$$

*Dimostrazione.* Sappiamo dalla teorema 4.3 che la mappa dell'ipotesi, è un omomorfismo iniettivo fra $U(\mathbb{Z}/m\mathbb{Z})$ e $\mathrm{Gal}\left(\mathbb{Q}[\zeta_m]/\zeta\right)$. Inoltre

$$\#\,\mathrm{Gal}\left(\mathbb{Q}[\zeta_m]/\mathbb{Q}\right) = \left[\mathbb{Q}[\zeta_m] : \mathbb{Q}\right],$$

dove $\left[\mathbb{Q}[\zeta_m] : \mathbb{Q}\right] = \varphi(m)$ per la proprietà precedente. Quindi $U(\mathbb{Z}/m\mathbb{Z})$ e $\mathrm{Gal}\left(\mathbb{Q}[\zeta_m]/\zeta\right)$ hanno lo stesso numero di elementi. Ne segue che l'omomorfismo iniettivo è necessariamente un isomorfismo. □

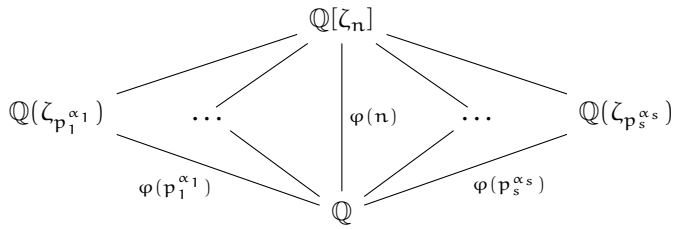
*Osservazione.* Riepiloghiamo quanto visto finora. Posto $K_n = \mathbb{Q}[\zeta], \zeta = e^{\frac{2\pi i}{n}}$, $K_n$ è il campo di spezzamento di $X^n - 1$. Quindi $K_n$ è Galois poiché $X^n - 1$ è separabile.
É un'estensione abeliana, infatti

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z}) = \{\, k \in \{1, \ldots, n\} \mid (k, n) = 1 \,\}.$$

Inoltre

$$[K_n : \mathbb{Q}] = \#\,\mathrm{Gal}(K_n/\mathbb{Q}) = \varphi(n).$$

In generale se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, si ha il seguente reticolo:




**Esercizio 4.1.** Si determini il campo di Galois di $\mathbb{Q}[\zeta_8]/\mathbb{Q}$ e il corrispondente reticolo dei sottocampi.

*Soluzione.* Osserviamo che

$$\zeta_8 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i).$$

Inoltre $\zeta_8^2 = \zeta_4 = i$, quindi si mostra facilmente che

$$\mathbb{Q}[z_8] = \mathbb{Q}[\sqrt{2}, i].$$

Possiamo quindi scrivere gli elementi di $\mathrm{Gal}\left(\mathbb{Q}[\zeta_8]/\mathbb{Q}\right)$ tramite le immagini dei generatori:

$$\sigma_0 = \mathrm{id}; \quad \sigma_1 = \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \end{pmatrix}; \quad \sigma_2 = \begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \end{pmatrix}; \quad \sigma_1 \circ \sigma_2 = \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \end{pmatrix}.$$

D'altronde, grazie alla teoria sviluppata in questo paragrafo, abbiamo un altro modo per esprimere questi elementi. Sappiamo infatti che

$$\mathrm{Gal}\left(\mathbb{Q}[\zeta_8]/\mathbb{Q}\right) \cong \mathrm{U}(\mathbb{Z}/8\mathbb{Z}) = \{\pm 1, \pm 3\},$$

che inducono i seguenti automorfismi:

$$\tau_0 \colon \zeta_8 \mapsto \zeta_8; \qquad \tau_1 \colon \zeta_8 \mapsto \zeta_8^{-1}; \qquad \tau_2 \colon \zeta_8 \mapsto \zeta_8^3; \qquad \tau_1 \circ \tau_2 \colon \zeta_8 \mapsto \zeta_8^{-3}.$$

Cerchiamo di dare una corrispondenza fra le due scritture:

- chiaramente $\sigma_0 = \tau_0 = \mathrm{id}$.
- $\tau_1 \colon \zeta_8 \mapsto \zeta_8^{-1}$, dove

  $$\zeta_8^{-1} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} \implies \frac{\sqrt{2}}{2}(1+i) \mapsto \frac{\sqrt{2}}{2}(1-i).$$

  Quindi $\tau_1 = \sigma_2$.
- $\tau_2 \colon \zeta_8 \mapsto \zeta_8^3$, dove

  $$\zeta_8^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \implies \frac{\sqrt{2}}{2}(1+i) \mapsto \frac{\sqrt{2}}{2}(-1+i).$$

  Quindi $\tau_2 = \sigma_1$.
- Dai punti precedenti segue immediatamente che $\tau_1 \circ \tau_2 = \sigma_1 \circ \sigma_2$.

**Esercizio 4.2.** Si determini il gruppo di Galois di $K_7 = \mathbb{Q}[\zeta_7]$.

*Soluzione.* Sappiamo

$$\mathrm{Gal}(K_7/\mathbb{Q}) \cong \mathrm{U}(\mathbb{Z}/7\mathbb{Z}) = \{1,2,3,4,5,6\} \cong \mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}.$$

Osserviamo che in generale è più comodo lavorare con $\mathrm{U}(\mathbb{Z}/7\mathbb{Z})$ in quanto costituisce un gruppo moltiplicativo, tale struttura si avvicina di più a quella del gruppo di automorfisimi.

I generatori di $\mathrm{U}(\mathbb{Z}/7\mathbb{Z})$ e $\mathbb{Z}/6\mathbb{Z}$ sono rispettivamente 3 e 1. Quindi l'isomorfismo fra i due gruppi si costruisce con la mappa $1 \mapsto 3$.

Ricordiamo dalla teoria dei gruppi che i sottogruppi di un gruppo ciclico sono in corrispondenza biunivoca con i divisori dell'ordine. In $\mathbb{Z}/6\mathbb{Z}$ i divisori dell'ordine sono $6, 3, 2, 1$ a cui corrispondono

$$\langle 1\rangle = \mathbb{Z}/6\mathbb{Z}; \qquad \langle 2\rangle; \qquad \langle 3\rangle; \qquad \langle 0\rangle.$$

I corrispondenti del gruppo di Galois, in vista dell'isomorfismo

$$\mathbb{Z}/6\mathbb{Z} \longrightarrow \mathrm{U}(\mathbb{Z}/7\mathbb{Z}) \colon \begin{aligned} 1 &\longmapsto 3 \\ 2 &\longmapsto 2 \\ 3 &\longmapsto 6 \\ 4 &\longmapsto 4 \\ 5 &\longmapsto 5 \\ 0 &\longmapsto 1 \end{aligned}$$

sono determinati da

$$\begin{aligned}
&\langle 1\rangle \longleftrightarrow \langle \sigma_3\rangle = \left\{ \sigma_{3^k} : K_7 \to K_7, \zeta_7 \mapsto \zeta_7^{3^k} \right\} = \mathrm{Gal}(K_7/\mathbb{Q});\\
&\langle 2\rangle \longleftrightarrow \langle \sigma_2\rangle = \{\sigma_2, \sigma_4, \sigma_1 = \mathrm{id}\};\\
&\langle 3\rangle \longleftrightarrow \langle \sigma_6\rangle = \{\sigma_6, \sigma_1 = \mathrm{id}\};\\
&\langle 0\rangle \longleftrightarrow \langle \sigma_1\rangle = \{\sigma_1 = \mathrm{id}\}.
\end{aligned}$$

Per il Teorema Fondamentale della Corrispondenza di Galois, avremo una corrispondenza con i sottocampi di $K_7$. I corrispondenti banali sono

$$\begin{aligned}
\langle \sigma_3\rangle = G &\longleftrightarrow K_7^{\mathrm{Gal}(K_7/\mathbb{Q})} = \mathbb{Q};\\
\langle \sigma_1\rangle = \{\mathrm{id}\} &\longleftrightarrow K_7^{\{\mathrm{id}\}} = K_7.
\end{aligned}$$

Consideriamo ora il corrispondente di $\langle \sigma_6\rangle$:

$$\langle \sigma_6\rangle = \langle \sigma_{-1}\rangle \longleftrightarrow K_7^{\langle \sigma_{-1}\rangle} = \{\, \alpha \in K_7 \mid \sigma_{-1}(\alpha) = \alpha \,\} = \{\, \alpha \in K_7 \mid \overline{\alpha} = \alpha \,\} = K_7 \cap \mathbb{R}.$$

Abbiamo già visto in esempi precedenti che $K_7 \cap \mathbb{R} = \mathbb{Q}[\cos {}^{2\pi}/_{7}]$. Infine

$$\langle \sigma_2\rangle \longleftrightarrow K_7^{\langle \sigma_2\rangle} = \{\, \alpha \in K_7 \mid \sigma_2(\alpha) = \alpha \,\}.$$

Cerchiamo di determinare esplicitamente $K_7^{\langle \sigma_2\rangle}$. Per prima cosa osserviamo che $K_7^{\langle \sigma_2\rangle}/\mathbb{Q}$ è Galois in quanto $\langle \sigma_2\rangle \triangleleft G$ e ciò è sempre vero nei campi ciclotomici poiché $G$ è abeliano. Inoltre

$$[K_7^{\langle \sigma_2\rangle} : \mathbb{Q}] = \frac{[K_7 : \mathbb{Q}]}{[K_7 : K_7^{\langle \sigma_2\rangle}]} = \frac{6}{\#\langle \sigma_2\rangle} = 2,$$

quindi $K_7^{\langle \sigma_2\rangle}$ è un'estensione quadratica di $\mathbb{Q}$. Definiamo

$$\eta = \sum_{\sigma \in \langle \sigma_2\rangle} \sigma(\zeta_7) = \sigma_2(\zeta) + \sigma_4(\zeta) + \sigma_8(\zeta) = \zeta^2 + \zeta^4 + \zeta.$$

Osserviamo che $\sigma_2(\eta) = \eta$, quindi $\mathbb{Q}[\eta] \subseteq K_7^{\langle \sigma_2\rangle}$. Ora

$$\mathbb{Q} \subseteq \mathbb{Q}[\eta] \subseteq K_7^{\langle \sigma_2\rangle} \qquad \text{dove } [K_7^{\langle \sigma_2\rangle} : \mathbb{Q}] = 2.$$

Quindi se dimostriamo che $\mathbb{Q}[\eta] \neq \mathbb{Q}$ segue necessariamente $\mathbb{Q}[\eta] = K_7^{\langle \sigma_2\rangle}$. Per prima cosa troviamo il polinomio minimo di $\eta$ sfruttando la teorema 3.10:

$$\eta^G = \{\eta, \sigma_2(\eta), \sigma_3(\eta), \sigma_4(\eta), \sigma_5(\eta), \sigma_6(\eta)\} = \{\eta, \sigma_3(\eta)\} = \{\zeta + \zeta^2 + \zeta^4, \zeta^3 + \zeta^5 + \zeta^6\}.$$

Quindi

$$f_\eta(X) = (X - \eta)(X - \sigma_3(\eta)) = X^2 - (\eta + \sigma_3(\eta))X + \eta\,\sigma_3(\eta),$$

dove

$$\begin{aligned}
\eta + \sigma_3(\eta) &= \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = -1;\\
\eta\,\sigma_3(\eta) &= (\zeta + \zeta^2 + \zeta^4)(\zeta^3 + \zeta^5 + \zeta^6) = \zeta^4 + \zeta^6 + 1 + \zeta^5 + 1 + \zeta + 1 + \zeta^2 + \zeta^3 = 2.
\end{aligned}$$

Per cui

$$f_\eta(X) = x^2 + x + 2 \implies \eta, \sigma_3(\eta) = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-7}.$$

Concludendo $Q[\eta] = \mathbb{Q}[\sqrt{-7}] \neq \mathbb{Q}$, quindi $Q[K_7^{\langle \sigma_2\rangle}] = Q[\sqrt{-7}]$.

*Osservazione.* In generale se consideriamo $\mathbb{Q}[\zeta_p]$ con $p \geqslant 3$, avremo sempre che

$$\mathrm{Gal}\left(\mathbb{Q}[\zeta_p]/\mathbb{Q}\right) \cong U(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^*$$

che è ciclico. Quindi ha un sottogruppo per ogni divisore dell'ordine. Per il TFCG i sottocampi sono in corrispondenza biunivoca con i divisori di $\varphi(p) = p-1$.
In particolare avremo sempre

$$\mathbb{Q}\left[\cos\frac{2\pi}{p}\right] \text{ di grado } \frac{p-1}{2} \qquad \text{e} \qquad \mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p}\right] \text{ di grado } 2.$$

**Proprietà 4.8.** Sia $p$ primo, allora vale la seguente identità

$$D_{\Phi_p} = -p^{p-2}.$$

*Dimostrazione.* Per definizione di discriminante

$$D_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 \qquad \text{dove } \alpha_i, \alpha_j \text{ sono radici di } f.$$

É possibile dimostrare la seguente definizione equivalente:

$$D_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} f'(\alpha_j).$$

Applicandola al discriminante di $\Phi_p(X)$, otteniamo

*la $p$ come esponente di $(-1)$ è ininfluente*

$$D_{\Phi_p} = (-1)^{\frac{p(p-1)}{2}} \prod_{k=1}^{p-1} \Phi_p'(\zeta^k) = (-1)^{\frac{p-1}{2}} \prod_{k=1}^{p-1} \Phi_p'(\zeta^k).$$

Ora

$$\Phi_p'(X) = \frac{pX^{p-1}(X-1) - (X^p-1)}{(X-1)^2} \implies \Phi_p'(\zeta^k) = p\,(\zeta^{p-1})^k(\zeta^k-1)^{-1}.$$

Quindi

$$\begin{aligned}\prod_{k=1}^{p-1}\Phi_p'(\zeta^k) &= p^{p-1}(\zeta^{p-1})^{\sum_{k=1}^{p-1}k}\left(\prod_{k=1}^{p-1}(1-\zeta^k)\right)^{-1}(-1)^{\sum_{k=1}^{p-1}k} \\ &= p^{p-1}\underbrace{(\zeta^{p-1})^{\frac{p(p-1)}{2}}}_{=1}\underbrace{\Phi_p(1)^{-1}}_{=p^{-1}}(-1)^{\frac{p(p-1)}{2}} \\ &= (-1)^{\frac{p-1}{2}}p^{p-2}.\end{aligned}$$

Da cui

$$D_{\Phi_p} = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}p^{p-2}$$

DA FINIRE PERCHE' SBAGLIATO □

## Proposizione 4.9 – Sottocampi di $\mathbb{Q}[\zeta_p]$

Consideriamo $\mathbb{Q}[\zeta], \zeta = e^{\frac{2\pi i}{p}}$ e sia $G = \mathrm{Gal}\left(\mathbb{Q}[\zeta]/\mathbb{Q}\right)$. Per ogni $H \subseteq G$, sia

$$\eta_H = \sum_{h\in H}\zeta^h \in \mathbb{Q}[\zeta].$$

Allora $\mathbb{Q}[\zeta]^H = \mathbb{Q}[\eta_H]$.

*Dimostrazione.* Da questo momento faremo uso dell'isomorfismo canonico di $G$ con $(\mathbb{Z}/p\mathbb{Z})^*$, rendendo di fatto indistinguibili di due gruppi tramite la mappa

$$k \longmapsto \sigma_k \colon \zeta \mapsto \zeta^k.$$

Per prima cosa osserviamo che

$$\sigma_k(\eta_H) = \sum_{h \in H} \zeta^{kh}, \ \forall\ \sigma_k \in G.$$

Inoltre, per ogni $k \in H$ si avrà $\sigma_k(\eta_H) = \eta_H$ da cui $\mathbb{Q}[\eta_H] \subseteq \mathbb{Q}[\zeta]^H$. Quindi, per dimostrare l'uguaglianza, basta mostrare che

$$\big[\mathbb{Q}[\eta_H] : \mathbb{Q}\big] = \big[\mathbb{Q}[\zeta]^H : \mathbb{Q}\big] \qquad \text{dove } \big[\mathbb{Q}[\zeta]^H : \mathbb{Q}\big] = \frac{\big[\mathbb{Q}[\zeta] : \mathbb{Q}\big]}{\big[\mathbb{Q}[\zeta] : \mathbb{Q}[\zeta]^H\big]} = \frac{\#G}{\#H},$$

ovvero che

$$\big[\mathbb{Q}[\eta_H] : \mathbb{Q}\big] = \big[(\mathbb{Z}/p\mathbb{Z})^* : H\big].$$

Sfruttando l'espressione del polinomio minimo che abbiamo precedentemente dimostrato, avremo che

$$\big[\mathbb{Q}[\eta_H] : \mathbb{Q}\big] = \deg f_{\eta_H} = \#(\eta_H)^G.$$

Quindi il teorema si riduce a verificare che

$$\#(\eta_H)^G = [G : H].$$

Se $y \in (\mathbb{Z}/p\mathbb{Z})^*$ definiamo il seguente periodo:

$$\eta_{yH} = \sum_{h \in H} \zeta^{yh}.$$

In altre parole $\eta_{yH} = \sigma_y(\eta_H)$. Osserviamo che, presi $y_1, y_2 \in (\mathbb{Z}/p\mathbb{Z})^*$, se $y_1 H = y_2 H$, allora chiaramente $\eta_{y_1 H} = \eta_{y_2 H}$. Inoltre se $y_1 H \neq y_2 H$, allora sosteniamo che

$$\eta_{y_1 H} \neq \eta_{y_2 H}.$$

Ricordiamo che le classi laterali costituiscono una partizione per il gruppo, quindi

$$y_1 H \neq \psi_2 H \implies y_1 H \cap y_2 H = \emptyset.$$

Inoltre sappiamo che $(1, \zeta, \dots, \zeta^{p-2})$ è una $\mathbb{Q}$-base di $\mathbb{Q}[\zeta]$. D'altronde anche $(\zeta, \zeta^2, \dots, \zeta^{p-1})$ lo è. Infatti

$$\mathbb{Q}[\zeta] \longrightarrow \mathbb{Q}[\zeta], \alpha \longmapsto \zeta\alpha$$

è un'applicazione lineare di $\mathbb{Q}$-spazi vettoriali invertibile. Per cui

$$\eta_{y_1 H} - \eta_{y_2 H} = \sum_{h \in H} \zeta^{y_1 H} - \sum_{h \in H} \zeta^{y_2 H} \neq 0$$

proprio perché $(\zeta, \zeta^2, \dots, \zeta^{p-1})$ è una base.
Infine

$$(\eta_H)^G = \{\, \sigma_k \eta_h \mid k \in (\mathbb{Z}/p\mathbb{Z})^* \,\} = \{\, \eta_{kH} \mid k \in (\mathbb{Z}/p\mathbb{Z})^* \,\} = \{\, \eta_{g_1 H}, \dots, \eta_{g_s H} \,\}.$$

Da cui $\#(\eta_H)^G = [G : H]$ in quanto $G/H = \{\, g_1 H, \dots, g_s H \,\}$. □

*Osservazione.* In particolare vale

$$f_{\eta_H}(X) = \prod_{j=1}^{s}(X - \eta_{g_j H}).$$

*Osservazione.* Ricordiamo dalla definizione di classe laterale, che $g_1 H = g_2 H \iff g_1 g_2^{-1} \in H$. Quindi

$$\#\{\, y \in G \mid yH = kH \,\} = \#\{\, k\,h \mid h \in H \,\} = \#H,$$

da cui

$$\prod_{k\in G}(X - \eta_{kH}) = \prod_{k=1}^{p-1}(X - \eta_{kH}) = f_{\eta_H}(X)^{\#H}.$$

**Proposizione 4.10 – Due sottocampi importanti di $\mathbb{Q}[\zeta_p]$**

Sia $G = \mathrm{Gal}\left(\mathbb{Q}[\zeta_p]/\mathbb{Q}\right) = (\mathbb{Z}/p\mathbb{Z})^*$. $G$ è ciclico quindi $G = \langle g \rangle$. Allora

- Il sottocampo associato a $\langle g^{\frac{p-1}{2}} \rangle$ è $\mathbb{Q}\left[\cos\frac{2\pi}{p}\right]$.
- Il sottocampo associato a $\langle g^2 \rangle$ è $\mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p}\right]$.

*Dimostrazione.* Dal momento che $G = \langle g \rangle$ è ciclico, sappiamo che ogni sottogruppo $H \leqslant G$ è del tipo

$$H = \langle g^d \rangle \qquad \text{con } d \mid p-1.$$

Inoltre avremo $\#H = \frac{p-1}{d}$. Nel nostro caso $\langle g^{\frac{p-1}{2}} \rangle$ ha 2 elementi. Ora $\langle g^{\frac{p-1}{2}} \rangle = \langle -1 \rangle$, quindi per la proposizione precedente, il sottocampo associato sarà

$$\mathbb{Q}[\zeta_p]^{\langle -1 \rangle} = \mathbb{Q}[\eta_{\langle -1 \rangle}]$$

che sarà un'estensione di grado $\frac{p-1}{2}$ su $\mathbb{Q}$. Infatti

$$\mathbb{Q}[\eta_{\langle -1 \rangle}] = \mathbb{Q}[\zeta + \zeta^{-1}] = \mathbb{Q}\left[\cos\frac{2\pi}{p}\right].$$

Descriviamo ora il sottocampo associato a $H = \langle g^2 \rangle$. Sappiamo

$$\#H = \frac{p-1}{2} \qquad \text{e} \qquad \eta_H = \sum_{t=1}^{\frac{p-1}{2}} \zeta^{g^{2t}}.$$

Inoltre sappiamo che $\deg f_{\eta_{\langle g^2 \rangle}} = 2$. Ora

$$\sigma_g(\eta_{\langle g^2 \rangle}) = \eta_{g\langle g^2 \rangle} = \sum_{k=1}^{\frac{p-1}{2}} \zeta^{g^{2k+1}}.$$

Da cui, come abbiamo visto nella prima osservazione alla proposizione,

$$f_{\eta_{\langle g^2 \rangle}}(X) = (X - \eta_{\langle g^2 \rangle})(X - \eta_{g\langle g^2 \rangle}) = X^2 - (\eta_{\langle g^2 \rangle} + \eta_{g\langle g^2 \rangle})X + \eta_{\langle g^2 \rangle}\eta_{g\langle g^2 \rangle}.$$

Dove

$$\eta_{\langle g^2 \rangle} + \eta_{g\langle g^2 \rangle} = \sum_{k=1}^{\frac{p-1}{2}} \zeta^{g^{2k}} + \sum_{k=1}^{\frac{p-1}{2}} \zeta^{g^{2k+1}} = \zeta + \zeta^2 + \ldots + \zeta^{p-1} = -1.$$

Resta da calcolare $\eta_{\langle g^2\rangle}\eta_{g\langle g^2\rangle}$ che sappiamo essere in $\mathbb{Z}$. Per semplicità di notazione scriviamo

$$\eta_0 = \eta_{\langle g^2\rangle} \qquad \text{e} \qquad \eta_1 = \eta_{g\langle g^2\rangle}.$$

Se riusciamo a determinare $\eta_0 - \eta_1 = A$, avremo

$$\begin{cases} \eta_0 + \eta_1 = -1 \\ \eta_0 - \eta_1 = A \end{cases} \implies \eta_0 = \frac{1}{2}(-1+A), \eta_1 = \frac{1}{2}(-1-A).$$

Ora

$$A = \eta_0 - \eta_1 = \sum_{k=1}^{\frac{p-1}{2}} \zeta^{g^{2k}} - \sum_{k=1}^{\frac{p-1}{2}} \zeta^{g^{2k+1}} = \sum_{j=1}^{p-1} \varepsilon_j \zeta^j,$$

dove

$$\varepsilon_j = \left(\frac{j}{p}\right)_L = \begin{cases} 1 & j = g^{2k} \\ -1 & j = g^{2k+1} \end{cases}$$

è il simbolo di Legendre. Tramite alcune manipolazioni algebriche che sfruttano le proprietà del simbolo di Legendre, si può dimostrare che

*guardare gli appundi di TN410 per alcune proprietà sul simbolo di Legendre*

$$A^2 = \left(\frac{-1}{p}\right)_L p.$$

Da cui

$$A = \pm\sqrt{(-1)^{\frac{p-1}{2}}p} \implies \eta_0, \eta_1 = \frac{1}{2}\left(1 \pm \sqrt{(-1)^{\frac{p-1}{2}}p}\right)$$

Che ci dice proprio $\mathbb{Q}[\eta_0] = \mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p}\right]$. □

## 4.2 GRUPPO TRANSITIVO DI UN POLINOMIO

Nei prossimi paragrafi $f(X) \in F[X]$ sarà sempre monico e separabile.

Se $f \in F[X]$ separabile, allora il suo campo di spezzamento $F_f$ è Galois su $F$. In particolare se

$$f(X) = \prod_{j=1}^{n}(X - \alpha_j), \qquad \text{con } \alpha_1, \dots, \alpha_n \in F_f,$$

preso

$$\beta = \prod_{i<j}(\alpha_i - \alpha_j),$$

certamente $\beta \in F_f$, inoltre $\beta^2 = D_f$. Quindi

$$F \subseteq F[\sqrt{D_f}] \subseteq F_f,$$

dove $F[\sqrt{D_f}]/F$ è quadratica se $D_f$ non è un quadrato perfetto, altrimenti $F[\sqrt{D_f}] = F$.

**Definizione 4.11 – Gruppo di Galois di un polinomio**

Sia $f \in F[X]$ un polinomio separabile. Definiamo il *gruppo di Galois di* $f$ come il gruppo di Galois di $F_f/F$:

$$\mathrm{Gal}(f) := \mathrm{Gal}(F_f/F).$$

**Proposizione 4.12**

Sia $E/F$ un'estensione di Galois. Dove $E = F_f$ con $f \in F[X], n = \deg f$. Allora

$$\mathrm{Gal}(f) \lesssim S_n.$$

*Dimostrazione.* Supponiamo che

$$f(X) = (X-\alpha_1)(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n) \implies E = F_f = F[\alpha_1,\ldots,\alpha_n].$$

Vogliamo dimostrare che

$$\mathrm{Gal}(f) \longrightarrow \mathrm{Sym}\big(\{\alpha_1,\ldots,\alpha_n\}\big) \cong S_n, \sigma \longmapsto \begin{pmatrix} \alpha_1 & \ldots & \alpha_n \\ \sigma(\alpha_1) & \ldots & \sigma(\alpha_n) \end{pmatrix}$$

è un omomorfismo. Ma ciò segue da

$$f\big(\sigma(\alpha_j)\big) = \sigma\big(f(\alpha_j)\big) = 0 \implies \forall\, j\, \exists!\, k : \sigma(\alpha_j) = \alpha_k.$$

Da cui segue che $\mathrm{Gal}(f) \lesssim S_n$ per il teorema fondamentale dell'omomorfismo di gruppi. □

*Osservazione.* Da ciò segue che $\#\,\mathrm{Gal}(f) \mid n!$. Inoltre se $f$ è irriducibile e $f(\alpha) = 0$ avremo

$$F \subset F[\alpha] \subseteq F_f \qquad \text{con } \big[F[\alpha] : F\big] = n.$$

Da cui $n \mid \#\,\mathrm{Gal}(f)$.

**Esempio** (Controesempio)**.** Il viceversa non è sempre vero, ad esempio se prendiamo

$$f(X) = (X^2-2)(X^2+1),$$

avremo che $f$ ha grado 4 ed è riducibile. Ma il suo campo di spezzamento $\mathbb{Q}[\sqrt{2}, i]$ ha ancora grado 4.

**Corollario.** Se $f$ ha grado $n > 2$, allora

$$\mathrm{Gal}(f) \ncong \mathbb{Z}/n!\mathbb{Z}.$$

*Dimostrazione.* Segue da $\mathbb{Z}/n!\mathbb{Z} \ncong S_n$, infatti pur avendo la stessa dimensione, $\mathbb{Z}/n!\mathbb{Z}$ è abeliano mentre $S_n$ non lo è. □

## Definizione 4.13 – Sottogruppo transitivo

Un sottogruppo $H \leqslant S_n$ si dice *transitivo* se

$$\forall\, i,j \in \{1,\ldots,n\} \exists\ \sigma \in H : \sigma(i) = j.$$

*Osservazione.* Chiaramente è possibile dare una nozione più generale di sottogruppo transitivo, in questo corso si è preferito richiamarla solo per i sottogruppi di $S_n$.

**Esempio.** $S_n, A_n, C_n = \langle(1\ 2\ \ldots\ n)\rangle, D_n$ sono tutti sottogruppi transitivi su $S_n$. $S_{n-1} \leqslant S_n$ non è transitivo.

**Tabella 4.1:** Sottogruppi transitivi di $S_n$

| Gruppo | #Sottogruppi transitivi | Descrizione |
|---|---|---|
| $S_2$ | 1 | $S_2$ |
| $S_3$ | 2 | $S_3 = D_3, A_3 = C_3$ |
| $S_4$ | 5 | $S_4, A_4, C_4, D_4, V$ |
| $S_5$ | 5 | $S_5, A_5, C_5, D_5, F_5$ |
| $S_6$ | 16 | |
| $S_7$ | 7 | |
| $S_8$ | 50 | |
| $\vdots$ | | |
| $S_{24}$ | 26813 | |

**Esempio** (Sottogruppi isomorfi ma diversamente transitivi)**.** Consideriamo $\langle (1\,2), (3\,4)\rangle \leqslant S_4$. Osserviamo che tale sottogruppo non è transitivo (ad esempio non esiste $\sigma$ tale che $\sigma(2) = 3$) e che è isomorfo a $C_2 \times C_2$.
Consideriamo ora il gruppo di Klein

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

Si mostra facilmente che $V$ è transitivo. Inoltre anche $V$ è isomorfo a $C_2 \times C_2$. Quindi la transitività non è una proprietà invariante per isomorfismi.

## Proposizione 4.14 – Caratterizzazione gruppi di Galois transitivi

Sia $f \in F[X]$ separabile. Allora $f$ è irriducibile se e soltanto se $\mathrm{Gal}(f) \lesssim S_n$ è transitivo sulle radici.

*Dimostrazione.* Supponiamo che $f$ sia irriducibile. Quindi avremo ⇒)

$$f(X) = \prod_{j=1}^{n} (X - \alpha_j) \qquad \text{e} \qquad F_f = F[\alpha_1, \ldots, \alpha_n].$$

Siano $\alpha, \beta \in \{\alpha_1, \ldots, \alpha_n\}$. $F[\alpha], F[\beta]$ sono campi col gambo $f$. Vi è chiaramente un isomorfismo $F[\alpha] \xrightarrow{\sim} F[\beta], \alpha \mapsto \beta$. Definisco $f_1$ la composizione di tale isomorfismo con l'immersione in $F_f$:

$$f_1 \colon F[\alpha] \xrightarrow{\sim} F[\beta] \hookrightarrow F_f.$$

Sappiamo, assumendo $\alpha = \alpha_1$, che $f_1$ può essere esteso, passo dopo passo, a un $F$-omomorfismo

*per la costruzione possiamo usare il teorema 2.4*

$$f_n \colon F[\alpha_1, \ldots, \alpha_n] = F_f \longrightarrow F_f, \alpha \longmapsto \beta.$$

Quindi ho trovato $f_n \in \mathrm{Aut}(F_f/F) = \mathrm{Gal}(F_f/F)$ tale che $f_n(\alpha) = \beta$. Dal momento che posso trovare una tale mappa per ogni coppia di radici di $f$, ciò significa che $\mathrm{Gal}(f)$ è transitivo su $S_n$.
Supponiamo che $\mathrm{Gal}(f)$ sia transitivo. Sia $g(X) \in F[X]$ un fattore irriducibile di $f(X)$. Se $\alpha$ è una radice di $g$, allora per ogni radice $b$ di $f$, sia $\sigma \in \mathrm{Gal}(f)$ tale che $\sigma(\alpha) = \beta$. Da cui ⇐)

$$g(\beta) = g\big(\sigma(\alpha)\big) = \sigma\big(g(\alpha)\big) = 0.$$

Quindi ogni radice di $f$ è radice di $g$, ne segue che $f \mid g$ e quindi $f(X) = g(X)$ irriducibile. □

**Esempio.** Consideriamo $f(X) = (X^2-2)(X^2+1)$. Sappiamo che $\mathbb{Q}_f = \mathbb{Q}[\sqrt{2}, i]$ e

$$\mathrm{Gal}(\mathbb{Q}_f, \mathbb{Q}) = \left\{ \sigma_1, \sigma_4 = \begin{pmatrix} \sqrt{2} \mapsto \pm\sqrt{2} \\ i \mapsto \pm i \end{pmatrix}, \sigma_2, \sigma_3 = \begin{pmatrix} \sqrt{2} \mapsto \pm\sqrt{2} \\ i \mapsto \mp i \end{pmatrix} \right\}$$

Ora, se denotiamo $\left\{ \alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = i, \alpha_4 = -i \right\}$, possiamo sfruttare l'immersione isomorfa

$$\mathrm{Gal}(f) \xhookrightarrow{\sim} \mathrm{Sym}\big(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}\big) \cong S_4$$

In particolare avremo

$$\begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto i \end{pmatrix} \longleftrightarrow (1) \qquad \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \end{pmatrix} \longleftrightarrow (1\ 2)$$

$$\begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \end{pmatrix} \longleftrightarrow (3\ 4) \qquad \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \end{pmatrix} \longleftrightarrow (1\ 2)(3\ 4)$$

Ovvero $\mathrm{Gal}(f) \cong \{ (1), (1\ 2), (3\ 4), (1\ 2)(3\ 4) \} \leqslant S_n$ che come ci aspettavamo dalla proposizione non è transitivo.

*Osservazione.* Se invece consideriamo $\mathbb{Q}[\sqrt{2}+i] = \mathbb{Q}[\sqrt{2}, i]$ che è il campo di spezzamento di

$$g(X) = f_{\sqrt{2}+i}(X) = \prod_{j=1}^{4} \big(X - \sigma_j(\sqrt{2}+i)\big) = X^4 - 2x^2 + 9,$$

ci aspettiamo che $\mathrm{Gal}(g)$ sia transitivo poiché $g$ è irriducibile su $\mathbb{Q}[X]$. Ce lo aspettiamo nonostante $\mathrm{Gal}(g) \cong \mathrm{Gal}(f)$, poiché abbiamo visto che la transitività non è invariante per isomorfismi. Denotiamo $\left\{ \beta_1 = \sqrt{2}+i, \beta_2 = -\sqrt{2}+i, \beta_3 = \sqrt{2}-i, \beta_4 = -\sqrt{2}-i \right\}$. Ora, dal momento che $\mathbb{Q}[\sqrt{2}+i] = \mathbb{Q}[\sqrt{2}, i]$, avremo che $\mathrm{Gal}(g)$ ha gli stessi automorfismi di $\mathrm{Gal}(f)$. In particolare

$$\sigma_1 : \begin{matrix} \beta_1 \mapsto \beta_1 \\ \beta_2 \mapsto \beta_2 \\ \beta_3 \mapsto \beta_3 \\ \beta_4 \mapsto \beta_4 \end{matrix} \qquad \sigma_2 : \begin{matrix} \beta_1 \mapsto \beta_2 \\ \beta_2 \mapsto \beta_1 \\ \beta_3 \mapsto \beta_4 \\ \beta_4 \mapsto \beta_1 \end{matrix} \qquad \sigma_3 : \begin{matrix} \beta_1 \mapsto \beta_3 \\ \beta_2 \mapsto \beta_4 \\ \beta_3 \mapsto \beta_1 \\ \beta_4 \mapsto \beta_2 \end{matrix} \qquad \sigma_4 : \begin{matrix} \beta_1 \mapsto \beta_4 \\ \beta_2 \mapsto \beta_3 \\ \beta_3 \mapsto \beta_2 \\ \beta_4 \mapsto \beta_1 \end{matrix}$$

da cui

$$\sigma_1 \longleftrightarrow (1) \qquad \sigma_2 \longleftrightarrow (1\ 2)(3\ 4) \qquad \sigma_3 \longleftrightarrow (1\ 3)(2\ 4) \qquad \sigma_4 \longleftrightarrow (1\ 4)(2\ 3).$$

Ovvero $\mathrm{Gal}(g) \cong V \leqslant S_n$ che è transitivo. In conclusione $\mathrm{Gal}(g) = \mathrm{Gal}(f)$ ed entrambi sono isomorfi a $C_2 \times C_2 \leqslant S_4$, ma solo $\mathrm{Gal}(g)$ è transitivo. Questo accade poiché $g$ è irriducibile mentre $f$ non lo è.

## 4.3 GRUPPO DI UN POLINOMIO NEL GRUPPO ALTERNO

In questo paragrafo cercheremo di capire sotto quali ipotesi il gruppo di Galois di un polinomio $f$ di grado $n$, è contenuto nel gruppo alterno $A_n$.

Cominciamo con un breve richiamo sul segno di una permutazione.

### Definizione 4.15 – Segno permutazione

Sia $\sigma \in S_n$. Scritto $\sigma = c_1 \circ c_2 \circ \ldots \circ c_k$ prodotto di cicli disgiunti, diremo che il *segno* di $\sigma$ è

$$\operatorname{sgn}(\sigma) = (-1)^{l(c_1)+\ldots+l(c_k)-k},$$

dove con $l(c_j)$ indichiamo la lunghezza di $c_j$.

*Osservazione.* Alternativamente, scritto $\sigma = \tau_1 \circ \ldots \circ \tau_s$ prodotto di trasposizioni, potevamo definire il segno di $\sigma$ come

$$\operatorname{sgn}(\sigma) = (-1)^s.$$

Chiaramente le due definizioni sono equivalenti.

**Esempio.**

$$\operatorname{sgn}(1\ 2) = (-1)^1 = -1 \qquad \text{e} \qquad \operatorname{sgn}(1\ 2\ \ldots\ n) = (-1)^{n-1}.$$

### Definizione 4.16 – Gruppo alterno

Considero la mappa

$$\operatorname{sgn}\colon S_n \longrightarrow \{\pm 1\}, \sigma \longmapsto \operatorname{sgn}(\sigma)$$

che costituisce un omomorfismo suriettivo. Definisco il *gruppo alterno* di $S_n$ come il nucleo di sgn:

$$A_n := \operatorname{Ker}(\operatorname{sgn}) = \{\, \sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1 \,\}.$$

*Osservazione.* $A_n$ è di fatto l'insieme delle permutazioni pari di $S_n$. La definizione come nucleo di un omomorfismo però ci garantisce che

$$A_n \trianglelefteq S_n \qquad \text{e} \qquad [S_n : A_n] = 2.$$

**Esempio.** Consideriamo il gruppo delle permutazioni di ordine 3:

$$S_3 = \{\, (1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \,\}.$$

In $S_3$ i 2-cicli hanno $\operatorname{sgn} = -1$ mentre i 3-cicli hanno $\operatorname{sgn} = 1$. Quindi

$$A_3 = \{\, (1), (1\ 2\ 3), (1\ 3\ 2) \,\} \cong C_3.$$

**Proprietà 4.17.** Sia $f \in F[X]$. Allora $D_f \in F$.

*Dimostrazione.* Ricordiamo la definizione di discriminante

$$D_f = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Tale definizione, per via del quadrato, non dipende dall'etichettatura delle radici di $f$. Quindi, per ogni $\sigma \in \operatorname{Gal}(f)$, avremo

$$\sigma D_f = \prod_{i<j} \big(\sigma(\alpha_i) - \sigma(\alpha_j)\big)^2 = D_f$$

in quanto abbiamo solo riordinato le radici. Da ciò segue

$$D_f \in F_f^{\mathrm{Gal}(f)} = F.$$

□

**Definizione 4.18 – Radice del discriminante**

Preso $f \in F[X]$, definiamo

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j) = \sqrt{D_f}.$$

**Proprietà 4.19.** Siano $f \in F[X]$ e $\sigma \in \mathrm{Gal}(f)$. Allora

$$\sigma\Delta_f = \mathrm{sgn}(\sigma)\Delta_f.$$

*Dimostrazione.* Non fornita. La tesi è comunque intuitiva poiché $\sigma$ scambia gli indici delle radici, facendo comparire un segno meno ogni volta che $i < j$ e $\sigma(i) > \sigma(j)$. □

**Teorema 4.20 – Quando $\mathrm{Gal}(f) \leqslant A_n$?**

Sia $f \in F[X]$. Allora $\mathrm{Gal}(f) \leqslant A_n$ se e soltanto se $\Delta_f \in F$, ovvero se $D_f$ è un quadrato perfetto in $F$.

*Dimostrazione.* Dalla proprietà precedente sappiamo che $\sigma\Delta_f = \mathrm{sgn}(\sigma)\Delta_f$. Da cui

$$\sigma \in A_n \iff \sigma\Delta_f = \Delta_f \iff \Delta_f \in F_f^{A_n \cap \mathrm{Gal}(f)}.$$

In particolare segue facilmente che

$$F[\Delta_f] = F_f^{A_n \cap \mathrm{Gal}(f)}.$$

Inoltre $\big[F[\Delta_f] : F\big] \leqslant 2$ in quanto $\Delta_f^2 = D_f \in F$.
In conclusione

$$\mathrm{Gal}(f) \leqslant A_n \iff \mathrm{Gal}(f) \cap A_n = \mathrm{Gal}(f) \iff F[\Delta_f] = F_f^{A_n \cap \mathrm{Gal}(f)} = F_f^{\mathrm{Gal}(f)} = F.$$

Da cui segue la tesi. □

**Proposizione 4.21 – Gruppo di Galois di un polinomio di grado 3**

Sia $f \in F[X]$ un polinomio di grado 3. Allora

- Se $f$ è irriducibile,
$$\begin{cases} \mathrm{Gal}(f) \cong A_3 & \text{se } D = \square \\ \mathrm{Gal}(f) \cong S_3 & \text{se } D \neq \square \end{cases}$$
- Se $f$ è totalmente riducibile,
$$\mathrm{Gal}(f) = \{\mathrm{id}\}.$$
- Se $f$ è parzialmente riducibile in un fattore di secondo grado e uno di primo,
$$\mathrm{Gal}(f) \cong \mathbb{Z}/2\mathbb{Z}.$$

**Tabella 4.2:** Sottogruppi transitivi di $S_4$.

| Sottogruppo | Elementi | Normale su $S_4$? |
|---|---|---|
| $S_4$ | $(1), (i\ j), (i\ j\ k), (i\ j\ k\ l), (i\ j)(k\ l)$ | Sì |
| $A_4$ | $(1), (i\ j\ k), (i\ j)(k\ l)$ | Sì |
| $D_4$ | $(1), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (i\ j)(k\ l)$ | No |
| $C_4$ | $\langle(1\ 2\ 3\ 4)\rangle$ | No |
| $V$ | $(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$ | Sì |

*Dimostrazione.* Per definizione $\mathrm{Gal}(f) = \mathrm{Gal}(F_f/F)$. D'altronde sappiamo che

$$\#\,\mathrm{Gal}(F_f/F) = [F_f : F] \leqslant (\deg f)! = 6.$$

Quindi $\mathrm{Gal}(f)$ ha ordine un divisore di 6.
Se $f$ è totalmente riducibile, è chiaro che $F_f = F$ e quindi $\mathrm{Gal}(f) = \{\mathrm{id}\}$. Se $f$ ha un fattore di grado 2 irriducibile, allora $F_f/F$ è un'estensione quadratica, in particolare

$$\#\,\mathrm{Gal}(f) = [F_f : F] = 2 \implies \mathrm{Gal}(f) \cong \mathbb{Z}/2\mathbb{Z}.$$

Supponiamo ora che $f$ sia irriducibile. Avremo che se $f[\alpha] = 0$, $F \subset F[\alpha] \subset F_f$, da cui

$$\big[F[\alpha] : F\big] = \deg f = 3 \implies 3 \mid [F_f : F] = \#\,\mathrm{Gal}(f).$$

Per cui $3 \mid \#\,\mathrm{Gal}(f) \mid 6$, ovvero $\#\,\mathrm{Gal}(f) \in \{3, 6\}$. Dal teorema precedente sappiamo che $\mathrm{Gal}(f) \leqslant A_3$ se e soltanto se $\Delta_f \in F$, ovvero se $D_f$ è un quadrato perfetto in $F$. Da cui

$$\#\,\mathrm{Gal}(f) = [F_f : F] = \begin{cases} 3 & \text{se } D_f = \square \\ 6 & \text{se } D_f \neq \square \end{cases}$$

□

## 4.4 POLINOMI DI QUARTO GRADO

In questo paragrafo forniremo dei criteri per determinare il gruppo di Galois di un polinomio $f \in F[X]$ di quarto grado che sia irriducibile e separabile.

Sappiamo che $G_f := \mathrm{Gal}(f) \subseteq \mathrm{Sym}\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \cong S_4$, dove $\alpha_i$ sono radici di $f$. Inoltre $G_f$ è transitivo su $S_4$ poiché $f$ è irriducibile. $G_f$ deve pertanto essere uno dei sottogruppi di $S_4$ elencati nella tabella 4.2.

*Osservazione.* Forniamo qualche spiegazione sulla normalità dei sottogruppi transitivi di $S_4$:

- $S_4$ è banalmente normale in se stesso.
- $A_4$ è normale in $S_4$ poiché ha indice 2.
- $D_4$ non è normale, infatti $(1\ 2)(1\ 2\ 3\ 4)(1\ 2) = (1\ 3\ 4\ 2) \notin D_4$.
- $C_4$ non è normale per lo stesso motivo di $D_4$.
- $V$ è normale poiché coniugando un k-ciclo si ottiene sempre un k-ciclo. In particolare tutti gli elementi di $V$ distinti da $(1)$ sono $2 \times 2$-cicli, quindi $V$ è normale.

**Definizione 4.22 – Risolvente cubica**

Supponiamo che $f \in F[X]$ sia un polinomio irriducibile e separabile di grado 4. Il suo campo di spezzamento sarà $F_f = F[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ dove $\alpha_i$ sono le radici di $f$. Presi

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4; \qquad \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4; \qquad \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Definiamo la *risolvente cubica* di $f$ come

$$g(X) = (X-\alpha)(X-\beta)(X-\gamma).$$

*Osservazione.* Per prima cosa osserviamo che $F \subseteq F[\alpha,\beta,\gamma] \subseteq F_f$. Inoltre, dal momento che $f$ è separabile, $\alpha, \beta, \gamma$ sono tutti distinti. Ad esempio

$$\alpha - \beta = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_4) \neq 0.$$

Infine si può facilmente verificare che $S_4$ permuta $\alpha, \beta, \gamma$, cioè se $\sigma \in S_4 = \mathrm{Sym}\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, si ha

$$\sigma\{\alpha,\beta,\gamma\} = \{\alpha,\beta,\gamma\}.$$

**Proprietà 4.23.** La risolvente cubica ha coefficienti in $F$.

*Dimostrazione.* Dall'osservazione precedente sappiamo che $S_4$ permuta $\alpha, \beta, \gamma$. In particolare da

$$g(X) = (X-\alpha)(X-\beta)(X-\gamma) \implies \sigma g(X) = g(X),\ \forall\ \sigma \in S_4.$$

In particolare $G_f \subseteq S_4$, quindi

$$g(X) \in F^{G_f}[X] = F[X].$$

□

**Proposizione 4.24 – Forma esplicita della risolvente cubica**

Supponiamo che $f(X) \in F[X]$ sia un polinomio separabile e irriducibile della forma

$$f(X) = X^4 + b\,X^3 + c\,X^2 + d\,X + e.$$

Allora la risolvente cubica di $f$ è

$$g(X) = X^3 - c\,X^2 + (b\,d - 4e)X + 4c\,e - d^2.$$

*Dimostrazione.* Per definizione

$$g(X) = (X-\alpha)(X-\beta)(X-\gamma) = X^3 - (\alpha+\beta+\gamma)X^2 + (\alpha\,\beta + \alpha\,\gamma + \beta\,\gamma)X - \alpha\,\beta\,\gamma.$$

Inoltre

$$f(X) = \prod_{i=1}^{4}(X-\alpha_i) = X^4 - (\alpha_1+\alpha_2+\alpha_3+\alpha_4)X^3 + \ldots + \alpha_1\alpha_2\alpha_3\alpha_4.$$

A questo punto è sufficiente verificare l'esattezza delle identità sui coefficienti. □

**Tabella 4.3:** Caratterizzazione dei gruppi di Galois per polinomi di grado 4.

| $G_f$ | $\#V \cap G_f$ | $\#(G_f/V \cap G_f) = \#G_g = [F[\alpha,\beta,\gamma] : F]$ |
|---|---|---|
| $S_4$ | 4 | 6 |
| $A_4$ | 4 | 3 |
| $V$ | 4 | 1 |
| $D_4$ | 4 | 2 |
| $C_4$ | 2 | 2 |

*Osservazione.* Se in $f$ sostituiamo $X - b/4$ ad $X$, otteniamo

$$f(X - b/4) = X^4 + A X^2 + B X + C,$$

che sappiamo avere lo stesso gruppo di Galois di $f(X)$. A questo punto la risolvente cubica ha una forma più compatta:

$$g(X) = X^3 - A X^2 - 4C X + 4A C - B^2.$$

**Proposizione 4.25 – Campo di spezzamento della risolvente cubica**

Sia $f \in F[X]$ un polinomio irriducibile e separabile di grado 4 e sia $G_f = \mathrm{Gal}(f)$. Se $g(X)$ è la risolvente cubica di $f$, allora

$$F_g = F_f^{V \cap G_f},$$

dove $V \leqslant S_4$ è il gruppo di Klein.

*Dimostrazione.* In questa dimostrazione mostreremo solo una delle due implicazioni, poiché la seconda richiede una parte di teoria dei gruppi che esula dagli argomenti di questo corso.
Per definizione sappiamo che $F_g = F[\alpha,\beta,\gamma]$. Mostriamo che $F[\alpha,\beta,\gamma] \subseteq F_f^{V \cap G_f}$. Se $\sigma \in V$ è facile verificare che

$$\sigma\alpha = \alpha; \qquad \sigma\beta = \beta; \qquad \sigma\gamma = \gamma.$$

In particolare ciò vale se $\sigma \in V \cap G_f$, da cui

$$\alpha,\beta,\gamma \in F_f^{V \cap G_f} \implies F[\alpha,\beta,\gamma] \subseteq F_f^{V \cap G_f}.$$

□

**Corollario.** L'estensione $F[\alpha,\beta,\gamma]/F$ è Galois con gruppo di Galois

$$G_g \cong \frac{G_f}{V \cap G_f}.$$

*Dimostrazione.* Siccome $V \cap G_f$ è normale in $G_f$, avremo che $F_f^{V \cap G_f} = F[\alpha,\beta,\gamma]/F$ è normale è quindi di Galois. In particolare, sempre per la normalità del gruppo corrispondente, avremo

$$G_g \cong \frac{G_f}{V \cap G_f}.$$

□

*Osservazione.* Da ciò segue un'importante caratterizzazione dei gruppi di Galois dei polinomi separabili e irriducibili di grado 4. Nella tabella 4.3 possiamo vedere come il

gruppo di Galois $G_g$ ci permetta di determinare $G_f$, tranne nel caso in cui $G_f = D_4$ o $G_f = C_4$. Per dare una determinazione in quest'ultimo caso, osserviamo che se $g(X)$ ha un fattore di grado due irriducibile, allora

$$G_g = C_2 \implies F_g = F[\sqrt{D}].$$

Consideriamo $f$ in $F[\sqrt{D}][X]$. Se $f$ risulta ancora irriducibile, allora

$$[F_f : F[\sqrt{D}]] = 4 \implies G_f = D_4. \text{ Quindi } \qquad G_f = \begin{cases} D_4 & f \in \operatorname{Irr}(F[\sqrt{D}][X]) \\ C_4 & \text{altrimenti} \end{cases}$$

**Esempio.** Troviamo il gruppo di Galois di alcuni polinomi di quarto grado:

- $X^4 - 4x + 2$ è irriducibile poiché è un 2-eisenstain. La sua risolvente cubica è $X^3 - 8X - 16$ che è irriducibile e il suo discriminante non è un quadrato perfetto. Quindi $G_g = S_3$ da cui $G_f = S_4$.
- $X^4 + 4X^2 + 2$ è irriducibile poiché è un 2-eisenstain. La sua risolvente cubica è $(X-4)(X^2-8)$. Quindi $G_g = C_2$ da cui $G_f$ è $D_4$ oppure $C_4$. Osserviamo che $\mathbb{Q}_g = \mathbb{Q}[\sqrt{2}]$, su cui $f$ si scrive come $(X^2 + 2 - \sqrt{2})(X^2 + 2 + \sqrt{2})$. Quindi $G_f = C_4$.
- $X^4 - 2$ è irriducibile. La sua risolvente cubica è $X(X^2 + 8)$. Quindi $G_g = C_2$ e $G_f$ è $D_4$ oppure $C_4$. Osserviamo che $\mathbb{Q}_g = \mathbb{Q}[\sqrt{-2}]$, su cui $f$ si può dimostrare essere ancora irriducibile. Quindi $G_f = D_4$.
- $X^4 + 10X^2 + 2$ è irriducibile. La sua risolvente cubica è $(X+10)(X+4)(X-4)$. Quindi $G_g = C_1$ da cui $G_f = V$.

## 4.5 POLINOMI DI GRADO PRIMO

In questo paragrafo ci occuperemo di polinomi irriducibili che hanno grado primo. In particolare studieremo il loro gruppo di Galois nel caso in cui abbiano precisamente $p-2$ radici reali.

**Lemma 4.26.** Sia $H$ un sottogruppo di $S_p$. Supponiamo che $H$ contenga una trasposizione e un $p$-ciclo. Allora $H = S_p$.

*Dimostrazione.* Non fornita. □

**Proposizione 4.27**

Sia $f \in F[X]$ un polinomio irriducibile tale che $\deg f = p$ e $f$ ha $p-2$ radici reali e 2 radici complesse. Allora

$$\operatorname{Gal}(f) = S_p.$$

*Dimostrazione.* Sia $G_f = \operatorname{Gal}(f)$. Vogliamo applicare il lemma precedente a $G_f$. Supponiamo che $\alpha$ sia una radice di $f$, avremo

$$F \subseteq F[\alpha] \subseteq F_f, \qquad \text{con } [F[\alpha] : F] = p.$$

*il fatto a cui facciamo riferimento è il teorema di Cauchy*

Quindi $p \mid [F_f : F] = \#G_f$. Da un fatto di teoria dei gruppi, se $p \mid \#G$ con $G$ un gruppo finito, allora esiste $g \in G$ tale che $\operatorname{ord}(g) = p$. Quindi nel nostro caso esiste $\sigma \in G_f$ tale che $\operatorname{ord}(\sigma) = p$. Dal momento che $G_f \leqslant S_p$, $\sigma$ è necessariamente un $p$-ciclo, infatti non esistono altri elementi di $S_p$ con tale ordine.

Per trovare la trasposizione, osserviamo che, per ipotesi, vi sono solo due radici complesse. In particolare se $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \mathbb{R}$ sono tali radici, necessariamente $\alpha_1 = \overline{\alpha_2}$. Quindi se consideriamo l'automorfismo

$$k\colon F_f \longrightarrow F_f, \alpha \longmapsto \overline{\alpha},$$

avremo che

$$k(\alpha_1) = \alpha_2; \qquad k(\alpha_2) = \alpha_1; \qquad k(\alpha_j) = \alpha_j, \ \forall\, j \geqslant 3.$$

Quindi $k = (1\ 2)$. Dal lemma segue che $G_f = S_p$. □

*Osservazione.* Per ogni $p$ primo esiste sempre un polinomio con le proprietà descritte nella proposizione precedente. Se $p = 2, 3$ è facile dare degli esempi, supponiamo quindi $p \geqslant 5$. Siano $n_1 < \ldots < n_{p-2} \in \mathbb{N}$ pari e $m > 0$ pari. Definiamo

$$g(X) = (X^2 + m)(X - n_1) \cdot \ldots \cdot (X - n_{p-2}).$$

Tale polinomio ha precisamente $p - 2$ radici reali. Cerchiamo di traslarlo opportunamente in modo da renderlo irriducibile senza cambiare il numero di radici reali. Definiamo

$$e = \min\{\, |g(x)| > 0 : g'(x) = 0 \,\}; \qquad n \in \mathbb{N} \text{ dispari tale che } \frac{2}{n} < e$$

Prendiamo quindi

$$f(X) = g(X) - \frac{2}{n} \in \mathbb{Q}[X]$$

che $p$ irriducibile. Infatti, per come abbiamo definito $g$, si mostra facilmente che $n\, f(X) = n\, g(X) - 2$ è un 2-eisenstain.

## 4.6 PROBLEMA DI GALOIS INVERSO (CENNI)

Questo paragrafo vuole solo accennare in cosa consiste il problema di Galois inverso. Per una trattazione più approfondita si rimanda ad un testo più approfondito.

Il problema inverso consiste nel determinare, dato $G$ un gruppo finito, se esiste $f \in F[X]$ tale che

$$G_f \cong G.$$

Tale questione resta un problema aperto nella sua forma più generale. In alcuni casi particolari è comunque possibile fornire una risposta certa.

**Teorema 4.28 – Problema inverso per gruppi abeliani**

Sia $G$ un gruppo abeliano. Allora esiste $f \in F[X]$ tale che $G_f \cong G$.

## 4.7 CAMPI FINITI

In questo paragrafo per denotare un generico campo finito useremo il simbolo $\mathbb{F}$. Cominciamo con il riepilogare alcune proprietà dei campi finiti.

**Proprietà 4.29.** Esistono $n \in \mathbb{N}$ e $p$ primo tali che

$$\#\mathbb{F} = p^n.$$

**Proprietà 4.30.** Se $\mathbb{F}$ ha cardinalità $p^n$, allora

$$\mathbb{F} = \mathbb{F}_{p^n}.$$

*Osservazione.* In generale $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$.

**Proprietà 4.31.** $\mathbb{F}_{p^n}/\mathbb{F}_p$ è un'estensione finita di grado $n$.

**Proprietà 4.32.** Per ogni $x \in F_{p^n}$ si ha $x^{p^n} = x$.

**Proprietà 4.33.** $\mathbb{F}_{p^n}/\mathbb{F}_p$ è sempre un'estensione di Galois.

*Dimostrazione.* Il polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$ è separabile in quanto $(X^{p^n} - X)' = -1$. Quindi

$$\mathbb{F}_{p^n} = (\mathbb{F}_p)_{X^{p^n}-X}$$

è il campo di spezzamento di un polinomio separabile. □

**Proprietà 4.34.** Due campi finiti $\mathbb{F}_{q_1}$ e $\mathbb{F}_{q_2}$ sono isomorfi se e solo se $q_1 = q_2$.

**Proprietà 4.35.** Per ogni $q = p^n$ esiste un campo finito $\mathbb{F}_q$ di ordine $q$.

*Dimostrazione.* Consideriamo $K = (\mathbb{F}_p)_{X^q-X}$ il campo di spezzamento di $X^q - X \in \mathbb{F}_p[X]$. Definiamo $S = \{\, \alpha \in K \mid \alpha^q = \alpha \,\}$ l'insieme delle radici di $X^q - X$. Osserviamo che $|S| = q$ in quanto sappiamo dalle proprietà precedenti che $X^q - X \in \mathbb{F}_p[X]$ è un polinomio separabile. Certamente $S \subseteq K$, se dimostriamo che $S$ è un campo, esso deve necessariamente essere il campo di spezzamento di $X^q - X$, da cui $S = K$. Ora $S$ è chiaramente chiuso rispetto alla moltiplicazione e al calcolo degli inversi. D'altronde è chiuso anche rispetto alla somma, infatti, presi $\alpha, \beta \in S$, per la formula sbagliata avremo

$$(\alpha+\beta)^q = (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \implies \alpha + \beta \in S.$$ □

**Teorema 4.36 – Gruppo di Galois di $\mathbb{F}_{p^n}/\mathbb{F}_p$**

Sia $q = p^n$ con $p$ primo. Allora

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}.$$

*Dimostrazione.* Sappiamo già che $\#\,\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Quindi, affinché $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, ci basta dimostrare che $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ è ciclico. Dobbiamo quindi esibire un generatore. Consideriamo l'automorfismo di Frobenius:

$$\Phi\colon \mathbb{F}_{p^n} \longrightarrow F_{p^n}, x \longmapsto x^p.$$

Osserviamo che $\Phi$ fissa gli elementi di $\mathbb{F}_p$, quindi $\Phi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. A questo punto

dobbiamo mostrare che $\Phi$ ha ordine $n$. Osserviamo che

$$\Phi^k(X) := \underbrace{\Phi \circ \ldots \circ \Phi}_{k \text{ volte}}(X) = X^{p^k}.$$

Quindi

$$\Phi^n(x) = x^{p^n} = x, \ \forall\, x \in \mathbb{F}_{p^n}.$$

Resta da mostrare che per ogni $k < n$, $\Phi^k \neq \mathrm{id}$, cioè che esite $y \in \mathbb{F}_{p^n}$ tale che $y^{p^k} \neq y$. Per un fatto di teoria dei gruppi, $\mathbb{F}_{p^n}^*$ è ciclico. Sia $y$ un generatore di $\mathbb{F}_{p^n}^*$, allora

$$\mathrm{ord}(y) = p^n - 1, k < n \implies y^{p^k-1} \neq 1 \implies y^{p^k} \neq y.$$

Quindi $\mathrm{ord}(\Phi) = n$ e $\langle \Phi \rangle = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. □

*Osservazione.* Alla luce delle proprietà precedenti, sappiamo che per ogni $q = p^n$ con $p$ primo, esiste $\mathbb{F}_q$ il campo finito con $q$ elementi. Inoltre due campi con $q$ elementi sono isomorfi. Infine $\mathbb{F}_q/\mathbb{F}_p$ è Galois e il teorema ci dice che

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}.$$

**Teorema 4.37 – $\mathbb{F}_{p^n}$ come estensione semplice**

Consideriamo l'estensione $\mathbb{F}_{p^n}/\mathbb{F}_p$. Allora esiste $\zeta \in \mathbb{F}_{p^n}$ tale che

$$\mathbb{F}_{p^n} = \mathbb{F}_p[\zeta].$$

*Dimostrazione.* Sia $\zeta$ un generatore di $\mathbb{F}_{p^n}^*$, che sappiamo esistere per un fatto di teoria dei gruppi. Segue immediatamente che $\mathbb{F}_p[\zeta] = \mathbb{F}_{p^n}$, infatti

$$\mathbb{F}_{p^n} = \left\{ 0, \zeta, \zeta^2, \ldots, \zeta^{p^n-1} \right\}.$$

□

*Osservazione.* Più in generale, tramite il teorema dell'elemento primitivo, si può dimostrare che se $K/\mathbb{Q}$ è finita, allora esiste $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$.

**Teorema 4.38 – Sottocampi di $\mathbb{F}_{p^n}$**

Consideriamo l'estensione $\mathbb{F}_{p^n}/\mathbb{F}_p$. Per ogni $k \mid n$ esiste un unico sottocampo $\mathbb{F}_{p^k}$ con $p^k$ elementi.

*Dimostrazione.* Abbiamo mostrato che $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z} = \langle \Phi \rangle$. Per le proprietà dei gruppi ciclici, sappiamo che per ogni divisore $k$ dell'ordine di $\langle \Phi \rangle$ vi è un solo sottogruppo di indice $k$. Quindi per ogni $k \mid n$ avremo il sottogruppo $\langle \Phi^k \rangle \cong \mathbb{Z}/\frac{n}{k}\mathbb{Z}$ a cui corrisponde il sottocampo

$$\mathbb{F}_{p^n}^{\langle \Phi^k \rangle} = \mathbb{F}_{p^k}.$$

□

*Osservazione.* Vale anche il viceversa, cioè se $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$ allora $k \mid n$.

**Definizione 4.39 – Funzione enumeratrice dei polinomi irriducibili in $\mathbb{F}_p$**

Sia $p$ primo. Definiamo la *funzione che enumera i polinomi irriducibili di grado* $d$ in $\mathbb{F}_p$ come

$$N_d(p) = \#\left\{ f \in \operatorname{Irr}\left(\mathbb{F}_p[X]\right) \;\middle|\; \deg f = d \right\}.$$

**Proposizione 4.40 – Numero di polinomi irriducibili in $\mathbb{F}_p$**

Sia $p$ primo. Allora

$$\sum_{d|n} d\, N_d(p) = p^n.$$

*Dimostrazione.* Consideriamo $f(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. Se mostriamo

$$f(X) = \prod_{\substack{f \in \operatorname{Irr}(\mathbb{F}_p[X]) \\ \deg f | n}} f, \tag{$\star$}$$

seguirebbe

$$p^n = \deg f = \deg \prod_{d|n} \prod_{\substack{f \in \operatorname{Irr}(\mathbb{F}_p[X]) \\ \deg f = d}} f = \sum_{d|n} N_d(p)\, d.$$

Mostriamo quindi $(\star)$. Sia $g$ un fattore irriducibile di $X^{p^n} - X$ e sia $\alpha$ una radice di $g$. Avremo

$$\mathbb{F}_p \subseteq \mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^n} \implies \deg g = \left[\mathbb{F}_p[\alpha] : \mathbb{F}_p\right] \mid n.$$

In particolare, dal momento che $X^{p^n} - X$ è il prodotto di tali fattori irriducibili ed è anche separabile, segue

$$X^{p^n} - X \mid \prod_{\substack{f \in \operatorname{Irr}(\mathbb{F}_p[X]) \\ \deg f | n}} f.$$

Per concludere basta dimostrare che se $h \in \operatorname{Irr}\left(\mathbb{F}_p[X]\right)$ e $\deg h \mid n$, allora

$$h \mid X^{p^n} - X.$$

Sia $\beta$ una radice di $h$. Per la corrispondenza e l'unicità dei campi finiti, $\mathbb{F}_p[\beta]$ si inietta isomorficamente in $\mathbb{F}_{p^n}$. Nel sottocampo di $\mathbb{F}_{p^n}$ isomorfo a $\mathbb{F}_p[\beta]$ ci sono tutte le radici di $h$, le quali sono in particolare radici di $X^{p^n} - X$. □

*Osservazione.* Se $n = l$ primo, allora la formula si riduce a

$$N_1(p) + l\, N_l(p) = p^l \implies N_l(p) = \frac{p^l - p}{l},$$

poiché chiaramente $N_1(p) = p$.

# 5 COSTRUZIONI CON RIGA E COMPASSO

## 5.1 INTRODUZIONE

I greci credevano che la dimostrazione ideale facesse uso della riga e del compasso. Furono tre i problemi classici che questo metodo non riuscì mai ad attaccare:

- la duplicazione del cubo;
- la trisezione di un angolo;
- la quadratura del cerchio.

Nell'800 Wantzel dimostrò che tali problemi non erano risolubili con il metodo della riga e del compasso.

In questo paragrafo daremo una struttura a tale approccio. Introdurremo i numeri "costruibili" che costituiscono un'estensione usata dai greci nella loro struttura numerica.

**Definizione 5.1 – Punti d'orgine**

Nella struttura delle costruzioni con riga e compasso, i punti $O = (0,0)$ e $(1,0)$, sono "assiomaticamente" intesi come costruibili.

**Definizione 5.2 – Operazioni con riga e compasso**

Le seguenti sono tutte e le sole operazioni consentite con riga e compasso:

1. Si può costruire la retta per due punti costruibili.
2. Si può costruire la circonferenza data il suo centro e un suo punto.

*Osservazione.* Il compasso viene inteso come "rigido", ciò significa che a priori non è possibile replicare il raggio di una circonferenza già tracciata per disegnarne un'altra.

**Definizione 5.3 – Punti costruibili**

Sono *costruibili* tutti e soli i punti di intersezione di

- due rette costruibili;
- due cerchi costruibili;
- una retta e un cerchio costruibile.

*Osservazione.* In generale un punto del piano si dice costruibile se, attraverso le operazioni sopra elencata, lo si può ottenere dai due punti di origine $(0,0)$ e $(1,0)$.

**Notazione.** Dati due punti $A, B$, indicheremo con

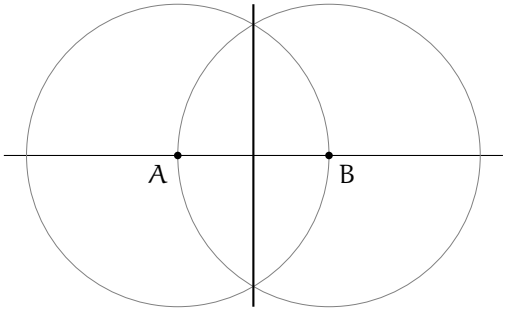
- $AB$ la retta passante per $A, B$;
- $C(A, B)$ la circonferenza di centro $A$ e passante per $B$.

## 5.2 COSTRUZIONI ELEMENTARI

**Proposizione 5.4 – Retta mediana**

Siano $A, B$ due punti costruibili. Allora possiamo costruire la mediana del segmento $AB$.

*Dimostrazione.* Prendiamo le circonferenze $C(A, B)$ e $C(B, A)$. Dai punti di intersezione delle due circonferenze possiamo costruire la mediana.

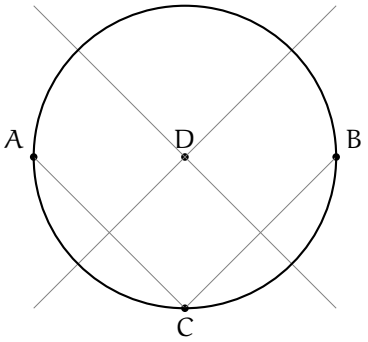



□

**Proposizione 5.5 – Cerchio per tre punti non allineati**

Siano $A, B$ e $C$ tre punti costruibili non allineati. Allora possiamo costruire la circonferenza passante per $A, B, C$.

*Dimostrazione.* Tramite la teorema 5.4 costruiamo le mediane di $AC$ e $BC$. La loro intersezione $D$ costituisce il centro della circonferenza cercata.

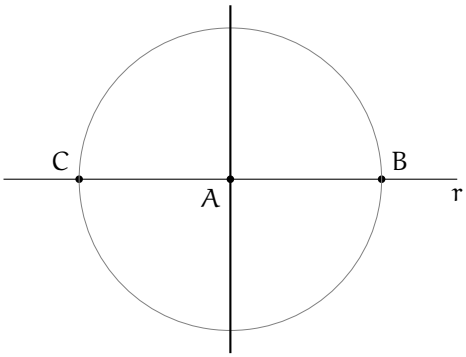



□

**Proposizione 5.6 – Perpendicolare passante per un punto sulla retta**

Sia $r$ una retta costruibile e sia $A$ un punto costruibile sulla retta data. Allora possiamo costruire la perpendicolare ad $r$ passante per $A$.

*Dimostrazione.* Sia B un altro punto sulla retta anch'esso costruibile, tale punto esiste sicuramente dal momento che possiamo costruire rette a partire da almeno due punti. Costruiamo la circonferenza $C(A, B)$ e chiamiamo C l'intersezione, distinta da B, di tale circonferenza con r. La mediana del segmento BC costituisce la perpendicolare cercata.

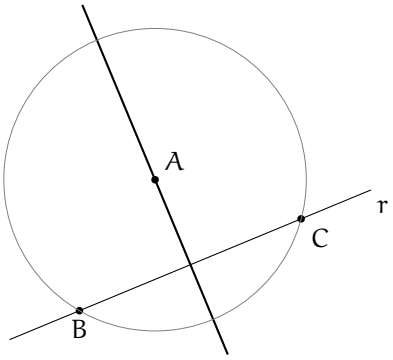



□

**Proposizione 5.7 – Perpendicolare passante per un punto fuori dalla retta**

Sia r una retta costruibile e sia A un punto costruibile fuori da r. Allora possiamo costruire la retta perpendicolare ad r passante per A.

*Dimostrazione.* Prendiamo B un punto costruibile su r e consideriamo $C(A, B)$. Se $C(A, B) \cap r = \{B\}$ allora la circonferenza è tangente alla retta. Per cui AB è la perpendicolare cercata. Supponiamo quindi che via sia un altro punto $C \neq B$ nell'intersezione $C(A, B) \cap r$. La mediana di BC è la perpendicolare cercata.



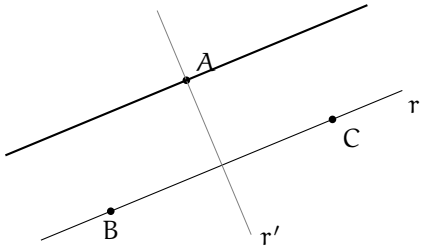

□

**Proposizione 5.8 – Parallela ad una retta**

Sia r una retta costruibile e sia A un punto costruibile fuori da r. Allora possiamo costruire la retta parallela ad r passante per A.

*Dimostrazione.* Per la teorema 5.7 possiamo costruire la perpendicolare $r'$ ad r passante per A. A questo punto sfruttiamo la teorema 5.6 per costruire la perpendicolare ad $r'$

passante ancora per A. Abbiamo così ottenuto la parallela cercata.

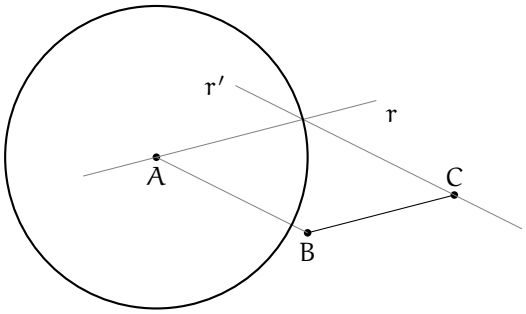



□

## Proposizione 5.9 – Circonferenza di dato raggio

Sia A un punto costruibile e sia BC un segmento costruibile. Allora possiamo costruire la circonferenza di centro A e raggio |BC|.

*Dimostrazione.* Per la teorema 5.8 possiamo costruire la parallela r a BC passante per A. Costruiamo la retta AB. Ancora per la teorema 5.8 costruiamo la parallela r′ ad AB passante per C. Intersecando r′ con r otteniamo un punto D a distanza |BC| da A.



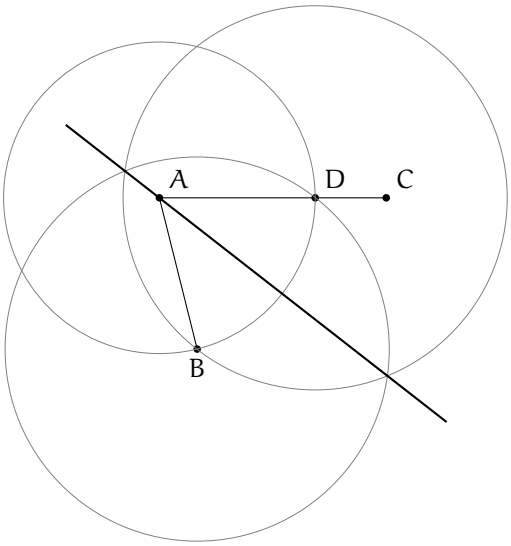

□

## Proposizione 5.10 – Bisezione di un angolo

Siano A, B, C punti costruibili. Allora possiamo dividere l'angolo $B\hat{A}C$ in due parti uguali.

*Dimostrazione.* Prendiamo la circonferenza C(A, B) e D il suo punto di intersezione con AC. Adesso prendiamo C(D, B) e C(B, D). La retta passante per le intersezioni delle due

circonferenze biseca l'angolo dato.




□

## 5.3 NUMERI COSTRUIBILI

**Definizione 5.11 – Numero reale costruibile**

Un numero reale $\alpha$ si dice *costruibile* se il punto $(\alpha, 0)$ è costruibile.

*Osservazione.* Più in generale è sufficiente richiedere che esista $y \in \mathbb{R}$ tale che il punto $(\alpha, y)$ sia costruibile.

**Definizione 5.12 – Numero complesso costruibile**

Un numero complesso $\alpha = x + iy$ si dice *costruibile* se il punto $(x, y)$ è costruibile.

**Definizione 5.13 – F-piano**

Sia $F$ un sottocampo di $\mathbb{R}$. Definiamo un $F$-piano come

$$F \times F \subset \mathbb{R} \times \mathbb{R}.$$

**Notazione.** Per un $\alpha \in F$ positivo, definiamo $\sqrt{\alpha}$ come la radice *positiva* di $\alpha$.

**Definizione 5.14 – F-retta**

Consideriamo un $F$-piano. Una $F$-retta è una retta in $\mathbb{R} \times \mathbb{R}$ passante per due punti dell'$F$-piano. Tali rette hanno equazione

$$ax + by + c = 0, \qquad \text{con } a, b, c \in F.$$

**Definizione 5.15 – F-circonferenza**

Consideriamo un F-piano. Una F-circonferenza è una circonferenza di $\mathbb{R}\times\mathbb{R}$ di centro un punto dell'F-piano e di raggio un elemento di F.

**Lemma 5.16.** Consideriamo un F-piano. Siano $r \neq r'$ due F-rette e $C \neq C'$ due F-circonferenze. Allora

1. $r \cap r'$ è vuoto oppure consiste di un solo F-punto.
2. $r \cap C$ è vuoto oppure consiste di uno o due $F[\sqrt{e}]$-punti, per qualche $e \in F$ positivo.
3. $C \cap C'$ è vuoto oppure consiste di uno o due $F[\sqrt{e}]$-punti, per qualche $e \in F$ positivo.

*Dimostrazione.* Segue da semplici considerazioni geometriche. □

**Lemma 5.17.** Siano $a, b \in \mathbb{R}$ costruibili, con $b \neq 0$. Allora

$$a+b, \qquad a-b, \qquad a\,b, \qquad \frac{a}{b}, \qquad \sqrt{a}$$

sono costruibili.

*Dimostrazione.* $a, b$ sono costruibili, quindi per definizione i punti $A = (a, 0), B = (b, 0)$ sono costruibili. Per costruire $a + b$ supponiamo che $b > a$, prendiamo quindi $C(B, A)$ e consideriamo la sua intersezione con la retta $AB$. Tale punto avrà coordinate $(a + b, 0)$. Analogamente si costruisce $a - b$.
Per costruire $a\,b$ consideriamo $O = (0, 0), A = (a, 0), B = (1, 0), C = (0, b)$ che sono tutti punti costruibili. Prendiamo $r$ la retta $BC$ e poi prendiamo la parallela ad $r$ passante per $A$. Chiamato $D$ l'intersezione della parallela con $OC$ ottengo due triangoli simili $OBC$ e $OAD$. In particolare

$$\frac{|OC|}{|OB|} = \frac{|OD|}{|OA|} \implies \frac{b}{1} = \frac{|OD|}{a} \implies |OD| = a\,b.$$

Analogamente si costruisce $a/b$.
Infine per costruire $\sqrt{a}$, poniamo $A = (0, 0)$ e $B = (a, 0)$, così da avere $|AB| = a$. Costruiamo $C$ a sinistra di $A$ tale che $|CA| = 1$. Prendiamo il punto medio $M$ di $CB$ e quindi costruiamo la circonferenza ci centro $M$ e passante per $B$ e $C$. Prendiamo la perpendicolare per $A$ ad $AB$: Chiamato $D$ l'intersezione superiore della perpendicolare con la circonferenza, otteniamo due triangoli simili $ACD$ e $ADB$. In particolare

$$\frac{|AD|}{|AC|} = \frac{|AB|}{|AD|} \implies |AD|^2 = |AB| = a \implies |AD| = \sqrt{a}.$$

□

**Teorema 5.18 – Caratterizzazione dei reali costruibili**

Un numero reale $\alpha$ è costruibile se e soltanto se è contenuto in un sottocampo di $\mathbb{R}$ della forma

$$\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_n}], \qquad \text{con } a_i \in \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}].$$

*Dimostrazione.* Segue dai due lemmi precedenti. □

**Esempio** (Duplicazione del cubo)**.** Duplicare un cubo equivale a costruire una radice di $X^3 - 2$. D'altronde tale radice genere un'estensione che contiene numeri non costruibili

**Esempio** (Trisezione di un angolo)**.** Supponiamo di voler trisecare un angolo $3\alpha$. Tramite semplici manipolazioni algebriche otteniamo

$$\cos(3\alpha) = 4\cos^3\alpha - 3\cos\sigma.$$

Posto $\cos\alpha = X$ otteniamo

$$4X^3 - 3X - \cos(3\alpha) = 0$$

che in generale determina un'estensione cubica i cui elementi non sono tutti costruibili.

**Esempio** (Quadratura del cerchio)**.** Per quadrare il cerchio bisognerebbe costruire $\sqrt{\pi}$ che è un elemento trascendente e pertanto non costruibile.

# INDICE ANALITICO