Algebra IV I1

24 settembre 2021

wikitolearn
collaborative textbooks

This book is the result of a collaborative effort of a community of people like you, who believe that knowledge only grows if shared.
We are waiting for you!

Get in touch with the rest of the team by visiting http://join.wikitolearn.org

Indice

Capitolo 1

Richiami sui campi

1.1 Ripasso di teoria dei campi

1.1.1 Estensioni di campi

Definizione 1.1

Sia M un campo, e K un sottoanello di M , che è a sua volta un campo. Diciamo che $M \supseteq K$ è un'*estensione di campi* (si scrive anche M/K). Il campo M può essere visto come spazio vettoriale su K . La dimensione di M come spazio vettoriale su K si dice *grado dell'estensione*, e si indica con $|M : K|$.

Teorema 1.1 (teorema della torre)

Supponiamo di avere K, L, M campi con $K \subseteq L \subseteq M$, allora $|M : K|$ è finito se e solo se sono finiti $|M : L|$ e $|L : K|$. In tal caso: $|M : K| = |M : L| * |L : K|$.

Dimostrazione

$1 \longrightarrow 2$: Supponiamo che $|M : K|$ sia finito, allora siccome $L \subseteq M$, anche $|L : K|$ è finito (infatti L e' un sottospazio di M). Sia inoltre $\{\gamma_1, \ldots, \gamma_t\}$ una base per M su K .

Allora ogni $\alpha \in M$ si può scrivere come

$$\sum_i k_i \gamma_i$$

per certi $k_i \in K \subseteq L$, quindi $\{\gamma_i\}_{i=1}^t$ è un insieme finito di generatori per M su L , e anche $|M : L|$ è finito.

$2 \longrightarrow 1$: Viceversa, siano $n = |M : L| < \infty$ e $m = |L : K| < \infty$, e siano $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_m\}$ basi rispettivamente di M su L e di L su K . **Affermo che** $\mathcal{B} = \{\alpha_i \beta_j | i = 1, \ldots, n,\ j = 1 \ldots, m\}$ **è una base per** M **su** K , infatti:

1. $\mathcal{B}$ **genera** M . Prendo $\alpha \in M$, allora siccome gli $\{\alpha_i\}_{i=1}^n$ sono una base

per M su L posso scrivere

$$\alpha = \sum_i l_i \alpha_i$$

per certi $l_i \in L$. Inoltre i $\{\beta_i\}_{i=1}^m$ sono una base di L su K , quindi per $i = 1, \ldots, n$ posso scrivere

$$l_i = \sum_j k_{ij} \beta_j$$

e sostituendo nell'espressione di α :

$$\alpha = \sum_i \sum_j k_{ij} \beta_j \alpha_i,$$

cioè $\mathcal{B}$ genera M .

2. **Gli elementi di $\mathcal{B}$ sono linearmente indipendenti**, infatti supponiamo per assurdo che non lo siano, allora per certi $\bar{k}_{ij} \in K$ si ha

$$\sum_{i,j} \bar{k}_{ij} \alpha_i \beta_j = 0$$

$$\longrightarrow \sum_i (\sum_j \bar{k}_{ij} \beta_j) \alpha_i = 0$$

Posto $\bar{l}_i = \sum_j \bar{k}_{ij} \beta_j$ la condizione si riscrive come

$$\sum_i \bar{l}_i \alpha_i = 0$$

e siccome gli $\{\alpha_i\}_{i=1}^m$ sono una base per M su L , si deve avere $\bar{l}_i = 0, \ \forall i = 1, \ldots, n$, e considerando l'espressione degli $\bar{l}_i$, si ha

$$\sum_j \bar{k}_{ij} \beta_j = 0$$

Siccome i $\{\beta_i\}_{i=1}^m$ sono una base per L su K , l'unica possibilità per cui la condizione sia verificata è che $\bar{k}_{ij} = 0, \ \forall i, \forall j$, cioè segue l'indipendenza lineare degli elementi di $\mathcal{B}$.

1.1.2 Estensioni semplici

Sia $E \supseteq F$ un'estensione di campi, e sia S un sottoinsieme di E . Allora indichiamo con $F[S]$ il minimo sottoanello di E contenente S e F ,

cioè $F[S] := \bigcap R$ al variare di R sottoanello di E tale che $F, S \subset R$ ovvero

$$F[S] := \bigcap_{R \, sottoanello \, di \, E \, con \, F, S \subseteq R} R.$$

Indichiamo invece con $F(S)$ il minimo sottocampo di E contenente S, F , cioè $F(S) := \bigcap K$, al variare di K sottocampo di E tale che $F, S \subset K$,

ovvero

$$F(S) := \bigcap_{K \text{ sottocampo di } E, \text{ con } F,S\subseteq K} K.$$

In particolare, quando $S = \{\alpha\}$, il minimo sottoanello e sottocampo si indicano rispettivamente con $F[\alpha], F(\alpha)$.

Più in generale, dato $S = \{\alpha_1, \ldots, \alpha_n\}$, $\alpha_i \in E$, posso scrivere $F[\alpha_1, \ldots, \alpha_n]$ per indicare $F[S]$ e $F(\alpha_1, \ldots, \alpha_n)$ per indicare $F(S)$, eliminando le parentesi graffe che racchiudono il contenuto degli insiemi.

1.1.3 Elementi algebrici e trascendenti

Sia $\alpha \in E$, e' facile convincersi che

$$F[\alpha] = \{f(\alpha) : f(x) \in F[x]\}$$
$$F(\alpha) = \{f(\alpha)g(\alpha)^{-1} : f(x), g(x) \in F[x],\ g(\alpha) \neq 0\}$$

Per caratterizzare ulteriormente l'anello $F[\alpha]$ e il campo $F(\alpha)$ devo distinguere due casi:

Definizione 1.2

1. α si dice *algebrico* su F se esiste un polinomio non nullo in $F[x]$ che ammette α come radice.
2. α si dice *trascendente* su F altrimenti, ovvero se l'unico polinomio di $F[x]$ che si annulla in α è il polinomio nullo.

Definizione 1.3

Indico con ϕ_α l'*omomorfismo di valutazione* : $F[x] \to E$ tale che $g(x) \mapsto g(\alpha)$, così l'immagine di ϕ_α è $F[\alpha]$ (x una indeterminata su F).

CASO 1: se α è trascendente su F , $\ker \phi_\alpha = \{0\}$, allora l'omomorfismo di valutazione è iniettivo e $F[\alpha] \cong F[x]$. Inoltre ϕ_α si solleva (in modo unico) a un omomorfismo iniettivo, $\bar{\phi}_\alpha : F(x) \to E$, tale che $\frac{f(x)}{g(x)} \mapsto f(\alpha)g(\alpha)^{-1}$, la cui immagine coincide con $F(\alpha)$. Abbiamo quindi $F(\alpha) \cong F(x)$ dove $F(x)$ è il campo delle funzioni razionali su F .

CASO 2: se α è algebrico su F , esiste in $F[x]$ un polinomio monico, di grado minimo tra i polinomi non nulli in $F[x]$ che ammettono α come radice. Dalla definizione segue subito che è unico e irriducibile in $F[x]$, e viene chiamato il *polinomio minimo di* α e indicato con $m(x)$. Osservo che $\ker \phi_\alpha$ coincide con l'ideale generato da $m(x)$, e quindi $F[\alpha] \cong \frac{F[x]}{(m(x))}$. Il polinomio $m(x)$ è irriducibile e quindi $(m(x))$ è massimale in $F[x]$, allora $\frac{F[x]}{(m(x))}$ è un campo, e quindi deduco che $F[\alpha] = F(\alpha)$.

1.2 Campo di spezzamento di un polinomio

1.2.1 Definizione

Definizione 1.4

Sia K un campo, e $f(x) \in K[x]$ un polinomio di grado ≥ 1 . Un *campo* $M \supseteq K$ sidice *di spezzamento* per il polinomio $f(x)$ sul campo K se:

1. $f(x)$ si spezza su M in fattori lineari, cioè esistono $\alpha_1, \ldots, \alpha_n \in M$ non necessariamente distinti ed esiste $c \in M$ tale che
$$f(x) = c(x - \alpha_1) * (x - \alpha_2) * \cdots * (x - \alpha_n).$$
2. su nessun sottocampo proprio di M $f(x)$ si spezza in fattori lineari, o equivalentemente M è il più piccolo campo che contiene K e le radici di $f(x)$.

1.2.2 Esistenza del campo di spezzamento

Proposizione 1.1

Sia K un campo e $f(x) \in K[x]$ un polinomio irriducibile di grado n . Allora esiste un campo M che soddisfa queste tre proprietà:

1. $M \supseteq K$;
2. $|M : K| = n$;
3. $f(x)$ ammette una radice in M .

Dimostrazione

$f(x)$ è irriducibile su K , quindi $(f(x))$ è massimale in $K[x]$, e $M := \frac{K[x]}{(f(x))}$ è un campo. Chiamo π la proiezione canonica $\pi \colon K[x] \to M$ definita da $\pi(h(x)) = h(x) + (f(x))$, per $h(x) \in K[x]$.
Sia

$$\bar{K} = \pi(K) = \{a + (f(x)),\, a \in K\}.$$

Allora

1. la restrizione di π a K , $\pi_{|_K} \colon K \to \bar{K}$ è iniettiva, quindi $\bar{K} \cong K$. Inoltre $M \supseteq \bar{K}$ .Identificando gli elementi di K con gli elementi di $\bar{K}$, segue che $M \supseteq K$ e **è verificata la condizione I)**.
2. gli elementi di M si scrivono in modo unico nella forma $g(x) + (f(x))$, al variare di $g(x) \in K[x]$ tali che gr(g(x)) < gr(f(x)) .Gli elementi $1 + (f(x))$, $x + (f(x))$, $x^{n-1} + (f(x))$ costituiscono una base per M su K , e quindi $|M : K| = n$, ed **è verificata la condizione 2**.

3. pongo $\alpha = x + (f(x))$, e considero $\pi\colon K[x] \to \frac{K[x]}{(f(x))}$. Preso un generico polinomio $p(x) = b_0 + b_1x + \cdots + b_nx^n$, per le proprietà di omomorfismo segue che

$$p(x)^\pi = b_0^\pi + b_1^\pi x^\pi + \cdots + b_n^\pi (x^n)^\pi = b_0 + b_1 x^\pi + \cdots + b_n (x^\pi)^n$$

e siccome $\pi(x) = \alpha$:

$$= b_0 + b_1\alpha + \cdots + b_n\alpha^n = p(\alpha)$$

In particolare, $0 = f(x)^\pi = f(\alpha)$, e quindi $f(x)$ ammette la radice α e **è verificata la condizione III)**.

Proposizione 1.2

Sia K un campo, $f(x) \in K[x]$ un polinomio, di grado $n \geq 1$. Allora esiste un campo M che soddisfa queste tre proprietà:

1. $M \supseteq K$
2. $|M : K| \leq n!$
3. $f(x)$ ammette tutte le sue radici in M .

Dimostrazione

La dimostrazione è per induzione su n .

Se $n = 1$ o se $f(x)$ si spezza in fattori lineari su K , basta prendere $M = K$. Allora posso supporre $n > 1$, e che esista un fattore irriducibile $g(x)$ di $f(x)$ in $K[x]$. Così gr(g(x)) < n . Applicando la proposizione precedente al polinomio $g(x)$ che è irriducibile, esiste un campo L tale che $L \supset K$, $|L : K| = \text{gr(g(x))} \leq \text{n}$, e tale che $g(x)$ ammette una radice $\alpha \in M$.

α è anche radice di $f(x)$, quindi in $L[x]$ posso scrivere

$$f(x) = (x - \alpha) * h(x)$$

con $h(x)$ polinomio di grado $n - 1$.

Allora per l'ipotesi induttiva esiste un campo M che estende L , con $|M : L| \leq (n-1)!$ e tale che $h(x)$ ammette tutte le sue radici in M . Ma le radici di $f(x)$ sono tutte e sole α e le radici di $h(x)$, e quindi sono tutte contenute in M , inoltre per il teorema della torre

$$|M : K| = |M : L| * |L : K| \leq (n-1)! * n \leq n!$$

quindi M soddisfa le tre condizioni richieste.

1.2.3 Unicità di un campo di spezzamento

Osservazione 1.1

Supponiamo di avere due campi, $F, \bar{F}$, e di avere un isomorfismo $\sigma : F \to \bar{F}$. Allora σ induce un isomorfismo di anelli, che chiamo ancora σ , $\sigma : F[x] \to \bar{F}[x]$ tale che $\sum_i a_i x^i \mapsto \sum_i a_i^\sigma x^i$.

Proposizione 1.3

Siano $F, \bar{F}$ due campi, $\sigma : F \to \bar{F}$ un isomorfismo. Considero un polinomio $f(x)$ monico e irriducibile su F , e pongo $\bar{f}(x) = f(x)^\sigma$.

Suppongo di avere due estensioni $K_1 \supseteq F$ e $K_2 \supseteq \bar{F}$, e siano $\alpha_1 \in K_1$ e $\alpha_2 \in K_2$ radici di $f(x)$ e di $\bar{f}(x)$ rispettivamente. Allora esiste un unico isomorfismo $\phi : F[\alpha_1] \to \bar{F}[\alpha_2]$, tale che $\alpha_1 \mapsto \alpha_2$, e tale che ristretto a F sia uguale a σ .

Dimostrazione

Osserviamo che α_1 è algebrico su F , quindi l'anello $F[\alpha_1] = F(\alpha_1) \cong \frac{F[x]}{(f(x))}$ e chiamo g_1 l'isomorfismo dato dall'omomorfismo di valutazione : $\frac{F[x]}{(f(x))} \to F[\alpha_1]$, e vale un ragionamento analogo per α_2 e quindi esiste un isomorfismo $g_2 \colon \frac{\bar{F}[x]}{(\bar{f}(x))} \to \bar{F}[\alpha_2]$.

Considero il seguente diagramma:

$$\begin{array}{ccc} F[x] & \to^\sigma & \bar{F}[x] \\ \downarrow^{\pi_f} & & \downarrow^{\pi_{\bar{f}}} \\ \frac{F[x]}{(f(x))} & & \frac{\bar{F}[x]}{(\bar{f}(x))} \\ \downarrow^{g_1} & & \downarrow^{g_2} \\ F[\alpha_1] & & \bar{F}[\alpha_2] \end{array}$$

Considero l'applicazione $\psi := \pi_{\bar{f}} \circ \sigma : F[x] \to \frac{\bar{F}[x]}{(\bar{f}(x))}$. ψ è un omomorfismo suriettivo, inoltre $f(x) \in \ker \psi$ perché

$$\psi(f) = \pi_{\bar{f}} \circ \sigma(f) = \pi_{\bar{f}}(\bar{f}) = 0$$

allora $(f(x)) \subset \ker \psi$, e siccome l'ideale $(f(x))$ è massimale in $F[x]$, allora $(f(x)) = \ker \psi$ perché ψ non è identicamente nullo, infatti ad esempio

$$\psi(1) = \pi_{\bar{f}} \circ \sigma(1) = \bar{1} + (\bar{f}(x)) = 1 + (\bar{f}(x))$$

Quindi ho un isomorfismo $\eta : \frac{F[x]}{(f(x))} \to \frac{\bar{F}[x]}{(\bar{f}(x))}$, tale che $h(x) + (f(x)) \mapsto \bar{h}(x) + (\bar{f}(x))$, dove $\bar{h}(x) = h(x)^\sigma$.

Il diagramma considerato prima si riduce a

$$\begin{array}{ccc} \frac{F[x]}{(f(x))} & \to^{\eta} & \frac{\bar{F}[x]}{(\bar{f}(x))} \\ \downarrow^{g_1} & & \downarrow^{g_2} \\ F(\alpha_1) & & \bar{F}(\alpha_2) \end{array}$$

Allora posso considerare $\phi := g_2 \circ \eta \circ g_1^{-1} \colon F(\alpha_1) \to \bar{F}(\alpha_2)$. Inoltre

$$\phi(\alpha_1) = g_2 \circ \eta \circ g_1^{-1}(\alpha_1) = g_2 \circ \eta(x + (f(x))) = g_2(x + (\bar{f}(x))) = \alpha_2$$

Inoltre $\phi = \sigma$ se restringo il dominio di ϕ a F . Infati, dato $a \in F$, segue che

$$\phi(a) = g_2 \circ \eta \circ g_1^{-1}(a) = g_2 \circ \eta(a + (f(x))) = g_2(\bar{a} + (\bar{f}(x))) = \bar{a} = \alpha^s.$$

L'unicità di ϕ segue dal fatto che è determinato univocamente il modo in cui agisce su α_1 e su F .

Proposizione 1.4

Dati due campi $F, \bar{F}$ e $\sigma : F \to \bar{F}$ un isomorfismo, considero $f(x) \in F[x]$, monico di grado ≥ 1 , e chiamo $\bar{f}(x) = f(x)^{\sigma}$.

Supponiamo che E_1 sia un campo di spezzamento per il polinomio $f(x)$ su F , ed E_2 un campo di spezzamento per $\bar{f}(x)$ su $\bar{F}$. Allora esiste un isomorfismo $\phi : E_1 \to E_2$ che ristretto a F coincide con σ .

Nel caso particolare in cui $F = \bar{F}$ e σ è l'identità si ottiene che il campo di spezzamento di un polinomio $f(x)$ su F è unico a meno di isomorfismi che sono la identita' su

K .

Dimostrazione

La dimostrazione è per induzione sul grado di E_1 su F . Se $|E_1 : F| = 1$, il teorema è vero, perché $E_1 = F$.

Notiamo anche che $E_1 = F$ se $f(x)$ ha tutte le sue radici in F .

In caso contrario, possiamo considerare un fattore irriducibile $g(x)$ di $f(x)$, con gr(g(x)) > 1 .

Chiamo $\bar{g}(x) = g(x)^{\sigma}$. Siano α_1 una radice di $g(x)$ in E_1 e α_2 una radice di $\bar{g}(x)$ in E_2 . Allora per la proposizione precedente, esiste un isomorfismo $\psi \colon F[\alpha_1] \to \bar{F}[\alpha_2]$ tale che $\psi = \sigma$ se ristretta a F .

E_1 è campo di spezzamento per $f(x)$ su F , e quindi è anche campo di spezzamento per $f(x)$ su $F[\alpha_1] = F(\alpha_1)$. Analogamente E_2 è campo di spezzamento per $\bar{f}(x)$ su $\bar{F}$, e dunque anche campo di spezzamento per $\bar{f}(x)$ su $F(\alpha_2)$. Inoltre, $|E_1 : F(\alpha_1)| < |E_1 : F| = n$, e quindi posso applicare l'ipotesi induttiva.

1.3 Lemma di Zorn e relative applicazioni

Definizione 1.5

Sia $(S \leq)$ un insieme parzialmente ordinato, allora una *catena* T è un sottoinsieme di S che sia totalmente ordinato, cioè dati $x, y \in T$, $x \leq y$ o $y \leq x$.

Definizione 1.6

Un *maggiorante* per T in S è un elemento $s \in S$ tale che per ogni $t \in T$, $t \leq s$.

Lemma di Zorn: Sia $(\Sigma, \leq)$ un insieme non vuoto parzialmente ordinato. Se ogni catena in Σ ammette un maggiorante in Σ allora Σ ha almeno un elemento massimale.

1.3.1 Applicazione 1 esistenza di un ideale massimale

Usando il lemma di Zorn possiamo provare il seguente

Lemma 1.1

Sia A un anello non banale (commutativo e unitario), allora A ha almeno un ideale massimale.

Dimostrazione

Prendo l'insieme Σ di tutti gli ideali propri I di A cioè $I \neq (1)$. Per poter applicare il lemma di Zorn, **voglio mostrare che ogni catena in questo insieme ha un maggiorante**.

Osservo che Σ è non vuoto perché contiene l'ideale banale ridotto al solo 0.

Ordiniamo Σ rispetto all'inclusione, cioè stabiliamo che dati due elementi $I, J \in \Sigma$, $I \leq J$ se $I \subset J$.

Sia $\{I_\alpha\}_{\alpha \in \lambda}$ una catena in Σ . Chiamo $I = \bigcup_\alpha I_\alpha$ e **mostro che I è un elemento di Σ** :

- I è un ideale dell'anello, mostro ad esempio la chiusura rispetto alla differenza: prendo $x, y \in I$, allora esisteranno indici α, β tali che $x \in I_\alpha, y \in I_\beta$. Siccome sto considerando una catena, $I_\alpha \subset I_\beta$ oppure $I_\beta \subset I_\alpha$, diciamo che $I_\alpha \subset I_\beta$. Allora $x, y \in I_\beta$, e siccome I_β è un ideale, è chiuso rispetto alla differenza e $x - y \in I_\beta$, quindi $x - y \in I$.
- I è un ideale proprio, infatti, poiché $1 \notin I_\alpha \forall \alpha$, 1 non può stare in I .

Di conseguenza I è un maggiorante per la catena considerata, e posso applicare il lemma di Zorn, quindi Σ ha un elemento massimale.

Osservazione 1.2

Non si può ripetere lo stesso ragionamento per dimostrare che ogni gruppo ha un sottogruppo massimale (il ragionamento precedente non vale perché, mentre negli anelli esistono due elementi "speciali", 0 e 1, nei gruppi se ne ha solo uno).

Lemma 1.2 (generalizzazione)

Sia $A \neq 0$ un anello (commutativo e unitario), e J un ideale di A con J proprio, allora esiste un ideale massimale di A che contiene J .

Dimostrazione

Per la dimostrazione basta ripetere il procedimento precedente, considerando l'insieme Σ degli ideali propri I di A tali che $J \subset I$ e $I \neq A$.

1.3.2 Applicazione 2 basi in spazi vettoriali

Utilizzando il lemma di Zorn si mostra che **ogni spazio vettoriale ammette una base**.

Lemma 1.3

Sia $V \neq \{0\}$ uno spazio vettoriale sul campo K , sia Γ un insieme di generatori per V su K e $S \subset \Gamma$ un insieme linearmente indipendente. Allora esiste una base $\mathcal{B}$ di V con $S \subseteq \mathcal{B} \subseteq \Gamma$.

Dimostrazione

Sia

$$\Sigma = \{T \, t.c. \, S \subseteq T \subseteq \Gamma, \, T \, linearmente \, indipendente\}$$

Si ha che $\Sigma \neq \emptyset$ perché contiene almeno S .

Considero poi una catena in Σ , $\{T_\alpha\}_{\alpha \in \Lambda}$. Chiamo $T = \bigcup_\alpha T_\alpha$. Allora $S \subset T$ perché $S \subset T_\alpha$, inoltre T è linearmente indipendente, quindi $T \in \Sigma$ ed è un maggiorante per la catena.

Per il lemma di Zorn, Σ ammette almeno un elemento massimale $\mathcal{B}$, e sia W il sottospazio generato da $\mathcal{B}$ sopra K . **Voglio mostrare che** $V = W$ e quindi che $\mathcal{B}$ è una base.

Supponiamo per assurdo che $W \neq V$, allora esisterà $x \in \Gamma$ tale che $x \notin W$.

Considero $\mathcal{B} \cup \{x\}$, **voglio mostrare che** $\mathcal{B} \cup \{x\} \in \Sigma$, infatti se questo avviene ho una contraddizione perché per i punti precedenti, $\mathcal{B}$ è massimale.

Mostro che $\mathcal{B} \cup \{x\}$ è linearmente indipendente. Suppongo di avere una combinazione lineare

$$\sum_{y \in \mathcal{B}} a_y y + bx = 0, \text{ formula}*$$

con $b, a_y \in K$. Allora necessariamente $b = 0$, infatti, se così non fosse, si avrebbe

$$x = -\sum_{y \in \mathcal{B}} b^{-1} a_y y$$

cioè si avrebbe $x \in W$, contro l'ipotesi.

Quindi la formula $*$ si riscrive come

$$\sum_{y\in\mathcal{B}} a_y y = 0$$

ma siccome gli elementi di $\mathcal{B}$ sono linearmente indipendenti, necessariamente $a_y = 0 \forall y \in \mathcal{B}$. Questo mostra che $\mathcal{B}\cup\{x\}$ è un elemento di Σ contro la massimalità di $\mathcal{B}$, rimane allora provato che $V = W$.

1.4 Chiusura algebrica di un campo

1.4.1 Osservazioni introduttive

Osservazione 1.3

Sia K un campo, e siano $\alpha_1, \ldots, \alpha_n$ elementi algebrici su K . Posso quindi considerare l'estensione $K(\alpha_1, \ldots, \alpha_n) \supseteq K$, allora quest'estensione ha grado finito e quindi è algebrica.

Dimostrazione

Ho una successione di estensioni semplici di grado finito: $M = K(\alpha_1, \ldots, \alpha_n) \supseteq K(\alpha_1, \ldots, \alpha_{n-1}) \supseteq \cdots \supseteq K(\alpha_1) \supseteq K$, e applicando il teorema del grado anche $|M : K|$ è finito.

Osservazione 1.4 (transitività delle estensioni algebriche)

Siano $K \subseteq L \subseteq M$ estensioni di campi, e suppongo che $M \supseteq L$ e $L \supseteq K$ siano algebriche. Allora anche $M \supseteq K$ è algebrica.

Dimostrazione

Prendo $\alpha \in M$, allora α è algebrico su L e posso considerare il polinomio minimo $f(x)$ di α in $L[x]$, esso è della forma:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_i \in L$$

Essendo $L \supseteq K$ algebrica, ciascun a_i è algebrico su K . Considero $K_0 = K(a_0, a_1, \ldots, a_{n-1})$ che per l'osservazione precedente ha grado finito, e considero la catena di estensioni

$K_0(\alpha) \supseteq K_0 \supseteq K$.

$K_0(\alpha)$ come estensione di K_0 è di grado finito, e lo stesso vale per $K_0 \supseteq K$, allora per il teorema della torre $K_0(\alpha) \supseteq K$ è di grado finito e quindi è algebrica. In particolare α è algebrico su K .

Osservazione 1.5

Vale anche il viceversa: se $M \supseteq K$ è algebrica, allora anche $M \supseteq L$ e $L \supseteq K$ sono algebriche.

Dimostrazione

Sia $\alpha \in M$, allora siccome $M \supseteq K$ è algebrica, esiste $f(x) \in K[x]$ tale che $f(\alpha) = 0$. $f(x)$ può essere considerato anche come polinomio a coefficienti in L , e quindi $M \supseteq L$ è algebrica. Inoltre, se ogni $\alpha \in M$ è algebrico su K , a maggior ragione ogni $\alpha \in L \subseteq M$ è algebrico su K , cioè $L \supseteq K$ è algebrica.

1.4.2 Chiusura algebrica e campo algebricamente chiuso

Definizione 1.7

Un campo K si dice *algebricamente chiuso* se vale una delle seguenti condizioni equivalenti tra loro:

1. ogni polinomio $f(x) \in K[x]$ non costante ammette almeno una radice in K .
2. ogni polinomio $f(x) \in K[x]$ non costante ammette tutte le sue radici in K .
3. ogni polinomio $f(x) \in K[x]$ si spezza in fattori lineari in $K[x]$.
4. i soli polinomi irriducibili in $K[x]$ sono i polinomi di primo grado.
5. K non ammette estensioni algebriche proprie.

1.4.3 Esistenza di una chiusura algebrica

Definizione 1.8

Dato un campo K , un campo $\bar{K} \supset K$ si dice una *chiusura algebrica* di K se

1. $\bar{K}$ è algebricamente chiuso
2. $\bar{K} \supseteq K$ è un'estensione algebrica.

Teorema 1.2

Sia K un campo, allora esiste un campo L che estende K , con L algebricamente chiuso.

Dimostrazione

Considero la famiglia $\mathcal{F}$ di tutti i polinomi $f(x) \in K[x]$ di grado ≥ 1 . Considero un insieme di indeterminate $\mathcal{X}$ indicizzate sugli elementi della famiglia $\mathcal{F}$, cioè

$$\mathcal{X} = \{x_f,\ f \in \mathcal{F}\}$$

e considero l'anello dei polinomi $K[\mathcal{X}]$.

(Nota sugli anelli di polinomi in infinite indeterminate: sia $Y = \{y_i\}_{i\geq 1}$ un insieme di indeterminate, allora $K[Y] = \{f(y_{t_1}, y_{t_2}, \ldots, y_{t_r}) : r \geq 1\}$ cioe' l'anello dei polinomi $K[Y]$ contiene polinomi in un numero finito ma arbitrario di variabili di Y).

Sia I l'ideale generato dagli elementi $f(x_f)$ al variare di $f \in \mathcal{F}$. **Affermo che I è un ideale proprio dell'anello** $K[\mathcal{X}]$. Per assurdo, suppongo che $1 \in I$, allora

$$1 = g_1 * f_1(x_1) + g_2 * f_2(x_2) + \cdots + g_n * f_n(x_n), \text{formula}\star$$

dove $x_i = x_{f_i}$, e dove $g_1, \ldots, g_n$ sono polinomi in $K[\mathcal{X}]$, con

$$g_i = g_i(x_1, x_2, \ldots, x_M) \quad (M \geq n)$$

Considero un'estensione finita $K_1 \supseteq K$ in cui ciascun polinomio f_i ammette una radice α_i .

L'uguaglianza $\star$ può essere considerata in $K_1[\mathcal{X}]$, e sostituendo x_1 con α_1 , x_2 con α_2 , ... , x_n con α_n e x_i con 0 per $i > n$ nella formula $\star$, ottengo che $1 = 0$, assurdo.

Allora I è un ideale proprio, e quindi esiste in $K[\mathcal{X}]$ un ideale massimale M che contiene I per la conseguenza del lemma di Zorn.

Pongo $L_1 = \frac{K[\mathcal{X}]}{M}$, siccome M è un ideale massimale, L_1 è un campo che estende K . Inoltre ogni polinomio non costante a coefficienti in K ammette una radice in L_1 (per lemma sull'esistenza dei campi di spezzamento).

Itero il procedimento e ottengo una catena di estensioni: $L_0 = K \subset L_1 \subset L_2 \subseteq \cdots \subseteq L_{n-1} \subseteq L_n \subseteq \ldots$.

Chiamo $L = \bigcup_{k\geq 0} L_k$ e **affermo che L è un campo**: infatti, dati $\alpha, \beta \in L$, esistono indici h, k tali che $\alpha \in L_k, \beta \in L_h$. Supponiamo $L_k \subseteq L_h$, allora $\alpha, \beta \in L_h$, L_h è un campo, allora $\alpha + \beta \in L_h$ quindi $\alpha + \beta \in L$. Analogamente $\alpha\beta$ e $\alpha\beta^{-1}$ appartengono a L .

Sappiamo inoltre che $K \subseteq L$, e **mostriamo che L è algebricamente chiuso**.

Considero f un polinomio a coefficienti in L , allora f ha al più un numero finito di coefficienti non nulli. Di conseguenza esiste un indice n tale che $f \in L_n[x]$. Per costruzione dato un polinomio non costante a coefficienti in L_n , esso ammette una radice in L_{n+1} , allora anche $f(x)$ ammette una radice in $L_{n+1} \subseteq L$, quindi L è algebricamente chiuso.

Possiamo quindi concludere con il seguente teorema:

Teorema 1.3

Sia K un campo, allora esiste una chiusura algebrica di K .

Dimostrazione

Per il teorema precedente esiste un campo $L \supseteq K$ che è algebricamente chiuso. Allora considero

$$\bar{K} = \{\alpha \in L \, t.c. \, \alpha \, algebrico \, su \, K\}$$

Mostro che $\bar{K}$ è un campo: siano $\alpha, \beta \in \bar{K}$, allora α è algebrico su K , quindi $|K(\alpha) : K| < \infty$, inoltre β è algebrico su K ,

quindi anche su $K(\alpha)$ allora $|K(\alpha, \beta) : K(\alpha)| < \infty$. Dal teorema della torre segue che l'estensione $K(\alpha, \beta) \supseteq K$ è di grado finito, in quanto $|K(\alpha, \beta) : K| = |K(\alpha, \beta) : K(\alpha)| * |K(\alpha) : K| < \infty$, ed essendo di grado finito è algebrica. Gli elementi $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ sono contenuti in $K(\alpha, \beta)$, e quindi sono algebrici su K , quindi per definizione stanno in $\bar{K}$ che è un campo.

Inoltre, **$\bar{K}$ è un'estensione algebrica di K** , infatti

$$\bar{K} = \{\alpha \in L \, t.c. \, \alpha \, algebrico \, su \, K\}$$

Rimane da mostrare che **$\bar{K}$ è algebricamente chiuso**. Considero un polinomio non costante a coefficienti in $\bar{K}$, con gr(f(x)) ≥ 1 .

Siccome $\bar{K} \subseteq L$, f ha coefficienti in L , ma L è algebricamente chiuso, quindi esiste una radice β di $f(x)$ in L , cioè $f(\beta) = 0$.

Ora considero la catena di estensioni $\bar{K}(\beta) \supseteq \bar{K} \supseteq K$, allora $\bar{K}$ come estensione di K è algebrica per il punto precedente, e $\bar{K}(\beta)$ come estensione di $\bar{K}$ è algebrica perché β è radice di un polinomio a coefficienti in $\bar{K}$. Per la transitività delle estensioni algebriche,

$\bar{K}(\beta) \supseteq K$ è algebrica, quindi β è algebrico su K , e quindi sta in $\bar{K}$, che è algebricamente chiuso.

Esempio 1.1

Si può considerare ad esempio il caso in cui $K = \mathbb{Q}$, $L = \mathbb{C}$ e

$$\bar{K} = \{\alpha \in \mathbb{C} \, t.c. \, \alpha \, algebrico \, su \, \mathbb{Q}\}.$$

Si può osservare che la chiusura algebrica dei razionali ha grado infinito: supponiamo per assurdo che $|\bar{K} : \mathbb{Q}| = m < \infty$, allora ogni elemento di $\bar{K}$ dovrebbe avere polinomio minimo di grado $\leq m$. Se p è primo e $n \geq 1$, l'elemento $\sqrt[n]{p}$ è radice del polinomio $x^n - p$, che è un polinomio a coefficienti razionali, monico e irriducibile per il criterio di Eisenstein. Quindi $\sqrt[n]{p}$ è algebrico su $\mathbb{Q}$ (pertanto e' un elemento di $\bar{K}$) con polinomio minimo (su $\mathbb{Q}$) $x^n - p$. Dall'arbitrarietà di n si ha l'assurdo.

1.5 (Non) unicità della chiusura algebrica

Due chiusure algebriche in un campo K sono isomorfe secondo un isomorfismo che è l'identità su K , sebbene in modo non canonico perché ci sono più isomorfismi tra due chiusure algebriche.

Consideriamo un contesto più generale: sia K un campo, L un campo algebricamente chiuso, e sia $E \supseteq K$ un'estensione di campi con E algebrico su K . Sia $\sigma : K \to L$ un omomorfismo (iniettivo), mostriamo che σ si solleva a un omomorfismo $\bar{\sigma} : E \to L$.

Rappresentando questo in un diagramma: se chiamo ι l'inclusione : $K \to E$, si ha

$$\begin{array}{ccc} K & \to^{\sigma} & L \\ \downarrow^{\iota} & & \\ E & & \end{array}$$

e voglio provare che posso chiudere il diagramma con una freccia diagonale da E a L .

CASO 1: $E = K(\alpha)$ ESTENSIONE ALGEBRICA SEMPLICE. Sia $f(x) \in K[x]$ il polinomio minimo di α su K , $f_0(x) = f(x)^{\sigma}$, e sia $K_0 := K^{\sigma}$, allora $K_0 \subseteq L$. Sia $\beta \in L$ una radice di $f_0(x)$, per un risultato precedente esiste un (unico) isomorfismo $\eta : K(\alpha) \to K_0(\beta)$ tale che $\alpha \mapsto \beta$, e che ristretto a K coincide con $\sigma : K \to K_0$. Se compongo η con l'inclusione $\iota : K_0(\beta) \to L$, ottengo un

omomorfismo $\bar{\sigma} = \iota \circ \eta$: $K(\alpha) = E \to L$ che solleva σ .

Osservazione 1.6

Se $\eta : E = K(\alpha) \to L$ è un omomorfismo che solleva σ , allora α^{η} è radice di $f_0(x)$, infatti applicando η all'uguaglianza $f(\alpha) = 0$ ottengo $0 = (f(\alpha))^{\eta} = f_0(\alpha^{\eta})$. Poiché L è algebricamente chiuso, L contiene tutte le radici di $f_0(x)$, allora i sollevamenti di σ sono tanti quante le radici di $f_0(x)$ ovvero di $f(x)$.

CASO 2: CASO GENERALE. Vale il seguente

Teorema 1.4

Siano K un campo e L un campo algebricamente chiuso, $\sigma : K \to L$ un omomorfismo. Sia $E \supseteq K$ un'estensione algebrica di campi, allora esiste un omomorfismo $\bar{\sigma} : E \to L$ che solleva σ .

Dimostrazione

Per la dimostrazione si utilizza il lemma di Zorn. Sia § insieme delle coppie (M, η) dove M è un campo, $K \subseteq M \subseteq E$ e $\eta : M \to L$ è un omomorfismo che solleva σ . § è non vuoto perché almeno la coppia $(K, \sigma) \in$ § . Dati $(M_1, \eta_1), (M_2, \eta_2) \in$ § , ordiniamo § ponendo $(M_1, \eta_1) \leq (M_2, \eta_2)$ se $M_1 \subseteq M_2$, $\eta_{2|_{M_1}} = \eta_1$. Questa è una relazione d'ordine parziale.

Sia $(M_1, \eta_1) \leq (M_2, \eta_2) \leq \cdots \leq (M_k, \eta_k) \leq \ldots$ una catena in § . **Mostro che questa catena ha un maggiorante in** § .

Considero $M = \bigcup_k M_k$ allora M è un campo con $K \subseteq M \subseteq E$, e la mappa $\eta : M \to L$ tale che $\eta_{|_{M_k}} = \eta_k$. Allora η è ben definito e la coppia (M, η) è un maggiorante per la catena. (Nota: se ho $((M_\alpha, \eta_\alpha))_{\alpha \in \Lambda}$ una catena in § , pongo $M = \bigcup_\alpha M_\alpha$ e $\eta_{|_{M_\alpha}} = \eta_{M_\alpha}$).

Per il lemma di Zorn § ha un elemento massimale F in § . **Voglio provare che $F = E$.**

Supponiamo per assurdo che questo non sia vero e quindi che $E \neq F$, allora posso prendere $\alpha \in E \setminus F$ e considerare $F(\alpha)$. Si ha il diagramma:

$$\begin{array}{ccc} F & \to^{\bar{\sigma}} & L \\ \downarrow & & \\ F(\alpha) & & \end{array}$$

Per il caso 1 esiste $\delta : F(\alpha) \to L$ omomorfismo che solleva $\bar{\sigma}$, e quindi che solleva σ , cioè $(F(\alpha), \delta) \in$ § , contro la massimalità della coppia $(F, \bar{\sigma})$.

Osservazione 1.7

Sia $\sigma : K \to L$, $E \supseteq K$ un'estensione algebrica, allora σ si solleva a $\bar{\sigma} : E \to L$. Supponiamo che E sia algebricamente chiuso, e L algebrico su $K_0 = K^{\sigma}$. Allora $E^{\bar{\sigma}}$ **è ancora algebricamente chiuso**: infatti, preso un polinomio $\bar{g}(x) \in E^{\bar{\sigma}}$, esso sarà della forma

$$\bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_m x^m, \, \bar{a}_i \in E^{\bar{\sigma}} \forall i$$

In particolare $\bar{a}_i = a_i^{\sigma}$, $a_i \in E$. Se $g(x) = \sum_i a_i x^i$ è la preimmagine di $\bar{g}(x)$, allora per ipotesi esso ha tutte le radici in E , allora $\bar{g}(x)$ ha tutte le sue radici in $E^{\bar{\sigma}}$.

Inoltre $E^{\bar{\sigma}} \subseteq L$, e contiene K_0 . L è algebrico su K_0 , e quindi anche su $E^{\bar{\sigma}}$, ma siccome $E^{\bar{\sigma}}$ è algebricamente chiuso non ammette estensioni algebriche proprie e quindi è uguale a L .

In particolare, due chiusure algebriche di un campo K sono isomorfe secondo un isomorfismo che è l'identità su K .

Capitolo 2

Teoria di Galois

2.1 Teoria di Galois

2.1.1 Definizione del gruppo di Galois

Definizione 2.1

Sia $M \supseteq K$ un'estensione di campi, il *gruppo di Galois* di M su K è definito come

$$G = \mathcal{G}(M/K) := \{g : M \to M \; t.c. \; g \, automorfismo, \; g_{|_K} = 1_K\}$$

Esempio 2.1

Sia $K = \mathbb{Q}$, e $M = \mathbb{Q}(\sqrt[3]{2})$, allora $M \supseteq K$ è un'estensione algebrica semplice, perché se pongo $\alpha = \sqrt[3]{2}$, α è radice del polinomio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. f è monico e irriducibile in $\mathbb{Q}[x]$, e in particolare è polinomio minimo di α . Allora gli elementi di M si scrivono come

$$\{a_0 + a_1\alpha + a_2\alpha^2, \; a_i \in \mathbb{Q}\}.$$

Sia $g \in G = \mathcal{G}(M/K)$, allora dato un generico elemento $p = a_0 + a_1\alpha + a_2\alpha^2$ in M si ha:

$$(a_0 + a_1\alpha + a_2\alpha^2)^g = a_0^g + a_1^g\alpha^g + a_2^g(\alpha^g)^2$$

e siccome sugli elementi di K g coincide con l'identità:

$$= a_0 + a_1\alpha^g + a_2(\alpha^g)^2$$

e quindi l'immagine p^g è determinata una volta stabilita l'immagine di α mediante g . Inoltre $f(\alpha) = 0$, e applicando g a quest'uguaglianza si ha

$$0 = 0^g = (f(\alpha))^g = f(\alpha^g)$$

e quindi α^g è ancora una radice di f^g .

Le radici di $f(x)$ sono $\alpha, \alpha\omega, \alpha\omega^2$ con ω radice terza dell'unità diversa da 1 , per esempio

$$\omega = \cos(2\pi/3) + i\sin(2\pi/3)$$
$$\omega^2 = \cos(4\pi/3) + i\sin(4\pi/3)$$

e ω, ω^2 stanno in $\mathbb{C}$ ma non in $\mathbb{R}$.

Ora $M \subset \mathbb{R}$, quindi $\alpha^g \neq \alpha\omega, \alpha^g \neq \alpha\omega^2$. L'unica possibilita'e' $\alpha^g = \alpha$, pertanto g fissa ogni elemento di M , e $G = \{1\}$.

Fatto: sia $M \supseteq K$ un'estensione di campi, $f(x) \in K[x]$ un polinomio monico e irriducibile, e supponiamo che $\alpha \in M$ sia una radice di $f(x)$ (dunque $f(x)$ è polinomio minimo di α su K).

Sia $g : M \to M$ un automorfismo di campi con $g_{|_K} = 1_K$, allora α^g è radice di $f(x)$ (dall'uguaglianza $f(\alpha) = 0$ ottengo $0 = (f(\alpha))^g = f(\alpha^g)$).

2.1.2 Insiemi L e H

Sia $M \supseteq K$ un'estensione di campi, e sia $G = \mathcal{G}(M/K)$, definiamo i due insiemi seguenti:

- $\mathcal{L}$ insieme dei campi intermedi tra K e M , cioè

$$\mathcal{L} = \{L \text{ campo } t.c.\ K \subseteq L \subseteq M\}$$

- $\mathcal{H}$ insieme dei sottogruppi di G :

$$\mathcal{H} = \{H : H \leq G\}$$

2.1.3 Definizioni delle applicazioni 'primo'

Definisco due applicazioni, una da $\mathcal{L}$ in $\mathcal{H}$ e l'altra da $\mathcal{H}$ a $\mathcal{L}$, che indichiamo entrambe con 'primo' (apice $'$).

- L'applicazione $' : \mathcal{L} \to \mathcal{H}$, è tale che

$$L \mapsto L' := \{g \in G\, t.c.\, \alpha^g = \alpha,\ \forall \alpha \in L\}$$

In altre parole, l'immagine di L è $\mathcal{G}(M/L)$.

- La mappa $' : \mathcal{H} \to \mathcal{L}$, è tale che

$$H \mapsto H' = \{\alpha \in M\, t.c.\, \alpha^h = \alpha,\ \forall h \in H\} = \text{Fix(H)}$$

Esercizio 2.1

Verificare che le due mappe sono ben definite, cioè che $H' \in \mathcal{L}$ e $L' \in \mathcal{H}$ per $H \in \mathcal{H}, L \in \mathcal{L}$.

Casi particolari: Vediamo come agiscono le mappe 'primo' su M , K , 1 e G (qui 1 e' il sottogruppo banale di G).

- M' è il gruppo di Galois $\mathcal{G}(M/M)$ che contiene solo l'identità.
- K' è tutto $G = \mathcal{G}(M/K)$.
- $1' = M$ (insieme degli elementi fissati da 1).
- Infine
$$G' = \mathrm{Fix(G)} = \{\alpha \in \mathrm{M\,t.c.}\, \alpha^{\mathrm{g}} = \alpha \forall \mathrm{g} \in \mathrm{G}\}$$
è un campo K_0 che contiene K , ma in generale è diverso da K .

Definizione 2.2

Diciamo che l'estensione $M \supseteq K$ è *normale* se $G' = K$ (ovvero, per ogni $\alpha \in M \setminus K$, esiste $g \in G$ tale che $\alpha^g \neq \alpha$).

2.1.4 Proprietà delle applicazioni 'primo'

Siano X, Y oggetti entrambi in $\mathcal{L}$ o entrambi in $\mathcal{H}$. Allora valgono queste due proprietà:

1. Se $X \subseteq Y$, allora $X' \supseteq Y'$.
2. $X'' \supseteq X$.

Verifico la prima proprietà: siano $X, Y \in \mathcal{L}$, siano $K \subseteq L \subseteq T \subseteq M$ estensioni di campo. $L \subseteq T$, e mostro che $L' \supseteq T'$ dove $L' = \mathcal{G}(M/L)$, $T' = \mathcal{G}(L/T)$.

Prendo un elemento $t \in T'$, mostro che $t'_{|_L} = 1_M$. Se $\alpha \in L$, siccome $L \subseteq T$, $\alpha \in T$, quindi $\alpha^t = \alpha$, cioè vale la proprietà da dimostrare.

Dalle proprietà 1 e 2 deduco in maniera del tutto formale che per ogni oggetto $X \in \mathcal{L} \cup \mathcal{H}$, $X''' = X'$.

Dimostrazione

INCLUSIONE 1: Dalla proprietà 2 segue che $X'' \supset X$, e quindi applicando la proprietà 1, $X''' \subset X'$.

INCLUSIONE 2: Posso scrivere $X''' = (X')''$, e per la proprietà 2 $(X')'' \supset X'$, quindi $X''' \supset X'$.

Osservazione 2.1

Equivalentemente, posso dire che l'estensione $M \supseteq K$ è normale se $K'' = K$ infatti, per quanto visto prima, l'estensione e' normale se $G' = K$. Ma $G = K'$ quindi ottengo che l'estensione e' normale se $K = K''$.

Proposizione 2.1

Sia $M \supseteq K$ un'estensione di campi. Allora $M \supseteq K''$ è un'estensione normale, e tra i gruppi di Galois vale la relazione $\mathcal{G}(M/K) = \mathcal{G}(M/K'')$.

(Nell'esempio iniziale, in cui $K = \mathbb{Q}$ e $M = \mathbb{Q}(\sqrt[3]{2})$, $G = \mathcal{G}(M/K) = 1$, allora $G' = K'' = \mathrm{Fix}(1) = \mathrm{M}$. Quindi possiamo 'rimediare' alla non normalita' di una estensione rimpiazzando K con K'' . Sebbene questo puo' portarci a una banalita', come in questo esempio).

Dimostrazione

Sappiamo che $K''' = K'$, allora $(K''')' = (K')'$, cioè $(K'')'' = K''$, e quindi $M \supseteq K''$ **è normale**.

Mostriamo che $\mathcal{G}(M/K) = \mathcal{G}(M/K'')$.

Siano $G = \mathcal{G}(M/K)$ e $\bar{G} = \mathcal{G}(M/K'')$.

INCLUSIONE 1: $G \subset \bar{G}$. Sia $\tilde{g} \in G$, mostro che $\tilde{g}$ fissa K'' elemento per elemento.

$$K'' = G' = \{\alpha \in M \, t.c. \, \alpha^g = \alpha \forall g \in G\}$$

Preso $\alpha \in K''$, siccome $K'' \subset M$, allora $\alpha^{\tilde{g}} = \alpha$, da cui $\tilde{g} \in \bar{G}$.

INCLUSIONE 2: $G \supset \bar{G}$. Sia $\hat{g} \in \bar{G}$; siccome per la proprietà 2 $K'' \supset K$, preso $\beta \in K$ si ha $\beta \in K''$, e quindi $\beta^{\hat{g}} = \beta$, cioè $\hat{g} \in G$.

2.1.5 Riepilogo

Sia $L \supseteq K$ un'estensione di campi, allora possiamo definire due applicazioni:

$$' : \mathcal{L} \to \mathcal{H} \, t.c. \, L \in \mathcal{L} \mapsto L' = \mathcal{G}(M/L)$$
$$' : \mathcal{H} \to \mathcal{L} \, t.c. \, H \in \mathcal{H} \mapsto H' = \mathrm{Fix(H)}$$

Se $X, Y \in \mathcal{L}$ o $X, Y \in \mathcal{L}'$, allora

- $X \subseteq Y$ implica $Y' \subseteq X'$
- $X'' \supseteq X$

da cui discende la proprietà $X''' = X'$.

Un'estensione è normale se $G' = K$, o equivalentemente se $K'' = K$.

2.1.6 Oggetti chiusi

Definizione 2.3

Un oggetto $X \in \mathcal{L} \cup \mathcal{H}$ è *chiuso* se $X'' = X$.

Osservazione 2.2

Essere chiuso significa "essere il primo" di qualcosa, infatti se X è chiuso, $X = X'' = (X')'$, viceversa, se $X = Y'$, allora $X' = (Y')' = Y''$ quindi $X'' = Y'''' = Y' = X$, da cui $X'' = X$.

Dato $X \in \mathcal{L} \cup \mathcal{H}$, chiamo X'' la *chiusura* di X : essa è il più piccolo oggetto chiuso che contiene X . Infatti se $X \subseteq Y$, con Y chiuso, allora $Y' \subseteq X'$ quindi $X'' \subseteq Y'' = Y$, cioè X'' è contenuto in ogni chiuso Y che contiene X .

Teorema 2.1 (Corrispondenza di Galois)

Sia $M \supseteq K$ un'estensione di campi, e $G = \mathcal{G}(M/K)$. Le applicazioni 'primo' stabiliscono una corrispondenza biunivoca tra oggetti chiusi di $\mathcal{L}$ e di $\mathcal{H}$.

Dimostrazione

Se $X \in \mathcal{H} \cup \mathcal{L}$ è un oggetto chiuso, allora $X \mapsto X' \mapsto X'' = X$.

Osservazione 2.3

Queste osservazioni valgono anche più in generale, siano $\mathcal{A}$ e $\mathcal{B}$ due insiemi parzialmente ordinati e supponiamo che si possano definire due mappe 'primo', una $: \mathcal{A} \to \mathcal{B}$ e l'altra $: \mathcal{B} \to \mathcal{A}$, che soddisfano le due proprietà: dati due oggetti $X, Y \in \mathcal{A} \cup \mathcal{B}$, $X \supseteq Y$ implica $X' \subseteq Y'$ e $X'' \supseteq X$.

Ad esempio, Sia $\mathcal{A} = \mathcal{B}$ insieme dei sottogruppi di un gruppo G , e $' : \mathcal{A} \to \mathcal{A}$ l'applicazione che manda H nel suo centralizzante in G , $C_G(H)$.

2.2 Oggetti chiusi

Vogliamo caratterizzare gli oggetti chiusi in $\mathcal{L} \cup \mathcal{H}$. "Oggetti chiusi si ottengono da oggetti chiusi per estensioni finite".

Lemma 2.1

Siano $K \subseteq L \subseteq M \subseteq N$ estensioni di campi, con $|M : L| = n < \infty$. Allora l'indice di M' in L' (indicato con $|L' : M'|$), è $\leq n$. In altre parole

$$|L' : M'| \leq |M : L|.$$

Dimostrazione

Procediamo per induzione su n . Se $n = 1$, $M = L$ e non c'è niente da dimostrare, e possiamo supporre $n > 1$. **Supponiamo che esista un campo intermedio proprio T tra L e M** (cioè tale che $L \subset T \subset M$). Siccome grado e indice sono entrambi moltiplicativi l'induzione risolve. Infatti pongo $|M : T| = r$ e $|T : L| = s$, dunque si ha $|M : L| = |M : T| * |T : L| = rs = n$. Poiche' T e' un campo propriamente contenuto tra L e M deve essere $r, s > 1$ e dunque $r, s < n$. Ora $|M : T| = r < n$, e per induzione $|T' : M'| \leq r$. Analogamente la condizione $|T : L| = s < n$ implica $|L' : T'| \leq s$. Infine l'indice e' moltiplicativo dunque $|L' : M'| = |L' : T'| * |T' : M'| \leq rs = n$.

Supponiamo ora che non esistano campi propriamente compresi tra L e M , considero $\alpha \in M \setminus L$, allora il campo $L(\alpha)$ contiene L propriamente ed è contenuto in M . Dato che per ipotesi non esistono campi intermedi tra L e M , segue subito che $L(\alpha) = M$.

Sia $f(x) \in L[x]$ il polinomio minimo di α , e chiamo Ω l'insieme delle radici di $f(x)$ contenute in N .

In particolare, $\Omega \neq \emptyset$ perché contiene almeno α . Considero $L' = \mathcal{G}(N/L)$, che agisce su Ω in questo modo: dati $\beta \in \Omega$ e $g \in L'$, allora $(\beta, g) \mapsto \beta^g$. **mostro che β^g sta ancora in Ω** , infatti

$$\beta \in \Omega \longrightarrow f(\beta) = 0$$

e se applico l'automorfismo g a entrambi i membri ottengo

$$0 = 0^g = (f(\beta))^g = f(\beta^g)$$

infatti g agisce come l'identità sui coefficienti di f che stanno in L , e quindi β^g è ancora una radice di $f(x)$.

Nell'azione di gruppo considerata, gli elementi dello stabilizzatore di α fissano M elemento per elemento (infatti, devono fissare L elemento per elemento, essendo elementi di $\mathcal{G}(N/L)$, e devono fissare α essendo elementi del suo stabilizzatore), quindi lo stabilizzatore di α e' M' .

Infine osservo che $|L' : M'|$, indice di M' in L' , è uguale alla cardinalità dell'orbita, $\alpha^{L'}$, di α sotto l'azione di L' , e l'orbita è contenuta in Ω . Ma $|\Omega| \leq n = \mathrm{gr(f(x))} = |\mathrm{M : L}|$ quindi $|L' : M'| \leq |\alpha^{L'}| \leq |M : L|$.

Lemma 2.2

Sia $K \subseteq M$ un'estensione di campi, e $G = \mathcal{G}(M/K)$.

Siano H, S sottogruppi di G , con $H \subset S$. Se l'indice di H in S è uguale a $n < \infty$, allora $|H' : S'| \leq n$. In altre parole

$$|H' : S'| \leq |S : H|$$

Dimostrazione

Per definizione, si ha che $H' = \mathrm{Fix(H)}$, $\mathrm{S'} = \mathrm{Fix(S)}$.

PASSO 1: Considero i laterali destri di H in S , e per $\alpha \in H'$ e Hs laterale destro di H in S , definisco $\alpha^{Hs} := \alpha^s$. Questa definizione è ben posta e non dipende dalla scelta del laterale, perché se $Hs_1 = Hs_2$, allora $s_1 = hs_2$ per un certo $h \in H$, e quindi

$$\alpha^{Hs_1} = \alpha^{s_1} = \alpha^{hs_2} = \alpha^{s_2} = \alpha^{Hs_2}$$

dove l'ultimo passaggio vale perché $\alpha \in \text{Fix(H)}$.

PASSO 2: per assurdo, suppongo che $|H' : S'| > n$, allora esistono $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ elementi di H' , linearmente indipendenti su S' . Considero il sistema

$$\begin{cases} x_1(\alpha_1 C_1) + x_2(\alpha_2 C_1) + \cdots + x_{n+1}(\alpha_{n+1} C_1) = 0 \\ x_1(\alpha_1 C_2) + x_2(\alpha_2 C_2) + \cdots + x_{n+1}(\alpha_{n+1} C_2) = 0 \\ \ldots \\ x_1(\alpha_1 C_n) + x_2(\alpha_2 C_n) + \cdots + x_{n+1}(\alpha_{n+1} C_n) = 0 \end{cases}$$

dove $C_1, C_2, \ldots, C_n$ sono i laterali destri di H in S , e $C_1 = H$, e dove $\alpha_i C_j = \alpha_i^{C_j}$.

Il sistema lineare scritto sopra è omogeneo della forma $AX = 0$, dove A è una matrice $n \times n+1$ e il sistema ha $n+1$ incognite. Dunque il sistema ammette soluzioni non banali. Tra tutte le soluzioni non banali, ne considero una per cui il numero r di elementi non nulli sia minimo.

A meno di riordinamenti posso scrivere questa soluzione in modo che abbia gli zeri nelle ultime posizioni, cioè

$$(u_1, u_2, \ldots, u_r, 0, \ldots, 0),\ u_i \neq 0,\ \forall i = 1, \ldots, r$$

Posso supporre, a meno di moltiplicare tutto per u_1^{-1} (e posso farlo perche' ottengo ancora una soluzione del sistema che e' omogeneo), che il primo coefficiente sia uguale a 1 e che la soluzione sia

$$(1, u_2, \ldots, u_r, 0, \ldots, 0)$$

PASSO 3: Se gli u_i stanno in S' per ogni i , si ha un assurdo, perché la prima equazione del sistema diventa

$$\alpha_1 C_1 + u_2(\alpha_2 C_1) + \cdots + u_{n+1}(\alpha_{n+1} C_1) = 0,$$

dove $C_1 = H$. Ora $\alpha_i C_1 = \alpha_i{}^H = \alpha_i \forall i$, quindi la prima equazione si riscrive come

$$1\alpha_1 + u_2\alpha_2 + \cdots + u_{n+1}\alpha_{n+1} = 0$$

e ho una relazione di dipendenza lineare degli α_i su S' , ma questo è assurdo perché sono stati scelti linearmente indipendenti. Quindi deve esistere almeno un elemento u_i che non sta in S' . A meno di riordinamenti suppongo che $u_2 \notin S'$. Quindi $u_2 \notin \text{Fix(S)}$, ed esiste pertanto un elemento $s \in S$ tale che $u_2^s \neq u_2$.

PASSO 4: Considero la i-esima equazione del sistema precedente:

$$1(\alpha_1 C_i) + u_2(\alpha_2 C_i) + \cdots + u_{n+1}(\alpha_{n+1} C_i) = 0.$$

Applico s a quest'equazione e ottengo

$$1^s * (\alpha_1 C_i)^s + u_2^s(\alpha_2 C_i)^s + \cdots + u_{n+1}^s(\alpha_{n+1} C_i)^s = 0,$$

dove, posto $C_i = Hs_i$, si ha che

$$(\alpha_j C_i)^s = (\alpha_j^{s_i})^s = \alpha_j^{s_i s} = \alpha_j C_i s.$$

La sequenza $(C_1 s, C_2 s, \ldots, C_n s)$ è una permutazione di $(C_1, C_2, \ldots, C_n)$. Applicando questo ragionamento a tutte le righe, trovo che se il vettore $u = (1, u_2, \ldots, u_r, 0, \ldots, 0)$ è una soluzione del sistema $AX = 0$, allora anche $u_s = (1^s, u_2^s, \ldots, u_r^s, 0, \ldots, 0)$ è una soluzione di $AX = 0$ (perche' il ragionamento di prima prova che il secondo vettore e' soluzione di un sistema che si ottiene da $AX = 0$ permutandone le righe).

Allora anche la differenza

$$u - u^s = (0, u_2 - u_2^s, \ldots, u_r - u_r^s, 0, \ldots, 0)$$

è ancora una soluzione del sistema $AX = 0$, e non e' la soluzione banale perche' ${u_2}^s - u_2 \neq 0$. Ma questo va contro la minimalità di r perché $u - u^s$ ha un numero di

entrate non nulle minore di r , assurdo!

2.2.1 Caratterizzazione di oggetti chiusi

Sono stati dimostrati i seguenti lemmi:

Lemma 2.3 (versione campi intermedi)

Siano $K \subseteq L \subseteq T \subseteq M$ estensioni di campi, e sia $|T : L| = n < \infty$, allora l'indice $|L' : T'| \leq n$.

Lemma 2.4 (versione sottogruppi)

Sia $N \supseteq K$ un'estensione di campi, e sia $G = \mathcal{G}(N/K)$. Siano H, S sottogruppi di G con $H \leq S$, e sia $|S : H| = n < \infty$, allora $|H' : S'| \leq n$ (grado).

"Oggetti chiusi si ottengono da oggetti chiusi per estensioni finite", e precisamente

Lemma 2.5

campi intermedi Siano $K \subseteq L \subseteq M \subseteq N$ estensioni di campi, con $|M : L| = n < \infty$ e L chiuso. Allora M è chiuso, e l'indice di M' in L' è uguale al grado di M su L , in simboli $|L' : M'| = |M : L|$.

sottogruppi Sia $N \supseteq K$ un'estensione di campi, $G = \mathcal{G}(N/K)$, e H, S sottogruppi di G , con $H \subseteq S$ e $|S : H| = n < \infty$. Sia H chiuso, allora S è chiuso e $|H' : S'| = |S : H|$.

Dimostrazione

VERSIONE PER CAMPI INTERMEDI: Sia $K \subseteq L \subseteq M \subseteq N$, allora se applico i lemmi 1 e 2 si ha

$$|M'' : L''| \leq |L' : M'| \leq |M : L| = n, \text{ relazione 1}$$

ma $M'' \supseteq M$, inoltre L è chiuso, quindi $L'' = L$. In termini di estensioni di campi si ha $M'' \supset M \supseteq L$, e $M'' \supseteq M$ implica $|M'' : L| \geq |M : L|$ (relazione 2). Per le relazioni 1 e 2 segue $|M'' : L| = |M : L|$ e quindi $M'' = M$ cioè M è chiuso. Se riscrivo la relazione 1 ottengo

$$|M : L| \leq |L' : M'| \leq |M : L|$$

e quindi $|L' : M'| = |M : L|$.

VERSIONE PER I SOTTOGRUPPI: La parte 2 si dimostra in modo analogo. Infatti

$$|S'' : H''| \leq |H' : S'| \leq |S : H|$$

ma H è chiuso, allora $H'' = H$, e $S'' \supseteq S$, allora per un ragionamento simile al precedente $S'' = S$, e $|H' : S'| = |S : H|$.

2.2.2 Teorema fondamentale della teoria di Galois

Osservazione 2.4

Sia $M \supseteq K$ un'estensione di campi, $G = \mathcal{G}(M/K)$. Il sottogruppo banale 1 di G , e' sempre chiuso perche' si ha

$$1 \mapsto 1' = \text{Fix}(1) = \text{M} \mapsto 1'' = \text{M}' = 1.$$

Per quanto visto, sono chiusi tutti i sottogruppi di G di ordine finito.

Osservazione 2.5

Se $M \supseteq K$ è normale, K è chiuso, e quindi sono chiusi tutti i campi intermedi L tra K ed M dove $K \subseteq L \subseteq M$ con L estensione di grado finito di K .

Abbiamo allora provato il *teorema fondamentale della teoria di Galois*:

Teorema 2.2

Sia $M \supseteq K$ un'estensione normale, di grado finito, e sia $G = \mathcal{G}(M/K)$. Allora tutti i campi intermedi tra K ed M e tutti i sottogruppi di G sono chiusi. Le

applicazioni "primo" stabiliscono una corrispondenza biunivoca tra campi intermedi e sottogruppi di G . In tale corrispondenza la dimensione relativa tra due campi intermedi è uguale all'indice relativo tra i sottogruppi corrispondenti. In particolare

$$|G| = |M : K|.$$

Osservazione 2.6

Dire che 'la dimensione relativa tra due campi intermedi è uguale all'indice relativo tra i sottogruppi corrispondenti' significa che, se $K \subseteq L \subseteq T \subseteq M$ si ha $|T : L| = |L' : T'|$. In particolare l'ordine di G e' dato dall'indice di 1 in G e dunque è uguale a $|1' : G'| = |M : K|$, cioè l'ordine del gruppo di Galois è uguale al grado dell'estensione.

2.3 Esempio di studio di estensione

2.3.1 Determinazione del grado dell'estensione

Sia $\omega = \cos(2\pi/5) + i\sin(2\pi/5)$, e studio l'estensione $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$. Ora ω è una radice quinta dell'unità, e quindi è radice del polinomio $x^5 - 1$, che è un polinomio in $\mathbb{Q}[x]$, e quindi ω è algebrico su $\mathbb{Q}$.

Osservo che $x^5 - 1$ si può fattorizzare come

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = (x-1)\phi_5(x)$$

dove $\phi_5(x)$ è un polinomio a coefficienti razionali. Siccome $\omega \neq 1$, ω è radice di $\phi_5(x)$, cioè $\phi_5(\omega) = 0$.

Vogliamo provare che $\phi_5(x)$ è proprio il polinomio minimo di ω su $\mathbb{Q}$.

Osservazione 2.7

Osservo che dato un anello A commutativo unitario, e dati due elementi $a, b \in A$, posso considerare l'omomorfismo (di valutazione) $\phi : A[x] \to A[x]$ tale che $x \mapsto ax + b$ e $c \mapsto c$ per ogni $c \in A$.

Se $f(x)$ è un polinomio in $A[x]$, allora

$$(f(x))^{\phi} = f(ax + b)$$

Se a è invertibile nell'anello A , allora ϕ è un isomorfismo, con inverso l'omomorfismo (di valutazione) $\phi^{-1} : A[x] \to A[x]$ tale che $x \mapsto a^{-1}x - a^{-1}b$, e $c \mapsto c$, $\forall c \in A$.

In particolare, se F è un campo, preso $a \neq 0$ segue che $\phi : F[x] \to F[x]$ tale che $x \mapsto ax + b$ e $c \mapsto c$, $\forall c \in F$ è un isomorfismo, e quindi un polinomio $f(x) \in F[x]$ è irriducibile in $F[x]$ se e solo se lo è $f(x)^{\phi} = f(ax + b)$, con $a, b \in F$, $a \neq 0$.

In base all'osservazione precedente, mostrare che $\phi_5(x)$ è irriducibile su $\mathbb{Q}$ equivale a mostrare che $\phi_5(x + 1)$ è irriducibile su $\mathbb{Q}$.

$$\phi_5(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$$
$$\phi_5(x+1) = \frac{(x+1)^5 - 1}{x + 1 - 1} = \frac{(x+1)^5 - 1}{x}$$
$$= 1/x \sum_{k=1}^{5} \binom{5}{k} x^k$$

(infatti $\binom{5}{0} = 1$ e si elide con il -1 già presente)

$$= \sum_{k=1}^{5} \binom{5}{k} x^{k-1}$$
$$= x^4 + \binom{5}{4} x^3 + \binom{5}{3} x^2 + \binom{5}{2} x + \binom{5}{1}$$

e per $p = 5$ posso applicare Eisenstein ($p = 5 \mid \binom{5}{k}$, per $k = 1, \ldots, 4$, non divide il coefficiente direttivo e p^2 non divide il termine noto), e quindi $\phi_5(x+1)$ è irriducibile sopra $\mathbb{Q}$, e lo è anche $\phi_5(x)$.

Osservazione 2.8

Più in generale se p è un numero primo, si ha che $x^p - 1 = (x-1) * (x^{p-1} + x^{p-2} + \cdots + x + 1)$. Chiamo $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, questo polinomio è irriducibile su $\mathbb{Q}$ per argomenti analoghi a quelli precedenti.

Infatti, come prima

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{x + 1 - 1}$$
$$= 1/x * \sum_{k=1}^{p} \binom{p}{k} x^k = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$$

e $p \mid \binom{p}{k}$ per $k = 1, \ldots, p-1$, per il criterio di Eisenstein $\phi_p(x+1)$ è irriducibile su $\mathbb{Q}$.

Tornando a $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$, abbiamo mostrato che $\phi_5(x)$ è il polinomio minimo di ω . In particolare, $\mathbb{Q}(\omega)$ contiene tutti (e soli) gli elementi della forma $a + b\omega + c\omega^2 + d\omega^3$, $a, b, c, d \in \mathbb{Q}$, tali che ω è radice di $\phi_5(x)$.

Segue che $|\mathbb{Q}(\omega) : \mathbb{Q}| = 4$. Di più, $\mathbb{Q}(\omega)$ è il campo di spezzamento di $\phi_5(x)$ sopra $\mathbb{Q}$, perché $\omega \in \mathbb{Q}(\omega)$ implica che $\omega^2, \omega^3, \omega^4 \in \mathbb{Q}(\omega)$ e quindi $\mathbb{Q}(\omega)$ contiene tutte le radici di $\phi_5(x)$.

2.3.2 Ordine ed elementi del gruppo di Galois G

Come vedremo, **l'estensione $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ è normale**. Se chiamo $G = \mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$, si ha che $o(G) = 4$ per il teorema fondamentale della teoria di Galois.

Sia $g \in G$, allora ω^g è ancora una radice di $\phi_5(x)$. D'altra parte, presa una radice ω^i di $\phi_5(x)$, considero la mappa tale che $H : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^i)$ che fissa $\mathbb{Q}$ elemento

per elemento e manda ω in ω^i . Osservo che $h \in G$, perché $\mathbb{Q}(\omega^i) = \mathbb{Q}(\omega)$, infatti

INCLUSIONE 1: $\omega^i \in \mathbb{Q}(\omega)$ e quindi $\mathbb{Q}(\omega^i) \subseteq \mathbb{Q}(\omega)$;

INCLUSIONE 2: $|\mathbb{Q}(\omega^i) : \mathbb{Q}| = 4$ perché ϕ_5 è polinomio minimo di ogni sua radice. ω^i è invertibile perché i e 5 sono primi tra loro, allora, per opportuni s, t posso scrivere

$$1 = 5s + it, \longrightarrow \omega = \omega^{5s+it} = \omega^{it}$$

cioè $\omega \in \mathbb{Q}(\omega^i)$ e quindi $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\omega^i)$.

Si ha anche che h è invertibile.

Posso scrivere gli elementi di G :

$$G = \{1, g_2, g_3, g_4\},$$

dove $\omega^{g_i} = \omega^i$.

Verifico le relazioni tra gli elementi di G :

$$\omega^{g_2^2} = (\omega^{g_2})^2 = \omega^4 = \omega^{g_4}, \longrightarrow g_2^2 = g_4$$
$$\omega^{g_2^3} = \omega^{g_4 * g_2} = (\omega^4)^{g_2} = (\omega^2)^4$$
$$= \omega^8 = \omega^5 * \omega^3 = \omega^3 = \omega^{g_3}, \longrightarrow g_2^3 = g_3$$

Allora g **è ciclico di ordine 4**, se pongo $g_2 = g$, allora gli elementi di g sono $\{1, g, g^2, g^3\}$.

2.3.3 Corrispondenza di Galois

Essendo ciclico di ordine 4, G ha un solo sottogruppo proprio di ordine 2, che è $H = \{1, g^2\}$.

Segue che $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ **ha un solo campo intermedio** $L = H' = \mathrm{Fix(H)}$ **, e** $|L : \mathbb{Q}| = |G : H| = 2$.

Determiniamo esplicitamente gli elementi di L , per definizione:

$$L = H' = \{a+b\omega+c\omega^2+d\omega^3 \in \mathbb{Q}(\omega)\, t.c.\, (a+b\omega+c\omega^2+d\omega^3)^{g^2} = a+b\omega+c\omega^2+d\omega^3\}$$

Osservo che

$$(a + b\omega + c\omega^2 + d\omega^3)^{g^2}$$
$$= a + b\omega^4 + c(\omega^4)^2 + d(\omega^4)^3$$
$$= a + b\omega^4 + c\omega^3 + d\omega^2$$

siccome ω è radice di $\phi_5(x)$, si ha $\omega^4 = -1 - \omega - \omega^2 - \omega^3$, e sostituendo nell'espressione sopra ottengo

$$= a - b - b\omega - b\omega^2 - b\omega^3 + c\omega^3 + d\omega^2$$
$$= (a-b) - b\omega + (d-b)\omega^2 + (c-b)\omega^3$$

L'insieme $\{1, \omega, \omega^2, \omega^3\}$ è una base per $|\mathbb{Q}(\omega) : \mathbb{Q}|$, quindi chiedere che

$$(a + b\omega + c\omega^2 + d\omega^3)^{g^2} = a + b\omega + c\omega^2 + d\omega^3$$

equivale a chiedere che

$$\begin{cases} a - b = a \\ -b = b \\ d - b = c \\ c - b = d \end{cases}$$

da cui

$$b = 0, d = c$$

quindi L **è il campo intermedio che contiene gli elementi della forma**

$$a + c\omega^2 + c\omega^3 = a + c(\omega^2 + \omega^3),\ a, c \in \mathbb{Q}.$$

Se chiamo $\alpha = \omega^2 + \omega^3$, si ha

$$\alpha^2 = (\omega^2+\omega^3)^2 = \omega^4+\omega^6+2\omega^5 = \omega^4+\omega+2 = -1-\omega-\omega^2-\omega^3+\omega+2 = 1-\omega^2-\omega^3 = 1-\alpha$$

allora $\alpha^2 + \alpha - 1 = 0$, e il polinomio minimo di α è $m(x) = x^2 + x - 1$.

2.4 Stabilità e normalità

2.4.1 Stabilità

Definizione 2.4

Siano $K \subseteq L \subseteq M$ estensioni di campi, e sia $G = \mathcal{G}(M/K)$, allora L è un *campo intermedio stabile* (relativamente a M e K) se succede che $L^g \subseteq L,\ \forall g \in G$.

Osservazione 2.9

Un campo intermedio L è stabile se e solo se $L^g = L,\ \forall g \in G$.

Infatti, se $L^g = L,\ \forall g \in G$, è chiaro che L è stabile.

Viceversa, mostro che se L è stabile, si ha $L \subseteq L^g$. Prendo $g \in G, l \in L$, allora siccome L è stabile e la relazione vale per ogni g , deve valere anche per g^{-1} e quindi $l^{g^{-1}} \in L$, e dunque, applicando g , $(l^{g^{-1}})^g = l \in L^g$, cioè $L \subseteq L^g$.

2.4.2 Corrispondenza tra campi stabili e sottogruppi normali

Proposizione 2.2

Sia $M \supseteq K$ un'estensione di campi, e $G = \mathcal{G}(M/K)$. Allora,

1. se L è un campo intermedio stabile, L' è un sottogruppo normale in G , ovvero $L' = \mathcal{G}(M/L)$ è normale in $\mathcal{G}(M/K)$.
2. se H è un sottogruppo normale di G , allora $H' = \text{Fix(H)}$ è un campo intermedio stabile.

Dimostrazione

1. Per ipotesi, L è un campo intermedio stabile, e **mostro che L' è normale in G** , cioè, applicando la definizione, mostro che dati $h \in L', g \in G$, $g^{-1}hg \in L'$; equivalentemente mostro che $g^{-1}hg$ fissa L elemento per elemento. Prendo $l \in L$, e calcolo
$$l^{g^{-1}hg} = (l^{g^{-1}})^{hg}$$
ma $l^{g^{-1}} \in L$ e h fissa L elemento per elemento, quindi
$$= l^{g^{-1}*g} = l$$
e quindi la tesi è vera.
2. Sia H un sottogruppo normale di G , allora **mostro che $H' = \text{Fix(H)}$ è un campo intermedio stabile**, ovvero che $(H')^g \subseteq H'$ per ogni $g \in G$. Considero $\alpha \in H'$ e mostro che, fissato arbitrariamente $g \in G$, si ha $\alpha^g \in \text{Fix(H)}$ .Siccome H è normale, si ha $gh = kg$ per un certo $k \in H$. Allora $\alpha^{gh} = \alpha^{kg} = \alpha^g$ (infatti $k \in H \longrightarrow \alpha^k = \alpha$), e quindi $\alpha^g \in \text{Fix(H)}$.

La stabilità di L è legata alla normalità dell'estensione $L \supseteq K$.

Per la dimostrazione della prossima proposizione è necessario il seguente lemma:

Lemma 2.6

Sia $M \supseteq K$ un'estensione di campi normale, e sia $f(x) \in K[x]$ un polinomio monico e irriducibile. Se $f(x)$ ammette una radice in M , allora si spezza in $M[x]$ in prodotto di fattori lineari distinti.

Dimostrazione

Sia $\alpha \in M$ una radice di $f(x)$, che esiste per ipotesi. Sia $G = \mathcal{G}(M/K)$, e A l'insieme delle immagini distinte di α sotto l'azione di G . Se β è un elemento di A , allora sarà della forma α^g per $g \in G$. Sappiamo che β è radice di $f(x)$, e quindi A è finito, e ha cardinalità $r \leq \text{gr(f(x))}$. Scriviamo $A = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r\}$.

Consideriamo il polinomio $p(x) = (x - \alpha_1)(x - \alpha_2) * \cdots * (x - \alpha_r) \in M[x]$. I coefficienti di $p(x)$ sono le funzioni simmetriche elementari in $\alpha_1, \ldots, \alpha_r$, definite come segue

$$\begin{aligned}
&\sigma_0(\alpha_1,\ldots,\alpha_n) = 1\\
&\sigma_1(\alpha_1,\ldots,\alpha_r) = \sum_j \alpha_j\\
&\sigma_2(\alpha_1,\ldots,\alpha_r) = \sum_{j_1<j_2} \alpha_{j_1} * \alpha_{j_2}\\
&\qquad\ldots\ldots \qquad\qquad\qquad \ldots\\
&\sigma_i(\alpha_1,\ldots,\alpha_r) = \sum_{j_1<j_2<\cdots<j_i} \alpha_{j_1} * \alpha_{j_2} * \cdots * \alpha_{j_i}\\
&\qquad\ldots\ldots \qquad\qquad\qquad \ldots\\
&\sigma_r(\alpha_1,\ldots,\alpha_r) = \alpha_1 * \alpha_2 * \cdots * \alpha_r
\end{aligned}$$

Quindi

$$p(x) = \sum_{h=0}^{r} (-1)^h \sigma_h(\alpha_1,\ldots,\alpha_r) x^{r-h}$$

Le funzioni elementari sono invarianti se permuto $\alpha_1,\ldots,\alpha_r$. D'altra parte gli elementi di G permutano $\alpha_1,\ldots,\alpha_r$ e quindi fissano i coefficienti di $p(x)$. $M \supseteq K$ è normale per ipotesi, allora $p(x)$ è un polinomio a coefficienti in K (i coefficienti stanno in $G' = \text{FixG}$). D'altra parte $p(\alpha) = 0$, e $f(x)$, essendo irriducibile, è il polinomio minimo di α . Allora $f(x) \mid p(x)$. In particolare gr(p(x)) = r $\geq$ gr(f(x)) , e siccome si aveva $r \leq$ gr(f(x)) , segue che $r =$ gr(f(x)) . Poi $f(x)$ e $p(x)$ sono entrambi monici dunque $p(x) = f(x)$, cioè $f(x)$ si spezza su M .

Proposizione 2.3

1. supponiamo che $M \supseteq L \supseteq K$ siano estensioni di campi, con $M \supseteq K$ normale e L stabile. Allora l'estensione $L \supseteq K$ è normale.
2. Siano $M \supseteq L \supseteq K$ estensioni di campi, e supponiamo che $L \supseteq K$ sia normale e algebrica. Allora L è stabile.

Dimostrazione

1. Considero $\alpha \in L \setminus K$, e mostro che esiste $h \in \mathcal{G}(L/K)$ tale che $\alpha^h \neq \alpha$. Siccome $M \supseteq K$ è normale e α sta in M , esiste $g \in G$ tale che $\alpha^g \neq \alpha$. Se considero $h = g_{|_L} : L \to L^g = L$, ($L^g = L$ perché L è stabile), allora $h \in \mathcal{G}(L/K)$.
2. Per la seconda parte è necessario il lemma dimostrato prima.Mostro che dato $\alpha \in L$ e $g \in \mathcal{G}(M/K)$, allora $\alpha^g \in L$. Per ipotesi $\alpha \in L$ è algebrico su K , allora posso considerare il polinomio minimo $f(x) \in K[x]$ di α su K .Per il lemma precedente, $f(x)$ si spezza in fattori lineari distinti in $L[x]$ .D'altra parte, α^g è una radice di f , e quindi $\alpha^g \in L$.

Sia $M \supseteq K$, L un campo intermedio stabile, allora possiamo considerare l'applicazione $\phi : \mathcal{G}(M/K) \to \mathcal{G}(L/K)$, tale che $g \mapsto g_{|_L}$. ϕ è un omomorfismo di gruppi, con

$$\ker \phi = L' = \mathcal{G}(M/L)$$

$Im\phi$ è l'isieme degli automorfismi di L su K (cioè che fissano K elemento per elemento), che si sollevano ad automorfismi di M su K .

Dalle proposizioni precedenti si ha il seguente risultato:

Proposizione 2.4 (conseguenza)

Supponiamo che $M \supseteq K$ sia normale e di grado finito. Allora L campo intermedio è stabile se e solo se $L \supseteq K$ è normale. Inoltre l'omomorfismo $\phi : \mathcal{G}(M/K) \to \mathcal{G}(L/K)$ è suriettivo.

Dimostrazione

Osservo in particolare che il fatto che $M \supseteq K$ sia di grado finito implica che $L \supseteq K$ è algebrica, e quindi il "se e solo se" segue dalla proposizione precedente.

Per quanto riguarda la suriettività di ϕ , per il teorema fondamentale

$$o(\mathcal{G}(L/K)) = |L : K| = |K' : L'| = |\frac{\mathcal{G}(M : K)}{\mathcal{G}(M : L)}| = \frac{o(\mathcal{G}(M/K))}{o(\mathcal{G}(M/L))} = \frac{o(\mathcal{G}(M/K))}{\ker \phi}.$$

Possiamo aggiungere al teorema fondamentale della teoria di Galois anche il seguente fatto:

Teorema 2.3

Sia L un campo intermedio tra K e M , allora $L \supseteq K$ è un'estensione normale se e solo se L' è normale in G , e in tal caso G/L' è isomorfo a $\mathcal{G}(L/K)$.

Dimostrazione

Va giustificato solo il fatto che $L \supseteq K$ è normale se e solo se L' è normale in G .

Dalla "conseguenza" segue che L è stabile, allora L' è normale in G per la relazione tra la normalità di sottogruppi e la stabilità dei campi intermedi. Viceversa, L' normale in G implica che L'' è stabile, ma siccome L e' chiuso si ha $L'' = L$ e quindi L è stabile.

2.5 Caratterizzazione delle estensioni normali di grado finito

2.5.1 Separabilità

Proposizione 2.5

Sia K un campo, $f(x) \in K[x]$ un polinomio non nullo, $\bar{K}$ una chiusura algebrica di K . Allora un elemento $\alpha \in \bar{K}$, con $f(\alpha) = 0$, è una radice multipla di

$f(x)$ (cioè $(x-\alpha)^2 \mid f(x)$) se e solo se, posto $f'(x)$ la derivata formale di $f(x)$, $f'(\alpha) = 0$.

Dimostrazione

$1 \longrightarrow 2$: se α è una radice multipla di $f(x)$, allora $f(x) = (x-\alpha)^2 * g(x)$, e derivando ottengo

$$f'(x) = (x-\alpha)^2 * g'(x) + (x-\alpha)g(x)$$

e valutando in α , ovviamente $f'(\alpha) = 0$.

$2 \longrightarrow 1$: viceversa, so che α è una radice di f , quindi $f(x) = (x-\alpha)h(x)$. Derivando:

$$f'(x) = h(x) + (x-\alpha)h'(x)$$

Se valuto in α , siccome per ipotesi $f'(\alpha) = 0$, segue che $h(\alpha) = 0$, e quindi $x-\alpha \mid h(x)$ e $h(x) = (x-\alpha)g(x)$ e $f(x) = (x-\alpha)^2 g(x)$, cioè α è radice multipla di $f(x)$.

Osservazione 2.10

Sia K un campo, $\bar{K}$ una chiusura algebrica di K , e $f(x)$ un polinomio in $K[x]$. Allora

1. $f(x)$ ha una radice multipla se e solo se, detto $d(x) = MCD(f(x), f'(x))$, risulta $d(x) \neq 1$ .In tal caso le radici multiple di $f(x)$ sono tutte e sole le radici di $d(x)$.
2. se inoltre f è irriducibile, $f(x)$ ha radici multiple se e solo se $f'(x) = 0$.

Dimostrazione

1. $\alpha \in \bar{K}$ è una radice multipla di $f(x)$ se e solo se $f(\alpha) = 0 = f'(\alpha)$, quindi se e solo se $x-\alpha \mid f(x)$ e $x-\alpha \mid f'(x)$, cioè $x-\alpha \mid MCD(f(x), f'(x))$, ovvero α è una radice di $d(x)$.
2. siccome f è irriducibile, $d(x) = 1$ oppure $d(x) = f(x)$. Si esclude la possibilità $d(x) = 1$ altrimenti $f(x)$ non avrebbe radici multiple, e quindi $f(x)$ ha radici multiple se e solo se $MCD(f, f') = f(x)$, ma allora $f(x) \mid f'(x)$. Se $f'(x) \neq 0$ questo non è possibile perché $f'(x)$ ha grado minore di $f(x)$. L'unica possibilità è quindi $f'(x) = 0$.

Definizione 2.5

- Siano K un campo, $\bar{K}$ una chiusura algebrica di K , sia $f(x) \in K[x]$ un polinomio irriducibile, dico che $f(x)$ è *separabile* su K se le sue radici in $\bar{K}$ sono tutte distinte.

- Data un'estensione di campi $M \supseteq K$, allora $\alpha \in M$ algebrico su K si dice *separabile* (su K) se è separabile il polinomio minimo di α in $K[x]$.
- Se $M \supseteq K$ è algebrica, dico che è separabile su K se ogni elemento di M è separabile su K .

Osservazione 2.11

Sia K un campo, $f(x) \in K[x]$ un polinomio non costante, allora

- se la caratteristica di K è 0, la derivata $f'(x)$ è un polinomio non nullo.
- Se la caratteristica di K è un numero primo positivo, $f'(x) = 0$ se e solo se

$f(x) = g(x^p)$ per $g(x)$ polinomio in $K[x]$.

Dimostrazione

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ a_n \neq 0$$

quindi

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1},$$

e in un campo di caratteristica 0, $a_n \neq 0$ implica $na_n \neq 0$ ovvero $f'(x) \neq 0$.

In caratteristica p ,

$$f'(x) = \sum_{i} i a_i x^{i-1} = 0$$

quando $ia_i = 0 \in K,\ \forall i$. Questo accade se $p \mid a_i$ oppure $p \mid i$.

Se p divide a_i il monomio $a_i x^i$ non e' presente in $f(x)$. Rimangono allora in $f(x)$ i monomi $a_i x^i$ con $p \mid i$. Segue che $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ è della forma $b_m x^{pn} + b_{m-1} x^{p(m-1)} + \cdots + b_1 x^p + b_0$.

Se chiamo $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$, si ha che $f(x) = g(x^p)$. E' anche chiaro che, viceversa, se $f(x) = g(x^p)$ allora $f'(x) = 0$.

In particolare, i polinomi di grado 1 sono separabili.

In caratteristica 0 un polinomio irriducibile è separabile.

Teorema 2.4 (caratterizzazione delle estensioni normali di grado finito)

Sia $M \supseteq K$ un'estensione normale di grado finito. Sono equivalenti

1. l'estensione $M \supseteq K$ è normale
2. M è separabile su K e M è campo di spezzamento su K

3. M è campo di spezzamento su K di un polinomio i cui fattori irriducibili sono separabili.

Prima della dimostrazione sono necessarie le seguenti osservazioni.

Osservazione 2.12

Supponiamo di avere una catena di estensioni $M \supseteq L \supseteq K$, e supponiamo che M sia un campo di spezzamento di $f(x)$ su K . Allora M è campo di spezzamento di $f(x)$ su L .

Dimostrazione

Posso considerare $f(x)$ come un polinomio a coefficienti in L , $f(x)$ si spezza in fattori lineari in $M[x]$ perché M è campo di spezzamento di $f(x)$ su K per ipotesi. Devo provare la minimalità di M . Se chiamo M_0 il campo di spezzamento di f su L , allora $M_0 \subseteq M$ per la minimalità di M_0 come campo di spezzamento. Viceversa, siccome M_0 è campo di spezzamento di f su L allora M_0 contiene L e dunque contiene K e contiene tutte le radici di $f(x)$. Segue che $M \subset M_0$, cioè, per le due inclusioni, $M = M_0$.

Osservazione 2.13

Se M è campo di spezzamento su L di un polinomio $f(x) \in K[x]$ e L è generato su K da alcune radici di $f(x)$, allora M è campo di spezzamento di f su K .

Dimostrazione

Sia M_0 il campo di spezzamento di f su K e mostro che $M = M_0$.

Inclusione 1: $f(x) \in K[x]$ si spezza su M , e $K \subseteq L \subseteq M$ quindi $M_0 \subseteq M$ per la minimalità di M_0 .

Inclusione 2: Sia $L = K(\alpha_1, \ldots, \alpha_r)$ con α_i radice di $f(x)$. Allora M_0 contiene K essendo campo di spezzamento di f su K , e contiene tutte le radici di $f(x)$, quindi contiene L .

Si ha quindi $M = M_0$.

2.6 Condizioni equivalenti alla normalità di un'estensione

Teorema 2.5

Sia $M \supseteq K$ un'estensione di grado finito, allora sono equivalenti le seguenti affermazioni:

1. $M \supseteq K$ è un'estensione normale
2. M è separabile su K e M è campo di spezzamento di un polinomio $f(x)$ su K .

3. M è campo di spezzamento su K di un polinomio i cui fattori irriducibili sono separabili.

Dimostrazione

$1 \longrightarrow 2$: **prima mostro che** M **è separabile su** K . Prendo $\alpha \in M$, e considero il suo polinomio minimo $g(x) \in K[x]$. Poiché $g(x)$ ammette una radice $\alpha \in M$ e l'estensione $M \supseteq K$ è normale, allora $g(x)$ si spezza su M in fattori lineari distinti (per un risultato sulle estensioni normali dimostrato parlando di stabilita', precisamente il Lemma 0.2.4 della Lezione del 17 marzo). Allora $g(x)$ è separabile pertanto lo è α . Consideriamo ora una base $\{\alpha_1, \ldots, \alpha_r\}$ per M su K ; siccome $M \supseteq K$ è finita ciascun α_i è algebrico su K , e sia $f_i(x) \in K[x]$ il polinomio minimo di α_i su K . Poniamo $f(x) = f_1(x) * f_2(x) * \cdots * f_r(x) \in K[x]$. **Mostro che** M **è campo di spezzamento di** f **su** K .

Ciascun $f_i(x)$ si spezza su M in fattori lineari (distinti), e quindi anche $f(x)$ si spezza su M in fattori lineari. Osservo che $M = K(\alpha_1, \ldots, \alpha_r)$, infatti ovviamente $K(\alpha_1, \ldots, \alpha_r) \subseteq M$, e viceversa, siccome gli α_i sono una base per M su K , ogni elemento $\xi \in M$ si può scrivere come

$$\xi = \sum_{i=1}^{r} k_i \alpha_i,\ k_i \in K,$$

allora $\xi \in K(\alpha_1, \ldots, \alpha_r)$.

Sia M_0 il campo di spezzamento di $f(x)$ su K . Siccome $f(x)$ si spezza in fattori lineari su M , $M_0 \subseteq M$ per la minimalità di M_0 . Viceversa, $K \subseteq M_0$ e $\alpha_1, \alpha_2, \ldots, \alpha_r \in M_0$ essendo radici di f . Ma M_0 è un campo e quindi contiene $K(\alpha_1, \ldots, \alpha_r) = M$.

$2 \longrightarrow 3$: per ipotesi M è il campo di spezzamento su K di un certo polinomio $f(x)$ a coefficienti in K . Sia

$$f(x) = f_1(x) * f_2(x) * \cdots * f_r(x)$$

la fattorizzazione in irriducibili di $f(x)$ in $K[x]$. Ciascun f_i è il polinomio minimo di ogni sua radice, e le radici di ciascun $f_i(x)$ sono tutte in M . Dall'ipotesi che $M \supseteq K$ è separabile segue che ogni f_i dev'essere separabile.

$3 \longrightarrow 1$: per mostrare che $M \supseteq K$ è normale **è sufficiente mostrare che** $|M : K| = o(G)$ **con** $G = \mathcal{G}(M/K)$. Infatti, sappiamo che $K'' \supseteq K$, e $\mathcal{G}(M/K) = \mathcal{G}(M/K'')$, inoltre $M \supseteq K''$ è sempre normale. Consideriamo la catena di estensioni $M \supseteq K'' \supseteq K$. Allora $|M : K| = |M : K''| * |K'' : K|$; di conseguenza, per la normalità di K'' , $|M : K''| = o(\mathcal{G}(M/K'')) = o(\mathcal{G}(M/K))$, quindi

$$|M : K| = o(G) * |K'' : K|.$$

Se provo che $o(G) = |M : K|$, sostituendo nella formula precedente ottengo che $o(G) = o(G) * |K'' : K|$, cioè $|K'' : K| = 1$ cioè $K'' = K$, e quindi $M \supseteq K$ è normale.

Per mostrare la relazione, **procedo per induzione sul grado di M su K** . Se $M = K$, non c'è niente da dimostrare, perché $G = \{1\}$. Allora posso supporre $M \neq K$. Per ipotesi M è campo di spezzamento su K di un polinomio $f(x)$, i cui fattori irriducibili sono separabili. $M \neq K$ significa che $f(x)$ ammette un fattore $g(x) \in K[x]$ irriducibile di grado $r > 1$. Considero $\alpha \in M$ radice di $g(x)$, che esiste perché M è campo di spezzamento di f , e sia $\Omega = \{\beta \in M \, t.c. \, g(\beta) = 0\}$. $g(x)$ è separabile quindi $|\Omega| = r$.

Pongo $L = K(\alpha)$. $G = \mathcal{G}(M/K)$ agisce su Ω e lo stabilizzatore di α (indicato con G_α) è L' . Allora $|G : L'| = |\alpha^G|$ (cardinalità dell'orbita). Inoltre G **agisce transitivamente su** Ω , infatti dato $\beta \in \Omega$, esiste un isomorfismo $\sigma : K(\alpha) \to K(\beta)$ tale che $\alpha \mapsto \beta$ e $\sigma_{|_K} = 1_K$. M è campo di spezzamento per $f(x)$ su K , e quindi anche per $f(x)$ sia su $K(\alpha)$ che su $K(\beta)$. Allora, per un lemma dimostrato parlando dell'unicità dei campi di spezzamento, σ si solleva a un automorfismo g di M che manda α in β ed è l'identità su K , cioè esiste $g \in G$ con $\alpha^g = \beta$. Allora $\alpha^G = \Omega$, e $|G : L'| = |\alpha^G| = |\Omega| = r$ (relazione 1).

Considero la catena di estensioni $M \supseteq L = K(\alpha) \supseteq K$, e $|M : L| < |M : K|$ perché $r = |M : K| > 1$. M è campo di spezzamento per $f(x)$ su K e quindi anche per $f(x)$ su L . I fattori irriducibili di f in $L[x]$ dividono quelli di $f(x)$ in $K[x]$. Allora siccome i secondi sono separabili, anche i primi sono separabili. Per induzione, $|M : L| = o(\mathcal{G}(M/L)) = o(L')$.

Per concludere, sfruttando l'ipotesi induttiva e il fatto che $|L : K| = r$, si ha

$$|M : K| = |M : L| * |L : K| = o(L') * r = o(L') * |G : L'| = o(G)$$

Da questa dimostrazione si evince il seguente *fatto*: sia $M \supseteq K$ un'estensione di campi, con M campo di spezzamento su K di un certo polinomio $f(x) \in K[x]$. Sia $g(x) \in K[x]$ un polinomio irriducibile e sia

$$\Omega = \{\alpha \in M \, t.c. \, g(\alpha) = 0\}$$

Se $\Omega \neq \emptyset$, allora $\mathcal{G}(M/K)$ agisce *transitivamente* su Ω .

2.7 Esempio di campo di spezzamento non normale

2.7.1 Caratteristica di un campo finito

Dato un campo K possiamo considerare l'applicazione $\eta : \mathbb{Z} \to K$ tale che $\eta(z) = z1_K$. η è un omomorfismo di anelli, e $\mathbb{Z}^\eta \subseteq K$. In particolare, siccome K è un campo, $\mathbb{Z}^\eta$ è un dominio. Se K è finito,

$$\ker \eta := \{z \in \mathbb{Z} \, t.c. \, z * 1_K = 0_K\} \neq \{0\}$$

(se per assurdo fosse $\ker \eta = \{0\}$, K contiene K^η che sarebbe una copia isomorfa di $\mathbb{Z}$ e non sarebbe finito).

Perché $\frac{\mathbb{Z}}{\ker \eta}$ sia un dominio, dev'essere $\ker \eta = (p)$ con p numero primo. Allora si dice che K ha caratteristica p . Notiamo anche che $K^\eta \cong F_p$, dove pongo $F_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$

(campo con p elementi). Identificando K^η con F_p , segue che F_p è un sottocampo di K ; in particolare F_p coincide con il campo primo di K ovvero l'intersezione di tutti i sottocampi di K .

2.7.2 Ordine di un campo finito

K campo finito di caratteristica p avrà necessariamente ordine p^n per un certo $n \geq 1$. Infatti K può essere considerato come spazio vettoriale su F_p . La dimensione di K come spazio vettoriale su F_p dev'essere necessariamente finita, diciamo n , allora esiste una base $\{\alpha_1, \ldots, \alpha_n\}$ per K su F_p . Ogni elemento di K si scrive in modo unico come

$$\sum_{i=1}^{n} a_i \alpha_i, \quad a_i \in F_p.$$

e quindi gli elementi di K sono p^n perché ciascun a_i può essere scelto in p modi.

Teorema 2.6

Un campo K ha p^n elementi se e solo se K è il campo di spezzamento su F_p di $f(x) = x^{p^n} - x$.

Dimostrazione

$1 \longrightarrow 2$: Sia K un campo con $o(K) = p^n$, allora K^* ha $p^n - 1$ elementi ed è un gruppo; segue che per ogni $\alpha \in K^*$, $\alpha^{p^n - 1} = 1$, equivalentemente per ogni $\alpha \in K$, $\alpha^{p^n} = \alpha$. Allora $f(x)$ ha p^n radici distinte in K e pertanto si spezza in fattori lineari su K . Siccome le radici di $f(x)$ costituiscono tutto K abbiamo che K è campo di spezzamento di $f(x)$ su F_p .

$2 \longrightarrow 1$: Viceversa, prendo M campo di spezzamento di $f(x)$ su F_p , sia E l'insieme delle radici di $f(x)$ in M , cioè

$$E = \{\alpha \in M \, t.c. \, \alpha^{p^n} = \alpha\}$$

Affermiamo che E è un campo, infatti:

- $0, 1 \in E$;
- *chiusura rispetto alla somma*: per $\alpha, \beta \in E$, segue che $\alpha + \beta \in E$, infatti

  $$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

  dove nel secondo passaggio ho sfruttato il fatto che il campo ha caratteristica p ;
- *chiusura rispetto al prodotto*: dati $\alpha, \beta \in E$, anche $\alpha\beta \in E$ infatti si ha

  $$(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta;$$

- *chiusura rispetto agli inversi*: per $\alpha \in E$, $-\alpha \in E$ infatti $(-\alpha)^{p^n} = -\alpha^{p^n} = -\alpha$;

se $\alpha \neq 0$, $\alpha^{-1} \in E$ infatti $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$.

Segue che E è un campo, la cardinalità di E è p^n perché $f'(x) = -1$ e quindi $f(x)$ non ha radici multiple.

E contiene F_p , allora E deve necessariamente coincidere con M .

Da quest'ultima proposizione, per i risultati sull'esistenza e unicità dei campi di spezzamento, segue che dati un primo p e un intero $n \geq 1$, esiste sempre un campo di ordine p^n , e due campi di ordine p^n sono isomorfi tra loro.

2.7.3 Normalità delle estensioni finite e gruppo di Galois

Mostriamo che, dati M, K campi finiti, l'estensione $M \supseteq K$ è normale, e $\mathcal{G}(M/K)$ è ciclico.

Mostro prima che basta considerare il caso in cui $K = F_p$: in generale, considero la catena di estensioni $M \supseteq K \supseteq F_p$, allora $M \supseteq F_p$ normale implica $M \supseteq K$ normale. Infatti, sia $M \supseteq F_p$ normale, allora M è campo di spezzamento su F_p di un polinomio i cui fattori irriducibili sono separabili. Allora M è anche campo di spezzamento su K di tale polinomio, e i suoi fattori irriducibili in $K[x]$ devono dividere i fattori irriducibili in $F_p[x]$. Siccome i secondi sono separabili per ipotesi, lo sono anche i primi, e quindi segue che $M \supseteq K$ è normale. Inoltre, se $\mathcal{G}(M/F_p)$ è ciclico, anche $\mathcal{G}(M/K)$, che è un sottogruppo in esso, è ciclico.

Consideriamo allora il caso $K = F_p$, identificando M con F_{p^n} .

NORMALITÀ DI $M \supseteq K$: L'estensione $M \supseteq K$ è normale perché M è campo di spezzamento su F_p di $f(x) = x^{p^n} - x$ che non ha radici multiple. CICLICITÀ DEL GRUPPO DI GALOIS: considero l'omomorfismo di Frobenius $\phi : M \to M$ tale che $\phi(\alpha) = \alpha^p$. Osservo che:

1. ϕ è un omomorfismo perché$\#^*$ $\phi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p+\beta^p = \phi(\alpha)+\phi(\beta)$;$\#^*$ $\phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \phi(\alpha) * \phi(\beta)$.
2. ϕ è iniettivo perché manda 1 in sé, è anche suriettivo perché M è un campo finito;
3. ϕ fissa il campo F_p elemento per elemento, cioè per ogni $a \in F_p$, $\phi(a) = a^p = a$.

Segue quindi che $\phi \in \mathcal{G}(M/K)$.

Determino l'ordine di ϕ e considero le sue potenze: per ogni k , $\phi^k : M \to M$ è tale che $\phi^k(\alpha) = \alpha^{p^k}$. Allora $\phi^n = 1$, perché è tale che $\alpha \mapsto \alpha^{p^n} = \alpha$.

Se per assurdo $o(\phi) < n$, esiste $d < n$ tale che $\phi^d = 1$, allora per ogni $\alpha \in M$ si avrebbe $\alpha^{p^d} = \alpha$: quindi gli elementi di M sarebbero radici del polinomio $f(x) = x^{p^d} - x$; ma questo polinomio ha esattamente p^d radici distinte, e gli elementi di M sono $p^n > p^d$, assurdo. Allora $o(\phi) = n$.

Segue quindi che $\mathcal{G}(M/K)$ contiene $< \phi >= \{1, \phi, \phi^2, \ldots, \phi^{n-1}\}$. Ma $o(\mathcal{G}(M/K)) = |M : K| = n$, e quindi $\mathcal{G}(M/K)$ coincide con il gruppo ciclico generato da ϕ .

Un gruppo ciclico G di ordine n ha uno e un solo sottogruppo ciclico di ordine m per ogni m divisore di n . Allora F_{p^n} ha uno e un solo sottocampo di ordine p^m per ogni m divisore di n .

2.7.4 Esempio di un campo di spezzamento non normale

In caratteristica 0, ogni campo di spezzamento da luogo a una estensione normale perché ogni polinomio irriducibile è separabile.

Non posso nemmeno scegliere di lavorare con campi finiti, infatti **mostro che ogni polinomio irriducibile su un campo finito è anche separabile**. Sia $K = F_p$ e $f(x)$ un polinomio in $K[x]$ monico e irriducibile; sia α una radice di $f(x)$, e considero $K(\alpha) \supseteq K$. Si ha $|K(\alpha) : K| = \text{gr(f(x))} = \text{n}$, allora $K(\alpha) = F_{p^n}$. $F_{p^n} \supseteq F_p$ è normale per le osservazioni precedenti, quindi $K(\alpha) \supseteq K$ è normale, e $f(x)$ ammette una radice in $K(\alpha)$. Segue quindi che $f(x)$ si spezza su $K(\alpha)$ in fattori lineari distinti, e inparticolare è separabile.

Questo argomento si può generalizzare al caso di $K = F_{p^s}$ con s intero.

COSTRUZIONE DEL CAMPO DI SPEZZAMENTO NON NORMALE: Sia $F = F_p$, t un'indeterminata su F e consideriamo $M = F(t)$ campo delle funzioni razionali nell'indeterminata t a coefficienti in F . Sia $K = F(t^p)$, campo delle funzioni razionali nell'indeterminata t^p . Valgono le seguenti osservazioni:

- $t \notin K$, perché se lo fosse, si avrebbe $t = \frac{f(t^p)}{g(t^p)}$ dove $f(t), g(t)$ sono polinomi in $F[t]$, $g \neq 0$. Sia $n = \text{gr(f(t))}$ e $m = \text{gr(g(t))}$, allora

$$t = \frac{f(t^p)}{g(t^p)}$$

$$\longrightarrow t * g(t^p) = f(t^p)$$

  e i gradi dei polinomi ai due membri devono essere uguali, cioè $mp+1 = np$, che non può avvenire.

- $M = K(t)$ **e** $M \supseteq K$ **è un'estensione algebrica semplice**. Mostro che $M = K(t)$, e quindi che valgono le due inclusioni: $K(t) \subseteq M$ perché $K \subseteq M$ e $t \in M$; viceversa, $M = F(t)$, $F \subseteq K$ e quindi $M \subseteq K(t)$.

t è algebrico su K , perché può essere visto come radice del polinomio $\psi(x) = x^p - t^p$, a coefficienti in K .

Inoltre, $\psi(x)$ è il polinomio minimo di t sopra K . Infatti, in M si ha $\psi(x) = (x-t)^p$ (siamo in caratteristica p e $t \in M$). Se esiste una fattorizzazione non banale di $\psi(x)$ in $K[x]$ essa dev'essere della forma:

$$\psi(x) = (x-t)^a * (x-t)^b,\ 0 < a, b < p$$

Sviluppando $(x-t)^a$ ottengo

$$(x-t)^a = \sum_k \binom{a}{k} x^k t^{a-k}$$

$$= x^a - atx^{a-1} + \text{termini di grado minore}$$

Siccome i coefficienti di questo polinomio devono stare in K , in particolare si ha $at \in K$, e siccome $a \neq 0$, $t \in K$, ma questo non avviene per quanto detto prima.

Allora $\psi(x)$ è irriducibile su K ed è il polinomio minimo di t su K . Ha come unica radice t di molteplicità p .

- **Il gruppo $\mathcal{G}(M/K)$ si riduce all'identità**. Infatti, siccome M è un'estensione algebrica semplice di K , si ha $|M : K| = p$. Allora preso $g \in \mathcal{G}(M/K)$, t^g dev'essere radice di $\psi(x)$, però l'unica radice di $\psi(x)$ è t , allora $t^g = t$, cioè g fissa K e fissa t , quindi fissa $M = K(t)$, cioè $g = 1$.
- $M = K(t)$ è campo di spezzamento di $\psi(x)$ su K , e $M \supseteq K$ non è normale perché M non è separabile.

2.8 Chiusura spezzante e chiusura normale

Osservazione 2.14

Siano $M \supseteq L \supseteq K$ estensioni di campi, e supponiamo che M sia campo di spezzamento su L di un polinomio $f(x)$ a coefficienti in K . Supponiamo anche che L si ottenga da K estendendolo con alcune radici di f . Allora M è anche campo di spezzamento su K di f .

Dimostrazione

M è campo di spezzamento di f su L , allora $f(x)$ si spezza in fattori lineari su M . Scriviamo poi $L = K(\alpha_1, \ldots, \alpha_r)$ dove $f(\alpha_i) = 0$ per $i = 1, \ldots, r$. Sia M_0 il campo di spezzamento di $f(x)$ su K , mostro che valgono le due inclusioni:

1. $M_0 \subseteq M$ perché M contiene K e contiene le radici di $f(x)$ essendo campo di spezzamento di $f(x)$ su L .
2. Viceversa, per definizione $K \subseteq M_0$, $\alpha_i \in M_0 \forall i = 1, \ldots, r$ e quindi $L = K(\alpha_1, \ldots, \alpha_r) \subset M_0$; siccome f si spezza su M_0 , $M \subseteq M_0$ per la minimalità di M come campo di spezzamento su L .

Vale la seguente proposizione:

Proposizione 2.6

Sia $M \supseteq K$ un'estensione di grado finito, allora sono equivalenti queste due affermazioni:

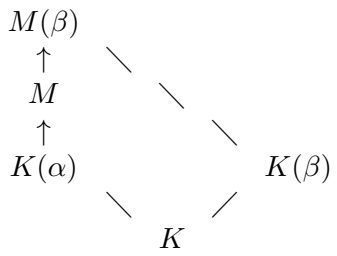
1. M è campo di spezzamento su K (di un certo polinomio a coefficienti in K);
2. per ogni polinomio monico e irriducibile $g(x) \in K[x]$, se $g(x)$ ammette una radice in M , allora $g(x)$ ammette tutte le sue radici in M (o equivalentemente, $g(x)$ si spezza in fattori lineari su M).

Dimostrazione

$1 \longrightarrow 2$: per ipotesi M è campo di spezzamento di un polinomio $f(x)$ su K . Sia $g(x) \in K[x]$ un polinomio monico e irriducibile che ammette una radice α in M . Per assurdo, supponiamo che esista un elemento β con $g(\beta) = 0$ e $\beta \notin M$. Considero il diagramma fatto in questo modo: DESCRIZIONE:

(in particolare M non contiene $K(\beta)$)

RAPPRESENTAZIONE:



Esiste un isomorfismo $\sigma : K(\alpha) \to K(\beta)$ tale che $\alpha \mapsto \beta$ e $\sigma_{|_K} = 1_K$. Considero la catena di estensioni $M \supseteq K(\alpha) \supseteq K$. Osservo che M è campo di spezzamento per $f(x)$ su K , e quindi lo è anche su $K(\alpha)$.

Inoltre $M(\beta)$ è campo di spezzamento per $f(x)$ su $K(\beta)$: infatti sia M_0 il campo di spezzamento di $f(x)$ su $K(\beta)$, allora valgono le due inclusioni:

- $K(\beta) \subseteq M(\beta)$ e $f(x)$ si spezza su $M(\beta)$, allora per la minimalità di M_0 , $M_0 \subseteq M(\beta)$;
- Viceversa, f si spezza su M_0 e $M_0 \supseteq K$, e quindi per la minimalità di M come campo di spezzamento per $f(x)$ su K , $M \subseteq M_0$.

Inoltre $\beta \in M_0$ (M_0 infatti contiene $K(\beta)$) e quindi $M_0 \supseteq M(\beta)$.

Allora σ si solleva a un isomorfismo $\bar{\sigma} : M \to M(\beta)$, tale che $\bar{\sigma}_{|_K} = 1_K$, e che conserva le dimensioni su K , cioè $|M(\beta) : K| = |M : K|$, ma per il teorema della torre vale anche la relazione $|M(\beta) : K| = |M(\beta) : M| * |M : K|$, cioè $|M(\beta) : M| = 1$ e quindi $M(\beta) = M$ e questo è assurdo perché abbiamo scelto $\beta \notin M$.

$2 \longrightarrow 1$: per ipotesi, M è un'estensione di K di grado finito. Considero una base $\{\alpha_1, \ldots, \alpha_r\}$ di M su K , ogni α_i è algebrico su K , allora posso considerare il polinomio minimo $f_i(x) \in K[x]$ di α_i per ogni i . Pongo $f(x) = \prod_{i=1}^{r} f_i(x)$. Ciascun $f_i(x)$ ammette una radice $\alpha_i \in M$; allora per ipotesi $f_i(x)$ si spezza in fattori lineari su M , e lo stesso è vero per $f(x)$. **Voglio mostrare che** M **è campo di spezzamento per** $f(x)$ **su** K . La minimalità segue dal fatto che $M = K(\alpha_1, \ldots, \alpha_r)$ (se M_0 è campo di spezzamento per $f(x)$ su K , sia K che $\alpha_1, \ldots, \alpha_r$ stanno in M_0 , e quindi $M \subseteq M_0$).

Proposizione 2.7 (esistenza della chiusura spezzante)

Sia $L \supseteq K$ è un'estensione di grado finito. Allora esiste M campo tale che $M \supseteq L \supseteq K$ che soddisfa queste due proprietà:

1. M è campo di spezzamento su K ;

2. nessun campo T compreso tra M e L e diverso da M è campo di spezzamento su K .

Inoltre se M_0 è un campo con $M_0 \supseteq L \supseteq K$ e M_0 soddisfa le proprietà 1 e 2, allora esiste un isomorfismo $\sigma : M \to M_0$ tale che $\sigma_{|_L} = 1_L$.

Dimostrazione

Per ipotesi, L è un'estensione di K di grado finito, e quindi posso considerare $\{\alpha_1, \ldots, \alpha_r\}$ base di L su K . Sia $f_i(x) \in K[x]$ il polinomio minimo di α_i su K , e sia $f(x) = \prod_{i=1}^{r} f_i(x)$. Sia M il campo di spezzamento su L di $f(x)$. Mostro che M soddisfa le due richieste della proposizione:

1. L si ottiene estendendo K con alcune radici di $f(x)$, cioè $L = K(\alpha_1, \ldots, \alpha_r)$, e M è campo di spezzamento per $f(x)$ su L . Segue quindi che M è campo di spezzamento di $f(x)$ su K .

2. sia T un campo tale che $K \subseteq L \subseteq T \subseteq M$, e suppongo che T sia campo di spezzamento per $f(x)$ su K . Ora $L \subseteq T$ allora $\alpha_i \in T$ per $i = 1, \ldots, r$ perché $\alpha_i \in L$. Il polinomio minimo $f_i(x)$ di α_i ammette una radice in T , e T è campo di spezzamento su K , perciò $f_i(x)$ si spezza su T . Allora anche $f(x)$ si spezza in fattori lineari su T , e T contiene L , pertanto T contiene M che è campo di spezzameno di $f(x)$ su L . L'altra inclusione vale per ipotesi, allora $M = T$.

Infine, sia M_0 un campo con $M_0 \supseteq L \supseteq K$, che soddisfa le condizioni 1 e 2. Con argomenti analoghi ai precedenti segue che esiste un isomorfismo $\sigma : M \to M_0$ che è l'identità su L , perché M, M_0 sono campi di spezzamento dello stesso polinomio $f(x)$ su L .

Definizione 2.6

Data un'estensione $M \supseteq K$ di grado finito, il campo M di cui la proposizione precedente afferma l'esistenza si dice *chiusura spezzante* di L su K . Se L come estensione di K è separabile, $M \supseteq K$ è normale e in questo caso M si dice *chiusura normale* di L su K .

Osservazione 2.15

Il fatto che se $L \supseteq K$ è separabile allora $M \supseteq K$ è normale è vero perché M è campo di spezzamento su K di $f(x) = \prod_{i=1}^{r} f_i(x)$, dove $f_i(x)$ è il polinomio minimo di $\alpha_i \in L$; se suppongo che L è separabile su K , allora $f_i(x)$ dev'essere un polinomio separabile per ogni i , e quindi M è campo di spezzamento su K di un polinomio i cui fattori irriducibili sono separabili.

Osservazione 2.16 (come ottenere M da L)

Considero una base $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ di L su K e considero il polinomio minimo $f_i(x)$ di α_i , per $i = 1, \ldots, r$. Pongo $f(x) = \prod_{i=1}^{r} f_i(x)$, e sia M il campo di spezzamento di $f(x)$ su L , allora M contiene tutte le radici di ciascun $f_i(x)$.

Siano α_i, β radici di $f_i(x)$. Esiste un isomorfismo $\sigma : K(\alpha_i) \to K(\beta)$ tale che $\alpha_i \mapsto \beta$ e $\sigma_{|_K} = 1_K$. M è anche campo di spezzamento di $f(x)$ su $K(\alpha_i)$ e $K(\beta)$. Allora σ si solleva a un elemento $g \in \mathcal{G}(M/K)$, tale che $\alpha_i^g = \beta \in M$. D'altra parte $\alpha_i^g \in L^g$, e M è generato da $(L^g)_{g \in \mathcal{G}(M/K)}$.

Capitolo 3

Estensioni ciclotomiche

3.1 Estensioni ciclotomiche

3.1.1 Radici primitive dell'unità

Definizione 4.1

Sia $M \supseteq K$ un'estensione di campi, allora $\omega \in M$ con $\omega^n = 1$ si dice *radice n -esima dell'unità*, e si dice *radice primitiva* se $\omega^k \neq 1,\ \forall k = 1, \dots, n-1$.

L'estensione $K(\omega) \supseteq K$ si dice *n -esima estensione ciclotomica*.

Osservazione 4.1

Sia M campo di spezzamento su K di $x^n - 1$. Se K ha caratteristica 0 oppure ha caratteristica p con p numero primo e $p \nmid n$, allora le radici n -esime dell'unità formano un gruppo ciclico di ordine n , che ha $\varphi(n)$ generatori con φ funzione di Eulero (nota $*$), cioè $\varphi(n)$ radici sono primitive.

Infatti, se prendo $\omega, \varepsilon \in M$ con $\omega^n = 1 = \varepsilon^n$, anche il loro prodotto è una radice n -esima dell'unità, quindi le radici n -esime dell'unità formano un sottogruppo del gruppo moltiplicativo del campo. Il polinomio $x^n - 1$ non ha radici multiple quindi ha n radici distinte.

Più in generale,

Lemma 4.1

Dato un sottogruppo finito G del gruppo moltiplicativo K^* di un campo, esso è necessariamente ciclico.

Dimostrazione

Sia $n = o(G) = p_1^{n_1} * p_2^{n_2} * \cdots * p_r^{n_r}$, dove p_i è primo per ogni i e $p_i \neq p_j$ per $i \neq j$.

Considero il polinomio $x^{n/p_i} - 1$, che in K ha al più n/p_i radici.

Siccome G ha n elementi, essi non possono essere tutte radici. Allora esiste $b_i \in G$

con $b_i^{n/p_i} \neq 1$. Definisco

$$a_i = b_i^{\frac{n}{p_i^{n_i}}}, \; i = 1, \ldots, r$$

Osservo che

$$a_i^{p_i^{n_i}} = b_i^n = 1 \longrightarrow o(a_i) \mid p_i^{n_i}$$
$$a_i^{p_i^{n_i-1}} = b_i^{n/p_i} \neq 1 \longrightarrow o(a_i) = p_i^{n_i}.$$

Se pongo $g := a_1 * a_2 * \cdots * a_r$, siccome K^* è commutativo, si ha che $o(g) = l.c.m.(o(a_i))_{i=1,\ldots,r} = l.c.m.(p_i^{n_i})_{i=1,\ldots,r} = n$, cioè g genera G che è ciclico.

3.2 Nota

Si definisce funzione φ di Eulero la funzione
$\varphi : \mathbb{N}^* \to \mathbb{N}^*$ definita da: $\varphi(1) = 1$ e per $n > 1$

$$\varphi(n) := |\{k \in \mathbb{N} \, t.c. \, 0 < k < n \text{ e } M.C.D.(k, n) = 1\}|$$

La funzione di Eulero soddisfa le seguenti proprietà:

1. Se p è primo, $\varphi(p) = p - 1$ e $\varphi(p^n) = p^n - p^{n-1} = p^{n-1} * (p - 1)$.
2. Se $M.C.D.(m, n) = 1$, $\varphi(mn) = \varphi(n) * \varphi(m)$ (φ è moltiplicativa).

Per il teorema fondamentale dell'aritmetica, ogni numero può essere fattorizzato nella forma $n = p_1^{n_1} * p_2^{n_2} * \cdots * p_r^{n_r}$. Quindi per le proprietà precedenti:

$$\varphi(n) = \varphi(p_1^{n_1}) * \varphi(p_2^{n_2}) * \cdots * \varphi(p_n^{n_r})$$
$$= p_1^{n_1-1} * p_2^{n_2-1} * \cdots * p_r^{n_r-1} * (p_1 - 1) * (p_2 - 1) * \cdots * (p_r - 1).$$

Osservazione 4.2

Se K ha caratteristica p , e $p \mid n$, posso scrivere $n = p^s * m$ con $p \nmid m$. Le radici n -esime dell'unità sono radici di $x^n - 1 = x^{p^s * m} - 1 = (x^m - 1)^{p^s}$, e quindi sono radici m -me dell'unita'.

3.2.1 Polinomi ciclotomici

Sia $K = \mathbb{Q}$, per la formula di de Moivre le radici n -esime dell'unità nei complessi sono

$$\omega = \cos(2\pi k/n) + i \sin(2\pi k/n), \; k = 0, \ldots, n - 1$$

(sono i vertici di un n -agono regolare, che ha un vertice in $\omega_0 = (1, 0)$).

Tali radici dividono il cerchio unitario in n archi uguali (da qui il nome di estensione ciclotomica).

Esempio 4.1

- Se $n = 1$, l'unica radice dell'unità è $1 = \cos(2\pi) + i\sin(2\pi)$.
- Se $n = 2$, le radici seconde dell'unità sono $\omega_0 = 1$, $\omega_1 = \cos(\pi) + \sin(\pi) = -1$.
- Se $n = 3$, le radici terze dell'unità sono $\omega_0 = 1$, $\omega_1 = \cos(2\pi/3) + i\sin(2\pi/3) = -1/2 + i\sqrt{3}/2$, $\omega_2 = \cos(4\pi/3) + i\sin(4\pi/3) = -1/2 - i\sqrt{3}/2$.
- Se $n = 4$, le radici quarte dell'unità sono $\omega_0 = 1$, $\omega_1 = \cos(\pi/2) + i\sin(\pi/2) = i$, $\omega_2 = \cos(\pi) + i\sin(\pi) = -1$, $\omega 3 = \cos(3\pi/2) + i\sin(3\pi/2) = -i$.
- Se $n = 8$, le radici ottave dell'unità sono radici di $x^8 - 1 = (x^4 - 1) * (x^4 + 1)$. Tra queste, le radici di $x^4 + 1$ sono quelle primitive, se pongo $\omega = \omega_1 = \cos(\pi/4) + i\sin(\pi/4) = \sqrt{2}/2 + i\sqrt{2}/2$, le radiciprimitive sono della forma ω^k con k coprimo con 8, e sono, oltre a ω stesso

$$\omega^3 = -\sqrt{2}/2 + i\sqrt{2}/2$$

$$\omega^5 = -\sqrt{2}/2 - i\sqrt{2}/2$$

$$\omega^7 = \sqrt{2}/2 - i\sqrt{2}/2.$$

Invece le radici di $x^4 - 1$ non hanno ordine 8 (sono radici quarte di 1).

3.2.2 Polinomio ciclotomico

Definizione 4.2

Si dice *n-esimo polinomio ciclotomico* il polinomio

$$\phi_n(x) := \prod_{\xi \in \Omega_p} (x - \xi)$$

dove chiamo Ω_p l'insieme delle radici n -esime primitive dell'unità.

Se $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$, le radici n -esime primitive dell'unità sono tutte e sole le potenze della forma ω^k con k coprimo con n . Quindi

$$\phi_n(x) = \prod_{M.C.D.(k,n)=1,\, k=0}^{n-1} (x - \omega^k)$$

Esempio 4.2 (esempi di polinomi ciclotomici)

1. Se $n = 1$, l'unica radice prima dell'unità è 1, quindi $\phi_1(x) = x - 1$.

2. Se $n = 2$, le radici seconde dell'unità sono $\omega_1 = 1, \omega_2 = -1$, e solo ω_2 è primitiva, quindi $\phi_2(x) = x + 1$.

3. Se $n = p$ primo, le radici p -esime primitive dell'unità sono tutte le potenze $\omega^k, k = 1, \ldots, p-1$. Quindi

$$\phi_p(x) = \prod_{k=1}^{p-1}(x - \omega^k)$$

con $\omega = \cos(2\pi/p) + i\sin(2\pi/p)$. Siccome $x^p - 1 = \prod_{k=0}^{p-1}(x - \omega^k)$, moltiplicando e dividendo $\phi_p(x)$ per l'unico fattore che manca, cioè per $x - 1$, si ha

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

3.2.3 Calcolo di polinomi ciclotomici

Lemma 4.2

Vale la formula

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

Dimostrazione

Mostro che ω è una radice n -esima dell'unità se e solo se ω è una radice d -esima primitiva dell'unità con d divisore di n .

$1 \longrightarrow 2$: Le radici n -esime dell'unità formano un gruppo ciclico di ordine n generato da ω . Se prendo una potenza ω^k , segue che $o(\omega^k) = \frac{n}{M.C.D.(n,k)}$. Posto $d := \frac{n}{M.C.D.(n,k)}$, d è un divisore di n e ω^k è una radice d -esima primitiva dell'unita'. Dunque ω^k e' una radice di $\phi_d(x)$. $2 \longrightarrow 1$: Viceversa, se α è una radice primitiva d -esima dell'unità, con $d \mid n$, allora $\alpha^d = 1$ e $n = dc$, per un certo $c \in \mathbb{N}$. Allora anche $\alpha^n = 1$, cioè α è una radice n -esima dell'unità.

CONCLUSIONE: Sappiamo che

$$x^n - 1 = \prod_{\varepsilon \in \Omega}(x - \varepsilon)$$

dove chiamo Ω l'insieme delle radici n -esime dell'unità, e sfruttando le osservazioni precedenti, posso raggruppare le radici e scrivere:

$$x^n - 1 = \prod_{d|n} \prod_{o(\varepsilon)=d} (x - \varepsilon).$$

$$= \prod_{d|n} \phi_d(x)$$

Conseguenza: Dato $n = p$ numero primo, si ha

$$x^p - 1 = \prod_{d|p} \phi_d(x) = \phi_1(x) * \phi_p(x)$$

da cui

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Esempio 4.3 (calcolo di polinomi ciclotomici)

1. Se $n = 6$,

$$x^6 - 1 = \prod_{d|6} \phi_d(x) = \phi_1(x) * \phi_2(x) * \phi_3(x) * \phi_6(x)$$

da cui

$$\phi_6(x) = \frac{x^6 - 1}{\phi_1(x) * \phi_2(x) * \phi_3(x)}$$

ma $\phi_1(x) * \phi_3(x) = x^3 - 1$, quindi, fattorizzando anche il numeratore:

$$\phi_6(x) = \frac{(x^3 - 1)(x^3 + 1)}{\phi_2(x) * (x^3 - 1)}$$

$$\phi_6(x) = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

2. Se $n = 4$:

$$x^4 - 1 = \phi_1(x) * \phi_2(x) * \phi_4(x)$$

$$\phi_4(x) = \frac{(x^2 - 1)(x^2 + 1)}{\phi_1(x) * \phi_2(x)}$$

e siccome $\phi_1(x) * \phi_2(x) = x^2 - 1$:

$$\phi_4(x) = x^2 + 1$$

3. Se $n = 8$,

$$\begin{aligned} \phi_8(x) &= \frac{x^8 - 1}{\phi_1(x) * \phi_2(x) * \phi_4(x)} \\ &= \frac{x^8 - 1}{x^4 - 1} \\ &= x^4 + 1 \end{aligned}$$

In particolare, se chiamo $\omega = \cos(\pi/4) + i \sin(\pi/4)$, si ha

$$\phi_8(x) = x^4 + 1 = (x - \omega)(x - \omega^3)(x - \omega^5)(x - \omega^7)$$

3.2.4 Proprietà dei polinomi ciclotomici

Lemma 4.3

Per ogni $n \geq 1$, $\phi_n(x)$ è un polinomio a coefficienti interi, monico di grado $\varphi(n)$.

Dimostrazione

Bisogna dimostrare che $\phi_n(x) \in \mathbb{Z}[x]$, e lo mostriamo per induzione su n .

Per $n = 1$, $\phi_1(x) = x - 1$ e l'asserto è vero. Supponiamo che l'asserto valga per tutti i polinomi ciclotomici $\phi_r(x)$ con $r < n$, e lo dimostriamo per n .

Per il lemma precedente, $x^n - 1 = \prod_{d|n} \phi_d(x)$, allora, separando l'ultimo termine del prodotto, possiamo scrivere

$$x^n - 1 = \phi_n(x) * \prod_{d|n,\, d<n} \phi_d(x)$$

e per induzione per $d < n$ si ha $\phi_d(x) \in \mathbb{Z}[x]$ e quindi, posto $g(x) = \prod_{d|n, d<n} \phi_d(x)$, si ha che $g(x)$ è a coefficienti interi.

Pongo

$$\phi_n(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0,$$
$$g(x) = x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0.$$

Supponiamo per assurdo che $\phi_n(x)$ non sia a coefficienti interi; sia $a_m \notin \mathbb{Z}$, e $a_{r-1}, \ldots, a_{r-2}, \ldots a_{m+1} \in \mathbb{Z}$.

Svolgendo il prodotto $\phi_n(x) * g(x)$ il coefficiente di x^{m+s} è dato da

$$\sum_{i+j=m+s} a_i b_j = a_m + a_{m+1}b_{s-1} + a_{m+2}b_{s-2} + \cdots +$$

ed escluso a_m , gli altri termini della somma sono interi perché i b_i sono interi per induzione e gli $a_i, i > m$ sono interi per costruzione. Ma allora, il fatto che a_m non sia intero è assurdo, perché il risultato del prodotto dev'essere il polinomio $x^n - 1$ che è a coefficienti interi.

Teorema 4.1 (irriducibilità dei polinomi ciclotomici)

Il polinomio $\phi_n(x)$ è irriducibile in $\mathbb{Q}[x]$ per ogni $n \geq 1$.

Dimostrazione

Per il lemma di Gauss, basta dimostrare che il polinomio è irriducibile in $\mathbb{Z}[x]$. Supponiamo che $\phi_n(x)$ si possa scrivere come prodotto $f(x) * g(x)$ con f, g polinomi a coefficienti interi, gr(g(x)) > 0 e $g(x)$ irriducibile (e $f(x)$ e $g(x)$ monici).

Mostriamo che $\phi_n(x) = g(x)$: vogliamo quindi provare che ogni radice n -esima primitiva dell'unità è radice di $g(x)$.

$g(x)$ è un polinomio di grado positivo che ammette una radice nei complessi, cioè esiste $\omega \in \mathbb{C}$ con $g(\omega) = 0$. Allora $\phi_n(\omega) = 0$, e ω è una radice primitiva n -esima dell'unità.

Dobbiamo mostrare che $g(\omega^k) = 0,\ \forall k = 1, \ldots, n$ con $M.C.D.(n, k) = 1$, e consideriamo i due casi seguenti:

1. SIA $K = P$ PRIMO TALE CHE $M.C.D.(N, P) = 1$. Allora ω^p è una radice primitiva n -esima dell'unità, e $\phi_n(\omega^p) = 0 = f(\omega^p) * g(\omega^p)$. Supponiamo che $g(\omega^p) \neq 0$, allora si avrà $f(\omega^p) = 0$. Segue che $f(x^p)$ ammette ω come radice, ma anche $g(x)$ ammette ω come radice, quindi $g(x)$ e $f(x^p)$ hanno in comune il fattore $x - \omega$ .In particolare, $M.C.D.(f(x^p), g(x)) \neq 1$, ma $g(x)$ è irriducibile, e l'unica possibilità è che $g(x) \mid f(x^p)$, cioè vale l'uguaglianza $f(x^p) = g(x) * h(x)$ e il lemma di Gauss ci assicura che $h(x) \in \mathbb{Z}[x]$ .Guardiamo l'ultima uguaglianza in $F_p[x]$, e, indicando con una barra i polinomi coinvolti i cui coefficienti sono stati ridotti modulo p , otteniamo

$$\bar{f}(x^p) = \bar{g}(x) * \bar{h}(x), \text{ uguaglianza } *$$

Mostro che in caratteristica p risulta $\bar{f}(x^p) = (\bar{f}(x))^p$: Sia $\bar{f}(x) = x^r + \bar{a}_{r-1}x^{r-1} + \cdots + \bar{a}_1 x + \bar{a}_0$, allora

$$\begin{aligned}\bar{f}(x^p) &= x^p + (\bar{a}_{r-1}x^p)^{r-1} + \cdots + \bar{a}_1 x^p + \bar{a}_0 \\ &= x^{pr} + \bar{a}_{r-1}^p x^{p(r-1)} + \cdots + \bar{a}_1^p x^p + \bar{a}_0^p \\ &= (x^r + \bar{a}_{r-1}x^{r-1} + \cdots + \bar{a}_1 x + a_0)^p = (\bar{f}(x))^p.\end{aligned}$$

Allora l'uguaglianza $*$ si riscrive come

$$(\bar{f}(x))^p = \bar{g}(x) * \bar{h}(x)$$

Se considero $\bar{s}(x)$ un fattore irriducibile di $\bar{g}(x)$ ($\bar{g}(x)$ potrebbe non essere irriducibile in F_p !), segue che $\bar{s}(x) \mid \bar{f}(x)$ .Abbiamo anche che $x^n - 1 = \phi_n(x) * q(x)$, e quindi $x^n - 1 = f(x) * g(x) * q(x) \in \mathbb{Z}[x]$, allora in F_p :

$$\overline{x^n - 1} = \bar{f}(x) * \bar{g}(x) * \bar{q}(x)$$

e dal fatto che $\bar{g}(x), \bar{f}(x)$ hanno un fattore irriducibile in comune, segue che $\overline{x^n - 1}$ ha una radice di molteplicità maggiore di 1. Ma questo e' assurdo, perché la derivata di $\overline{x^n - 1}$ è $nx^{n-1} \neq 0$ perché $p \nmid n$. Quindi $f(\omega^p) \neq 0 \in \mathbb{Q}$, rimane allora provato che $g(\omega^p) = 0$.

2. SIA K TALE CHE $M.C.D.(N, K) = 1$. Allora $k = p_1 * \cdots * p_s$ dove i p_i sono numeri primi non necessariamente distinti. Per la parte precedente, ω^{p_1} è radice di $g(x)$, perché $p_1 \nmid n$ ed è primo. Posso quindi applicare nuovamente la parte precedente con ω^{p_1} radice di $g(x)$ e $k = p_2$, eottengo che anche $(\omega^{p_1})^{p_2}$ è radice di $g(x)$ . ... Procedendo in questo modo, arrivo a dire che ω^k è radice di $g(x)$.

3.2.5 Gruppo di Galois di un'estensione ciclotomica

Sia $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$ e considero $\mathbb{Q}(\omega)$. E' chiaro che $\mathbb{Q}(\omega) = \mathbb{Q}(\varepsilon)$ per ogni ε radice primitiva n -esima dell'unita'. Poi $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ è normale, perché $\mathbb{Q}(\omega)$ è campo di spezzamento su $\mathbb{Q}$ di $x^n - 1$.

Il gruppo $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ può essere descritto in due modi (equivalenti):

1. come il gruppo degli automorfismi di un gruppo ciclico C di ordine n , indicato con $Aut(C)$.
2. come il gruppo degli elementi invertibili dell'anello $\mathbb{Z}/n\mathbb{Z}$, indicato con U_n .

Sia C un gruppo ciclico di ordine n , generato da a , e sia α un automorfismo di C in sé. Allora α è determinato da $\alpha(a)$, e $\alpha(a) = a^k$ con $o(a) = o(a^k)$ e quindi $M.C.D.(k, n) = 1$. Viceversa, se h è tale che $M.C.D.(n, h) = 1$, l'omomorfismo da C in C , definito da $\alpha(a) = a^h$ determina un automorfismo di C . Quindi $|Aut(C)| = \varphi(n)$.

Mostriamo che $Aut(C) \cong U_n$.

Possiamo assumere che $C = (\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$. Se $u \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ è invertibile, considero l'applicazione $\phi_u : C \to C$ che manda a in au , allora:

1. ϕ_u **è un automorfismo di** $\frac{\mathbb{Z}}{n\mathbb{Z}}$ **additivo**, infatti
$$\phi_u(a + b) = (a + b)u = au + bu = \phi_u(a) + \phi_u(b).$$
2. ϕ_u **è iniettiva**, infatti $\phi_u(a) = \phi_u(b)$ implica $ua = ub$ e moltiplicando per u^{-1} ottengo $a = b$;
3. ϕ_u **è suriettivo**: infatti, dato $b \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, esso ha come preimmagine bu^{-1} , infatti si ha $\phi_u(bu^{-1}) = b$.

Allora $\phi_u \in Aut(C)$.

L'applicazione che manda $u \in U_n$ **in** $\phi_u \in Aut(C)$ **è un omomorfismo iniettivo di gruppi, da** U_n **a** $Aut(C)$. Infatti, se $u \mapsto 1$ (cioe' se $\phi(u) = \phi_u = 1$) allora $au = a$ per ogni $a \in C$. In particolare per $a = 1$ si ha $1 * u = 1$ cioè $u = 1$, quindi l'omomorfismo ϕ e' iniettivo. Inoltre $o(U_n) = \varphi(n) = o(Aut(C))$ allora $U_n \cong Aut(C)$.

Concludiamo provando che $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong Aut(C)$ dove C è il gruppo ciclico di ordine n generato da ω .

Infatti, dato $g \in \mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$, ω^g e' ancora una radice n -esima dell'unita', ovvero $\omega^g \in C$. Considero la mappa $\phi : \mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \to Aut(C)$ tale che $g \mapsto g_{|_C}$. Questo omomorfismo di gruppi è iniettivo, infatti dati $g, h \in \mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$, $g_{|_C} = h_{|_C}$ implica $\omega^g = \omega^h$, e quindi g, h coincidono su tutto $\mathbb{Q}(\omega)$ (infatti, essendo elementi di $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$, essi fissano $\mathbb{Q}$ elemento per elemento e quindi coincidono su $\mathbb{Q}(\omega)$). La conclusione segue dal fatto che, siccome il polinomio ciclotomico $\phi_n(x)$ è il polinomio minimo di ω su $\mathbb{Q}$, si ha $o(\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})) = |\mathbb{Q}(\omega) : \mathbb{Q}| = \varphi(n)$, e quindi $o(\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})) = o(Aut(C))$.

In particolare U_n è sempre abeliano, e se $n = p$, U_p è un gruppo ciclico di ordine $p - 1$.

3.3 Complementi sui polinomi ciclotomici

3.3.1 Applicazione 1 caso particolare del teorema di Dirichlet

Usando i polinomi ciclotomici si può dimostrare un caso particolare del teorema di Dirichlet.

Teorema 4.2 (teorema di Dirichlet)

Siano m, n numeri interi positivi primi tra loro. Allora esistono infiniti numeri primi p congrui a m modulo n , cioè della forma $m + nk$, $k \in \mathbb{Z}$.

Nel caso particolare in cui $m = 1$, si ha

Teorema 4.3

Sia $n > 0$ un intero, allora esistono infiniti numeri primi p con $p \equiv 1 \mod n$.

Premettiamo alcuni risultati sui polinomi ciclotomici.

Lemma 4.4

Sia p un numero primo, tale che $p \mid \phi_n(m)$, $n, m \geq 1$. Allora

1. $p \nmid m$;
2. se $p \nmid n$, allora $p \equiv 1 \mod n$.

Dimostrazione

1. Sappiamo che $\phi_n(x) \mid x^n - 1$ in $\mathbb{Z}[x]$, allora valutando in m si ha che $\phi_n(m) \mid m^n - 1$ in $\mathbb{Z}$. Per ipotesi $p \mid \phi_n(m)$ quindi $p \mid m^n - 1$ (formula 1), allora $m^n \equiv 1 \mod p$, pertanto p non può dividere m (altrimenti si avrebbe $m^n \equiv 0 \mod p$), e quindi la prima affermazione è vera.
2. Per ipotesi, $p \nmid n$, allora m definisce un elemento $\bar{m} \in (\mathbb{Z}/(p\mathbb{Z}))^*$: sia d l'ordine di $\bar{m}$ in $(\mathbb{Z}/(p\mathbb{Z}))^*$. Siccome $|(\mathbb{Z}/(p\mathbb{Z}))^*| = p - 1$, $d \mid p - 1$, cioè $p \equiv 1 \mod d$. L'asserto vale se **mostro che** $d = n$ .Per quanto detto $m^d \equiv 1 \mod p$ e per la formula 1 $m^n \equiv 1 \mod p$, allora $d \mid n$ (infatti $d = o(\bar{m})$ e quindi è il minimo intero tale che $(\bar{m})^d = 1$); posso quindi scrivere $n = d * e$, con $e > 0$.**Mostriamo che, se** $e > 1$ **, arriviamo all'assurdo che** $p \mid n$ **, contro l'ipotesi**. Siccome stiamo supponendo $e > 1$, allora d è un divisore proprio di n , e posso scrivere

$$x^n - 1 = \prod_{t|n} \phi_t(x) = \phi_n(x) * \prod_{t|n, t<n} \phi_t(x)$$

e raggruppando i divisori di d :

$$= \phi_n(x) * [\prod_{s|d} \phi_s(x)] * [\prod_{t<n, t|n,\, t\nmid d} \phi_t(x)]$$

e $\prod_{s|d} \phi_s(x) = x^d - 1$, quindi complessivamente

$$x^n - 1 = \phi_n(x) * (x^d - 1) * g(x),\ g(x) \in \mathbb{Z}[x]$$

$$\longrightarrow \phi_n(x) * g(x) = \frac{x^n - 1}{x^d - 1} = \frac{(x^d)^e - 1}{x^d - 1}$$

$$= (x^d)^{e-1} + (x^d)^{e-2} + \cdots + x^d + 1$$

e se valuto in m , in $\mathbb{Z}$ si ha

$$\phi_n(m) \mid (m^d)^{e-1} + (m^d)^{e-2} + \cdots + m + 1$$

e, siccome $p \mid \phi_n(m)$, $p \mid (m^d)^{e-1} + (m^d)^{e-2} + \cdots + m^d + 1$, ma $m^d \equiv 1$ mod p , e quindi $p \mid 1 + 1 + \cdots + 1 = e$ (sommo 1 per e volte).D'altra parte, $n = d * e$, e quindi $p \mid e \longrightarrow p \mid n$, e questo è assurdo per quanto detto sopra.

Corollario 4.1

Sia $n \geq 1$, e p un divisore primo di $\phi_n(n)$. Allora $p \equiv 1 \mod n$.

Dimostrazione

Applico la prima parte del lemma precedente con $m = n$, allora $p \nmid n$. Siccome è vera l'ipotesi della seconda parte, segue che $p \equiv 1 \mod n$.

Lemma 4.5

Sia $n > 1$, allora per ogni $x \in \mathbb{R}$ con $x \geq 2$, si ha che $|\phi_n(x)| > x - 1$.

Dimostrazione

Considero il cerchio unitario e un punto $x \geq 2$ sull'asse reale, siccome $x > 1$ esso sta fuori dalla circonferenza unitaria. Se $\omega \neq 1$ è una radice n -esima dell'unità che sta sul cerchio unitario, $d(x, \omega) = |x - \omega| > x - 1$, quindi

$$|\phi_n(x)| > (x - 1)^{\varphi(n)} \geq x - 1$$

(l'ultima disuguaglianza vale perché $x \geq 2$ implica $x - 1 \geq 1$)

Osservazione 4.3

Se $M.C.D.(m, n) = 1$, allora $U_{mn} \cong U_n \times U_m$.

Dimostrazione

Considero l'applicazione $\phi \colon \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}$ tale che $a \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$, che è un isomorfismo di anelli, di nucleo $m * n\mathbb{Z}$. Allora $\frac{\mathbb{Z}}{\ker \phi} = \frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}$.

Dimostriamo ora il teorema enunciato precedentemente:

Teorema 4.4

Per ogni intero positivo n , esistono infiniti numeri primi p tali che $p \equiv 1 \mod n$.

Dimostrazione

Per $n = 1$ questo è il teorema di Euclide (esistono infiniti numeri primi), quindi possiamo assumere $n > 1$.

Per ogni $k \geq 1$, pongo $N_k = \phi_{nk}(nk) \in \mathbb{Z}$.

Siccome $n \geq 2, k \geq 1$ allora $nk \geq 2$ e applicando il secondo lemma, $|N_k| > nk - 1 \geq 1$, cioè $|N_k| > 1$.

Sia p_k un divisore primo di N_k , che esiste perché $|N_k| > 1$. Per il corollario al primo lemma, $p_k \equiv 1 \mod nk$, e in particolare $p_k \equiv 1 \mod n$.

Per garantire che posso trovare infiniti numeri primi p_k osservo che $p_k \equiv 1 \mod nk$ e $p_k \neq 1$, allora $p_k > nk$. Dunque trovo numeri primi arbitrariamente grandi, e questo mi assicura che ne trovo infiniti.

3.3.2 Applicazione 2 problema inverso di Galois

Teorema 4.5

Sia G un gruppo abeliano finito, allora esiste $M \subseteq \mathbb{C}$ tale che $M \supseteq \mathbb{Q}$ è normale e $\mathcal{G}(M/\mathbb{Q}) \cong G$.

Dimostrazione

Per il teorema di struttura dei gruppi abeliani $G \cong C_1 \times C_2 \times \cdots \times C_r$ dove C_i è un gruppo ciclico di ordine n_i .

Per il caso particolare del teorema di Dirichlet esistono $p_1, p_2, \ldots, p_r$ primi distinti, con $p_i \equiv 1 \mod n_i, \forall i$. Sia $n = p_1 * p_2 * \cdots * p_r$, e sia ω una radice n - esima primitiva dell'unità. Considero l'estensione ciclotomica $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$. Allora $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U_n$, e per l'osservazione, siccome n è il prodotto di numeri primi tra loro, $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U_{p_1} \times U_{p_2} \times \cdots \times U_{p_r}$ (relazione 1).

U_{p_i} è un gruppo ciclico di ordine $p_i - 1$, ma $p_i \equiv 1 \mod n_i$, allora $n_i \mid p_i - 1$, e (siccome il teorema di Lagrange si invferte nei gruppi ciclici) esiste un (unico) sottogruppo W_i di U_{p_i} di indice n_i . Allora $G \cong \frac{U_{p_1}}{W_1} * \frac{U_{p_2}}{W_2} * \cdots * \frac{U_{p_r}}{W_r}$.

Per la relazione 1, $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U_{p_1} \times U_{p_2} \times \cdots \times U_{p_r}$ e quindi $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ contiene un sottogruppo H tale che $\frac{\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})}{H} \cong G$.

Pongo $M = H'$ allora M è un campo intermedio tra $\mathbb{Q}(\omega)$ e $\mathbb{Q}$. Poi H è normale in $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ e, per il teorema fondamentale della teoria di Galois, $M \supseteq \mathbb{Q}$ è normale con $\mathcal{G}(M/\mathbb{Q}) \cong \frac{\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})}{H}$. Ma, per quanto detto prima, $\frac{\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})}{H} \cong G$, allora $\mathcal{G}(M/\mathbb{Q}) \cong G$, cioè M è il campo cercato.

Capitolo 4

Costruzioni con righe e compasso

4.1 Definizioni di base

4.1.1 Regole

Supponiamo di avere due punti (distinti) A e B nel piano. Vogliamo costruire altri punti nel piano utilizzando due strumenti:

1. la riga, cioè possiamo costruire la retta passante per A e B ;
2. il compasso, cioè possiamo costruire la circonferenza di centro A passante per B .

Otteniamo un nuovo punto C in tre modi:

1. come intersezione tra due rette,
2. come intersezione tra due circonferenze,
3. come intersezione tra una retta e una circonferenza.

Nel seguito useremo le seguenti costruzioni:

COSTRUZIONE C_1 : data una retta $\mathcal{R}$ e due punti A e B su $\mathcal{R}$, possiamo costruire la **retta $\mathcal{L}$ perpendicolare a $\mathcal{R}$ e passante per il punto medio tra A e B** con le seguenti operazioni:

- disegno la retta $\mathcal{R}$ e i due punti A e B su $\mathcal{R}$ (supponiamo che A sia a sinistra di B);
- costruisco la circonferenza $\mathcal{C}_1$ di centro B e passante per A ;
- costruisco la circonferenza $\mathcal{C}_2$ di centro A e passante per B ;
- chiamo C e D i due punti di intersezione tra le circonferenze $\mathcal{C}_1$ e $\mathcal{C}_2$;

- chiamo $\mathcal{L}$ la retta passante per C e D : $\mathcal{L}$ è la retta cercata (mia nota: C e D sono equidistanti da A e B).

COSTRUZIONE C_2 : data una retta $\mathcal{R}$ e due punti A, B su $\mathcal{R}$, posso costruire la **retta $\mathcal{L}$ perpendicolare a $\mathcal{R}$ e passante per $B \in \mathcal{R}$** con le seguenti operazioni:

- costruisco la circonferenza $\mathcal{C}$ di centro B passante per A ;
- chiamo A' l'ulteriore punto di intersezione tra $\mathcal{R}$ e $\mathcal{C}$, $A' \neq A$;
- applico la costruzione C_1 alla retta $\mathcal{R}$ e ai punti A, A' e ottengo la retta cercata: infatti B è punto medio tra A e A' .

COSTRUZIONE C_3 : data una retta $\mathcal{R}$, un punto $A \in \mathcal{R}$ e un punto $B \notin \mathcal{R}$, posso costruire la **retta $\mathcal{L}$ che passa per $B \notin \mathcal{R}$ ed ortogonale ad $\mathcal{R}$** con le seguenti operazioni: (disegno $\mathcal{R}$ orizzontale e B sopra $\mathcal{R}$)

- costruisco la circonferenza $\mathcal{C}$ di centro B passante per A ;
- chiamo A' l'ulteriore punto di intersezione tra $\mathcal{C}$ ed $\mathcal{R}$, $A' \neq A$;
- $\mathcal{L}$ si ottiene applicando la costruzione C_1 a $\mathcal{R}$, A , A' : i segmenti AB e $A'B$ infatti sono uguali perché sono raggi della circonferenza, e quindi la retta che passa per il punto medio di AA' passa anche per B .

COSTRUZIONE C_4 : data una retta $\mathcal{R}$, un punto $A \in \mathcal{R}$ e $B \notin \mathcal{R}$, posso costruire la **retta $\mathcal{L}$ parallela a $\mathcal{R}$ e passante per B** con le seguenti operazioni:

- applicando la costruzione C_3 disegno la retta $\mathcal{S}$ passante per $B \notin \mathcal{R}$ e ortogonale a $\mathcal{R}$;
- chiamo A' il punto di intersezione tra $\mathcal{S}$ e $\mathcal{R}$.
- applicando la costruzione C_2 a $\mathcal{S}$, A', B , disegno la retta $\mathcal{L}$ perpendicolare a $\mathcal{S}$, passante per B ;

4.1.2 Campo dei punti costruibili

Dati due punti A, B , posso costruire un riferimento cartesiano nel piano, chiamo x la retta passante per A e B . Con la costruzione C_2 costruisco la retta y perpendicolare a x e passante per A . Pongo $d(A, B) = 1$, in modo che $A = (0, 0)$ e $B = (1, 0)$.

Se $a \in \mathbb{R}$, allora a è costruibile se il punto di coordinate $(a, 0)$ è costruibile (tramite un numero finito di operazioni con riga e compasso).

Dato un numero $\alpha = a + ib \in \mathbb{C}$, α è costruibile se (a, b) è costruibile.

Tutti i numeri interi sono costruibili, infatti:

- se costruisco la circonferenza $\mathcal{C}$ di centro $(1,0)$ passante per $(0,0)$, ottengo $(2,0)$ come punto di intersezione tra $\mathcal{C}$ e l'asse x ;
- se procedo in questo modo posso costruire tutti gli interi: in particolare, al passo n , il punto $(0,n)$ si ottiene come punto di intersezione tra l'asse x e la circonferenza di centro $(n-1,0)$ passante per $(n-2,0)$.

Teorema 5.1

Sia $K = \{a \in \mathbb{R}\, t.c.\, a\, costruibile\}$ allora K è un sottocampo di $\mathbb{R}$.

Dimostrazione

Dati $a, b \in K$, devo mostrare che $-a, a+b, a*b, a^{-1}$ sono ancora in K .

opposto siccome $(0,0)$ è costruibile e per ipotesi $a \in K$, posso costruire la circonferenza $\mathcal{C}$ di centro $(0,0)$ e passante per $(a,0)$; il punto di intersezione tra $\mathcal{C}$ e l'asse x diverso da $(a,0)$ è $(-a,0)$, quindi $-a \in K$.

somma Assumiamo $a, b, > 0$, $b > a$. Eseguo le seguenti operazioni:

- Costruisco $(0,1)$ come punto di intersezione tra l'asse y e la circonferenza di centro nell'origine e passante per $(1,0)$;
- costruisco la retta $\mathcal{S}$ ortogonale all'asse x e passante per $(b,0)$ usando la costruzione C_2 ;
- costruisco la retta $\mathcal{R}$ passante per $(0,1)$ e parallela all'asse x usando la C_4 : osservo che il punto di intersezione tra $\mathcal{S}$ e $\mathcal{R}$ è $(b,1)$;
- costruisco la retta $\mathcal{T}$ passante per $(0,1)$ e $(a,0)$;
- costruisco la retta $\mathcal{L}$ parallela a $\mathcal{T}$ e passante per $(b,1)$ con la C_4 ;

$\mathcal{L}$ interseca l'asse delle x in un punto di coordinate $(a+b,0)$ (è il quarto vertice di un parallelogramma, i cui altri vertici sono $(b,1)$, $(0,1)$ e $(a,0)$). Quindi $a+b \in K$.

prodotto eseguo le seguenti operazioni:

- costruisco i punti $(0,b)$ e $(a+1,0)$ (questo è possibile perché $a \in K$ per ipotesi e $1 \in K$ essendo un intero, quindi per il punto precedente $a+1 \in K$);
- traccio la retta $\mathcal{R}$ passante per $(1,0)$ e $(0,b)$;
- applicando C_4 traccio la retta $\mathcal{S}$ parallela a $\mathcal{R}$ passante per $(a+1,0)$;

Ora scrivo le equazioni di $\mathcal{R}$ e $\mathcal{S}$

$$\mathcal{R} : y - b = \frac{b-0}{0-1} * x$$
$$\mathcal{R} : y = b(1-x)$$

$\mathcal{S}$ è parallela a $\mathcal{R}$ e ha coefficiente angolare $-b$, quindi

$$\mathcal{S} : y = -bx + q$$

e imponendo che $\mathcal{S}$ passi per $(a+1, 0)$:

$$0 = -b * (a+1) + q, \longrightarrow q = b * (a+1)$$

quindi

$$\mathcal{S} : y = -bx + ab + b$$

Il punto di intersezione tra $\mathcal{S}$ e l'asse y è $(0, ab+b)$. Per i punti precedenti, $ab + b \in K \longrightarrow ab \in K$.

inverso a^{-1} ($a \neq 0$)

- costruisco $(0, a)$ e $(0, a+1)$ sull'asse y ;
- chiamo $\mathcal{R}$ la retta passante per $(0, a)$ e $(1, 0)$;
- traccio la retta $\mathcal{S}$ parallela a $\mathcal{R}$ passante per $(0, a+1)$.

Scrivo l'equazione della retta $\mathcal{S}$:

$$m_{\mathcal{R}} = m_{\mathcal{S}} = \frac{a-0}{0-1} = -a$$
$$\mathcal{S} : y = -ax + a + 1$$

allora il punto di intersezione tra $\mathcal{S}$ e l'asse x è $(1+1/a, 0)$, e per i punti precedenti posso costruire $1/a$, cioè $a^{-1} \in K$.

Osservazione 5.1

Dato un numero complesso $\alpha = a + ib$, esso è costruibile se e solo se lo sono a e b .

Dimostrazione

$2 \longrightarrow 1 : a, b \in K$ implica che sono costruibili i punti $(a, 0)$ e $(0, b)$. Traccio la parallela all'asse x passante per $(0, b)$ e la parallela all'asse y passante per $(a, 0)$, α è il punto di intersezione tra queste due parallele.

$1 \longrightarrow 2$: viceversa, se α è costruibile e traccio le parallele agli assi cartesiani e passanti per α , ottengo come punti di intersezione $(a, 0)$ e $(0, b)$, e quindi $a, b \in K$.

Corollario 5.1

Dato $K = \{\alpha \in \mathbb{C}\, t.c.\, \alpha\, costruibile\}$, allora K è un sottocampo di $\mathbb{C}$.

Dimostrazione

Dati $\alpha, \beta \in K$ della forma $\alpha = a + ib$, $\beta = c + id$, allora $\alpha + \beta = (a + c) + i(b + d)$, e siccome le componenti $a + c$ e $b + d$ sono costruibili, anche $\alpha + \beta$ è costruibile. Si applica lo stesso ragionamento per i prodotti, gli inversi e gli opposti.

4.2 Criterio per la costruibilità

4.2.1 Lemmi preliminari

Considereremo sottocampi $F \subseteq \mathbb{C}$ tali che

1. F contiene l'unità immaginaria, cioè $i \in F$;
2. F è chiuso rispetto al coniugio, cioè se $z \in F$, anche $\bar{z} \in F$.

Lemma 5.1

Sia $F \subseteq \mathbb{C}$ un campo che soddisfa le proprietà 1 e 2. Siano $z_1 = x_1 + iy_1$ e $z_2 = x_2 + iy_2$ due elementi di F , allora

1. $x_1, x_2, y_1, y_2 \in F$;
2. se $y = \alpha x + \beta$ è l'equazione della retta che passa per (x_1, y_1) e (x_2, y_2) , allora $\alpha, \beta \in F$.
3. se $(x - x_1)^2 + (y - y_1)^2 = r^2$ è l'equazione della circonferenza di centro (x_1, y_1) e passante per il punto di coordinate (x_2, y_2) , allora $r^2 \in F$.

Dimostrazione

1. $z_1 \in F$, e siccome F è chiuso per coniugio, anche $\bar{z}_1 = x_1 - iy_1 \in F$, allora siccome F è chiuso rispetto alla somma e alla differenza, si ha $z_1 + \bar{z}_1 = 2x_1 \in F$, e $z_1 - \bar{z}_1 = 2iy_1 \in F$. Di conseguenza, siccome $i \in F$ e $2 \in F$, anche $x_1, y_1 \in F$, e lo stesso vale per x_2, y_2 .
2. Se $y = \alpha x + \beta$ è la retta che passa per (x_1, y_1) e (x_2, y_2) , segue che $y_1 = \alpha x_1 + \beta$ e $y_2 = \alpha x_2 + \beta$, allora, facendo la differenza tra queste due condizioni, si ha
$$y_1 - y_2 = \alpha(x_1 - x_2)$$

$$\longrightarrow \alpha = \frac{y_1 - y_2}{x_1 - x_2}$$

quindi $\alpha \in F$, perché è espressa come somma e differenza e prodotto di elementi che per il punto 1 stanno in F . Di conseguenza, siccome per la prima equazione $\beta = y_1 - \alpha x_1$ si ha anche $\beta \in F$.

3. Se $(x-x_1)^2+(y-y_1)^2 = r^2$ è l'equazione della circonferenza di centro (x_1, y_1) e passante per (x_2, y_2) , sostituendo le coordinate di (x_2, y_2) nell'equazione segue che
$$r^2 = (x_1 - y_1)^2 + (x_2 - y_2)^2$$
cioè $r^2 \in F$.

Lemma 5.2

Sia $F \subseteq \mathbb{C}$ un campo che soddisfa le proprietà 1 e 2. Sia $z = u + iv \in \mathbb{C}$, dove (u, v) si ottiene come intersezione di

1. due rette definite a partire da punti in F ,
2. retta e circonferenza definite a partire da punti in F ,
3. due circonferenze definite a partire da punti di F .

Allora $|F(z) : F| \leq 2$.

Dimostrazione

Distinguiamo i tre casi:

1. (u, v) **è punto di intersezione di due rette**, $y = \alpha_1 x+\beta_1$ e $y = \alpha_2 x+\beta_2$. Per il lemma precedente $\alpha_1, \alpha_2, \beta_1, \beta_2 \in F$, allora
$$\begin{cases} v = \alpha_1 u + \beta_1 \\ v = \alpha_2 u + \beta_2 \end{cases}$$
e, sottraendo tra loro le due equazioni, ottengo
$$(\alpha_1 - \alpha_2)u = \beta_1 - \beta_2, \longrightarrow u = \frac{\beta_1 - \beta_2}{\alpha_1 - \alpha_2}$$
cioè $u \in F$. Per la prima equazione anche $v \in F$. Siccome F contiene l'unità immaginaria, $z \in F$ e quindi $F(z) = F$ e l'estensione ha grado 1.

2. (u, v) **è punto d'intersezione tra la retta di equazione** $y = \alpha x+\beta$ **e la circonferenza di equazione** $(x-a)^2+(y-b)^2 = r^2$ .Allora $\alpha, \beta, a, b, r^2 \in F$ per il lemma precedente. Sostituendo le coordinate di (u, v) nelle due equazioni ottengo
$$\begin{cases} v = \alpha u + \beta \\ (u - a)^2 + (v - b)^2 = r^2 \end{cases}$$
e sostituendo la prima equazione nella seconda ottengo
$$(u - a)^2 + (\alpha u + \beta - b)^2 = r^2$$

Quest'equazione è di secondo grado e ha coefficienti in F . Allora $|F(u) : F| \leq 2$ .Inoltre $v = \alpha u + \beta$, $\longrightarrow v \in F(u)$, si ha che $i \in F$, quindi $z = u + iv \in F(u)$, quindi $|F(z) : F| \leq 2$.

3. (u, v) **si ottiene come punto di intersezione di due circonferenze**,

$$\mathcal{C}_1 : x^2 + y^2 + ax + by + c = 0$$

$$\mathcal{C}_2 : x^2 + y^2 + \alpha x + \beta y + \gamma = 0$$

Allora (u, v) soddisfa l'equazione ottenuta sottraendo $\mathcal{C}_1$ a $\mathcal{C}_2$, cioè

$$(a - \alpha)x + (b - \beta)y + c - \gamma = 0$$

che è l'equazione di una retta, e quindi ci si riconduce al caso 2.

4.2.2 Condizione necessaria e sufficiente per la costruibilità

Teorema 5.2

Un numero complesso $z \in \mathbb{C}$ è costruibile se e solo se esiste una catena di campi della forma $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$, dove $z \in K_r$, e $|K_{i+1} : K_i| \leq 2$.

Dimostrazione

$1 \longrightarrow 2$: Supponiamo che z sia costruibile, allora esiste una successione

$$0,\ 1,\ z_1 = i,\ z_2, \ldots, z_s = z$$

dove gli z_i sono numeri complessi tali che z_{i+1} si ottiene come punto di intersezione di retta-retta, retta-circonferenza o circonferenza-circonferenza, definite a partire dagli elementi precedenti della successione, cioè a partire dai punti $0, 1, z_1, \ldots, z_i$.

Definiamo

$$E_0 = F_0 := \mathbb{Q}$$

$$E_1 = F_1 := \mathbb{Q}(i).$$

$$\textit{Supponendo di aver definito } E_i, \textit{ definiamo}$$

$$F_{i+1} = E_i(z_{i+1});\ E_{i+1} = F_{i+1}(\bar{z}_{i+1})$$

Supponiamo di aver dimostrato che E_i contenga l'unità immaginaria e sia chiuso per coniugio. Allora vogliamo provare che

1. $|F_{i+1} : E_i| \leq 2$
2. $|E_{i+1} : F_{i+1}| \leq 2$
3. anche E_{i+1} soddisfa le proprietà 1 e 2.

L'affermazione I) è vera perché E_i e z_{i+1} soddisfano le ipotesi del lemma 2. L'unita' immaginaria i è contenuta in ogni E_j . Per dimostrare le affermazioni I) e II) distinguiamo due casi:

- $Z_{i+1} \in E_i$, e quindi $F_{i+1} = E_i(z_{i+1}) = E_i$. Per ipotesi, E_i è chiuso per coniugio, quindi $\bar{z}_{i+1} \in E_i$, segue anche che $E_{i+1} = E_i$; per quest'ultimo fatto, ovviamente si ha $|E_{i+1} : F_{i+1}| = 1 \leq 2$ e E_{i+1} soddisfa le proprietà 1 e 2, e valgono quindi le affermazioni II) e III).
- Z_{I+1} HA GRADO 2 SU E_I , segue che z_{i+1} ha un polinomio minimo della forma $x^2 + \alpha x + \beta \in E_i[x]$, cioè z_{i+1} risolve l'equazione $z^2 + \alpha z + \beta = 0$. Passando ai coniugati, segue che $\bar{z}_{i+1}$ è radice del polinomio $z^2 + \bar{\alpha} z + \bar{\beta}$ a coefficienti in $E_i[x]$, e quindi anche in $F_{i+1}[x]$. Allora rimane vero che $|E_{i+1} : F_{i+1}| \leq 2$, perché $E_{i+1} = F_{i+1}(\bar{z}_{i+1})$, e vale l'affermazione II).

La chiusura per coniugio di E_{i+1} segue dal fatto che

$$E_{i+1} = F_{i+1}(\bar{z}_{i+1}) = E_i(z_{i+1}, \bar{z}_{i+1})$$

quindi, un generico elemento di E_{i+1} è della forma

$$(\alpha + \beta z_{i+1}) + (\gamma + \delta z_{i+1})\bar{z}_{i+1},\ \alpha, \beta, \delta, \gamma \in E_i$$

e quindi anche il coniugato di questo elemento sta ancora in E_{i+1} ($\bar{\alpha}, \bar{\beta}, \bar{\delta}, \bar{\gamma}$ stanno ancora in E_i perché E_i è chiuso rispetto al coniugio).

Provando le affermazioni I), II), e III) abbiamo costruito una catena di estensioni

$$E_0 = F_0 = \mathbb{Q} \subseteq E_1 = F_1 = \mathbb{Q}(i) \subseteq F_2 \subseteq E_2 \subseteq F_3 \subseteq E_3 \subseteq \cdots \subseteq F_t \subseteq E_t$$

come nell'enunciato.

$2 \longrightarrow 1$: viceversa, dobbiamo dimostrare che se esiste una catena di campi

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

dove $z \in K_r$ e $|K_{i+1} : K_i| \leq 2$ allora z è costruibile.

Basta dimostrare il seguente fatto: **se F è un sottocampo di $\mathbb{C}$, tutti gli elementi di F sono costruibili ed esiste E tale che $|E : F| = 2$, allora tutti gli elementi di E sono costruibili**. Vogliamo quindi mostrare che ogni $\alpha \in E \setminus F$ è costruibile. Siccome $|E : F| = 2$, dato $\alpha \in E \setminus F$, segue che $F(\alpha) = E$, e α sarà lo zero di un polinomio della forma $x^2 + bx + c$ a coefficienti in F . Posto $\Delta = b^2 - 4c$, si ha $\delta \in F$ e $\alpha = \frac{-b \pm \sqrt{\delta}}{2}$, e α è costruibile se $\sqrt{\delta}$ è costruibile, quindi non è restrittivo supporre che $\alpha^2 \in F$. Pongo $\alpha^2 = a$, **e mostriamo che $\sqrt{a}$ è costruibile**. Distinguiamo due casi:

CASO 1: $A \in \mathbb{R}, A > 0$. Allora $\sqrt{a}$ è costruibile con le seguenti operazioni:

- traccio la circonferenza $\mathcal{C}$ con centro in $((a+1)/2, 0)$ passante per $(0, 0)$;

- costruisco la retta $\mathcal{R}$ passante per $(1,0)$ e parallela all'asse delle y (per fissare le idee suppongo che $(a+1)/2 > 1$).
- chiamo P il punto di intersezione tra $\mathcal{C}$ ed $\mathcal{R}$ di ascissa positiva, e ne determino le coordinate.

$\mathcal{C}$ ha equazione

$$(x-(a+1)/2)^2 + y^2 = ((a+1)/2)^2$$

e ponendo $r = (a+1)/2$:

$$(x-r)^2 + y^2 = r^2$$
$$x^2 + r^2 - 2rx + y^2 = r^2$$

e il punto di intersezione tra $\mathcal{C}$ e la retta $\mathcal{R} : x = 1$ ottengo

$$y^2 = 2r - 1, \longrightarrow y^+ = \sqrt{2r-1} = \sqrt{2(a+1)/2 - 1} = \sqrt{a}$$

P ha coordinate $(1, \sqrt{a})$.

- costruisco la retta $\mathcal{L}$ passante per P e parallela all'asse x.
- il punto di intersezione tra $\mathcal{L}$ e l'asse y ha coordinate $(0, \sqrt{a})$.

CASO 2: $A \in \mathbb{C}$, cioè $a = re^{i\theta} = r(\cos\theta + i\sin\theta)$. $\sqrt{a}$ è costruibile con le seguenti operazioni:

- considero la circonferenza $\mathcal{C}$ centrata nell'origine e passante per $P = (r\cos\theta, r\sin\theta)$ (posso farlo perché per ipotesi $a \in F$).
- chiamo Q il punto di intersezione tra $\mathcal{C}$ e l'asse x, cioè $Q = (r, 0)$.
- chiamo $\mathcal{R}$ la retta passante per Q e P .
- Traccio la retta $\mathcal{L}$ ortogonale a $\mathcal{R}$ passante per il punto medio tra P e Q .
- ho individuato il punto T intersezione di $\mathcal{C}$ ed $\mathcal{L}$, che ha coordinate $(r\cos(\theta/2),\ r\sin(\theta/2))$ cioe' $re^{i\theta/2}$ e' costruibile.

Osservo che $\sqrt{a} = \sqrt{r}e^{i\theta/2}$, e siccome abbiamo appena mostrato che $b = re^{i\theta/2}$ è costruibile, allora possiamo costruire $a = 1/\sqrt{r} * b$ dove $\sqrt{r}$ è costruibile per il caso 1.

Corollario 5.2

Sia $z \in \mathbb{C}$, se z è costruibile allora $|\mathbb{Q}(z) : \mathbb{Q}| = 2^n$ con $n \geq 0$.

Dimostrazione

Se z è costruibile, esiste un campo $K_r \supseteq \mathbb{Q}$ con $z \in K_r$ e $|K_r : \mathbb{Q}| = 2^s$. Siccome $K_r \supseteq \mathbb{Q}(z) \supseteq \mathbb{Q}$, $|\mathbb{Q}(z) : \mathbb{Q}| \mid 2^s$ e quindi è una potenza di 2.

4.2.3 Tre problemi classici

Discutiamo i seguenti problemi classici:

1. QUADRATURA DEL CERCHIO: **si vuole costruire con riga e compasso un quadrato di area pari a quella di un cerchio dato**.Assumiamo che il cerchio abbia raggio 1, allora per risolvere il problema bisognerebbe costruire con riga e compasso $\sqrt{\pi}$. Questo non e' possibile perché $\sqrt{\pi}$ è trascendente su $\mathbb{Q}$, mentre per la proposizione precedente z è costruibile solo se $|\mathbb{Q}(z) : \mathbb{Q}| = 2^n$, $n \geq 0$.

2. DUPLICAZIONE DEL CUBO: **costruire con riga e compasso un cubo di volume doppio del volume di un cubo dato**. Assumiamo che il cubo dato abbia lato 1, allora bisognerebbe costruire con riga e compasso $\sqrt[3]{2}$, ma $\sqrt[3]{2}$ ha grado 3 su $\mathbb{Q}$, e quindi non è costruibile perché non soddisfa le ipotesi del corollario.

3. TRISEZIONE DELL'ANGOLO DI $\pi/3$: **costruire un angolo pari a un terzo di quello dato**. Posso costruire $\cos(\pi/3) + i\sin(\pi/3) = 1/2 + i\sqrt{3}/2$ con le seguenti operazioni:#*costruisco la circonferenza di centro l'origine e raggio 1;#*costruisco la retta $\mathcal{R}$ passante per $(1/2, 0)$ e parallela all'asse y.#*il punto $(1/2, \sqrt{3}/2)$ è uno dei punti di intersezione tra $\mathcal{C}$ e $\mathcal{R}$ .Tuttavia non posso costruire $e^{i\pi/9}$, perché questa è una radice primitiva 18-esima dell'unità, il cui polinomio minimo ha grado $\varphi(18) = 6$, e non è una potenza di 2.

4.2.4 Costruzione di poligoni regolari

Teorema 5.3

Sia $p > 2$ un numero primo, allora il poligono regolare con p lati è costruibile se e solo se p è della forma $2^{2^s} + 1$, $s \in \mathbb{N}$.

Dimostrazione

Il poligono regolare con p lati è costruibile se e solo se è costruibile una radice primitiva p -esima dell'unità.

$1 \longrightarrow 2$: per ipotesi, la radice primitiva $\omega = \cos(2\pi/p) + i\sin(2\pi/p) = e^{i2\pi/p}$ è costruibile, allora $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2^m$, $m \in \mathbb{N}$ per il corollario. Inoltre ω ha come polinomio minimo $\phi_p(x)$ e $\mathrm{gr}(\phi_\mathrm{p}(\mathrm{x})) = \varphi(\mathrm{p}) = \mathrm{p} - 1$, quindi $|\mathbb{Q}(\omega) : \mathbb{Q}| = p - 1$. Eguagliando le due espressioni di $|\mathbb{Q}(\omega) : \mathbb{Q}|$ segue quindi che $p - 1 = 2^m$, cioè $p = 2^m + 1$. **Proviamo che** $m = 2^s$.

Se m non è una potenza di 2, potrò scrivere $m = k * l$ con k numero dispari. Il polinomio $x^k + 1$ ammette -1 come radice quindi

$$x^k + 1 = (x + 1) * f(x),\ f(x) \in \mathbb{Z}[x]$$
$$\longrightarrow p = 2^m + 1 = 2^{kl} + 1 = (2^l)^k + 1 = (2^l + 1) * f(2^l)$$

ma questo contraddice il fatto che p sia primo. Rimane provato che m è una potenza di 2.

$2 \longrightarrow 1$: per ipotesi $p = 2^{2^s} + 1$, considero $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ con ω radice primitiva p -esima dell'unità. Il gruppo $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ è abeliano di ordine 2^{2^s} (anzi ciclico perché p è primo). Allora esiste una catena di sottogruppi $G = G_0 \supseteq G_1 \supseteq G_2 \cdots \supseteq G_s = 1$, dove G_{i+1} è normale in G_i e $o(G_i/G_{i+1}) = 2$. Per il teorema della corrispondenza di Galois, considerando i campi intermedi $(G_i)'$, trovo una catena di campi $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = \mathbb{Q}(\omega)$ con $|K_{i+1} : K_i| = 2$, e questo significa che ω è costruibile per il teoerma che fornisce un criterio per la costruibilita' (il primo teorema della sezione).

Più in generale, se considero un poligono regolare con n lati, esso è costruibile se è costruibile una radice n -esima primitiva dell'unità ω , e ω ha grado $\varphi(n)$ sopra $\mathbb{Q}$. Ora ω è costruibile se e solo se $n = 2^k * p_1 * p_2 * \cdots * p_s$, dove $p_i \neq p_j$ per $i \neq j$ e $p_i = 2^{2^{s_i}} + 1$.

Capitolo 5

Appendici

5.1 Teorema dell'elemento primitivo

Teorema 6.1 (teorema dell'elemento primitivo)

Ogni estensione separabile di grado finito è semplice.

5.1.1 Risultato preliminare

Per la dimostrazione serve il seguente risultato preliminare:

Proposizione 6.1

Sia $M \supseteq K$ un'estensione di grado finito. Allora $M \supseteq K$ è semplice se e solo se esiste un numero finito di campi intermedi tra K e M .

Dimostrazione

> Supponiamo che esista un numero finito di campi intermedi tra K e M : distinguiamo i due casi seguenti.

CASO 1: K FINITO. Se K è finito, anche M è finito, allora $M^* = \langle \alpha \rangle$ quindi $M = K(\alpha)$, cioè $M \supseteq K$ è semplice.

CASO 2: K INFINITO. Sia $\alpha \in M$ un elemento di grado massimo su K . **Vogliamo provare che** $M = K(\alpha)$. Supponiamo per assurdo che $K(\alpha) \subset M$, allora posso prendere $\beta \in M, \beta \notin K(\alpha)$ e considerare la famiglia di campi intermedi $\{K(\alpha + c\beta)\}_{c \in K}$. Siccome per ipotesi esiste solo un numero finito di campi intermedi, si ha $K(\alpha + k\beta) = K(\alpha + h\beta)$ per certi $h, k \in K$, $h \neq k$.

Quindi $K(\alpha + h\beta)$ contiene $\alpha + h\beta$ e $\alpha + k\beta$, e deve contenere anche la loro differenza, $(h - k) * \beta$. Ma $h - k \neq 0 \in K$ quindi $\beta \in K(\alpha + h\beta)$, e siccome $\alpha = (\alpha + k\beta) - k\beta$, anche α sta in $K(\alpha + h\beta)$. Allora $|K(\alpha + h\beta : K| > |K(\alpha) : K|$, assurdo perché α era stato scelto di grado massimo su M .

$1 \longrightarrow 2$: viceversa, sia $M = K(\alpha)$, considero un campo intermedio L tra K ed M . Sia $f(x)$ il polinomio minimo di α su K , e $g(x)$ il polinomio minimo di

α su L . $g(x)$ è monico, della forma $x^r + a_1x^{r-1} + \cdots + a_r$, $a_i \in L$. Considero il campo $K(a_1, \ldots, a_r)$. Siccome $a_i \in L$ per ogni i , $K(a_1, \ldots, a_r) \subseteq L$ e posso considerare la catena di estensioni $M \supseteq L \supseteq K(a_1, \ldots, a_r) \supseteq K$. **Mostro che** $|M : K(a_1, \ldots, a_r)| = r = |M : L|$ **.**

1. $|M : K(a_1, \ldots, a_r)| \geq r$, infatti $|M : L| = \mathrm{gr(g(x))} = \mathrm{r}$, e siccome $K(a_1, \ldots, a_r) \subseteq L$, $|M : K(a_1, \ldots, a_r)| \geq |M : L|$.
2. $|M : K(a_1, \ldots, a_r)| \leq r$, infatti $g(x) \in K(a_1, \ldots, a_r)[x]$ e $g(\alpha) = 0$ quindi $|M : K(a_1, \ldots, a_r)| \leq r$.

cioè dalle due disuguaglianze segue che $L = K(a_1, \ldots, a_r)$.

Ma $g(x)$ è anche un fattore di $f(x)$, e se penso a $f(x)$ in un suo campo di spezzamento, esso è della forma $\prod_i (x - \alpha_i)$. Il polinomio $g(x)$ si ottiene come prodotto di alcuni $x - \alpha_i$, e siccome questi sono in numero finito, anche i prodotti possibili sono un numero finito. Allora, siccome i campi intermedi si identificano con $K(c_1, \ldots, c_r)$ (dove i c_i sono i coefficienti di un fattore irriducibile di $f(x)$), esiste un numero finito di campi intermedi.

5.1.2 Teorema dell'elemento primitivo

Teorema 6.2 (teorema dell'elemento primitivo)

Ogni estensione separabile di grado finito di un campo è semplice.

Dimostrazione

Sia $M \supseteq K$ un'estensione separabile di grado finito. Sia N la chiusura spezzante di M su K , così $N \supseteq M \supseteq K$. Siccome $M \supseteq K$ è separabile, N è anche la chiusura normale di M su K , quindi $N \supseteq K$ è normale, e posso considerare $\mathcal{G}(N/K)$ che è finito e ha un numero finito di sottogruppi. Per il teorema fondamentale della teoria di Galois, esiste un numero finito di campi intermedi tra N e K : un campo intermedio tra M e K è anche un campo intermedio tra N e K , e quindi esiste solo un numero finito di campi intermedi tra M e K . Quindi $M \supseteq K$ è semplice per il risultato precedente.

5.2 Separabilità e inseparabilità

5.2.1 Campi perfetti

Sia F un campo di caratteristica p , con $p > 0$ primo. Allora esiste l'omomorfismo di Frobenius $\phi : F \to F$ tale che $\phi(a) = a^p$. Vale che

$$\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b)$$
$$\phi(ab) = (ab)^p = a^p * b^p = \phi(a) * \phi(b)$$

Inoltre $\phi(1) = 1$ e in particolare ϕ è iniettivo.

L'immagine di ϕ , indicata con F^p , è l'insieme $\{a^p,\ a \in F\}$ ed è un sottocampo di F .

Definizione 6.1

F si dice *perfetto* se $F^p = F$, cioè se ϕ è suriettivo: in altre parole, F è perfetto se comunque prendo $a \in F$, esiste $b \in F$ tale che $a = b^p$.

Esempio 6.1

Ogni campo F finito di caratteristica prima è tale che $|F| = |F^p|$, e quindi è perfetto.

Esempio 6.2 (esempio di campo non perfetto infinito)

Considero $F = F_p(t)$ campo delle funzioni razionali a coefficienti in F_p nell'indeterminata t . Allora $t \notin F^p$. Infatti, se $t \in F^p$, esisterebbe $f(t)/g(t) \in F$ con $f(t), g(t) \in F[t]$, tale che $t = (f(t)/g(t))^p = \frac{f(t)^p}{g(t)^p}$, cioè $t * (g(t))^p = (f(t))^p$, ma questo non può avvenire perché se così fosse si avrebbe $p$gr(f(t)) = 1 + p * gr(g(t)) .

Teorema 6.3

Sia $f(x) \in F(x)$ un polinomio irriducibile e non separabile. Allora carF = p primo, e F non è perfetto (e quindi in particolare non è finito).

Dimostrazione

Dire f irriducibile e non separabile significa che $f'(x) = 0$, e quindi necessariamente carF = p primo, e $f(x) = g(x^p)$ per un certo $g(x) \in F[x]$. Ora $g(x)$ è un polinomio della forma $\sum_i a_i x^i$, $a_i \in F$. Se F fosse perfetto, si avrebbe che $a_i = b_i^p$ per un certo $b_i \in F$, e quindi

$$f(x) = \sum_i a_i x^{ip} = \sum_i b_i^p (x^i)^p$$

$$= \sum_i (b_i x^i)^p = (\sum_i b_i x^i)^p = (h(x))^p$$

dove ho posto $h(x) = \sum_i b_i x^i$. Quindi $f(x) = (h(x))^p$ ma f è irriducibile quindi questo non può avvenire.

Corollario 6.1

Sia F un campo con carF = 0 o carF = p primo e F perfetto. Allora ogni estensione algebrica di F è separabile.

Dimostrazione

Sia $E \supseteq F$ un'estensione algebrica di F , allora ogni $\alpha \in E$ è algebrico su F . Il polinomio minimo di α che è irriducibile in $F[x]$ dev'essere separabile, altrimenti per il lemma precedente F non sarebbe perfetto.

Corollario 6.2

Sia F un campo con caratteristica prima, e $f(x) \in F[x]$ un polinomio irriducibile allora $f(x) = g(x^{p^n})$ per $n \geq 0$, e per un certo polinomio $g(x)$ irriducibile e separabile.

Dimostrazione

CASO 1: Se $f'(x) \neq 0$, $f(x)$ è separabile, allora il risultato è vero se prendo $n = 0$, e $g(x) = f(x)$.

CASO 2: Se invece $f'(x) = 0$, $f(x) = h(x^p)$ per un certo $h(x) \in F[x]$. Ora $h(x)$ dev'essere irriducibile, perché se h ammettesse una fattorizzazione propria, si avrebbe $h(x) = s(x) * t(x)$, e $f(x) = h(x^p) = s(x^p) * t(x^p)$, ma f è irriducibile e quindi questo non può avvenire. In particolare gr(h(x)) < gr(f(x)) .

Per induzione sul grado, il risultato è vero per $h(x)$, cioè posso scrivere $h(x) = g(x^{p^n})$, con $n \geq 0$ e $g(x)$ separabile e irriducibile. Allora $f(x) = h(x^p) = g(x^{p^{n+1}})$ e quindi vale l'asserto anche per f .

5.2.2 Estensione puramente inseparabile

Definizione 6.2

Data $E \supseteq F$ un'estensione algebrica, $E \supseteq F$ si dice *separabile* (su F) se ogni elemento di E è separabile su F , ovvero se per ogni $\alpha \in E$, il polinomio minimo di α in $F[x]$ è un polinomio separabile (su F).

Definizione 6.3

Data $E \supseteq F$ un'estensione algebrica, dico che $E \supseteq F$ è *puramente inseparabile* se gli unici elementi di E separabili su F sono gli elementi di F (un'estensione puramente inseparabile ha il minor numero possibile di elementi separabili).

Esempio 6.3

F come estensione di se stesso è puramente inseparabile.

Osservazione 6.1

Se $E \supset F$ è un'estensione algebrica e puramente inseparabile, allora carF = p e F non può essere perfetto per il primo teorema dimostrato.

Teorema 6.4

Sia $E \supseteq F$ un'estensione algebrica, con F campo di caratteristica p prima. Allora sono equivalenti queste tre affermazioni:

1. E è puramente inseparabile su F ;
2. comunque prendo $\alpha \in E$, $\alpha^{p^n} \in F$ per $n \geq 0$;
3. ogni elemento di E ha polinomio minimo su F della forma $x^{p^n} - a$, con $a \in F$ e $n \geq 0$.

Corollario 6.3

Sia $E = F(\alpha)$ un'estensione semplice, con F di caratteristica p primo, e $\alpha^{p^n} \in F$ per un certo $n \geq 0$. Allora E è puramente inseparabile su F .

Dimostrazione

Sia $\beta \in E = F(\alpha)$, **devo mostrare che** $\beta^{p^*} \in F$. Infatti, se questo avviene, E è puramente inseparabile su F per il teorema appena enunciato.

$\beta \in F(\alpha)$, allora $\beta = a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0$ con $a_i \in F$. Quindi, siccome siamo in caratteristica p

$$\beta^{p^n} = a_m^{p^n} * \alpha^{p^n * m} + a_{m-1}^{p^n} * \alpha^{p^n * (m-1)} + \cdots + a_1^{p^n}\alpha^{p^n} + a_0^{p^n} \in F$$

perché per ipotesi $\alpha^{p^n} \in F$.

Esempio 6.4

Per avere un esempio non banale di estensione puramente inseparabile prendo F un campo di caratteristica p primo, non perfetto. Allora esiste un elemento $a \in F \setminus F^p$. Pongo $f(x) = x^p - a \in F[x]$, sia M il campo di spezzamento per $f(x)$ su F , e α una radice di $f(x)$. Considero $E = F(\alpha)$. Siccome $f(\alpha) = 0$, $\alpha^p = a \in F$, quindi E è un'estensione di F puramente inseparabile.

Osservo che $E \neq F$, perché $a \notin F^p$. Inoltre $E = F(\alpha)$ è campo di spezzamento per $f(x)$ su F , perché $f(x) = x^p - a$ con $a = \alpha^p$, cioè $f(x) = x^p - \alpha^p = (x - \alpha)^p$.

Conclusione: se F è un campo con carF = p primo e F non perfetto, allora F ammette un'estensione puramente inseparabile non banale.

5.2.3 Condizioni equivalenti ad essere puramente inseparabile

Teorema 6.5

Data un'estensione algebrica $E \supseteq F$ con carF = p primo, allora sono equivalenti

1. $E \supseteq F$ è puramente inseparabile.
2. per ogni $\alpha \in E$, esiste $n \geq 0$ con $\alpha^{p^n} \in F$;
3. il polinomio minimo su F di ogni elemento di E è della forma $x^{p^n} - a$, $n \geq 0, a \in F$

Dimostrazione

$1 \longrightarrow 2$: sia $\alpha \in E$ e $f(x)$ il polinomio minimo di α su F . Allora per il corollario precedente posso scrivere $f(x) = g(x^{p^n})$ con $g(x) \in F[x]$ polinomio irriducibile e separabile. Allora $g(x)$ è polinomio minimo di α^{p^n} essendo $g(x)$ irriducibile e monico, e quindi α^{p^n} è separabile su F . Ma per l'ipotesi l'estensione è puramente inseparabile quindi tutti gli elementi separabili su F stanno in F , allora $\alpha^{p^n} \in F$.

$2 \longrightarrow 3$: per ipotesi, $\alpha^{p^n} \in F$, cioè α è radice del polinomio $x^{p^n} - \alpha^{p^n} \in F[x]$. Ma essendo in caratteristica p , $g(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$, quindi un fattore irriducibile di $g(x)$ in $F[x]$ sarà della forma $f(x) = (x - \alpha)^r$. Siccome $f(\alpha) = 0$, segue che $f(x)$ è il polinomio minimo di α su F e quindi $f(x)$ è univocamente determinato. Dunque $f(x)$ e' l'unico fattore irriducibile di $g(x)$ in $F[x]$ e pertanto $g(x)$ è una potenza di $f(x)$, quindi $r \mid p^n$ e $r = p^m$, $m \in \mathbb{N}$. Segue che $f(x) = x^{p^m} - a$ con $a = \alpha^{p^m} \in F$.

$3 \longrightarrow 1$: sia $\alpha \in E$ e supponiamo che α sia separabile su F . **Vogliamo mostrare che** $\alpha \in F$. Per ipotesi il polinomio minimo di α su F è della forma $f(x) = x^{p^n} - a$, $a \in F, n \geq 0$.

$f(\alpha) = 0$ implica che $a = \alpha^{p^n}$. Allora $f(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$. Se $n \geq 1$ (e quindi $p^n > 1$), $(x - \alpha)^2 \mid f(x)$ ma $f(x)$ dev'essere separabile, allora non può avere radici multiple, rimane provato che $n = 0$ e $\alpha \in F$.

Corollario 6.4

Sia F un campo di caratteristica p , con p primo, e E un'estensione di F puramente inseparabile. Allora

1. Se $E \supseteq L \supseteq F$, allora $E \supseteq L$ e $L \supseteq F$ sono puramente inseparabili.
2. se $|E : F|$ è finito, allora $|E : F| = p^*$.

Dimostrazione

1. $E \supseteq F$ è puramente inseparabile, quindi per il teorema appena dimostrato,dato $\alpha \in E$, si ha che $\alpha^{p^n} \in F$ per $n \geq 0$. Allora $\alpha^{p^n} \in L$, quindi $E \supseteq L$ è puramente inseparabile.Inoltre se $\beta \in L$, si ha $\beta \in E$, e siccome $E \supseteq F$ è puramente inseparabile, $\beta^{p^m} \in F$ per un certo $m \geq 0$, quindi $L \supseteq F$ è puramente inseparabile.
2. Procediamo per induzione su $|E : F|$. Se $|E : F| = 1$, allora $1 = p^0$ e quindi il passo base vale. Altrimenti, prendo $\alpha \in E \setminus F$, allora per la condizione 3 del teorema precedente, il polinomio minimo di α su F è della forma $x^{p^n} - a$. Quindi $|F(\alpha) : F| = p^n$. Considero la catena di estensioni $E \supseteq F(\alpha) \supseteq F$. Per la prima parte di questo corollario, $E \supseteq F(\alpha)$ è puramente inseparabile, e ha grado $< |E : F|$ perché hoscelto $\alpha \in E \setminus F$, allora per induzione $|E : F(\alpha)| = p^m$ e il resto segue dal teorema della torre, cioè $|E : F| = p^{n+m}$.

Corollario 6.5 (transitività delle estensioni puramente inseparabili)

Data la catena di estensioni $E \supseteq L \supseteq F$, con $E \supseteq L$ e $L \supseteq F$ estensioni puramente inseparabili, allora $E \supseteq F$ è puramente inseparabile.

Dimostrazione

Sia $E \supseteq F$, e $E \neq F$, allora $L \supset F$ oppure $E \supset L$, da cui segue che carF = p (voglio escludere il caso di caratteristica 0). Data $\alpha \in E$, $\alpha^{p^n} \in L$, ma $E \supseteq L$ è puramente inseparabile quindi posso applicare questa proprietà ad α^{p^n} , cioè $(\alpha^{p^n})^{p^m} = \alpha^{p^{n+m}} \in F$, e quindi $E \supseteq F$ è puramente inseparabile.

5.2.4 Proprietà del campo degli elementi separabili su F

Sia $E \supseteq F$ un'estensione algebrica, e considero l'insieme

$$S = \{\alpha \in E \, t.c. \, \alpha \, separabile \, su \, F\}$$

Allora S è un campo, ed è l'unico campo con $E \supseteq S \supseteq F$, $E \supseteq S$ puramente inseparabile e $S \supseteq F$ separabile.

Per dimostrare questo fatto è necessario il seguente lemma:

Lemma 6.1

Sia $E = F(\alpha, \beta)$ con α, β separabili su F , allora $E \supseteq F$ è separabile.

Dimostrazione

Siano $f(x), g(x)$ i polinomi minimi di α e β rispettivamente su F , e sia $h(x) = f(x) * g(x) \in F[x]$.

Sia L campo di spezzamento per $h(x)$ su F . Ora $h(x)$ è un polinomio i cui fattori irriducibili, f, g , sono separabili su F , allora $L \supseteq F$ è normale di grado finito.

Se considero la catena di estensioni $L \supseteq E \supseteq F$, con $L \supseteq F$ separabile, segue che anche $E \supseteq F$ è separabile.

Teorema 6.6

Sia $E \supseteq F$ un'estensione algebrica, e sia

$$S = \{\alpha \in E \, t.c. \, \alpha \, separabile \, su \, F\}$$

Allora S è un campo, ed è l'unico campo intermedio $E \supseteq S \supseteq F$ tale che $E \supseteq S$ è puramente inseparabile e $S \supseteq F$ è separabile.

Dimostrazione

1. Per dimostrare che S **è un campo**, basta mostrare che, dati $\alpha, \beta \in S$, $\alpha - \beta \in S$ e $\alpha\beta^{-1} \in S$ per $\beta \neq 0$. Considero $F(\alpha, \beta)$, che è un'estensione

separabile di F per il lemma precedente. $F(\alpha, \beta)$ contiene $\alpha - \beta$ e $\alpha\beta^{-1}$, e quindi sono separabili su F . In particolare stanno in S .

2. ovviamente $S \supseteq F$ **è separabile** per come S è definito.

3. Rimane da provare che $E \supseteq S$ **è puramente inseparabile**. Possiamo assumere che CarF = p , perché in caratteristica 0 , S esaurisce tutti gli elementi di E . Sia $\alpha \in E$, e considero $f(x)$ polinomio minimo di α su F .Si avrà $f(x) = g(x^{p^n})$ con $g(x)$ monico, irriducibile e separabile. Inoltre $0 = f(\alpha) = g(\alpha^{p^n})$, allora g è il polinomio minimo di α^{p^n} ed è separabile, quindi α^{p^n} è separabile su F , cioè per definizione $\alpha^{p^n} \in S$, quindi $E \supseteq S$ è puramente inseparabile perché vale la condizione 3 del teorema.

4. **Mostriamo l'unicità di** S . Sia T un campo con $E \supseteq T \supseteq F$, con $T \supseteq F$ separabile e $E \supseteq T$ puramente inseparabile. Mostriamo che $T = S$ .Dal fatto che $T \supseteq F$ è separabile, segue che tutti gli elementi di T sono separabili su F , quindi $T \subseteq S$. Allora considero la catena di estensioni $E \supseteq S \supseteq T$: siccome $E \supseteq T$ è puramente inseparabile, anche $S \supseteq T$ lo è. Considero ora la catena di estensioni $S \supseteq T \supseteq F$, siccome $S \supseteq F$ è separabile, anche $S \supseteq T$ è separabile. Allora $S = T$ perché S è contemporaneamente separabile e puramente inseparabile su T .

Corollario 6.6

Sia $E \supseteq F$ un'estensione di grado finito e non separabile, allora carF | |E : F| .

Dimostrazione

Siccome per ipotesi l'estensione è non separabile, si ha che CarF = p primo. Sia S l'insieme degli elementi di E separabili su S , allora $E \neq S$, $E \supseteq S$ è puramente inseparabile e $|E : S| = p^*$. Dal teorema della torre segue che carF = p | |E : S| | |E : F| = |E : S| ∗ |S : F| .

Proposizione 6.2

Sia $E \supseteq L \supseteq F$ una catena di estensioni con $E \supseteq L$ separabile e $L \supseteq F$ separabile, allora $E \supseteq F$ è separabile.

Dimostrazione

Sia S l'insieme degli elementi di E separabili su F . Siccome $L \supseteq F$ è separabile, segue che $L \subseteq S$, allora posso considerare la catena di estensioni $E \supseteq S \supseteq L$. Siccome $E \supseteq L$ è separabile segue che $E \supseteq S$ è separabile per un argomento già visto. Inoltre $E \supseteq S$ è puramente inseparabile e unendo le due condizioni si ha $E = S$, e quindi $E \supseteq F$ è separabile.

5.2.5 Grado di separabilità

Definizione 6.4

Sia $E \supseteq F$ un'estensione di grado finito, e sia S l'insieme degli elementi di E separabili su F . Si dice *grado di separabilità* di E su F il grado di S su F , cioè $|E : F|_s = |S : F|$.

L'estensione $E \supseteq F$ è separabile se e solo se $|E : F| = |E : F|_s$. In generale $|E : F|_s \mid |E : F|$, e il quoziente $\frac{|E:F|}{|E:F|_s}$ è una potenza di p .

Lemma 6.2

Sia $E \supseteq F$ un'estensione puramente inseparabile, e sia $f(x) \in F[x]$ monico, irriducibile e separabile. Allora $f(x)$ è irriducibile in $E[x]$.

Dimostrazione

Sia $g(x)$ un fattore monico e irriducibile di $f(x)$ in $E[x]$, e **mostriamo che** $g = f$, provando così che f rimane irriducibile in $E[x]$. Sia M il campo di spezzamento per $f(x)$ su E , quindi $M \supseteq E \supseteq F$. Allora in M , posso scrivere $g(x) = \prod_i (x - \alpha_i)$ dove gli α_i sono radici di $g(x)$ e quindi anche di $f(x)$.

Sia

$$S = \{\beta \in M \, t.c. \, \beta \; separabile \, su \, F\}$$

e voglio mostrare che $g(x) \in S[x]$. Gli α_i , radici di g , sono anche radici di f . Ora f è polinomio minimo di ciascuna sua radice in particolare di ciascun α_i . Per ipotesi $f(x)$ è separabile su F , allora gli α_i stanno in S , $x - \alpha_i \in S[x]$ allora $g(x) \in S[x]$. Inoltre $g(x) \in E[x]$ quindi i coefficienti di g stanno in $S \cap E$.

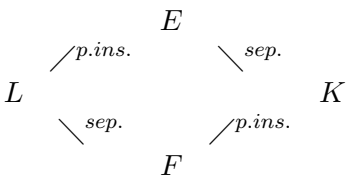
Concludo che $E \cap S = F$ infatti valgono questi fatti:

1. $E \supseteq E \cap S \supseteq F$ e $E \supseteq F$ è puramente inseparabile, allora $E \cap S \supseteq F$ è puramente inseparabile.
2. per costruzione $S \supseteq F$ è separabile, e quindi anche $E \cap S \supseteq F$ è separabile.

Allora $E \cap S = F$, cioè $g(x) \in F[x]$, allora $g = f$.

Teorema 6.7

Sia $E \supseteq F$ un'estensione di grado finito, e siano K, L campi intermedi tra E ed F con $E \supseteq L$ puramente inseparabile, $L \supseteq F$ separabile, $E \supseteq K$ separabile, $K \supseteq F$ puramente inseparabile, come mostra lo schema seguente:



Allora $|L : F| = |E : K|$.

Dimostrazione

Mostro le due disuguaglianze:

DISUGUAGLIANZA 1: $|L : F| \leq |E : K|$: Sia $\alpha \in L$, e sia $f(x) \in F[x]$ il suo polinomio minimo. Siccome $K \supseteq F$ è puramente inseparabile, $f(x)$ rimane irriducibile come polinomio in $K[x]$. Allora $|F(\alpha) : F| = |K(\alpha) : K|$. Per il teorema dell'elemento primitivo, siccome $L \supseteq F$ è separabile, posso scrivere $L = F(\alpha)$ (con abuso di notazione). Allora $|L : F| = |F(\alpha) : F| = |K(\alpha) : K| \leq |E : K|$. DISUGUAGLIANZA 2: $|E : K| \leq |L : F|$: $E \supseteq K$ e per il teorema dell'elemento primitivo posso scrivere $E = K(\beta)$ per un certo β . $E \supseteq L$ è puramente inseparabile, allora $\beta^{p^n} \in L$ per un certo $n \geq 0$, $p =$ carF (se carF $= 0$, $L = E$ e $K = F$). Considero $E = K(\beta) \supseteq K(\beta^{p^n})$. Da un lato, siccome $\beta^{p^n} \in K(\beta^{p^n})$, $E \supseteq K(\beta^{p^n})$ è puramente inseparabile; d'altra parte $E \supseteq K(\beta^{p^n}) \supseteq K$, e siccome $E \supseteq K$ è separabile, lo è anche $E \supseteq K(\beta^{p^n})$. Deduco che $E = K(\beta^{p^n})$.

Quindi

$$|E : K| = |K(\beta^{p^n}) : K| = |F(\beta^{p^n}) : F| \leq |L : F|$$

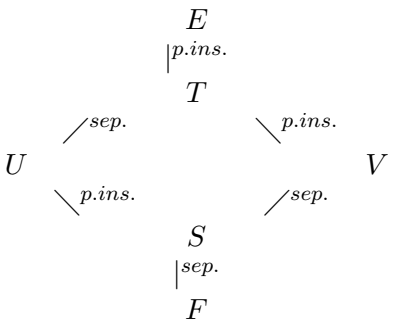
perché $\beta^{p^n} \in L$. Noto anche che la seconda uguglianza segue dallo stesso argomento usato all'inizio di questa dimostrazione.

Teorema 6.8 (moltiplicatività del grado di separabilità)

Siano $E \supseteq U \supseteq F$ campi con $|E : F|$ finito. Allora $|E : F|_s = |E : U|_s * |U : F|_s$.

Dimostrazione

Considero lo schema seguente:



Considero $E \supseteq U$, e chiamo

$$T = \{\beta \in E \, t.c. \, \beta \, separabile \, su \, U\}$$

allora segue che $E \supseteq T$ è puramente inseparabile, $T \supseteq U$ è separabile.

Considero poi $U \supseteq F$, e pongo

$$S = \{\alpha \in U \, t.c. \, \alpha \, separabile \, su \, F\}$$

allora segue che $U \supseteq S$ è puramente inseparabile e $S \supseteq F$ è separabile.

Considero la catena di estensioni

$$E \supseteq T \supseteq U \supseteq S \supseteq F$$

e pongo

$$V = \{\gamma \in T \, t.c. \gamma \, separabile \, su \, S\}$$

allora $T \supseteq V$ è puramente inseparabile, mentre $V \supseteq S$ è separabile.

Ogni pezzo della catena di estensioni $V \supseteq S \supseteq F$ è separabile. Allora $V \supseteq F$ **è separabile** per transitività.

Se considero $E \supseteq T \supseteq V$, $E \supseteq T$ è puramente inseparabile e $T \supseteq V$ è puramente inseparabile, allora $E \supseteq V$ **è puramente inseparabile**. Per l'unicità del campo intermedio V che soddisfa queste due condizioni segue che

$$V = \{\gamma \in E \, t.c. \, \gamma \, separabile \, su \, F\}$$

Segue che $|E : F|_s = |V : F|$, inoltre per il teorema della torre

$$|V : F| = |V : S| * |S : F| = |V : S| * |U : F|_s,$$

ma $|V : S| = |T : U|$ per il teorema precedente, e $|T : U| = |E : U|_s$ cioè, unendo queste formule, $|E : F|_s = |E : U|_s * |U : F|_s$.

5.3 Derivazioni

Definizione 6.5

Considero un anello A non necessariamente commutativo. Definisco una *derivazione di* A un'applicazione $\delta : A \to A$ tale che $\forall x, y \in A$,

1. $\delta(x + y) = \delta(x) + \delta(y)$,
2. $\delta(xy) = x * \delta(y) + \delta(x) * y$.

Esempio 6.5

Sia A un anello e prendo $a \in A$. Definisco l'applicazione $\delta_a : A \to A$ tale che $\delta_a(x) = xa - ax$. La mappa δ è una derivazione infatti:

1. $\delta_a(x+y) = (x+y)a - a(x+y) = xa + ya - ax - ay = (xa - ax) + (ya - ay) = \delta_a(x) + \delta_a(y)$.
2. $$x * \delta_a(y) + \delta_a(x) * y = x * (ya - ay) + (xa - ax) * ay = xya - xay + xay - axy$$
$$= xya - axy = \delta_a(xy)$$

Chiamo $Der(A)$ l'insieme delle derivazioni $\delta : A \to A$. Prendo δ, η due derivazioni di A , definisco la somma $\delta + \eta : A \to A$ ponendo $x \mapsto \delta(x) + \eta(x)$.

Il prodotto (nel senso della composizione) di due derivazioni in generale non è una derivazione. Definisco il prodotto

$$[\delta, \eta] := \delta\eta - \eta\delta$$

e in particolare **mostro che** $[\delta, \eta] \in Der(A)$:

Dimostrazione

Mostro la proprietà 2:

$$(\delta\eta - \eta\delta)(xy) = \delta\eta(xy) - \eta\delta(xy)$$
$$= \delta(x\eta(y) + \eta(x)y) - \eta(x\delta(y) + \delta(x)y)$$

sfrutto la linearità

$$= \delta(x\eta(y)) + \delta(\eta(x)y) - \eta(x\delta(y)) - \eta(\delta(x)y)$$

applico la proprietà 2 a δ e η :

$$= \delta(x)\eta(y) + x\delta\eta(y) + \delta\eta(x)y + \eta(x)\delta(y) - \eta(x)\delta(y) - x\eta(\delta(y)) - \eta\delta(x)y - \delta(x)\eta(y)$$
$$= x\delta\eta(y) + \delta\eta(x)y - x\eta(\delta(y)) - \eta\delta(x)y$$
$$= x(\delta\eta(y) - \eta\delta(y)) + (\delta\eta(x) - \eta\delta(x))y$$
$$= x * (\delta\eta - \eta\delta)(y) + (\delta\eta - \eta\delta)(x)y$$

Definizione 6.6

L è un anello di Lie se

1. L è un gruppo abeliano rispetto alla somma;
2. su L è definito un prodotto $[*, *] : L \times L \to L$ che è additivo nelle due componenti, cioè $[a, b + c] = [a, b] + [a, c]$ e $[a + b, c] = [a, b] + [b, c]$, e tale che $[a, a] = 0$;
3. per il prodotto vale l'identità di Jacobi, cioe':

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0, \ \forall a, b, c \in L$$

5.3.1 Proprietà delle derivazioni

Proprietà 1: Sia A un anello commutativo, e δ una derivazione di A , allora $\delta(1) = 0$.

Dimostrazione

$$\delta(1) = \delta(1 * 1) = 1 * \delta(1) + \delta(1) * 1 = 2 * \delta(1)$$

e quindi $\delta(1) = 2\delta(1)$ implica $\delta(1) = 0$.

Proprietà 2: dato $a \in A$, $\delta(a^n) = n * a^{n-1} * \delta(a)$.

Dimostrazione

Procedo per induzione. Il passo base, $\delta(1) = 0$, vale per la proprietà 1. Suppongo l'asserto vero per $n - 1$ e lo dimostro per n .

$$\delta(a^n) = \delta(a * a^{n-1}) = a * \delta(a^{n-1}) + a^{n-1} * \delta(a)$$

e applicando il passo induttivo al primo addendo:

$$= a * (n-1) * a^{n-2} * \delta(a) + a^{n-1}\delta(a)$$
$$= (n-1) * a^{n-1} * \delta(a) + a^{n-1}\delta(a) = n * a^{n-1}\delta(a)$$

5.3.2 Derivazione sullo spazio dei polinomi

Sia A un anello che sia una F -algebra con F campo, cioè A è un anello, A è uno spazio vettoriale su F e

$$(\lambda a) * b = a * (\lambda b) = \lambda * (ab),\ \forall \lambda \in F,\ \forall a, b \in A.$$

Sia $\delta : A \to A$ un'applicazione che sia F -lineare, e tale che

$$\delta(uv) = u * \delta(v) + \delta(u) * v,\ \forall u, v \in B,$$

dove B e' un insieme di generatori per A come spazio vettoriale su F .

Mostro che δ è una derivazione di A .

Dimostrazione

Definisco due applicazioni $\alpha, \beta : A \times A \to A$ tali che:

$$\alpha(u, v) := \delta(uv)$$
$$\beta(u, v) := u\delta(v) + \delta(u)v$$

α e β sono F -lineari in ciascuna componente, cioè, ad esempio, se considero la seconda componente, dati $u, v, w \in A$, $\lambda, \mu \in F$, segue che

$\alpha(u, \lambda v+\mu w) = \delta(u*(\lambda v+\mu w)) = \delta(\lambda(uv)+\mu(uw)) = \lambda\delta(uv)+\mu\delta(uw) = \lambda\alpha(u,v)+\mu\alpha(u,w)$.

Fissato $u \in B$ si ha che $\alpha(u,w) = \beta(u,w),\ \forall w \in A$ per linearita' e perche' $\delta(uv) = u*\delta(v) + \delta(u)*v$ in $B \times B$.

Analogamente, fissato $v \in B$, si ha $\alpha(w,v) = \beta(w,v),\ \forall w \in A$. Allora $\alpha = \beta$ in $A \times A$.

Teorema 6.9

Sia F un campo e considero l'anello dei polinomi $F[x]$. Allora esiste un'unica F -derivazione di $F[x]$, δ , con $\delta(x) = 1$, e tale che

$$\delta(\sum_{i=0}^{n} a_i x^i) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Dimostrazione

Mostriamo l'esistenza della derivazione. Una base $\mathcal{B}$ per $F[x]$ è data da $\{x^i\}_{i\geq 0}$. Se $\delta(x) = 1$, per le proprietà dimostrate prima si ha

$$\delta(1) = 0,\ \delta(x^i) = ix^{i-1},\ \forall i \geq 1$$

Per mostrare che δ è una F -derivazione, oltre a estenderla per linearità su $F[x]$, per l'osservazione precedente **basta mostrare che** $\delta(x^i * x^j) = x^i * \delta(x^j) + \delta(x^i) * x^j$. Questo è vero infatti

$$\delta(x^i * x^j) = \delta(x^{i+j}) = (i+j)x^{i+j-1}$$
$$x^i * \delta(x^j) + \delta(x^i) * x^j = j * x^i * x^{j-1} + i x^i x^{j-1} = (i+j) * x^{i+j-1}$$

Per mostrare l'unicità, basta mostrare che ogni derivazione agisce allo stesso modo sugli elementi della base, e questo è vero, infatti, siccome per ipotesi $\delta(x) = 1$, allora

$$\delta(x^i) = ix^{i-1}\delta(x) = ix^{i-1}$$

e $\delta(1) = 0$.

L'azione di δ sui polinomi segue per linearità.

5.4 Estensioni di grado infinito

Considero un'estensione $M \supseteq K$ normale algebrica, ma eliminiamo l'ipotesi che $M \supseteq K$ sia finita che era stata fondamentale in molte dimostrazioni della teoria di Galois. In questa situazione posso ancora definire $\mathcal{G}(M/K)$ e l'insieme $\mathcal{L}$ dei campi intermedi, l'insieme $\mathcal{H}$ dei sottogruppi di G e le mappe "primo". $\mathcal{G}(L/K)$

è un gruppo topologico, cioè un gruppo che è anche uno spazio topologico, in cui chiedo che le applicazioni : $G \times G \to G$ tale che $(x, y) \mapsto xy$ e : $G \to G \, t.c. \, x \mapsto x^{-1}$ siano continue.

Più precisamente, il gruppo di Galois di un'estensione algebrica infinita è un gruppo profinito.

Definizione 6.7

Diremo che l'insieme $(I, \leq)$ è *diretto* se comunque prendo $i, j \in I$, esiste $k \in I$ con $i \leq k$ e $j \leq k$.

5.4.1 Sistema inverso

Considero un insieme $\{G_i, \ i \in I\}$ con I insieme diretto. Per ogni $i, j \in I$ con $i \leq j$, considero la mappa $f_{j,i} \colon G_j \to G_i$ tale che

1. $f_{i,i} : G_i \to G_i$ è l'identità su G_i .
2. Considero $i \leq j \leq k$, e le mappe $f_{k,j} \colon G_k \to G_j$, $f_{j,i} \colon G_j \to G_i$ e $f_{k,i} : G_k \to G_i$. Richiedo che
$$f_{j,i} \circ f_{k,j} = f_{k,i}$$
In altre parole, richiedo che il diagramma seguente sia commutativo:
$$\begin{array}{ccc} G_k & & \\ \downarrow{\scriptstyle f_{k,j}} & \searrow{\scriptstyle f_{k,i}} & \\ G_j & \to{\scriptstyle f_{j,i}} & G_i \end{array}$$

Un insieme con queste proprietà si chiama *sistema inverso di gruppi*.

Definizione 6.8

Considero $\prod_{i \in I} G_i$ (prodotto diretto dei gruppi). L'insieme

$$\{(x_i)_{i \in I}, \in \prod_i G_i \, t.c. f_{j,i}(x_j) = x_i \forall i \leq j\}$$

indicato con il simbolo $\lim_{\leftarrow} G_i$ si definisce *limite inverso*.

5.4.2 Gruppo di Galois di un'estensione infinita

Considero un'estensione algebrica normale $M \supseteq K$. Le estensioni normali si possono caratterizzare come estensioni separabili e campi di spezzamento su K di una famiglia di polinomi (in analogia con le estensioni finite).

Considero la famiglia

$$\mathcal{F} = \{L_i, \ i \in I \, t.c. \, M \supseteq L_i \supseteq K, \ L_i \supseteq K \, normale \, di \, grado \, finito\}.$$

Ordino l'insieme I in modo che $i \leq j$ se $L_i \subseteq L_j$. Devo provare che I **è un insieme diretto**. Questo è vero infatti, date L_i, L_j estensioni normali di grado

finito, se pongo $L_k = \vee(L_i, L_j)$, allora LL_k è ancora un'estensione di grado finito normale che contiene L_j e L_i , cioè $i \leq k, j \leq k$. Questo dipende da due fatti.

1. $|L_i : K| < \infty$, allora posso considerare la base $\{\alpha_1, \ldots, \alpha_n\}$ di L_i su K . Posso pensare a $\vee(L_i, L_j) = L_j(\alpha_1, \ldots, \alpha_n)$, allora
$$\vee(L_i, L_j)' = L_i' \cap L_j'$$
2. Viceversa, dati $H, K \leq G$, segue che $(H \cap K)' = H' \vee K'$.

Chiamo $G_i = \mathcal{G}(L_i/K)$. Allora posso considerare l'insieme $\{G_i\}_{i\in I}$ con I insieme diretto per quanto dimostrato sopra. Per $i, j \in I$, $i \leq j$, definisco la mappa $f_{j,i} : G_j \to G_i$ tale che $g \in G_j \mapsto g_{|_{L_i}}$. Queste mappe sono ben definite poiché $L_i \subseteq L_j$. In questo modo $\{G_i\}_{i\in I}$ è un sistema inverso di gruppi.

Mostro che $\mathcal{G}(M/K) \cong \lim_{\leftarrow} G_i$. Posso considerare infatti l'isomorfismo $\phi\colon \mathcal{G}(M/K) \to \liminf_{\leftarrow} G_i$ tale che $g \mapsto (g_{|_{L_i}})_{i\in I}$. Mostriamo i seguenti fatti:

1. **L'elemento $(x_i)_{i\in I}$ con $x_i = g_{|_{L_i}}$ sta nel limite inverso**, cioè, per $i \leq j$, $f_{j,i}(x_j) = x_i$. Infatti
$$f_{j,i}(g_{|_{L_j}}) = [g_{|_{L_j}}]_{|_{L_i}} = G_{|_{L_i}}$$
e questo è vero perché $L_i \subseteq L_j$.
2. ϕ **è suriettiva**: dato $(g_i)_{i\in I}$ appartenente al limite inverso, esso definisce un elemento univocamente determinato di $\mathcal{G}(M/K)$. Questo dipende dal fatto che $M = \bigcup_{i\in I} L_i$ .In particolare, preso $\alpha \in M$, l'estensione $K(\alpha) \supseteq K$ è algebrica. Considero la chiusura spezzante N , che è anche chiusura normale, di $K(\alpha) \supseteq K$, allora $N \supseteq K$ è un'estensione di K normale e di grado finito. In $\mathcal{F}$ esiste L_s che contiene α .Allora definisco $g : M \to M$ che opera su α come $g_{|_{L_s}}$. g è un automorfismo, infatti dati $\alpha, \beta \in M$, $\alpha \in L_s, \beta \in L_t$, allora esiste $L_k \in \mathcal{F}$ che contiene α, β . g agisce su L_k come g_k . g_k è un automorfismo, allora anche g lo è.
3. ϕ **è anche iniettiva**. Dato $g \in \mathcal{G}(M/K), g \neq 1$, voglio mostrare che $\phi(g) \neq 1$. Prendo $\alpha \in M \setminus K$, allora α appartiene a un'estensione di grado finito di K , in particolare esiste s t.c. $\alpha \in L_s$ con $L_s \supseteq K$ normale. Allora, poiché $\alpha \notin K$,
$$\alpha^{g_s} = \alpha^{g_{|_{L_s}}} \neq \alpha$$
quindi $\alpha^g \neq \alpha$ e quindi $\phi(g) \neq 1$.

Suppongo di avere G_i gruppi finiti, lo si rende un gruppo topologico dando la topologia discreta. Considero $\prod_i G_i$ e ad esso do la topologia prodotto. Il limite inverso è un sottospazio del limite diretto. Il limite diretto e' compatto perché ogni G_i è compatto. Il limite inverso è un chiuso contenuto in un compatto e quindi è compatto, è Hausdorff ed è totalmente sconnesso. Dato $H \in G$, $H'' = H$ se e solo se H è chiuso in senso topologico, cioè se $\bar{H} = H$ in senso topologico.

Dato p primo e F_p campo con p elementi e F chiusura algebrica di F_p , posso considerare $\mathcal{G}(F/F_p)$ che è il limite inverso dei gruppi di Galois che ottengo pensando alle estensioni finite di F_p , $\lim_{\leftarrow}(\mathbb{Z}/(p^n\mathbb{Z}))_{n\geq 1}$.

Capitolo 6

Esercizi

6.1 Primo esercizio

Esercizio 7.1

Determinare il gruppo di Galois su $\mathbb{Q}$ del campo di spezzamento M del polinomio $f(x) = x^4 - 3x^2 - 10$.

6.1.1 Campo di spezzamento

Prima cerco il campo di spezzamento M : la fattorizzazione di $f(x)$ in irriducibili in $\mathbb{Q}[x]$ è

$$f(x) = (x^2 - 5)(x^2 + 2)$$

Osservo che $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$, e definisco il campo di spezzamento di questo polinomio:

$$K = \mathbb{Q}(\sqrt{5}) = \frac{\mathbb{Q}[x]}{(x^2 - 5)} = \{a + b\sqrt{5},\, a, b \in \mathbb{Q}\}$$

$K \subset \mathbb{R}$ quindi il polinomio $x^2 + 2$ non ammette radici in K , e si ha $x^2 + 2 = (x - i\sqrt{2})(x + i\sqrt{2})$.

Per trovare il campo di spezzamento di $f(x)$ estendo K e considero:

$$M = K(i\sqrt{2}) = \mathbb{Q}(\sqrt{5}, i\sqrt{2}) = \{\xi_0 + \xi_1 i\sqrt{2},\, \xi_0, \xi_1 \in K\}$$

e sostituendo le espressioni di ξ_0 e ξ_1 :

$$\begin{aligned} &= \{(a_0 + a_1\sqrt{5}) + (a_2 + a_3\sqrt{5}) * i\sqrt{2},\, a_i \in \mathbb{Q},\, \forall i\} \\ &= \{a_0 + a_1\sqrt{5} + a_2 i\sqrt{2} + a_3 i\sqrt{10},\, a_i \in \mathbb{Q},\, \forall i\} \end{aligned}$$

Applicando il teorema della torre segue che

$$|M:\mathbb{Q}| = |\mathbb{Q}(\sqrt{5}, i\sqrt{2}) : \mathbb{Q}(\sqrt{5})| * |\mathbb{Q}(\sqrt{5}) : \mathbb{Q}| = 2 * 2 = 4$$

6.1.2 Ordine ed elementi del gruppo di Galois

Siccome $\mathbb{Q}$ ha caratteristica 0 ogni polinomio irriducibile è separabile (infatti un polinomio irriducibile $f(x) \neq 0$ ha una radice multipla solo se $f'(x) = 0$, e questo in caratteristica 0 non può avvenire); dalla caratterizzazione delle estensioni normali di grado finito segue quindi che $M \supseteq \mathbb{Q}$ è normale, e $o(\mathcal{G}(M/\mathbb{Q})) = |M:\mathbb{Q}| = 4$.

G è isomorfo a un sottogruppo di S_4 perché gli elementi di G permutano le radici del polinomio di partenza che sono quattro. Detti $\Omega_1 = \{\pm\sqrt{5}\}$ e $\Omega_2 = \{\pm i\sqrt{2}\}$, sappiamo che G agisce transitivamente sia su Ω_1 che su Ω_2 . Quindi, gli elementi di G si possono elencare in questo modo:

$$\begin{aligned}
&g_1 t.c. && \text{identita} \\
&g_2 t.c. && \sqrt{5}^{g_2} = -\sqrt{5}, (i\sqrt{2})^{g_2} = i\sqrt{2} \\
&g_3 t.c. && \sqrt{5}^{g_3} = \sqrt{5}, (i\sqrt{2})^{g_3} = -i\sqrt{2} \\
&g_4 t.c. && \sqrt{5}^{g_4} = -\sqrt{5}, (i\sqrt{2})^{g_4} = i\sqrt{2}
\end{aligned}$$

Posso anche riscrivere gli elementi sopra in questo modo

$$g_1 = 1, g_2 : \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ i\sqrt{2} \mapsto i\sqrt{2} \end{cases} \quad g_3 : \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ i\sqrt{2} \mapsto -i\sqrt{2} \end{cases} \quad g_4 : \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ i\sqrt{2} \mapsto -i\sqrt{2} \end{cases} .$$

Osservo che il gruppo non è ciclico, infatti ogni elemento elevato al quadrato è uguale all'identità e ha quindi ordine 2. A meno di isomorfismo esistono solo due gruppi di ordine 4 che sono C_4 e $C_2 \times C_2$ (il gruppo di Klein). Nota: con C_n indichiamo il gruppo ciclico di ordine n e, se usiamo la notazione moltiplicativa per i gruppi, consideriamo il prodotto diretto $\times$. Se invece usiamo la notazione additiva per i gruppi, consideriamo la somma diretta (ma e' la stessa costruzione, cambia solo la notazione).

Siccome G non e' ciclico deduciamo che G è

il Klein. Posso elencare i suoi elementi nella forma

$$G = \{1, x, y, xy\}$$

dove $x = g_2$, $y = g_3$, $xy = g_4$.

6.1.3 Corrispondenza di Galois

I sottogruppi di G sono:

$$H_1 := \{1, x\}, \quad H_2 := \{1, y\}, \quad H_3 := \{1, xy\}$$

Determino i campi intermedi:

1. $H_1' = \mathrm{Fix}(\mathrm{H}_1) = \mathrm{Fix}(\{1, \mathrm{x}\})$, e siccome x fissa $i\sqrt{2}$, $H_1' \supseteq \mathbb{Q}(i\sqrt{2})$ .Inoltre per il teorema fondamentale della teoria di Galois

$$|G : H_1| = |H_1' : G'| = |H_1' : \mathbb{Q}|$$

e siccome $|G : H_1| = 2$, anche $|H_1' : \mathbb{Q}| = 2$. Poiche' $|\mathbb{Q}(i\sqrt{2} : \mathbb{Q}| = 2$ concludo che deve essere $H_1' = \mathbb{Q}(i\sqrt{2})$.

2. Per un ragionamento analogo si ha che $H_2' = \mathrm{Fix}(\mathrm{H}_2) = \mathrm{Fix}(\{1, \mathrm{y}\}) = \mathbb{Q}(\sqrt{5})$.

3. Ora determiniamo

$$H_3' = \mathrm{Fix}(\mathrm{H}_3) = \mathrm{Fix}(\{1, \mathrm{xy}\})$$

Determino gli elementi $\xi \in M$ che vengono fissati da H_2 e quindi da xy : un generico elemento in M è della forma

$$\xi = a_0 + a_1\sqrt{5} + a_2 i\sqrt{2} + a_3 i\sqrt{10}$$

e considerando come agisce xy si ha:

$$\xi^{xy} = a_0 - a_1\sqrt{5} - a_2 i\sqrt{2} + a_3 i\sqrt{10}$$

e imponendo $\xi = \xi^{xy}$ ottengo il sistema

$$\begin{cases} a_0 = a_0 \\ a_1 = -a_1 \\ a_2 = -a_2 \\ a_3 = a_3 \end{cases}$$

cioè $a_2 = a_1 = 0$ mentre a_0, a_3 sono liberi, quindi

$$H_3' = \{a_0 + a_3 i\sqrt{10},\ a_0, a_3 \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{10})$$

6.1.4 Diagrammi dei sottogruppi e dei campi intermedi

(per comodità lo scrivo solo a parole) SOTTOGRUPPI: Primo livello: G

Secondo livello: $\{1, x\}$, $\{1, y\}$, $\{1, xy\}$

Terzo livello: $\{1\}$

CAMPI INTERMEDI:

Primo livello:

$$\mathbb{Q}(\sqrt{5}, i\sqrt{2})$$

Secondo livello: $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i\sqrt{2})$, $\mathbb{Q}(i\sqrt{10})$

Terzo livello: $\mathbb{Q}$

Osserviamo anche che G e' abeliano dunque ogni suo sottogruppo e' normale. Segue dal Teorema Fondamentale della Teoria di Galois che le estensioni $\mathbb{Q}(\sqrt{5}) \supseteq \mathbb{Q}$, $\mathbb{Q}(i\sqrt{2}) \supseteq \mathbb{Q}$ e $\mathbb{Q}(i\sqrt{10}) \supseteq \mathbb{Q}$ sono normali (cosa che si verifica facilmente anche in maniera diretta peraltro).

6.2 Secondo esercizio

Esercizio 7.2

Determinare il gruppo di Galois su $\mathbb{Q}$ del campo di spezzamento M del polinomio $f(x) = x^3 - 2$.

6.2.1 Campo di spezzamento

Pongo $\alpha = \sqrt[3]{2}$, e $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$, allora le radici di $f(x)$ sono α , $\alpha\omega$, $\alpha\omega^2$.

$f(x)$ è separabile. Definisco il campo

$$K_1 = \mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2,\, a, b, c \in \mathbb{Q}\}$$

K_1 non contiene ω , quindi per trovare M devo estenderlo ulteriormente. Per calcoli precedenti si ha che il polinomio minimo di ω è $\phi_3(x) = x^2 + x + 1$. Definisco quindi

$$\begin{aligned} K_2 = K_1(\omega) = \mathbb{Q}(\alpha, \omega) &= \{\xi_0 + \xi_1\omega,\, \xi_0, \xi_1 \in K_1\} \\ &= \{(a_0 + a_1\alpha + a_2\alpha^2) + (a_3 + a_4\alpha + a_5\alpha^2)\omega,\, a_i \in \mathbb{Q} \forall i\} \\ &= \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\omega + a_4\alpha\omega + a_5\alpha^2\omega,\, a_i \in \mathbb{Q} \forall i\} \end{aligned}$$

e $K_2 = M$.

Per il teorema della torre:

$$|M : \mathbb{Q}| = |M : K_1| * |K_1 : \mathbb{Q}| = 2 * 3 = 6$$

6.2.2 Gruppo di Galois

In caratteristica zero un polinomio irriducubile e' separabile dunque l'estensione $M \supseteq \mathbb{Q}$ e' normale. Allora sappiamo che

$$o(\mathcal{G}(M/\mathbb{Q})) = |M : \mathbb{Q}| = 6$$

e G è isomorfo a un sottogruppo di S_3 , perché permuta le tre radici di $f(x)$. Siccome $o(S_3) = 6$, allora $G = S_3$.

Siano $x, y \in G$ definiti da

$$x : \begin{cases} \alpha \mapsto \alpha\omega \\ \alpha\omega \mapsto \alpha\omega^2 \\ \alpha\omega^2 \mapsto \alpha \end{cases} \quad y : \begin{cases} \alpha \mapsto \alpha \\ \alpha\omega \mapsto \alpha\omega^2 \\ \alpha\omega^2 \mapsto \alpha\omega \end{cases}$$

(se indentifico α con 1 , $\alpha\omega$ con 2 e $\alpha\omega^2$ con 3 , ho che x corrisponde al 3 -ciclo $(1, 2, 3)$ di S_3 e y allo scambio $(2, 3)$ in S_3).

Allora gli elementi di G si possono elencare nel seguente modo:

$$G = \{1, x, x^2, y, yx, yx^2\}$$

(dove x^2 corrisponde a $(1,2,3)^2 = (1,3,2)$, yx corrisponde a $(1,2)$ e yx^2 corrisponde a
$(1,3)$).

6.2.3 Corrispondenza di Galois

SOTTOGRUPPI:

$$H_1 = \{1,\, x\, x^2\} \text{ sottogrupponormalein\$G\$}$$
$$H_2 = \{1,\, y\} \text{ sottogrupponormalein\$G\$}$$
$$H_3 = \{1,\, yx\} \text{ sottogrupponormalein\$G\$}$$
$$H_4 = \{1,\, yx^2\} \text{ sottogrupponormalein\$G\$}$$

Campi intermedi

1. $H_1 = \{1, x, x^2\}$: per definizione $H_1' = \mathrm{Fix(H_1)}$ .Cerco gli elementi ξ di M tali che $\xi^x = \xi$.*Osservazione*: x fissa ω , infatti $\omega = \alpha^{-1}\alpha\omega$, e applicando x a entrambi i membri:

   $$\omega^x = (\alpha^{-1})^x(\alpha\omega)^x = (\alpha^x)^{-1}(\alpha\omega)^x = (\alpha\omega)^{-1}\alpha\omega^2 = \alpha^{-1}\omega^{-1}\alpha\omega^2 = \omega$$

   (mia nota: l'uguaglianza $(\alpha^{-1})^x = (\alpha^x)^{-1}$ è vera perché $1 = \alpha\alpha^{-1}$ e applicando x a entambi i membri, $1 = \alpha^x(\alpha^{-1})^x$, quindi l'inverso di α^x è $(\alpha^{-1})^x$).Un elemento in M è dato da

   $$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\omega + a_4\alpha\omega + a_5\alpha^2\omega$$

   $$\longrightarrow \xi^x = a_0 + a_1\alpha\omega + a_2\alpha^2\omega^2 + a_3\omega + a_4\alpha\omega^2 + a_5\alpha^2\omega^3$$

   e tenendo conto che $\omega^2 = -1 - \omega$ e che $\omega^3 = 1$:

   $$= a_0 + a_1\alpha\omega + a_2\alpha^2(-1-\omega) + a_3\omega + a_4\alpha(-1-\omega) + a_5\alpha^2$$

   $$= a_0 + (a_1 - a_4)\alpha\omega - a_4\alpha + (a_5 - a_2)\alpha^2 + a_3\omega + (a_1 - a_4)\alpha\omega + (-a_2)\alpha^2\omega$$

   Eguagliando i coefficienti di ξ e di ξ^x ottengo

   $$\begin{cases} a_1 = -a_4 \\ a_2 = a_5 - a_2 \\ a_4 = a_1 - a_4 \\ a_5 = -a_2 \end{cases}$$

   da cui segue

   $$a_1 = a_2 = a_4 = a_5 = 0$$

e quindi

$$H_1' = \{a_0 + a_3\omega,\ a_0, a_3 \in \mathbb{Q}\} = \mathbb{Q}(\omega)$$

Come prima

$$|H_1' : \mathbb{Q}| = |G : H_1| = 2$$

Procedimento alternativo: dal fatto che x fissa ω segue automaticamente che $\mathrm{Fix}(\mathrm{H}_1) \supseteq \mathbb{Q}(\omega)$, e vale l'uguaglianza per il teorema fondamentale della teoria di Galois.Infatti $|H_1' : \mathbb{Q}| = 2$ per il Teorema e si vede facilmente che $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$. H_1 è normale in G , allora $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ è normale (e questo si deduce anche dal fatto che $\mathbb{Q}(\omega)$ è il campo di spezzamento di $x^2 + x + 1$ su $\mathbb{Q}$).

2. $H_2 = \{1, y\}$. $H_2' \supseteq \mathbb{Q}(\alpha)$ (infatti y fissa α). Per il teorema fondamentale della teoria di Galois

$$3 = |G : H_2| = |H_2' : G'| = |H_2' : \mathbb{Q}|$$

($G' = \mathbb{Q}$ perché l'estensione è normale)Inoltre, $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$ allora concludo che $H_2' = \mathbb{Q}(\alpha)$. H_2' non è un'estensione normale di $\mathbb{Q}$ (cosa che posso anche dedurre dal fatto che $x^3 - 2$ ammette la radice α in $\mathbb{Q}(\alpha)$ ma non le altre due radici).

3. $H_3 = \{1, yx\}$. Svolgendo il prodotto (che e' la composizione di mappe da sinistra a destra per le notazioni che usiamo), osservo che

$$yx : \begin{cases} \alpha \mapsto \alpha\omega \\ \alpha\omega \mapsto \alpha \\ \alpha\omega^2 \mapsto \alpha\omega^2 \end{cases}$$

quindi yx fissa $\alpha\omega^2$ e per un ragionamento analogo al precedente, $H_3' = \mathbb{Q}(\alpha\omega^2)$.

4. $H_4 = \{1, yx^2\}$ e

$$yx^2 : \begin{cases} \alpha \mapsto \alpha\omega^2 \\ \alpha\omega \mapsto \alpha\omega \\ \alpha\omega^2 \mapsto \alpha \end{cases}$$

quindi yx^2 fissa $\alpha\omega$ e $H_4' = \mathbb{Q}(\alpha\omega)$.

6.3 Terzo esercizio

Esercizio 7.3

Determinare il gruppo di Galois sopra $\mathbb{Q}$ del campo di spezzamento M del polinomio $f(x) = x^4 - 2$.

6.3.1 Campo di spezzamento

Pongo $\alpha = \sqrt[4]{2}$, allora l'insieme delle radici di $f(x)$ è

$$\{\alpha, i\alpha, i^2\alpha, i^3\alpha\} = \{\alpha, -\alpha, i\alpha, -i\alpha\}$$

Considero

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3, a_i \in \mathbb{Q} \forall i\}$$

$\mathbb{Q}(\alpha) \subset \mathbb{R}$ e quindi non contiene le radici complesse di $f(x)$, allora lo estendo ulteriormente e considero

$$M = \mathbb{Q}(\alpha, i) = \{\alpha_0 + \alpha_1 i, \alpha_i \in \mathbb{Q}(\alpha) \forall i\}$$
$$= \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i, a_i \in \mathbb{Q}, \forall i\}$$

6.3.2 Gruppo di Galois

In caratteristica 0 un polinomio irriducibile è separabile, e quindi $M \supseteq \mathbb{Q}$ è normale. Segue che

$$|M : \mathbb{Q}| = |M : \mathbb{Q}(\alpha)| * |\mathbb{Q}(\alpha) : \mathbb{Q}| = 2 * 4 = 8 = o(G)$$

e G è isomorfo a un sottogruppo di S_4 .

6.4 Nota:

Con qualche nozione di Teoria dei Gruppi posso dedurre che G e' isomorfo a D_4 (definito sotto). Posso tranquillamente saltare questa parte e l'esercizio rimane comunque valido, oppure leggerla assumendo alcune cose (una sola per la verita') per vere.

Il primo fatto (che e' anche l'unico che non giustifichiamo) che serve e' che, a meno di isomorfismo, esistono 5 gruppi di ordine 8 . Tre sono abeliani (e questo lo sappiamo perche' $8 = 2^3$ e le partizioni di 3 sono 3) e precisamente

$$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$$

Poi ci sono il gruppo dei quaternioni Q (che pure conosciamo gia') e il gruppo diedrale D_4 che invece dobbiamo definire. Il modo piu' immediato per definirlo e' dire che D_4 e' un gruppo con 8 elementi, precisamente

$$D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$$

con il prodotto definito da $a^4 = 1 = b^2$ (nel senso che a ha ordine 4 e b ha ordine 2) e $bab = a^{-1}$. Questo basta per definire il prodotto di due elementi qualsiasi di D_4 . Infatti per esempio da $bab = a^{-1}$ segue che $ba^2b = a^{-2}$ perche' posso

scrivere $ba^2b = (bab)(bab) = a^{-1}a^{-1} = a^{-2}$. Qui ho usato il fatto che b ha ordine 2 dunque $bb = 1$. Naturalmente e' anche vero che $a^{-1} = a^3$ e $a^{-2} = a^2$. Allo stesso modo si prova che $ba^3b = a^{-3}$, dove $a^{-3} = a$. Posso scrivere in modo compatto che, da $bab = a^{-1}$, si deduce che $ba^kb = a^{-k}$.

Per fare un altro esempio calcolo il prodotto di ba^3 per ba e trovo

$$(ba^3)(ba) = (ba^3b)a = a^{-3}a = a^{-2} = a^2.$$

Se una avesse voglia e tempo potrebbe verificare che in questo modo abbiamo effettivamente definito un gruppo (oppure risparmiarsi la, pure un po' noiosa, verifica).

Piu' in generale il gruppo diedrale D_n di ordine $2n$ si puo' definire come il gruppo

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$$

dove $a^n = 1 = b^2$ (sempre nel senso che a ha ordine n e b ha ordine 2) e $bab = a^{-1}$. Ragionando come prima, in questo modo abbiamo definito il prodotto tra due elementi qualsiasi di D_n .

I gruppi diedrali hanno un'interpretazione geometrica. Infatti D_n e' il gruppo delle simmetrie di un poligono regolare con n lati. Consideriamo per semplicita' il caso di D_4 . Possiamo interpretare D_4 come il gruppo delle simmetrie di un quadrato. pensiamo un quadrato nel piano con vertici nei punti di coordinate $(1, 0), (0, 1), (-1, 0)$ e $(0, -1)$. Indichiamo con a la rotazione di centro l'origine, angolo $\pi/2$ in senso antiorario. Allora a manda il quadrato in se' e lo stesso fanno le sue potenze, che sono a^2 rotazione di centro l'origine e angolo π e a^3 rotazione di centro l'origine e angolo $(3/2)\pi$. Poi a^4 e' l'identita'. Questo corrisponde nel gruppo all'elemento a di ordine 4 . Le altre simmetrie del quadrato sono le riflessioni (che hanno tutte ordine 2 , perche' se le faccio due volte trovo l'identita') che, nel caso del quadrato, sono o riflessioni rispetto ad un asse di simmetria passante per due vertici opposti (e di queste riflessioni ce ne sono due) oppure riflessioni rispetto ad un asse di simmetria passante per i punti medi di due lati opposti (e anche di queste riflessioni ce ne sono due). Nel gruppo queste riflessioni corrispondono agli elementi b, ba, ba^2 e ba^3 che infatti hanno tutti ordine 2 come si puo' verificare facilmente.

Nel caso generale di D_n ho sempre una rotazione a di angolo $2\pi/n$ che avra' periodo n . Quindi ho in tutto n rotazioni che sono le potenze di a : $1, a, a^{n-1}, \ldots, a^{n-1}$.

Poi se n e' pari ho le riflessioni, di cui $n/2$ rispetto ad un asse passante per i punti medi di due lati opposti e $n/2$ rispetto ad un asse passante due vertici opposti. Se invece n e' dispari (per esempio $n = 5$), le riflessioni di un n -gono regolare (per esempio il pentagono) sono tutte rispetto ad un asse che passa per un vertice e per il punto medio del lato opposto (e sono n le riflessioni totali).

In modo molto compatto si puo' definire D_n per generatori (a e b) e relazioni scrivendo

$$D_n = \langle a, b | a^4 = 1 = b^2, bab = a^{-1} \rangle$$

Usando le relazioni ($a^4 = 1 = b^2, bab = a^{-1}$) si deduce che gli elementi di D_n sono proprio $1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}$ e il prodotto nel gruppo.

Quello che interessa noi e' che ogni gruppo di ordine 8 e' isomorfo a uno tra

$$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, Q, D_4.$$

Affermiamo che G e' isomorfo a D_4 . Infatti quello che distingue D_4 tra i 5 gruppi di ordine 8 e' il fatto di avere un sottogruppo non normale di ordine 2 , per esempio il sottogruppo $H = \{1, b\}$. Per mostrare che H non e' normale, osservo che:

$$a^{-1}ba = a^{-1}a^3b^{-1} = a^{-1}a^3b = a^2b \notin H,$$

dove abbiamo usato il fatto che $bab = a^3 \longrightarrow ba = a^3b^{-1}$.

Anche G ha un sottogruppo non normale di ordine 2 . Per provare l'esistenza del sottogruppo non normale di G , osservo che $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$ è un'estensione non normale: infatti, se fosse normale, ogni polinomio in $\mathbb{Q}[x]$ che ammette una radice in $\mathbb{Q}(\alpha)$ si dovrebbe spezzare in fattori lineari distinti su $\mathbb{Q}(\alpha)$, ma questo non avviene, basta considerare il polinomio $f(x) = x^4 - 2$. Segue quindi che $\mathbb{Q}(\alpha)'$ è un sottogruppo di G non normale; si ha anche $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$, allora $|\mathbb{Q}' : \mathbb{Q}(\alpha)'| = |G : \mathbb{Q}(\alpha)'| = 4$, cioè $o(\mathbb{Q}(\alpha)') = \frac{o(G)}{|G:\mathbb{Q}(\alpha)'|} = 8/4 = 2$. Concludo che **G è isomorfo a D_4** .

Affermiamo che esistono due elementi $x, y \in G$ che agiscono su i e α nel modo seguente: $i^x = i$, $i^x = \alpha i$; $i^y = -i$, $\alpha^y = \alpha$.

Per giustificare l'esistenza di x e y , osservo che sicuramente esiste un elemento $\bar{x} \in G$ tale che $\alpha^{\bar{x}} = \alpha i$ perché G agisce transitivamente sulle radici di $f(x)$. D'altra parte $\bar{x}$ agisce sulle radici del polinomio $x^2 + 1 \in \mathbb{Q}[x]$, quindi $i^{\bar{x}} = \pm i$. Se $i^{\bar{x}} = -i$,

posto y l'automorfismo di coniugio che manda i in $-i$ e fissa $\mathbb{Q}$, e pongo $x = y\bar{x}$. Segue che x soddisfa le condizioni richieste infatti:

$$\alpha^x = \alpha^{y\bar{x}} = \alpha^{\bar{x}} = \alpha i$$
$$i^x = i^{y\bar{x}} = (-i)^{\bar{x}} = i$$

Rimane da mostrare che il coniugio in $\mathbb{C}$ definisce per restrizione un automorfismo di M su $\mathbb{Q}$, e vale la seguente proposizione: *Supponiamo di avere una catena di estensioni $N \supseteq M \supseteq K$. Sia M campo di spezzamento su K di un polinomio $g(x) \in K[x]$. Sia $\sigma : M \to N$ un omomorfismo (non banale) con $\sigma_{|_K} = 1_K$. Allora $M^\sigma = M$.*

Dimostrazione

M^σ è campo di spezzamento su $K^\sigma = K$ del polinomio $(g(x))^\sigma = g(x)$ (è a coefficienti in K quindi viene fissato da σ). Allora M e M^σ sono entrambi campi di spezzamento (in N) su K di $g(x)$, ma il campo di spezzamento in N di un polinomio su K è unico, ed è dato da $K(\alpha_1, \ldots, \alpha_r)$ dove gli α_i sono radici di $g(x)$. Allora $M^\sigma = M$.

Quindi, applicando la proposizione, siccome il coniugio fissa $\mathbb{Q}$, esso definisce un automorfismo da M in sé che fissa $\mathbb{Q}$. Allora gli elementi x, y cercati esistono, ed essi soddisfano la condizione $x^4 = y^2 = 1$, infatti:

inoltre

$$i^{yxy} = i, \quad \alpha^{yxy} = -\alpha i$$

cioè $yxy = x^3$, allora

$$G = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$$

6.4.1 Sottogruppi

$$H_1 = \{1, x, x^2, x^3\} \quad \text{ciclico}$$
$$H_2 = \{1, x^2, y, x^2y\}$$
$$H_3 = \{1, x^2, xy, x^3y\}$$
$$H_4 = \{1, y\}$$
$$H_5 = \{1, x^2\}$$
$$H_6 = \{1, xy\}$$
$$H_7 = \{1, x^2y\}$$
$$H_8 = \{1, x^3y\}$$

Campi intermedi

1. $H_1 = \{1, x, x^2, x^3\}$; $H_1' \supseteq \mathbb{Q}(i)$, inoltre $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ e per il teorema fondamentale di Galois
$$2 = |G : H_1| = |H_1' : G'|$$
e quindi $H_1' = \mathbb{Q}(i)$.

2. $H_2 = \{1, x^2, y, x^2y\}$; considero $\xi \in M$ e per prima cosa impongo $\xi^{x^2} = \xi$.
$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$
e tenendo conto che $i^{x^2} = i$ e $\alpha^{x^2} = -\alpha$:
$$\xi^{x^2} = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 + a_4 i - a_5 i\alpha + a_6 i\alpha^2 - a_7\alpha^3 i$$
e imponendo l'uguaglianza segue che $a_1 = a_3 = a_5 = a_7 = 0$, e quindi gli elementi fissati da x^2 sono della forma
$$\xi_1 = a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i, \ a_i \in \mathbb{Q} \forall i$$
Ora, impongo che gli elementi trovati vengano fissati anche da y :
$$\xi_1^y = a_0 + a_2\alpha^2 - a_4 i - a_6\alpha^2 i$$
allora, imponendo l'uguaglianza, $a_4 = a_6 = 0$.
$$H_2'' = \{a_0 + a_2\alpha^2, \ a_0, a_2 \in \mathbb{Q}\} = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$$

3. $H_3 = \{1, x^2, xy, x^3y\}$; considero un generico elemento fissato da x^2 , della forma
$$\xi_1 = a_0 + a_2\alpha + a_4 i + a_6 i\alpha$$
$$\xi_1^{xy} = a_0 - a_2\alpha^2 - a_4 i + a_6\alpha^2 i$$
Imponendo l'uguaglianza
$$a_2 = a_4 = 0$$
quindi,
$$H_3' = \{a_0 + a_6\alpha^2 i\} = \mathbb{Q}(i\sqrt{2})$$

4. $H_4 = \{1, y\}$; $H_4' = \mathbb{Q}(\alpha)$, infatti y fissa α , $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 2$, $2 = |G : H_4| = |H_4' : \mathbb{Q}|$ quindi $H_4' = \mathbb{Q}(\alpha)'$.

5. $H_5 = \{1, x^2\}$; siccome gli elementi fissati da x^2 sono già stati calcolati prima, segue che
$$H_5' = \{a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i,\ a_i \in \mathbb{Q} \forall i\}$$
e in particolare se pongo $a_2 = a_6 = 0$, ottengo $\mathbb{Q}(i) \subset H_5'$ .Anche α^2 è fissato da x^2 ; osservo allora che $|\mathbb{Q}(\alpha^2, i) : \mathbb{Q}| = 4$, inoltre $4 = |G : H_5| = |H_5' : \mathbb{Q}|$ quindi $H_5' = \mathbb{Q}(\alpha^2, i)$.

6. $H_6 = \{1, xy\}$; calcolo gli elementi fissati da xy , tenendo conto che $i^{xy} = -i$, e $\alpha^{xy} = -\alpha i$:
$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$
$$\longrightarrow \xi^{xy} = a_0 - a_1\alpha i - a_2\alpha^2 + a_3\alpha^3 i - a_4 i - a_5\alpha + a_6 i\alpha^2 + a_7\alpha^3$$
Imponendo l'uguaglianza
$$\begin{cases} a_1 = -a_5, \\ a_2 = 0 \\ a_3 = a_7 \\ a_4 = 0 \end{cases}$$
da cui segue che
$$H_6' = \{a_0 + a_1(\alpha - i\alpha) + a_3(\alpha^3 + i\alpha^3) + a_6 i\alpha^2,\ a_i \in \mathbb{Q}\}$$
Mostro che $H_6' = \mathbb{Q}(\alpha - i\alpha)$ infatti, calcolando le potenze di $\alpha - i\alpha$ ottengo:
$$(\alpha - i\alpha)^2 = \alpha^2 - 2i\alpha^2 - \alpha^2 = -2i\alpha^2$$
$$(\alpha - i\alpha)^3 = -2i\alpha^2(\alpha - i\alpha) = -2i\alpha^3 - 2\alpha^3 = -2(i\alpha^3 + \alpha^3)$$
$$(\alpha - i\alpha)^4 = (-2i\alpha^2)^2 = -4\alpha^4 = -8$$
cioè $\alpha - i\alpha$ ha come polinomio minimo $x^4 + 8$. Quindi posso porre $\beta = \alpha - i\alpha$, e scrivere
$$H_6' = \{a_0 + a_1\beta + a_6\beta^2 + a_3\beta^3,\ a_i \in \mathbb{Q}\} = \mathbb{Q}(\beta).$$

7. $H_7 = \{1, x^2y\}$; tenendo conto che $i^{x^2y} = -i$ e $\alpha^{x^2y} = -\alpha$, e preso un generico elemento $\xi \in M$

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3,\ a_i \in \mathbb{Q}$$

$$\xi^{xy} = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 - a_4 i + a_5 i\alpha - a_6 i\alpha^2 + a_7 i\alpha^3$$

Imponendo l'uguaglianza si ha $a_1 = a_3 = a_4 = a_6 = 0$, quindi

$$H_7' = \{a_0 + a_2\alpha^2 + a_5 i\alpha + a_7 i\alpha^2,\ a_i \in \mathbb{Q}\}$$

e calcolando le potenze di $i\alpha$:

$$(i\alpha)^2 = \alpha^2,\ (i\alpha)^3 = -i\alpha^3,\ (i\alpha)^4 = \alpha^2 = 2$$

quindi $i\alpha$ ha come polinomio minimo $x^4 - 2$, $H_7' = \mathbb{Q}(i\alpha)$ e $H_7' \supseteq \mathbb{Q}$ ha grado 4.

8. $H_8 = \{1, x^3y\}$; $i^{x^3y} = -i$, $\alpha^{x^3y} = i\alpha$. Dato $\xi \in M$ della forma

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

$$\xi^{x^3y} = a_0 + a_1\alpha i - a_2\alpha^2 - a_3 i\alpha^3 - a_4 i + a_5\alpha + a_6 i\alpha^2 - a_7\alpha^3$$

e imponendo l'uguaglianza:

$$\begin{cases} a_1 = a_5 \\ a_2 = 0 \\ a_3 = -a_7 \\ a_4 = 0 \end{cases}$$

quindi

$$H_8' = \{a_0 + a_1(\alpha + i\alpha) + a_3(\alpha^3 + i\alpha^3) + a_6 i\alpha^2,\ a_i \in \mathbb{Q} \forall i\} = \mathbb{Q}(\alpha + i\alpha)$$

infatti

$$(\alpha + i\alpha)^2 = \alpha^2 + 2i\alpha^2 - \alpha^2 = 2i\alpha^2$$

$$(\alpha + i\alpha)^3 = 2i\alpha^3 - 2\alpha^3$$

$$(\alpha + i\alpha)^4 = (2i\alpha^2)^2 = -4\alpha^4 = -8$$

cioè $\alpha + i\alpha$ ha polinomio minimo $x^4 + 8$ e quindi $H_8' \supseteq \mathbb{Q}$ ha grado 4.

6.5 Quarto esercizio

Esercizio 7.4

Calcolare $\phi_n(x)$ per $n = 1 \ldots, 20$.

Per calcoli precedenti sappiamo che

$$\phi_1(x) = x - 1$$

$$\phi_2(x) = x + 1$$

$$\phi_4(x) = x^2 + 1$$
$$\phi_6(x) = x^2 - x + 1$$
$$\phi_8(x) = x^4 + 1$$

Inoltre, ricordiamo che in generale, per p primo

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

quindi conosciamo anche $\phi_3(x)$, $\phi_5(x)$, $\phi_7(x)$, $\phi_{11}(x)$, $\phi_{13}(x)$, $\phi_{17}(x)$, $\phi_{19}(x)$.
Calcoliamo i polinomi rimanenti:

1. $\phi_9 = \frac{x^9-1}{\phi_1(x)*\phi_3(x)}$ e $\phi_1(x) * \phi_3(x) = x^3 - 1$, quindi

   $$\phi_9(x) = \frac{x^9 - 1}{x^3 - 1}$$

   Aggiungendo e togliendo x^6 al numeratore:

   $$\phi_9(x) = \frac{x^9 - x^6 + x^6 - 1}{x^3 - 1}$$
   $$\phi_9(x) = \frac{x^6(x^3 - 1) + (x^3 + 1)(x^3 - 1)}{x^3 - 1}$$
   $$\phi_9(x) = \frac{(x^6 + x^3 + 1)(x^3 - 1)}{x^3 - 1}$$
   $$\phi_9(x) = x^6 + x^3 + 1$$

2. $\phi_{10}(x) = \frac{x^{10}-1}{\phi_1(x)*\phi_2(x)*\phi_5(x)}$

   $$= \frac{x^{10} - 1}{(x^5 - 1)\phi_2(x)}$$
   $$= \frac{(x^5 - 1)(x^5 + 1)}{(x^5 - 1)\phi_2(x)}$$
   $$= \frac{x^5 + 1}{x + 1}$$

   Eseguo la divisione:

   $$\frac{x^5 + 1}{x + 1} =$$
   $$q_1 = x^4,\ r_1 = x^5 + 1 - x^4(x + 1) = -x^4 + 1$$
   $$q_2 = -x^3,\ r_2 = -x^4 + 1 + x^3(x + 1) = x^3 + 1$$
   $$q_3 = x^2,\ r_3 = x^3 + 1 - x^2(x + 1) = -x^2 + 1$$
   $$q_4 = -x,\ r_4 = -x^2 + 1 + x(x + 1) = x + 1$$
   $$q_5 = 1$$

   Complessivamente,

   $$x^5 + 1 = (x + 1) * (x^4 - x^3 + x^2 - x + 1)$$

   quindi

   $$\phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

3. $\phi_{12}(x) = \frac{x^{12}-1}{\phi_1(x)*\phi_2(x)*\phi_3(x)*\phi_4(x)*\phi_6(x)}$

$$= \frac{(x^6+1)(x^6-1)}{\phi_4(x)*(x^6-1)}$$

$$= \frac{x^6+1}{x^2+1}$$

Eseguo la divisione

$$\frac{x^6+1}{x^2+1} =$$

$$q_1 = x^4,\ r_1 = x^6+1-x^4(x^2+1) = -x^4+1$$

$$q_2 = -x^2,\ r_2 = -x^4+1+x^2(x^2+1) = x^2+1$$

$$q_3 = 1,\ r_3 = 0$$

Quindi

$$x^6+1 = (x^4-x^2+1)*(x^2+1)$$

$$\longrightarrow \phi_{12}(x) = x^4-x^2+1$$

4. $\phi_{14} = \frac{x^{14}-1}{\phi_1(x)*\phi_2(x)*\phi_7(x)}$

$$= \frac{x^7+1}{\phi_2(x)}$$

$$= \frac{x^7+1}{x+1}$$

e questa divisione è simile a quella per il calcolo di $\phi_{10}(x)$, quindi

$$\phi_{14}(x) = x^6-x^5+x^4-x^3+x^2-x+1$$

5. $\phi_{15}(x) = \frac{x^{15}-1}{\phi_1(x)*\phi_3(x)*\phi_5(x)}$ e $\phi_1(x)*\phi_5(x) = x^5-1$, mentre $\phi_3(x) = x^2+x+1$, quindi

$$= \frac{x^{15}-1}{(x^2+x+1)(x^5-1)}$$

Eseguo la divisione:

$$\frac{x^{15}-1}{x^5-1} =$$

$$q_1 = x^{10},\ r_1 = x^{15}-1-x^{10}(x^5-1) = x^{10}-1$$

$$q_2 = x^5,\ r_2 = x^{10}-1-x^5(x^5-1) = x^5-1$$

$$q_3 = 1,\ r_3 = 0$$

quindi

$$x^{15}-1 = (x^{10}+x^5+1)(x^5-1)$$

$$\longrightarrow \phi_{15}(x) = \frac{x^{10}+x^5+1}{x^2+x+1}$$

Ora eseguo la divisione:

$$\frac{x^{10}+x^5+1}{x^2+x+1} =$$

$$q_1 = x^8,\ r_1 = x^{10}+x^5+1-x^8(x^2+x+1) = -x^9-x^8+x^5+1$$

$$q_2 = -x^7,\ r_2 = -x^9 - x^8 + x^5 + 1 + x^7(x^2 + x + 1) = x^7 + x^5 + 1$$
$$q_3 = x^5,\ r_3 = x^7 + x^5 + 1 - x^5(x^2 + x + 1) = -x^6 + 1$$
$$q_4 = -x^4,\ r_4 = -x^6 + 1 + x^4(x^2 + x + 1) = x^5 + x^4 + 1$$
$$q_5 = x^3,\ r_5 = x^5 + x^4 + 1 - x^3(x^2 + x + 1) = -x^3 + 1$$
$$q_6 = -x,\ r_6 = -x^3 + 1 + x(x^2 + x + 1) = x^2 + x + 1$$
$$q_7 = 1,\ r_7 = 0$$

Quindi

$$x^{10} + x^5 + 1 = (x^2 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$$
$$\longrightarrow \phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

6. $\phi_{16}(x) = \frac{x^{16}-1}{[\phi_1(x)*\phi_2(x)*\phi_4(x)]*\phi_8(x)}$ Il termine tra parentesi quadra è $x^4 - 1$, e uso l'espressione di $\phi_8(x)$:

$$= \frac{(x^8 + 1)(x^4 + 1)(x^4 - 1)}{(x^4 - 1)(x^4 + 1)}$$
$$= x^8 + 1$$

7. $\phi_{18}(x) = \frac{(x^9-1)*(x^9+1)}{\phi_1(x)*\phi_2(x)*\phi_3(x)*\phi_6(x)*\phi_9(x)}$

$$= \frac{(x^9 - 1) * (x^9 + 1)}{[\phi_1(x) * \phi_3(x) * \phi_9(x)] * \phi_2(x) * \phi_6(x)}$$
$$= \frac{x^9 + 1}{(x^2 - x + 1)(x + 1)}$$

Eseguo la divisione:

$$\frac{x^9 + 1}{x^2 - x + 1} =$$
$$q_1 = x^7,\ r_1 = x^9 + 1 - x^7(x^2 - x + 1) = x^8 - x^7 + 1$$
$$q_2 = x^6,\ r_2 = x^8 - x^7 + 1 - x^6(x^2 - x + 1) = -x^6 + 1$$
$$q_3 = -x^4,\ r_3 = -x^6 + 1 + x^4(x^2 - x + 1) = -x^5 + x^4 + 1$$
$$q_4 = -x^3,\ r_4 = -x^5 + x^4 + 1 + x^3(x^2 - x + 1) = x^3 + 1$$
$$q_5 = x,\ r_5 = x^3 + 1 - x(x^2 - x + 1) = x^2 - x + 1$$
$$q_6 = 1,\ r_6 = 0$$

quindi

$$x^9 + 1 = (x^2 - x + 1)(x^7 + x^6 - x^4 - x^3 + x + 1)$$
$$\phi_{18}(x) = \frac{x^7 + x^6 - x^4 - x^3 + x + 1}{x + 1}$$
$$\phi_{18}(x) = \frac{x^6(x + 1) - x^3(x + 1) + x + 1}{x + 1}$$
$$\phi_{18}(x) = \frac{(x^6 - x^3 + 1)(x + 1)}{x + 1}$$
$$\phi_{18}(x) = x^6 - x^3 + 1$$

8. $\phi_{20}(x) = \frac{(x^{10}-1)(x^{10}+1)}{\phi_1(x)*\phi_2(x)*\phi_4(x)*\phi_5(x)*\phi_{10}(x)}$

$$\phi_{20}(x) = \frac{(x^{10}-1)(x^{10}+1)}{\phi_2(x) * \phi_4(x) * \phi_{10}(x)}$$

e $\phi_4(x) = x^2 + 1$, e $\phi_{10}(x) = \frac{x^5+1}{x+1}$, allora

$$= \frac{(x^5+1)(x^{10}+1)}{(x^5+1)/(x+1) * (x+1) * (x^2+1)}$$

$$= \frac{x^{10}+1}{x^2+1}$$

$$= x^8 - x^6 + x^4 - x^2 + 1$$

(il risultato si ottiene facendo la sostituzione $y = x^2$, infatti abbiamo già eseguito la divisione $\frac{y^5+1}{y+1}$)

6.6 Quinto esercizio

Esercizio 7.5

Siano p, q primi distinti. Esprimere $\phi_{pq}(x)$ in termini di $\phi_p(x)$.

Per il primo lemma, siccome gli unici divisori del prodotto pq sono $1, p, q, pq$, si ha

$$\phi_{pq}(x) = \frac{x^{pq}-1}{\phi_1(x) * \phi_p(x) * \phi_q(x)}$$

$$\phi_{pq}(x) = \frac{x^{pq}-1}{\phi_p(x) * (x^q-1)}$$

Moltiplico e divido per $\phi_1(x) = x - 1$:

$$\phi_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x-1) * \phi_p(x) * (x^q-1)}$$

$$\phi_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1) * (x^q-1)}$$

$$\phi_{pq}(x) = \frac{((x^q)^p-1)(x-1)}{(x^p-1) * (x^q-1)}$$

$$\phi_{pq}(x) = \frac{(x^q)^p-1}{x^q-1} * \frac{x-1}{x^p-1}$$

$$= \frac{\phi_p(x^q)}{\phi_p(x)}$$

6.7 Sesto esercizio

Esercizio 7.6

Determinare le radici seste dell'unità su F_5 .

Trovare le radici seste dell'unità in F_5 equivale a trovare il campo di spezzamento del polinomio $f(x) = x^6 - 1$ su F_5 .

Osservo che gli elementi 1 e 4 in F_5 sono radici seste dell'unità, in particolare $x + 4 = x - 1 \mid f(x)$ e $x + 1 \mid f(x)$, e si ha

$$f(x) = x^6 - 1 = (x^3 + 1)(x^3 - 1) = (x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1)$$

Pongo $g(x) = x^2 + x + 1$ e $h(x) = x^2 - x + 1$.

Considero $K_0 = \frac{F_5[x]}{(x^2+x+1)} = F_5(\alpha)$ con α radice di $g(x)$, cioè $\alpha^2 = 4\alpha + 4$.

$$K_0 = \{a + b\alpha,\ a, b \in F_5,\ \alpha^2 = 4\alpha + 4\}$$

Verifico se K_0 contiene radici di $h(x)$, cioè, preso un elemento $a + b\alpha \in K_0$, verifico se soddisfa l'equazione $h(a + b\alpha) = 0$.

$$(a + b\alpha)^2 - a - b\alpha + 1 = 0$$
$$a^2 + 2ab\alpha + b^2\alpha^2 - a - b\alpha + 1 = 0$$

e siccome $\alpha^2 = 4\alpha + 4$,

$$a^2 + 1 + 2ab\alpha + b^2(4\alpha + 4) - a - b\alpha + 1 = 0$$
$$a^2 + 1 + 2ab\alpha + 4b^2\alpha + 4b^2 - a - b\alpha + 1 = 0$$
$$(2ab + 4b^2 - b)\alpha + 4b^2 - a + 2 + a^2 = 0$$

e quest'equazione è soddisfatta se

$$\begin{cases} a^2 + 4b^2 + 4a + 1 = 0 \\ 2ab + 4b^2 + 4b = 0 \end{cases}$$

Osservo che $a = 0, b = -1$, è una soluzione, quindi $-\alpha \in K_0$ è radice di $h(x)$.

Allora K_0 è campo di spezzamento per $f(x)$.

Determino l'altra radice di $g(x)$ eseguendo la divisione:

$$\frac{x^2 + x + 1}{x - \alpha} =$$
$$q_1 = x,\ r_1 = x^2 + x + 1 - x(x - \alpha) = (1 + \alpha)x + 1$$
$$q_2 = 1 + \alpha,\ r_2 = (1 + \alpha)x + 1 - (1 + \alpha)(x - \alpha) = \alpha^2 + \alpha + 1 = 0$$

quindi $x^2+x+1=(x-\alpha)(x-1-\alpha)$, cioè l'altra radice di $g(x)$ è $1+\alpha$.

Analogamente si verifica che l'altra radice di $h(x)$ è $-1-\alpha$.

Procedimento alternativo: si possono trovare le radici dei due polinomi $g(x), h(x)$ con la formula risolutiva per le equazioni di secondo grado.

Concludo che le radici seste dell'unità sono

$$\{1,\ -1,\ \alpha, -\alpha,\ \alpha+1,\ -\alpha-1\}$$

Si ha che $\varphi(6)=2$, quindi ci sono due radici primitive seste. Osservo che

$$\begin{gathered}\alpha^2=-\alpha-1\\ \alpha^3=\alpha*(-\alpha-1)=-\alpha^2-\alpha=\alpha+1-\alpha=1\ \longrightarrow o(\alpha)=3\\ (-\alpha)^2=-1-\alpha\\ (-\alpha)^3=(-1-\alpha)*(-\alpha)=\alpha+\alpha^2=-1\\ (-1)^2=1\ \longrightarrow o(\alpha)=2*3=6\\ (\alpha+1)^2=\alpha^2+2\alpha+1=\alpha\\ \alpha^3=1,\ \longrightarrow, o(\alpha)=6\end{gathered}$$

Quindi in particolare, le radici primitive seste sono $-\alpha, \alpha+1$.

6.8 Settimo esercizio

Esercizio 7.7

Sia $\omega\in\mathbb{C}$ radice primitiva p -esima dell'unità, cioè $\omega=\cos(2\pi/p)+i\sin(2\pi/p)$ e considero $\mathbb{Q}(\omega)\supseteq\mathbb{Q}$. Calcolare traccia e norma, $t(\omega)$ e $n(\omega)$, di ω in $\mathbb{Q}(\omega)\supseteq\mathbb{Q}$.

Per le osservazioni precedenti sappiamo che $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})\cong U_p$ e quindi è un gruppo ciclico di ordine $p-1$, chiamo i suoi elementi $\{g_1, g_2, \dots, g_{p-1}\}$.

Gli elementi di $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ sono determinati dalla loro azione su ω , e sono tali che $\omega\mapsto\omega^i$ per $i=1,\dots,p-1$, in particolare sia g_i tale che $\omega\mapsto\omega^i$.

CALCOLO DELLA TRACCIA: Per definizione

$$\begin{gathered}t(\omega)=\omega^{g_1}+\omega^{g_2}+\cdots+\omega^{g_n}\\ =\sum_{i=1}^{p-1}\omega^i=\omega+\omega^2+\cdots+\omega^{p-1}\end{gathered}$$

e in particolare, $t(\omega)+1=\phi_p(\omega)$, e siccome ω è radice del polinomio ciclotomico, $\phi_p(\omega)=0$ quindi $t(\omega)=-1$.

CALCOLO DELLA NORMA:

$$n(\omega)=\prod_{i=1}^{p-1}\omega^{g_i}=\prod_{i=1}^{p-1}\omega^i$$

$$= \omega^{\sum_{i=1}^{p-1} i} = \omega^{p(p-1)/2} = (1)^{(p-1)/2} = 1$$

6.9 Ottavo esercizio

Esercizio 7.8

Sia $\alpha = \sqrt{2+\sqrt{2}}$.

1. Calcolare il polinomio minimo $f(x)$ di α su $\mathbb{Q}$.
2. Sia M campo di spezzamento di $f(x)$ su $\mathbb{Q}$, mostrare che $\mathcal{G}(M/\mathbb{Q})$ è ciclico di ordine 4.
3. Determinare la corrispondenza di Galois tra campi intermedi e sottogruppi.

1. POLINOMIO MINIMO: Osservo che

   $$\alpha^2 = 2+\sqrt{2} \longrightarrow \alpha^2 - 2 = \sqrt{2}$$

   ed elevando al quadrato l'ultima identità si ha:

   $$\alpha^4 + 4 - 4\alpha^2 = 2, \longrightarrow \alpha^4 - 4\alpha^2 + 2 = 0$$

   cioè α è radice del polinomio $f(x) = x^4 - 4x^2 + 2$. $f(x)$ è monico, e **mostro che è irriducibile**. Pongo $x^2 = t$ e risolvo l'equazione

   $$t^2 - 4t + 2 = 0$$

   $$t_{1,2} = \frac{4 \pm \sqrt{8}}{2}$$

   $$t_{1,2} = \frac{4 \pm 2\sqrt{2}}{2}$$

   $$t_{1,2} = 2 \pm \sqrt{2}$$

   quindi $f(x)$ si fattorizza nel modo seguente:

   $$f(x) = (x^2 - \sqrt{2} - 2)(x^2 - 2 + \sqrt{2})$$

   quindi $f(x)$ non ammette una fattorizzazione in $\mathbb{Q}[x]$ ed è irriducibile in $\mathbb{Q}[x]$, quindi è il polinomio minimo di α su $\mathbb{Q}$ (potevo anche usare il Criterio di Eisenstein).

2. GRUPPO DI GALOIS: Pongo $\alpha = \sqrt{2+\sqrt{2}}$ e $\beta = \sqrt{2-\sqrt{2}}$, allora le radici di $f(x)$ sono $\pm\alpha$ e $\pm\beta$. gr(f(x)) $= |\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$, siccome dobbiamo mostrare che $\mathcal{G}(M/\mathbb{Q})$ è ciclico di ordine 4, **mostriamo che** $M = \mathbb{Q}(\alpha)$ **, equivalentemente che** $\beta \in \mathbb{Q}(\alpha)$. Moltiplico e divido β per $\sqrt{2+\sqrt{2}}$:

   $$\beta = \sqrt{2-\sqrt{2}} = \frac{\sqrt{2-\sqrt{2}} * \sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}}$$

$$= \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = (\alpha^2 - 2)/\alpha = (\alpha^2 - 2) * \alpha^{-1}$$

quindi $\beta \in \mathbb{Q}(\alpha)$ e $M = \mathbb{Q}(\alpha)$ .Segue quindi che $4 = |M : \mathbb{Q}| = o(\mathcal{G}(M/\mathbb{Q})$, e $G := \mathcal{G}(M/\mathbb{Q}) = \{g_1, g_2, g_3, g_4\}$. Gli elementi di G sono determinati dalla loro azione su α , e mandano α in una delle radici di $f(x)$; supponiamo che gli elementi di G siano definiti nel seguente modo:

$$\alpha^{g_1} = \alpha,\ \alpha^{g_2} = -\alpha,\ \alpha^{g_3} = \beta,\ \alpha^{g_4} = -\beta.$$

Per mostrare che G è ciclico, **basta trovare un elemento di ordine 4**. Esplicito le relazioni tra gli elementi di G :#*Per g_2 si ha:

$$\alpha^{g_2^2} = (-\alpha)^{g_2} = \alpha$$

quindi $o(g_2) = 2$. Considero allora g_3 :#*Per g_3 si ha

$$\alpha^{g_3^2} = \beta^{g_3} = (\beta^2 - 2)/\beta$$

e sostituendo l'espressione di β :

$$= \frac{2 - \sqrt{2} - 2}{\sqrt{2 - \sqrt{2}}}$$

$$= \frac{-\sqrt{2}}{\sqrt{2 - \sqrt{2}}}$$

moltiplico e divido per $\sqrt{2+\sqrt{2}}$:

$$= \frac{-\sqrt{2} * \sqrt{2+\sqrt{2}}}{\sqrt{2 - \sqrt{2}} * \sqrt{2+\sqrt{2}}}$$

$$= \frac{-\sqrt{2} * \sqrt{2+\sqrt{2}}}{\sqrt{2}}$$

$$= -\sqrt{2+\sqrt{2}} = -\alpha$$

quindi $\alpha^{g_3^2} = \alpha^{g_2}$, e $g_3^2 = g_2$. Allora g_3 non ha ordine 2 e quindi ha necessariamente ordine 4, cioè G è ciclico generato da g_3 , e pongo $g := g_3$, e si ha $g_2 = g^2$.#*Si verifica anche che $g_4 = g^3$, infatti

$$\alpha^{g^3} = \beta^{g^2} = (-\alpha)^g = -\beta$$

quindi $\alpha^{g^3} = \alpha^{g_4}$ e $g_4 = g^3$ .Concludo che $G = \{1, g, g^2, g^3\}$ con $\alpha^g = \beta$ .L'estensione $M \supseteq \mathbb{Q}$ è normale perché M è campo di spezzamento su $\mathbb{Q}$ di $f(x)$ e siamo in caratteristica 0.

3. CORRISPONDENZA DI GALOIS: L'unico sottogruppo proprio di G è $H = \{1, g^2\}$, e determino il corrispondente campo intermedio $H' = \mathrm{Fix(H)}$. Basta determinare gli elementi di M fissati da g^2 . Essendo M campo di spezzamento di $f(x)$ si ha

$$M = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3,\ a_i \in \mathbb{Q},\ \forall i, \alpha^4 = 4\alpha^2 - 2\}$$

Dato $\xi \in M$, siccome g^2 è tale che $\alpha \mapsto -\alpha$, si ha

$$\xi^{g^2} = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3$$

e $\xi^{g^2} = \xi$ se e solo se $a_1 = a_3 = 0$. Si ha quindi

$$H' = \{a_0 + a_2\alpha^2,\, a_i \in \mathbb{Q},\, \forall i\} = \mathbb{Q}(\alpha^2)$$

Diagramma dei campi: $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}(\alpha^2) \supseteq \mathbb{Q}$ (i tre campi sono uniti da un segmento)Diagramma dei sottogruppi: $1 \leq H \leq G$

6.10 Nono Esercizio

Esercizio 7.9

Determinare il gruppo di Galois $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ dove ω è una radice sedicesima dell'unità.

6.10.1 Gruppo di Galois

Avevamo precedentemente calcolato che $\phi_{16}(x) = x^8+1$, e sappiamo che $\mathcal{G}(M/\mathbb{Q}) \cong U_{16}$ con U_{16} gruppo degli elementi invertibili di $\frac{\mathbb{Z}}{16\mathbb{Z}}$, quindi

$$U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

e $|U_{16}| = \varphi(16) = 8$.

Determiniamo gli ordini degli elementi di U_{16} :

$$\begin{aligned}
3^2 = 9,\, 3^3 = 11,\, 3^4 = 81 = 1 &\longrightarrow \quad o(3) = 4\\
5^2 = 9,\, 5^3 = 13,\, 5^4 = 9^2 = 1 &\longrightarrow \quad o(5) = 4\\
7^2 = 49 = 1 &\longrightarrow \quad o(7) = 2\\
9^2 = 81 = 1 &\longrightarrow \quad o(9) = 2\\
11^2 = (-5)^2 = 9,\, 11^4 = 9^2 = 1 &\longrightarrow \quad o(11) = 4\\
13^2 = (-3)^2 = 9,\, 13^4 = 1 &\longrightarrow \quad o(13) = 4\\
15^2 = (-1)^2 = 1 &\longrightarrow \quad o(15) = 2
\end{aligned}$$

Allora

$$G = \{g_1, g_3, g_5, g_7, g_9, g_{11}, g_{13}, g_{15}\}$$

con g_i tale che $\omega^{g_i} = \omega^i$.

G è abeliano rispetto al prodotto e ha ordine 8. I gruppi abeliani di ordine 8 sono $C_2 \times C_2 \times C_2$, $C_2 \times C_4$ e C_8 . In particolare, siccome in G ci sono elementi di ordine 4, escludo che $G = C_2 \times C_2 \times C_2$, e siccome non è ciclico escludo $G = C_8$, quindi rimane $G = C_2 \times C_4$.

I sottogruppi di ordine 4 sono i seguenti:

1. $H_1 :=< g_3 >= \{1, g_3, g_3^2, g_3^3\} = \{1, g_3, g_9, g_{11}\}$ (infatti siccome $3^2 = 9, 3^3 = 11$, si ha $g_3^2 = g_9$, $g_3^3 = g_{11}$)
2. $H_2 :=< g_5 >= \{1, g_5, g_9, g_{13}\}$ (come prima, siccome $5^2 = 9$ e $5^3 = 13$, si ha $g_3^2 = g_9$ e $g^3 = g_{13}$)
3. Si ha poi un sottogruppo di ordine 4 della forma $C_2 \times C_2$,

$$< g_7 > \times < g_9 >= \{1, g_7, g_9, g_7 * g_9\}$$

$$\omega \mapsto^{g_9} \omega^9 \mapsto^{g_7} \omega^{63} = \omega^{15}, \longrightarrow g_7 * g_9 = g_{15}$$

quindi

$$H_3 :=< g_7 > \times < g_9 >= \{1, g_7, g_9, g_{15}\}$$

Determino i campi intermedi corrispondenti. Il polinomio ciclotomico $\phi_{16}(x)$ è polinomio minimo di ω su $\mathbb{Q}$ e $\mathbb{Q}(\omega) = \frac{\mathbb{Q}}{(\phi_{16})}$ quindi

$$\mathbb{Q}(\omega) = \{a_0+a_1\omega+a_2\omega^2+a_3\omega^3+a_4\omega^4+a_5\omega^5+a_6\omega^6+a_7\omega^7,\ a_i \in \mathbb{Q},\ \forall i,\ \omega^8 = -1\}$$

1. $H_1' = \{1, g_3, g_9, g_{11}\}$,

$$H_1' = \mathrm{Fix(H_1)} = \{\alpha \in \mathbb{Q}(\omega) \text{ t.c. } \alpha^{g_3} = \alpha\}.$$

Dato un generico $\alpha \in \mathbb{Q}(\omega)$, siccome $\omega \mapsto \omega^3$ mediante g_3 , si ha

$$\alpha^{g_3} = a_0 + a_1\omega^3 + a_2\omega^6 + a_3\omega^9 + a_4\omega^{12} + a_5\omega^{15} + a_6\omega^{18} + a_7\omega^{21}$$

e devo esprimere gli ω^i, $i > 7$ in termini della base $\{\omega^i\}_{i=1}^7$. Tenendo conto che $\omega^8 = -1$:

$$\alpha^{g_3} = a_0 + a_1\omega^3 + a_2\omega^6 - a_3\omega - a_4\omega^4 - a_5\omega^7 + a_6\omega^2 + a_7\omega^5$$

e chiedere la condizione $\alpha = \alpha^{g_3}$ equivale a chiedere

$$\begin{cases} a_1 = a_3 \\ a_2 = a_6 \\ -a_3 = a_1 \\ a_4 = -a_4 \\ a_7 = -a_5 \\ a_7 = a_5 \end{cases}$$

$$\longrightarrow a_1 = a_3 = a_4 = a_5 = a_7 = 0,\ a_2 = a_6$$

quindi

$$\mathrm{Fix(H_1)} = \{\mathrm{a_0 + a_2\omega^2 + a_2\omega^6},\ \mathrm{a_i} \in \mathbb{Q},\ \forall \mathrm{i}\} = \mathbb{Q}(\omega^2 + \omega^6)$$

infatti si ottiene che $(\omega^2 + \omega^6)^2 = 4$ e quindi $\omega^2 + \omega^6$ è radice di $x^2 - 4$.

2. $H_2 = \{1, g_5, g_9, g_{13}\}$, determino $H_2' = \mathrm{Fix}(\mathrm{H}_2)$. Basta determinare gli elementi di $\mathbb{Q}(\omega)$ fissati da g_5 . Prendo $\alpha \in \mathbb{Q}(\omega)$, allora

$$\alpha^{g_5} = a_0 + a_1\omega^5 + a_2\omega^{10} + a_3\omega^{15} + a_4\omega^{20} + a_5\omega^{25} + a_6\omega^{30} + a_7\omega^{35}$$

$$\alpha^{g_5} = a_0 + a_1\omega^5 - a_2\omega^2 - a_3\omega^7 + a_4\omega^4 + a_5\omega^9 - a_6\omega^6 + a_7\omega^3$$

allora $\alpha^{g_5} = \alpha$ implica

$$\begin{cases} a_1 = a_5 \\ a_2 = 0 \\ -a_3 = a_7 \\ -a_5 = a_1 \\ a_6 = 0 \\ a_7 = a_3 \end{cases}$$

$$\longrightarrow a_1 = a_2 = a_3 = a_5 = a_6 = a_7 == 0$$

$$\mathrm{Fix}(\mathrm{H}_2) = \{\mathrm{a}_0 + \mathrm{a}_4\omega^4,\ \mathrm{a}_\mathrm{i} \in \mathbb{Q},\ \forall \mathrm{i}\} = \mathbb{Q}(\omega^4) = \mathbb{Q}(\mathrm{i})$$

perché ω^4 è radice di $x^2 + 1$.

3. $H_3 = \{1, g_7, g_9, g_{15}\}$. **Ad un generico α applico prima g_7 , e poi ad α^{g_7} applico g_9 .**

$$\alpha^{g_7} = a_0 + a_1\omega^7 + a_2\omega^{14} + a_3\omega^{21} + a_4\omega^{28} + a_5\omega^{35} + a_6\omega^{42} + a_7\omega^{49}$$

$$\alpha^{g_7} = a_0 + a_1\omega^7 - a_2\omega^6 + a_3\omega^5 - a_4\omega^4 + a_5\omega^3 - a_6\omega^2 + a_7\omega$$

e imponendo $\alpha^{g_7} = \alpha$ si ha

$$\begin{cases} a_1 = a_7 \\ -a_2 = a_6 \\ a_3 = a_5 \\ -a_4 = 0 \\ a_5 = a_3 \end{cases}$$

$$\mathrm{Fixg}_7 = \{\mathrm{a}_0 + \mathrm{a}_1\omega + \mathrm{a}_2\omega^2 + \mathrm{a}_3\omega^3 + \mathrm{a}_3\omega^5 - \mathrm{a}_2\omega^6 + \mathrm{a}_1\omega^7\}$$
$$= \{a_0 + a_1(\omega + \omega^7) + a_2(\omega^2 - \omega^6) + a_3(\omega^3 + \omega^5)\}$$

Ora verifico quali tra gli elementi fissati da g_7 sono fissati anche da g_9 , e preso $\beta \in g_7$:

$$\beta^{g_9} = a_0 - a_1(\omega + \omega^7) + a_2(\omega^2 - \omega^6) + a_3(\omega^3 + \omega^5)$$

e imponendo $\beta^{g_9} = \beta$:

$$H_3' = \{\alpha = a_0 + a_2(\omega^2 - \omega^6),\ a_i \in \mathbb{Q},\ \forall i\} = \mathbb{Q}(\omega^2 - \omega^6) = \mathbb{Q}(\sqrt{2})$$

Gli elementi di ordine 2 nel gruppo considerato sono g_7, g_9, g_{15} , quindi i sottogruppi di ordine 2 sono $H_1 := \{1, g_7\}$, $H_2 := \{1, g_9\}$, $H_3 := \{1, g_{15}\}$. **Determiniamo i campi intermedi corrispondenti**:

- $H_1 = \{1, g_7\}$. Per calcoli precedenti

$$H_1' = \{a_0 + a_1(\omega + \omega^7) + a_2(\omega^2 - \omega^6) + a_3(\omega^3 + \omega^5),\ a_i \in \mathbb{Q},\ \forall i\} = \mathbb{Q}(\omega + \omega^7)$$

- $H_2 = \{1, g_9\}$; siccome $\omega^9 = -\omega$, preso $\alpha \in \mathbb{Q}(\omega)$ si ha

$$\alpha^{g_9} = a_0 - a_1\omega + a_2\omega^2 - a_3\omega^3 + a_4\omega^4 - a_5\omega^5 + a_6\omega^6 - a_7\omega^7$$

e imponendo $\alpha^{g_9} = \alpha$ si ottiene $a_1 = a_3 = a_5 = a_7 = 0$. Quindi

$$H_2' = \{a_0 + a_2\omega^2 + a_4\omega^4 + a_6\omega^6,\ a_i \in \mathbb{Q},\ \forall i\} = \mathbb{Q}(\omega^2)$$

- $H_3 = \{1, g_{15}\}$. Siccome $\omega^{15} = -\omega^7$, dato $\alpha \in \mathbb{Q}(\omega)$ si ha

$$\alpha^{g_{15}} = a_0 - a_1\omega^7 - a_2\omega^6 - a_3\omega^5 - a_4\omega^4 - a_5\omega^3 - a_6\omega^2 - a_7\omega$$

e imponendo $\alpha = \alpha^{g_{15}}$ si ha

$$\begin{cases} -a_1 = a_7 \\ -a_2 = a_6 \\ -a_3 = a_5 \\ a_4 = 0 \end{cases}$$

quindi

$$H_3' = \{a_0 + a_1(\omega - \omega^7) + a_2(\omega^2 - \omega^6) + a_3(\omega^3 - \omega^5),\ a_i \in \mathbb{Q},\ \forall i\} = \mathbb{Q}(\omega - \omega^7)$$

6.11 Decimo esercizio

Esercizio 7.10

Dare un esempio di campi tali che $K \subseteq L \subseteq M$ e $L \supseteq K$ è un'estensione normale, $M \supseteq L$ è un'estensione normale ma $M \supseteq K$ non è un'estensione normale.

Avevamo precedentemente mostrato che il campo di spezzamento su $\mathbb{Q}$ del polinomio $f(x) = x^4 - 2$ è $\mathbb{Q}(\sqrt[4]{2}, i)$. Pongo $K = \mathbb{Q}$ e $M = \mathbb{Q}(\sqrt[4]{2})$, in questo modo $M \supseteq K$ non è normale perché $x^4 - 2$ ammette una radice in M ma non si spezza su M .

Se pongo $L = \mathbb{Q}(\sqrt{2})$:

1. $M \supseteq L \supseteq K$.
2. $L \supseteq K$ è normale perché L è campo di spezzamento su K del polinomio $x^2 - 2$.
3. $M \supseteq L$ è normale perché M è campo di spezzamento su L del polinomio $x^2 - \sqrt{2}$;
4. $M \supseteq K$ non è normale perché il polinomio $x^4 - 2$ ha una radice in M ma non si spezza su M .

6.12 Undicesimo esercizio

Esercizio 7.11

Siano p primo e $n \geq 1$ un intero. Dimostrare che

$$\phi_{pn}(x) = \begin{cases} \phi_n(x^p) & p \mid n \\ \frac{\phi_n(x^p)}{\phi_n(x)} & p \nmid n \end{cases}$$

Sia Ω_n l'insieme delle radici primitive n -esime dell'unità, si ha

$$\phi_n(x^p) = \prod_{\xi \in \Omega_n} (x^p - \xi)$$

Se ω è radice di $x^p - \xi$, segue che $\omega^p = \xi$. Allora $o(\omega^p) = o(\xi) = n$ perché ξ è una radice primitiva n-esima. Siccome $\omega^p \in \langle \omega \rangle$ si ha anche che $o(\omega^p) = \frac{o(\omega)}{M.C.D.(p, o(\omega))}$, e eguagliando le due espressioni per $o(\omega^p)$ si ha:

$$\frac{o(\omega)}{M.C.D.(p, o(\omega))} = n, \text{ relazione } \star$$

segue che $n \mid o(\omega)$. Allora distinguo i due casi:

1. Se $p \mid n$, $p \mid o(\omega)$, allora $M.C.D.(o(\omega), p) = p$ e $o(\omega) = pn$ per la relazione $\star$. Allora le radici di $\phi_n(x^p)$ (cioè gli ω tali che $\omega^p = \xi$, $\xi \in \Omega_n$) coincidono con le radici primitive di pn -me di 1 , e quindi $\phi_n(x^p) = \phi_{pn}(x)$.

2. se $p \nmid n$, per la relazione $\star$ $o(\omega) = n * M.C.D.(o(\omega), p)$, quindisi verificano due possibilità: 1. $M.C.D.(o(\omega), p) = 1$ e quindi $o(\omega) = n$; 2. $M.C.D.(o(\omega), p) = p$ e quindi $o(\omega) = np$ .Allora tutte e sole le radici di $\phi_n(x^p)$ sono radici primitive di n -me di 1 oppure le radici primitive pn -me di 1 , e quindi $\phi_n(x^p) = \phi_n(x) * \phi_{np}(x)$, cioè $\phi_{pn}(x) = \frac{\phi_n(x^p)}{\phi_n(x)}$.

6.13 Dodicesimo esercizio

Esercizio 7.12

Sia M il campo di spezzamento di $x^4 - 2$ su $\mathbb{Q}$ in $\mathbb{C}$. Mostrare che $M = \mathbb{Q}(i + \sqrt[4]{2})$.

Suggerimento: trovare almeno cinque elementi distinti nell'orbita di $i + \sqrt[4]{2}$ sotto l'azione di $\mathcal{G}(M/\mathbb{Q})$.

Abbiamo dimostrato precedentemente che, se pongo $\alpha = \sqrt[4]{2}$, $M = \mathbb{Q}(\alpha, i)$ e $\mathcal{G}(M/\mathbb{Q}) = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$, con

$$x \, t.c. \, \alpha^x = \alpha i, \; i^x = i$$

$$y \, t.c. \, \alpha^y = \alpha, \; i^y = -i.$$

Pongo $\beta = i + \alpha$ e **cerco almeno cinque elementi distinti dell'orbita di** β **sotto l'azione di** $\mathcal{G}(M/\mathbb{Q})$:

$$\beta^x = i^x + \alpha^x = i + i\alpha = i * (1 + \alpha)$$
$$\beta^y = i^y + \alpha^y = -i + \alpha$$
$$\beta^{xy} = i^{xy} + \alpha^{xy} = i^y + (i\alpha)^y = -i - i\alpha = -i(1 + \alpha)$$
$$\beta^{x^2} = i^{x^2} + \alpha^{x^2} = i - \alpha$$
$$\beta^{x^3} = i^{x^3} + \alpha^{x^3} = i - i\alpha = i(1 - \alpha)$$

Ora mostro che $M = \mathbb{Q}(\beta)$. L'inclusione $\mathbb{Q}(\beta) \subseteq M$ è ovvia perché $\beta \in M$. Viceversa, proviamo che $M \subseteq \mathbb{Q}(\beta)$. Considero il polinomio minimo $h(x)$ di β sopra $\mathbb{Q}$. Gli elementi della forma β^g con $g \in \mathcal{G}(M/\mathbb{Q})$ sono ancora radici di $h(x)$, infatti, applicando g all'equazione $h(\beta) = 0$ ottengo $0 = g(\beta^g)$. Con i conti precedenti ho trovato almeno cinque radici distinte di $g(x)$, quindi grh(x) ≥ 5 , cioè $|\mathbb{Q}(\beta) : \mathbb{Q}| \geq 5$.

Sappiamo anche che $|M : \mathbb{Q}| = 8$, e quindi gr(h(x)) $= |\mathbb{Q}(\beta) : \mathbb{Q}| \mid 8$, ma allora unendo queste due condizioni l'unica possibilità è che $|\mathbb{Q}(\beta) : \mathbb{Q}| = 8$, cioè $\mathbb{Q}(\beta) = M$.

6.14 Tredicesimo esercizio

Esercizio 7.13

Siano $p_1, p_2, \ldots, p_n$ numeri primi distinti, e sia $M = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$.

1. Mostrare che $M \supseteq \mathbb{Q}$ è normale;
2. Mostrare che $G = \mathcal{G}(M/\mathbb{Q})$ è elementare abeliano di ordine 2^n . (dire che G è elementare abeliano significa che $G = C_2 \times \cdots \times C_2$, $o(G) = 2^n$, G è abeliano e tutti gli elementi di G esclusa l'unità hanno ordine 2)

Suggerimento: una possibilità per mostrare la parte 2 è mostrare che i campi $\mathbb{Q}(\sqrt{k})$ sono tutti distinti, al variare di k sui $2^n - 1$ prodotti non banali e distinti di elementi distinti dell'insieme che contiene $p_1, p_2, \ldots, p_n$.

1. Siamo in caratteristica 0 e M è campo di spezzamento del polinomio $(x^2 - p_1)(x^2 - p_2) * \cdots * (x^2 - p_n)$ sopra $\mathbb{Q}$, quindi $M \supseteq \mathbb{Q}$ è normale.
2. Considero la catena di estensioni:

   $$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1}) \subseteq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) \subseteq \cdots \subseteq M$$

   Per il teorema della torre

   $$|M : \mathbb{Q}| = |M : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})| * \cdots * |\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})/\mathbb{Q}(\sqrt{p_1})| * |\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}|$$

   dove ogni fattore è ≤ 2 perché per ogni i , $\sqrt{p_i}$ è uno zero del polinomio $x^2 - p_i \in \mathbb{Q}[x]$ .Allora $o(G) = |M : \mathbb{Q}| = 2^m$ per un certo $m \in \mathbb{N}, m \leq n$

e **dobbiamo provare che** $m = n$ **, cioè che** $o(G) = 2^n$ .Supponendo di aver argomentato il suggerimento, osservo che $\mathbb{Q}(\sqrt{k})$ è un campo intermedio fra $\mathbb{Q}$ e M di grado 2, allora, ponendo $H_k = \mathbb{Q}(\sqrt{k})'$,

$$2 = |\mathbb{Q}(\sqrt{k}) : \mathbb{Q}| = |G : H_k|.$$

Siccome supponiamo che i campi $\mathbb{Q}(\sqrt{k})$ siano tutti distinti, anche i corrispondenti sottogruppi H_k di indice 2 in G sono tutti distinti e sono almeno 2^n , di conseguenza esistono almeno 2^n elementi in G , cioè $o(G) > 2^n$. Segue che $m = n$.**Gli elementi di** G **hanno ordine 2, eccetto l'unita'**, infatti, dato $g \in \mathcal{G}(M/\mathbb{Q})$, esso manda l'elemento $\sqrt{p_i}$ in sé stesso oppure in $-\sqrt{p_i}$, e quindi $g^2 = 1$. G **è abeliano**: in generale dato un gruppo G , se $g^2 = 1$ per ogni $g \in G$, allora G è abeliano. Infatti, dati $x, y \in G$, segue che $xyxy = 1$. D'altra parte, $x^2 = 1$ implica $x = x^{-1}$ e $y^2 = 1$ implica $y = y^{-1}$. Dall'uguglianza $xyxy = 1$, moltiplicando a destra per y e poi per x , si ha $xy = yx$.**Infine argomentiamo il sugerimento**: Sia $k \neq h$, e suppongo per assurdo che $\mathbb{Q}(\sqrt{h}) = \mathbb{Q}(\sqrt{k})$. Se questo avviene, si deve avere in particolare che $\sqrt{k} \in \mathbb{Q}(\sqrt{h})$, cioè, preso un generico elemento in $\mathbb{Q}(\sqrt{h})$ della forma $a + b\sqrt{h}$, si deve avere.ì

$$(a + b\sqrt{h})^2 = k$$

e sviluppando il quadrato

$$a^2 + b^2h + 2ab\sqrt{h} = k, \longrightarrow ab = 0$$

Il caso $b = 0$ si esclude perché se così fosse si avrebbe $a^2 = k$, con $a \in \mathbb{Q}$. Se invece $a = 0$ si ha $b^2h = k$. Siccome abbiamo supposto $h \neq k$, esisterà un p_i che compare nella scrittura di h ma non di k , cioè esiste un p_i che divide h e non divide k , e quindi l'equazione sopra non può essere vera.

6.15 Quattordicesimo esercizio

Esercizio 7.14

Nelle ipotesi dell'esercizio 2, mostrare che per ogni indice i , esiste $g_i \in \mathcal{G}(M/\mathbb{Q})$ tale che $\sqrt{p_i}^{g_i} = -\sqrt{p_i}$, mentre $\sqrt{p_j}^{g_i} = \sqrt{p_j}$ per $j \neq i$. Usare questo fatto per mostrare che $\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}$ sono indipendenti su $\mathbb{Q}$.

Dato $g \in \mathcal{G}(M/\mathbb{Q})$, esso è determinato dalla sua azione sulle radici; abbiamo mostrato nell'esercizio precedente che in G ci sono esattamente 2^n elementi, quindi g deve necessariamente includere i morfismi g_i tali che $\sqrt{p_i}^{g_i} = -\sqrt{p_i}$ e $\sqrt{p_j}^{g_j} = \sqrt{p_j} \forall j \neq i$.

Mostriamo ora la lineare indipendenza dei g_i : Supponiamo di avere una combinazione lineare della forma

$$\sum_{j=1}^{n} \lambda_j \sqrt{p_j} = 0, \ \lambda_j \in \mathbb{Q}.$$

Applicando g_i a entrambi i membri ottengo

$$0 = \sum_j \lambda_j^{g_i} \sqrt{p_j}^{g_i}$$

e siccome i λ_j stanno in $\mathbb{Q}$ e vengono fissati si ha

$$0 = \sum_{j \neq i} \lambda_j \sqrt{p_j} - \lambda_i \sqrt{p_i}$$

ed eguagliando i coefficienti rispetto agli elementi della base nelle due combinazioni lineari ottengo $\lambda_i = -\lambda_i$, cioè $\lambda_i = 0$. Ripetendo questo procedimento per ogni i ottengo che tutti gli scalari sono nulli.

6.16 Quindicesimo esercizio

Esercizio 7.15

Nelle ipotesi degli esercizi 2 e 3, mostrare che $M = \mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n})$.

Suggerimento: mostrare che l'orbita di $\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n}$ sotto l'azione di $\mathcal{G}(M/\mathbb{Q})$ contiene almeno 2^n elementi distinti.

Cerco 2^n elementi distinti dell'orbita di β sotto l'azione di $\mathcal{G}(M/\mathbb{Q})$, dove pongo $\beta = \sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n}$. Osservo che

$$\beta^{g_i} = \sqrt{p_1} + \sqrt{p_2} - \sqrt{p_i} + \cdots + \sqrt{p_n}$$

e quindi le immagini di β mediante i g_i sono n elementi distinti dell'orbita. Poi, se considero prodotti della forma $g_i g_j$, si ha che

$$\beta^{g_i g_j} = \sqrt{p_1} + \sqrt{p_2} - \sqrt{p_i} + \cdots - \sqrt{p_j} + \cdots + \sqrt{p_n}$$

e ottengo $\binom{n}{2}$ elementi distinti dell'orbita.

Considero allora tutti i possibili prodotti di elementi distinti di $\mathcal{G}(M/\mathbb{Q})$, che sono 2^n ; applicandoli a β ottengo 2^n elementi nell'orbita di β , della forma

$$\sum_i \lambda_i \sqrt{p_i},\ \lambda_i = \pm 1$$

Mostro che gli elementi ottenuti sono tutti distinti: Considero due prodotti g, h di elementi di $\mathcal{G}(M/\mathbb{Q})$, devo mostrare che $\beta^g \neq \beta^h$. Sia $\beta^g = \sum_i \lambda_i \sqrt{p_i}$ e $\beta^h = \sum_i \lambda_i' \sqrt{p_i}$; Se supponiamo per assurdo che $\beta^g = \beta^h$ segue che

$$\beta^g - \beta^h = \sum_i (\lambda_i - \lambda_i') \sqrt{p_i} = 0$$

ma allora, siccome i $\sqrt{p_i}$ sono indipendenti, segue che $\lambda_i = \lambda_i' \forall i$, e quindi $g = h$.

Mostrare che l'estensione è semplice equivale a mostrare che $|\mathbb{Q}(\beta) : \mathbb{Q}| = 2^n$. Sappiamo che $|M : \mathbb{Q}| = 2^n$ e abbiamo appena mostrato che $|\mathbb{Q}(\beta) : \mathbb{Q}| \geq 2^n$,

però siccome vale l'inclusione $\mathbb{Q}(\beta) \subseteq M$, si deve avere $|\mathbb{Q}(\beta) : \mathbb{Q}| \mid |M : \mathbb{Q}|$, cioè $|\mathbb{Q}(\beta) : \mathbb{Q}| = 2^n$.

6.17 Sedicesimo esercizio

Esercizio 7.16

Trovare un polinomio esplicito $f(x) \in \mathbb{Q}[x]$ il cui gruppo di Galois abbia ordine 3 .

Suggerimento: Considerare $\mathbb{Q}(\omega)$ con ω radice settima primitiva di 1.

Data ω radice settima primitiva dell'unità, $G = \mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U_7$, e U_7 è un gruppo ciclico di ordine $\varphi(7) = 6$. Siccome il teorema di Lagrange si inverte nei gruppi ciclici, esiste un sottogruppo $H \leq G$ con $|H| = 2$, cioè $H = \{1, g\}$. Se ad esempio prendo g tale che $\omega \mapsto \omega^6$, si ha che $o(g) = 2$ perché $o(6) = 2$ in U_7 (infatti $6^2 = 36 \equiv 1 \mod 7$).

Calcolo il corrispondente campo intermedio:

$$\text{Fix(H)} = \{\alpha \in \mathbb{Q}(\omega) \,\text{t.c.}\, \alpha^{\text{g}} = \alpha\}$$

Siccome il polinomio minimo di ω è $\phi_7(x)$ che ha grado 6 , segue che $|\mathbb{Q}(\omega) : \mathbb{Q}| = 6$ e

$$\mathbb{Q}(\omega) = \{a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4 + a_5\omega^5,\ a_i \in \mathbb{Q} \forall i\}$$

Applico g ad un generico elemento di $\mathbb{Q}(\omega)$:

$$\alpha^g = \sum_i a_i(\omega^g)^i = \sum_i a_i\omega^{6i}$$
$$= a_0 + a_1\omega^6 + a_2\omega^{12} + a_3\omega^{18} + a_4\omega^{24} + a_5\omega^{30}$$

e riducendo i coefficienti modulo 7 :

$$= a_0 + a_1\omega^6 + a_2\omega^5 + a_3\omega^4 + a_4\omega^3 + a_5\omega^2$$

e siccome ω è radice del polinomio ciclotomico, si ha che $\omega^6 = -1 - \omega - \omega^2 - \omega^3 - \omega^4 - \omega^5$, quindi

$$= a_0 - a_1(\omega^5 + \omega^4 + \omega^3 + \omega^2 + \omega + 1) + a_2\omega^5 + a_3\omega^4 + a_4\omega^3 + a_5\omega^2$$

e imponendo $\alpha^g = \alpha$ ottengo

$$\begin{cases} a_0 + a_1 = 0 \\ a_1 = 0 \\ a_5 = a_2 \\ a_4 = a_3 \end{cases}$$

quindi gli elementi di Fix(H) sono della forma:

$$\alpha = a_0 + a_2(\omega^2 + \omega^5) + a_3(\omega^3 + \omega^4)$$

Osservo che

$$(\omega^2 + \omega^5)^2 = \omega^4 + 2\omega^7 + \omega^{10} = \omega^4 + \omega^3 + 2$$
$$(\omega^2 + \omega^5)^3 = (\omega^2 + \omega^5)(\omega^4 + \omega^3 + 2) =$$
$$= \omega^6 + \omega^5 + 2\omega^2 + \omega^9 + \omega^8 + 2\omega^5$$

e sostituendo l'espressione di ω^6 :

$$= -1 - \omega - \omega^2 - \omega^3 - \omega^4 + 2\omega^2 + \omega^2 + \omega + 2\omega^5$$
$$= -1 - \omega^3 - \omega^4 + 2\omega^2 + 2\omega^5 = 1 - \beta^2 + 2\beta$$

β è radice di $f(x) = x^3 + x^2 - 2x + 1$. Se pongo $L = H'$, segue che $L \supset \mathbb{Q}$ è normale perché H è normale in G . Se $f(x)$ ammette una radice in L , allora si spezza in fattori lineari su L . Inoltre $|L : \mathbb{Q}| = 3$ quindi L è campo di spezzamento di $f(x)$ su $\mathbb{Q}$. Infine $|L : \mathbb{Q}| = \mathcal{G}(L/\mathbb{Q}) = 3$, e quindi $f(x)$ è il polinomio cercato.

Capitolo 7

Fonti per testo e immagini; autori; licenze

7.1 Testo

- **Corso:Algebra IV I1/Richiami sui campi/Ripasso di teoria dei campi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Richiami_sui_campi/Ripasso_di_teoria_dei_campi?oldid=48355 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Richiami sui campi/Campo di spezzamento di un polinomio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Richiami_sui_campi/Campo_di_spezzamento_di_un_polinomio?oldid=48397 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Richiami sui campi/Lemma di Zorn e relative applicazioni** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Richiami_sui_campi/Lemma_di_Zorn_e_relative_applicazioni?oldid=48279 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Richiami sui campi/Chiusura algebrica di un campo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Richiami_sui_campi/Chiusura_algebrica_di_un_campo?oldid=48293 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Richiami sui campi/(Non) unicità della chiusura algebrica** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Richiami_sui_campi/(Non)_unicit%C3%A0_della_chiusura_algebrica?oldid=48384 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Teoria di Galois** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Teoria_di_Galois?oldid=48210 *Contributori:* Toma.luca95, Irene, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Oggetti chiusi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Oggetti_chiusi?oldid=48133 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Esempio di studio di estensione** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Esempio_di_studio_di_estensione?oldid=48506 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Stabilità e normalità** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Stabilit%C3%A0_e_normalit%C3%A0?oldid=48093 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Caratterizzazione delle estensioni normali di grado finito** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Caratterizzazione_delle_estensioni_normali_di_grado_finito?oldid=48328 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

- **Corso:Algebra IV I1/Teoria di Galois/Condizioni equivalenti alla normalità di un'estensione** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Condizioni_equivalenti_alla_normalit%C3%A0_di_un'estensione?oldid=48054 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Esempio di campo di spezzamento non normale** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Esempio_di_campo_di_spezzamento_non_normale?oldid=48441 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Teoria di Galois/Chiusura spezzante e chiusura normale** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Chiusura_spezzante_e_chiusura_normale?oldid=48195 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Estensioni ciclotomiche/Estensioni ciclotomiche** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Estensioni_ciclotomiche/Estensioni_ciclotomiche?oldid=48237 *Contributori:* Toma.luca95, V.e.padulano, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Estensioni ciclotomiche/Complementi sui polinomi ciclotomici** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Estensioni_ciclotomiche/Complementi_sui_polinomi_ciclotomici?oldid=48178 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Costruzioni con righe e compasso/Definizioni di base** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Costruzioni_con_righe_e_compasso/Definizioni_di_base?oldid=48139 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Costruzioni con righe e compasso/Criterio per la costruibilità** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Costruzioni_con_righe_e_compasso/Criterio_per_la_costruibilit%C3%A0?oldid=48059 *Contributori:* Toma.luca95, Irene, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Appendici/Teorema dell'elemento primitivo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Appendici/Teorema_dell'elemento_primitivo?oldid=48048 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Appendici/Separabilità e inseparabilità** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Appendici/Separabilit%C3%A0_e_inseparabilit%C3%A0?oldid=48536 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Appendici/Derivazioni** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Appendici/Derivazioni?oldid=48304 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Appendici/Estensioni di grado infinito** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Appendici/Estensioni_di_grado_infinito?oldid=48300 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Primo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Primo_esercizio?oldid=48400 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Secondo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Secondo_esercizio?oldid=48154 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Terzo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Terzo_esercizio?oldid=48223 *Contributori:* Toma.luca95, V.e.padulano, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Quarto esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Quarto_esercizio?oldid=48030 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Quinto esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Quinto_esercizio?oldid=48377 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Sesto esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Sesto_esercizio?oldid=48432 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

- **Corso:Algebra IV I1/Esercizi/Settimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Settimo_esercizio?oldid=48145 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Ottavo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Ottavo_esercizio?oldid=48363 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Nono Esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Nono_Esercizio?oldid=48439 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Decimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Decimo_esercizio?oldid=48228 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Undicesimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Undicesimo_esercizio?oldid=48417 *Contributori:* Toma.luca95, Mapelli Dario e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Dodicesimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Dodicesimo_esercizio?oldid=48241 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Tredicesimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Tredicesimo_esercizio?oldid=48311 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Quattordicesimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Quattordicesimo_esercizio?oldid=48465 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Quindicesimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Quindicesimo_esercizio?oldid=48481 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra IV I1/Esercizi/Sedicesimo esercizio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Sedicesimo_esercizio?oldid=48191 *Contributori:* Toma.luca95 e Mmontrasio

7.2 Immagini

7.3 Licenza dell'opera

- [Project:Copyright Creative Commons Attribution Share Alike 3.0 & GNU FDL]
- Creative Commons Attribution-Share Alike 3.0