Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali

Corso di Laurea in Matematica

ESTENSIONI CICLICHE ED ESTENSIONI CICLOTOMICHE DI CAMPI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Dora Pastore

III Sessione
Anno Accademico 2011/2012

Alle mie donne, Clementina e Sara,
che hanno imparato presto il significato della parola sacrificio.

Per tre cose vale la pena di vivere: la matematica, la musica e l'amore.
Renato Caccioppoli.

Introduzione

La Teoria di Galois è un'importante branca dell'algebra astratta che si sviluppa intorno alla prima metà del XIX secolo seguendo le orme degli studi dell'omonimo matematico francese. L'idea innovativa di Evariste Galois fu quella di usare i gruppi di permutazioni per descrivere le relazioni esistenti tra le soluzioni di un'equazione polinomiale e stabilirne la risolubilità per radicali o meno. L'approccio moderno alla sua Teoria, sviluppato da Dedekind, Kronecker e altri matematici, si basa sull'idea di ricondurre il problema della risolubilità per radicali di un'equazione algebrica allo studio delle estensioni di campi e di quello che oggi viene chiamato il *Gruppo di Galois* dell'estensione.
Lo scopo di questa tesi è quello di analizzare e dare una precisa caratterizzazione di due tipi di estensioni di campi: quelle cicliche (estensioni di Galois il cui gruppo corrispondente è ciclico) e quelle ciclotomiche, che furono studiate per la prima volta da Gauss agli inizi del XIX secolo. Si ricorda che queste estensioni di campi costituiscono i mattoni fondamentali per lo studio delle estensioni radicali caratterizzate dal *Teorema fondamentale di Galois*; inoltre trovano numerose applicazioni in teoria dei numeri e in geometria algebrica.
Per procedere nell'analisi delle estensioni cicliche, si è ritenuto opportuno fare delle distinzioni in base alla relazione tra grado dell'estensione e caratteristica del campo. Se $\mathbb{K}$ è un campo di caratteristica $p \neq 0$ e $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione ciclica di grado n, allora posto $n = mp^t$, con m coprimo con p, è possibile costruire una catena di t campi intermedi e in particolare di estensioni cicliche, una di grado m e tutte le altre di grado p. Nel caso particolare in cui n sia proprio uguale a p si ha che $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione ciclica di grado p se e solo se $\mathbb{F}$ è il campo di spezzamento di un polinomio della forma $x^p - x - a \in \mathbb{K}[x]$. Quando invece $(n, p) = 1$ cioè n non divide p oppure quando la caratteristica di $\mathbb{K}$ è 0 si è aggiunta l'ipotesi che il campo $\mathbb{K}$ contenga una radice primitva n-esima dell'unità per poter dimostrare che $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione ciclica di grado d, con d che divide n, se e solo se è il campo di spezzamento di un polinomio irriducibile della forma $x^d - b \in \mathbb{K}[x]$ o, equivalentemente se e solo se è il campo di spezzamento di un polinomio della

forma $x^n - a \in \mathbb{K}[x]$. Il caso in cui quest'ultimo polinomio sia del tipo $x^n - 1_{\mathbb{K}}$ è costituito dalle estensioni ciclotomiche di grado n. Per la caratterizzazione delle estensioni ciclotomiche si è considerato solo il caso in cui la caratteristica di $\mathbb{K}$ non divide il grado dell'estesione per ragioni che verranno specificate. E' interessante osservare che se $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione ciclotomica di grado n allora, se n è primo, è anche ciclica e il gruppo di Galois dell'estensione è isomorfo ad un sottogruppo del gruppo moltiplicativo delle unità di $\mathbb{Z}_n$. Definendo il polinomio ciclotomico n-esimo su $\mathbb{K}$ e studiando alcune sue proprietà si dimostra che le estensioni ciclotomiche del campo dei razionali hanno il corrispondente gruppo di Galois isomorfo proprio al gruppo moltiplicativo delle unità di $\mathbb{Z}_n$.

La tesi sviluppa in modo dettagliato i suddetti argomenti che sono divisi in tre capitoli. Il primo capitolo contiene alcuni richiami sulla Teoria dei Gruppi Ciclici e sulla Teoria di Galois necessari per la comprensione di quanto trattato in seguito.

Nel secondo capitolo viene affrontato lo studio delle estensioni cicliche distinguendo i vari casi elencati precedentemente e premettendo le definizioni di traccia e norma, di lineare indipendenza di un insieme di automorfismi e due teoremi che caratterizzano rispettivamente gli elementi di un campo che hanno traccia nulla e quelli che hanno norma nulla. Questi teoremi e definizioni, costituiscono insieme al concetto di radice primitiva n-esima dell'unità, gli strumenti più utilizzati nelle dimostrazioni di questo capitolo.

Il terzo e ultimo capitolo si apre con un'analisi della funzione di Eulero con le sue proprietà e si arriva poi ad una caratterizzazione generale delle estensioni ciclotomiche. Infine dopo aver introdotto e studiato i polinomi ciclotomici, si conclude con il caso particolare dell'estensioni ciclotomiche del campo dei razionali.

Indice

Capitolo 1

Richiami

Per analizzare le estensioni di Galois il cui corrispondente gruppo ha una struttura ciclica è necessario soffermarsi su alcuni concetti, riportati di seguito, che fanno da base e da strumento.

1.1 Richiami di Teoria dei Gruppi Ciclici

Definizione 1.1. Diciamo che un gruppo G è **ciclico** se esiste $a \in G$ tale che

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

In questo caso si dice che **a genera G** o che a è un **generatore** per G e lo si indica con $G =< a >$.

Riportiamo ora il Teorema 3.5, cap.I, tratto da [1] che descrive le proprietà fondamentali dei gruppi ciclici.

Teorema 1.1.1. *Dato gruppo ciclico G generato dall'elemento g, vale:*

(i) *G è abeliano;*

(ii) *ogni immagine omomorfa di G è ciclica;*

(iii) *per ogni sottogruppo non banale H di G si ha H=$< g^m >$, dove m è il più piccolo intero positivo tale che $g^m \in H$.*

Definizione 1.2. Sia G un gruppo. L'**ordine** di G è la cardinalità di G e si indica con $\mid G \mid$.

Proposizione 1.1.2. *Sia G un gruppo ciclico finito di ordine m, generato dall'elemento g. Allora esiste una corrispondenza biunivoca:*

$$\varphi : \{d \in \mathbb{N}^*, d \mid m\} \to \{sottogruppi\ di\ G\}$$

$$d \quad \mapsto \quad < g^d >= H$$

Il seguente Teorema descrive la struttura dei gruppi abeliani finiti. Si veda [1, Teorema 2.1, cap.II]

Teorema 1.1.3 (di struttura dei gruppi abeliani finiti)**.** *Ogni gruppo abeliano G finitamente generato è isomorfo ad una somma diretta finita di gruppi ciclici di ordine $m_1, ..., m_k$, con $m_1 > 1$ e $m_1|m_2|...|m_k$.*

Questo teorema è particolarmente utile nel dimostrare un risultato che sarà alla base della teoria delle estensioni cicliche:

Teorema 1.1.4. *Sia $\mathbb{F}$ un campo e G un sottogruppo finito del gruppo moltiplicativo degli elementi non nulli di $\mathbb{F}$, allora G è un gruppo ciclico. In particolare, il sottogruppo moltiplicativo degli elementi non nulli di un campo finito è ciclico.*

Dimostrazione.
Se $G \neq 1$ è un gruppo abeliano finito, per il *Teorema 1.1.3* :

$$G \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k}$$

ove C_{m_j} è un gruppo moltiplicativo ciclico di ordine m_j e vale $m_1 > 1$, $m_1|m_2|...|m_k$. Dato che $(C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k})^{m_k} = 0$, ogni $u \in G$ è una radice del polinomio $x^{m_k} - 1_{\mathbb{F}} \in \mathbb{F}[x]$, che ha al più m_k radici distinte in $\mathbb{F}$. Dunque $k = 1$ e $G \cong C_{m_k}$.

□

1.2 Richiami sulla Teoria di Galois

In questo capitolo daremo alcuni cenni sulla Teoria di Galois, cercando di porre l'attenzione su specifici risultati che verranno più volte utilizzati successivamente. Prima però richiamiamo alcune definizione generali e il cosiddetto Teorema della torre [3, Teorema 4.3.8].

Definizione 1.3. Dato un anello R, si definisce **caratteristica di** R e si indica con char$R$, il più piccolo intero posivo m tale che $m1_R = 1_R + 1_R + ... + 1_R = 0_R$, ove l'ultima somma ha m addendi.
Se non esite alcun intero m che soddisfa questa proprietà, allora char$R = 0$.

Si osserva subito che se R è un dominio di integrità o in particolare un campo vale:

$$\text{char}R = 0 \text{ oppure } \text{char}R = p \text{ con } p \text{ primo .}$$

Definizione 1.4. Sia $\mathbb{K} \subseteq \mathbb{F}$ un'estensione di campi. Se $\mathbb{F}$ ha dimensione finita come $\mathbb{K}$-spazio vettoriale, diciamo che $\mathbb{F}$ è un' **estensione finita** di $\mathbb{K}$ e poniamo

$$[\mathbb{F} : \mathbb{K}] = \dim_{\mathbb{K}}\mathbb{F}$$

e lo chiamiamo **grado** di $\mathbb{F}$ su $\mathbb{K}$.

Teorema 1.2.1 (della torre). *Supponiamo di avere le estensioni* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ *con* $[\mathbb{L} : \mathbb{K}] < \infty$ *e* $[\mathbb{F} : \mathbb{L}] < \infty$. *Allora vale:*

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}].$$

Definizione 1.5. Sia $\mathbb{K} \subseteq \mathbb{F}$ un'estensione algebrica, non necessariamente di grado finito. Il **gruppo di Galois** dell'estensione é:

$$\text{Gal}(\mathbb{F}/\mathbb{K}) = \{\sigma \in \text{Aut}\mathbb{F} \text{ tale che } \sigma(x) = x \text{ per ogni } x \in \mathbb{K}\}.$$

`NOTAZIONE`
Se H è un sottogruppo di Aut$\mathbb{F}$, si indica con $\mathbb{F}^H$ l'insieme:

$$\mathbb{F}^H = \{x \in \mathbb{F} \text{ tale che } \varphi(x) = x \quad \text{per ogni } \varphi \in H\}$$

e si chiama *campo fisso* di H.

Definizione 1.6. Un'estensione $\mathbb{K} \subseteq \mathbb{F}$ si dice **normale** se ogni polinomio irriducibile $g \in \mathbb{K}[x]$ che ha una radice in $\mathbb{F}$, si spezza completamente in $\mathbb{F}[x]$.

Definizione 1.7. Un polinomio $f \in \mathbb{K}[x]$ si dice **separabile** se nel suo campo di spezzamento non ha radici multiple.
Inoltre un'estensione algebrica $\mathbb{K} \subseteq \mathbb{F}$ si dice **separabile** se per ogni $\alpha \in \mathbb{F}$, il polinomio minimo di α su $\mathbb{K}$ è separabile.

Osservazione 1. Dato un polinomio $f \in \mathbb{K}[x]$, vale che:

- f è separabile $\Leftrightarrow$ f e la sua derivata f' sono primi tra loro;
- sia f irriducibile. Allora f è separabile $\Leftrightarrow$ $f' \neq 0$.

Definizione 1.8. Un'estensione algebrica $\mathbb{K} \subseteq \mathbb{F}$ si dice **di Galois** se è normale e separabile.

Osservazione 2. Supponiamo che $\mathbb{F}$ sia un'estensione semplice di $\mathbb{K}$, cioè $\mathbb{F} = \mathbb{K}(\alpha)$, con α algebrico su $\mathbb{K}$.
Sia p il polinomio minimo di α in $\mathbb{K}[x]$, $p = x^n + a_{n-1}x^{n-1} + ... + a_0$. Allora si ha che

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0 \qquad (*)$$

Sia $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Applichiamo σ all'espressione $(*)$ e otteniamo :

$$0 = \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + ... + \sigma(a_0) = \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + ... + a_0.$$

Dunque σ manda α in un'altra radice di p e se conosciamo $\sigma(\alpha)$ conosciamo anche come agisce l'automorfismo σ perchè $\mathbb{F} = \mathbb{K}(\alpha)$. Quindi in $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ ci sono tanti automorfismi quante sono le radici di p e c'è una mappa iniettiva :

$$\phi : \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \longrightarrow \{\textit{radici di } p \textit{ distinte}\}$$

$$\sigma \mapsto \sigma(\alpha).$$

Riportiamo ora alcuni importanti enunciati tratti da [3].
Precisamente in ordine: Teorema 5.2.4, Teorema 7.1.1, Teorema 7.2.5, Teorema 7.2.7, Teorema 7.3.1 .

Teorema 1.2.2. *Un'estensione di campi $\mathbb{K} \subseteq \mathbb{F}$ è normale e finita se e solo se $\mathbb{F}$ è il campo di spezzamento di un polinomio $f \in \mathbb{K}[x]$.*

Teorema 1.2.3. *Sia $\mathbb{K} \subseteq \mathbb{F}$ un'estensione finita. Allora le seguenti condizioni sono equivalenti:*

(i) $\mathbb{F}$ *è il campo di spezzamento di un polinomio separabile* $f \in \mathbb{K}[x]$;

(ii) $\mathbb{K} = \mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{K})}$;

(iii) $\mathbb{K} \subseteq \mathbb{F}$ *è di Galois ;*

(iv) $\mid \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \mid = [\mathbb{F} : \mathbb{K}]$.

Teorema 1.2.4. *Sia $\mathbb{K} \subseteq \mathbb{F}$ un'estensione finita di Galois. Sia $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$. Sono equivalenti:*

(i) $\mathrm{Gal}(\mathbb{F}/\mathbb{L})$ *è un sottogruppo normale di* $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$*;*

(ii) $\mathbb{K} \subseteq \mathbb{L}$ *è di Galois .*

Teorema 1.2.5. *Date $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ estensioni finite con $\mathbb{K} \subseteq \mathbb{L}$ e $\mathbb{L} \subseteq \mathbb{F}$ di Galois, allora :*

$$\mathrm{Gal}(\mathbb{F}/\mathbb{L}) \trianglelefteq \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \quad e \quad \frac{\mathrm{Gal}(\mathbb{F}/\mathbb{K})}{\mathrm{Gal}(\mathbb{F}/\mathbb{L})} \cong \mathrm{Gal}(\mathbb{L}/\mathbb{K}).$$

Teorema 1.2.6 (**FONDAMENTALE DI GALOIS**)**.**
Sia $\mathbb{K} \subseteq \mathbb{F}$ un'estensione finita di Galois. Allora:

(i) per ogni $\mathbb{L}$, con $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$, si ha che

- $\mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{L})} = \mathbb{L}$;
- $\mid \mathrm{Gal}(\mathbb{F}/\mathbb{L}) \mid = [\mathbb{F} : \mathbb{L}]$;
- $\mid \mathrm{Gal}(\mathbb{F}/\mathbb{K}) : \mathrm{Gal}(\mathbb{F}/\mathbb{L}) \mid = [\mathbb{L} : \mathbb{K}]$;

(ii) per ogni $H \leq \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ si ha che :

- $\mathrm{Gal}(\mathbb{F}/\mathbb{F}^H) = H$;
- $[\mathbb{F} : \mathbb{F}^H] = \mid H \mid$;
- $[\mathbb{F}^H : \mathbb{K}] = \mid \mathrm{Gal}(\mathbb{F}/\mathbb{K}) : H \mid$.

Dunque esiste una corrispondenza biunivoca

$$\gamma : \{\textit{sottogruppi di } \mathrm{Gal}(\mathbb{F}/\mathbb{K})\} \longrightarrow \{\textit{campi intermedi } \mathbb{L} : \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}\}$$

con $\gamma(H) = \mathbb{F}^H$ *e* $\gamma^{-1}(\mathbb{L}) = \mathrm{Gal}(\mathbb{F}/\mathbb{L})$.

Capitolo 2

Estensioni cicliche

Definizione 2.1. Un'estensione $\mathbb{K} \subseteq \mathbb{F}$ si dice **ciclica** se $\mathbb{F}$ è di Galois e $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è un gruppo ciclico. Se $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è un gruppo ciclico finito di ordine n, si dice che $\mathbb{F}$ **è un'estensione ciclica di ordine** n e per il *Teorema fondamentale di Galois* vale che $[\mathbb{F} : \mathbb{K}] = n$.

Iniziamo mostrando alcuni casi particolari in cui si hanno campi che ammettono estensioni necessariamente cicliche. A tale scopo, premettiamo una definizione e un lemma usato per costruire estensioni di Galois.

Definizione 2.2. Dato un campo $\mathbb{K}$, si chiama **chiusura algebrica** di $\mathbb{K}$ un campo algebricamente chiuso e algebrico su $\mathbb{K}$, e lo si indica con $\overline{\mathbb{K}}$.

Lemma 2.0.7. *Siano $\mathbb{K}$ un campo e $\bar{\mathbb{K}}$ una sua chiusura algebrica.*
Dato un altro campo $\mathbb{E}$, con $\mathbb{K} \subseteq \mathbb{E} \subseteq \bar{\mathbb{K}}$ e $[\mathbb{E} : \mathbb{K}] < \infty$, allora esiste un'estensione finita e normale $\mathbb{F}$ di $\mathbb{K}$, con $\mathbb{E} \subseteq \mathbb{F} \subseteq \bar{\mathbb{K}}$.

Dimostrazione.
Poichè $[\mathbb{E} : \mathbb{K}] < \infty$, $\mathbb{E}$ è finitamente generato su $\mathbb{K}$, dunque $\mathbb{E} = \mathbb{K}(a_1, ..., a_n)$.
Sia g_i il polinomio minimo di a_i su $\mathbb{K}$ per ogni $i = 1, ..., n$ e sia $g = g_1 g_2 \cdots g_n$.
A questo punto basta prendere $\mathbb{F}$ uguale al campo di spezzamento di g su $\mathbb{K}$ e si ha la catena di estensioni $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{F} \subseteq \bar{\mathbb{K}}$, con $\mathbb{F}$ estensione normale di $\mathbb{K}$ per il *Teorema 1.2.2* .

□

Proposizione 2.0.8. *Sia $\bar{\mathbb{Q}}$ una chiusura algebrica di $\mathbb{Q}$, cioè $\bar{\mathbb{Q}}$ è algebrico su $\mathbb{Q}$ e algebricamente chiuso. Sia $v \in \bar{\mathbb{Q}}, v \notin \mathbb{Q}$ e sia $\mathbb{E}$ un sottocampo di $\bar{\mathbb{Q}}$ massimale*

rispetto alla condizione $v \notin \mathbb{E}$. Allora ogni estensione di dimensione finita di $\mathbb{E}$ è ciclica.

Dimostrazione.
Sia $\mathbb{E} \subseteq \mathbb{E}'$ un'estensione finita. Se $\mathbb{E} = \mathbb{E}'$ non c'è niente da dimostrare. Sia dunque $\mathbb{E} \neq \mathbb{E}'$. Per *Lemma 2.0.7*, esiste un'estensione normale $\mathbb{E} \subset \mathbb{F}$ e tale che

$$\mathbb{E} \subset \mathbb{E}' \subseteq \mathbb{F} \subseteq \bar{\mathbb{K}}.$$

Dato che la caratteristica di $\mathbb{Q}$ è 0, per l'*Osservazione 1*, $\mathbb{E} \subset \mathbb{F}$ è anche un'estensione separabile e dunque di Galois. Poichè $\mathbb{E}$ è massimale rispetto alla condizione $v \notin \mathbb{E}$, $v \in \mathbb{F}$ e per ogni estensione propria finita $\mathbb{L}$, $\mathbb{E} \subset \mathbb{L} \subseteq \mathbb{F}$, si ha che $\mathbb{E}(v) \subseteq \mathbb{L}$. Dunque $\mathbb{E}(v) \subseteq \mathbb{E}'$. Dimostriamo ora che $\mathbb{E}'$ è ciclico su $\mathbb{E}$. Per la corrispondenza di Galois vale :

$$\begin{array}{ccc}
\mathbb{F} & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{F}) = id \\
\cup & & \cap \\
\mathbb{E}' & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{E}') \\
\shortmid\cup & & \shortmid\cap \\
\mathbb{E}(v) & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{E}(v)) \\
\cup & & \cap \\
\mathbb{E} & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{E})
\end{array}$$

cioè ogni sottogruppo proprio di $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ deve essere contenuto nel sottogruppo $\mathrm{Gal}(\mathbb{F}/\mathbb{E}(v))$. Sia ora $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{E}) \setminus \mathrm{Gal}(\mathbb{F}/\mathbb{E}(v))$. Il sottogruppo $H =< \sigma >$ è contenuto in $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ ma non è contenuto in $\mathrm{Gal}(\mathbb{F}/\mathbb{E}(v))$, quindi non può essere un sottogruppo proprio. Dunque $H = \mathrm{Gal}(\mathbb{F}/\mathbb{E}) =< \sigma >$, cioè $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ è ciclico e quindi abeliano. Allora $\mathrm{Gal}(\mathbb{F}/\mathbb{E}')$ è un sottogruppo normale di $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ e per il *Teorema 1.2.4* l'estensione $\mathbb{E} \subset \mathbb{E}'$ è di Galois. Dunque per il *Teorema 1.2.5*, $\mathrm{Gal}(\mathbb{E}'/\mathbb{E})$ è isomorfo ad un quoziente di $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ e quindi è ciclico.

□

Proposizione 2.0.9. *Siano $\mathbb{K}$ un campo e $\bar{\mathbb{K}}$ una sua chiusura algebrica. Sia $\sigma \in \mathrm{Gal}(\mathbb{K}/\bar{\mathbb{K}})$ e $\mathbb{E} = \{u \in \bar{\mathbb{K}} | \sigma(u) = u\}$. Allora ogni estensione di dimensione finita di $\mathbb{E}$ è ciclica.*

Dimostrazione.
Sia $\mathbb{E}'$ un'estensione finita di $\mathbb{E}$, proviamo che è ciclica. $\mathbb{E}'$ è finitamente generato su $\mathbb{E}$, allora si ha

$$\mathbb{E}' = \mathbb{E}(a_1, ..., a_n).$$

Sia f_i il polinomio minimo di a_i su $\mathbb{E}$ per ogni $i = 1, ..., n$ e sia $f = f_1 f_2 \cdot \cdot f_n$. Allora per il *Teorema 1.2.2*, il campo di spezzamento $\mathbb{F}$ di f su $\mathbb{E}$ è un'estensione normale di $\mathbb{E}$ e si avrà $\mathbb{F} = \mathbb{E}(\alpha_1, ..., \alpha_r)$, con $\alpha_1, ..., \alpha_r$ radici distinte di f. Supponiamo che f abbia grado m e che $f = e^m x^m + ... + e_0$ con $e_i \in \mathbb{E}$ per ogni $i = 1, ..., m$.
Mostriamo che $\sigma(\mathbb{F}) = \mathbb{F}$: basta far vedere che $\sigma(\alpha_i) \in \mathbb{F}$ per ogni $i = 1, ..., r$. Osserviamo che $f(\alpha_i) = e_m {\alpha_i}^m + ... + e_0 = 0$ e dunque $\sigma(f(\alpha_i)) = \sigma(e_m)\sigma(\alpha_i)^m + ... + \sigma(e_0)$. Poichè $e_i \in \mathbb{E}$ per ogni $i = 1, ..., m$, per come è definto $\mathbb{E}$ vale $\sigma(e_i) = e_i$. Quindi $\sigma(f(\alpha_i)) = e_m \sigma(\alpha_i)^m + ... + e_0$, cioè σ permuta le radici di f che appartengono tutte ad $\mathbb{F}$ in quanto l'estensione $\mathbb{E} \subseteq \mathbb{F}$ è normale. Quindi $\sigma(\mathbb{F}) \subseteq \mathbb{F}$. Inoltre $[\sigma(\mathbb{F}) : \mathbb{E}] = [\mathbb{F} : \mathbb{E}]$, allora $\sigma(\mathbb{F}) = \mathbb{F}$. Se indichiamo con σ' la restrizione di σ ad $\mathbb{F}$, si ha che $\sigma' \in \mathrm{Gal}(\mathbb{F}/\mathbb{E})$. Vogliamo ora dimostrare che $\mathbb{F}$ è un'estensione di Galois di $\mathbb{E}$: per il *Teorema 1.2.3*, basta provare che $\mathbb{F}^{\mathrm{Gal}(\mathbb{F}/\mathbb{E})} = \mathbb{E}$, cioè che per ogni $u \in \mathbb{F} \setminus \mathbb{E}$ esiste un elemento $\varphi \in \mathrm{Gal}(\mathbb{F}/\mathbb{E})$ tale che $\varphi(u) \neq u$. Se prendiamo $\varphi = \sigma'$ sicuramente si ha che $\sigma'(u) \neq u$ per ogni $u \in \mathbb{F} \setminus \mathbb{E}$. Dunque $\mathbb{F}$ è di Galois su $\mathbb{E}$. Consideriamo ora il sottogruppo $H =< \sigma' >$ di $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ e sia $\mathbb{L} = \mathbb{F}^{<\sigma'>}$ il suo campo fisso nella corrispondenza di Galois:

$$
\begin{array}{ccc}
\mathbb{F} & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{F}) = id \\
\shortmid\cup & & \shortmid\cap \\
\mathbb{L} = \mathbb{F}^{<\sigma'>} & \longrightarrow & H =< \sigma' > \\
\shortmid\cup & & \shortmid\cap \\
\mathbb{E}' & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{E}') \\
\shortmid\cup & & \shortmid\cap \\
\mathbb{E} & \longrightarrow & \mathrm{Gal}(\mathbb{F}/\mathbb{E})
\end{array}
$$

Per come è stato definito $\mathbb{L}$, per ogni $x \in \mathbb{L}$ si ha $\sigma'(x) = x$, dunque anche $\sigma(x) = x$. Ne viene che $\mathbb{L} \subset \mathbb{E}$ e di conseguenza $\mathbb{L} = \mathbb{E}$. Allora $H = \mathrm{Gal}(\mathbb{F}/\mathbb{L}) = \mathrm{Gal}(\mathbb{F}/\mathbb{E})$ $=< \sigma' >$, cioè $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$ è ciclico e dunque abeliano. Quindi per il *Teorema 1.2.4*, essendo $\mathrm{Gal}(\mathbb{F}/\mathbb{E}')$ un sottogruppo normale di $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$, si ha che $\mathbb{E} \subseteq \mathbb{E}'$ è un' estensione di Galois. Allora $\mathrm{Gal}(\mathbb{E}'/\mathbb{E})$ è ciclico perchè per il *Teorema 1.2.5*, è isomorfo ad un quoziente di $\mathrm{Gal}(\mathbb{F}/\mathbb{E})$.

□

Finora abbiamo utilizzato solo la definizione di estensione ciclica, per averne una precisa caratterizzazione è necessario introdurre alcune nozioni.

2.1 Definizione di traccia e norma

Definizione 2.3. Sia $\mathbb{F}$ un'estensione finita di Galois di un campo $\mathbb{K}$ e sia

$$\mathrm{Gal}(\mathbb{F}/\mathbb{K}) = \{\sigma_1, ..., \sigma_n\},$$

allora per ogni $u \in \mathbb{F}$ si definisce **norma** di u l'elemento

$$N_{\mathbb{K}}{}^{\mathbb{F}}(u) = \sigma_1(u)\sigma_2(u)\cdots\sigma_n(u),$$

e si definisce **traccia** di u l'elemento

$$T_{\mathbb{K}}{}^{\mathbb{F}}(u) = \sigma_1(u) + \sigma_2(u) + ... + \sigma_n(u).$$

Osservazione 3. Sia $\mathbb{F}$ un' estensione di Galois di $\mathbb{K}$ e $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) = \{\sigma_1, ..., \sigma_n\}$. Si ha che $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è un gruppo e allora per ogni $\sigma_i \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ fissato, gli elementi $\sigma_i\sigma_1, \sigma_i\sigma_2, \ ..., \sigma_i\sigma_n$ sono semplicemente $\sigma_1, \ \sigma_2, ..., \ \sigma_n$ con ordine diverso. Quindi per ogni $u \in \mathbb{F}$, $N_{\mathbb{K}}{}^{\mathbb{F}}(u)$ e $T_{\mathbb{K}}{}^{\mathbb{F}}(u)$ sono fissati da ogni $\sigma_i \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Dunque $N_{\mathbb{K}}{}^{\mathbb{F}}(u), T_{\mathbb{K}}{}^{\mathbb{F}}(u) \in \mathbb{K}$.

Il seguente teorema mostra che per la traccia e la norma vale la **proprietà di linearità**:

Teorema 2.1.1. *Sia $\mathbb{F}$ un'estensione finita di Galois di un campo $\mathbb{K}$.*
Allora per ogni $u, v \in \mathbb{F}$

(i) $N_{\mathbb{K}}{}^{\mathbb{F}}(u)N_{\mathbb{K}}{}^{\mathbb{F}}(v) = N_{\mathbb{K}}{}^{\mathbb{F}}(uv)$ *e* $T_{\mathbb{K}}{}^{\mathbb{F}}(u) + T_{\mathbb{K}}{}^{\mathbb{F}}(v) = T_{\mathbb{K}}{}^{\mathbb{F}}(u+v)$;

(ii) se $u \in \mathbb{K}$, allora $N_{\mathbb{K}}{}^{\mathbb{F}}(u) = u^{[\mathbb{F}:\mathbb{K}]}$ *e* $T_{\mathbb{K}}{}^{\mathbb{F}}(u) = [\mathbb{F} : \mathbb{K}]u$.

Dimostrazione.

(i) segue direttamente dalla definizione e dal fatto che σ è automorfismo.

(ii) poichè $u \in \mathbb{K}$, $\sigma(u) = u$ per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$.
Dato che $\mathbb{K} \subseteq \mathbb{F}$ è di Galois , per il teorema fondamentale:

$$[\mathbb{F} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{F}/\mathbb{K})|.$$

Allora $N_{\mathbb{K}}{}^{\mathbb{F}}(u) = u^{[\mathbb{F}:\mathbb{K}]}$ e $T_{\mathbb{K}}{}^{\mathbb{F}}(u) = [\mathbb{F} : \mathbb{K}]u$.

□

2.2 Lineare indipendenza di un insieme di automorfismi

Definizione 2.4. Sia S un insieme non vuoto di automorfismi di un campo $\mathbb{F}$. Si dice che S è **linarmente indipendente** se per ogni $\sigma_1, ..., \sigma_n \in S$ e per ogni $a_1, ..., a_n \in \mathbb{F}$ $(n \geq 1)$ vale:

se $a_1\sigma_1(u) + ... + a_n\sigma_n(u) = 0$ per ogni $u \in \mathbb{F}$, allora $a_i = 0$ per ogni $i = 1, ..., n$.

Lemma 2.2.1. *Sia S un insieme di automorfismi distinti di un campo $\mathbb{F}$. Allora S è linearmente indipendente.*

Dimostrazione.
Per assurdo supponiamo che S non sia lineramente indipendente, allora esistono $a_i \in \mathbb{F}, a_i \neq 0$ e $\sigma_i \in S$ distinti, tali che:

$$a_1\sigma_1(u) + a_2\sigma_2(u) + ... + a_n\sigma_n(u) = 0 \text{ per ogni } u \in \mathbb{F}. \tag{2.1}$$

Tra tutte le *relazioni di dipendenza* si sceglie quella con n minimale. Ovviamente è $n > 1$. Dato che σ_1 *e* σ_2 sono distinti, esite $v \in \mathbb{F}$ con $\sigma_1(v) \neq \sigma_2(v)$. Poichè la (2.1) vale per ogni $u \in \mathbb{F}$, applicandola all'elemento uv si ottiene:

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_2(v)... + a_n\sigma_n(u)\sigma_n(v) = 0; \tag{2.2}$$

e moltiplicando la (2.1) per $\sigma_1(v)$ si ha:

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_1(v)... + a_n\sigma_n(u)\sigma_1(v) = 0. \tag{2.3}$$

La differenza tra la (2.2) e la (2.3) è data dalla relazione : per ogni $u \in \mathbb{F}$

$$a_2[\sigma_2(v) - \sigma_1(v)]\sigma_2(u) + a_3[\sigma_3(v) - \sigma_1(u)]\sigma_3(u) + ... + a_n[\sigma_n(v) - \sigma_1(v)]\sigma_n(u) = 0. \tag{2.4}$$

Siccome $a_2 \neq 0$ e $\sigma_2(v) \neq \sigma_1(v)$ non tutti i coefficienti della (2.4) sono nulli e questo è assurdo perchè contraddice la minimalità di n che avevamo supposto.

□

Per completezza, mostriamo una proprietà di traccia e norma nel caso di campi finiti.

Proposizione 2.2.2. *Sia $\mathbb{K}$un campo finito e sia $\mathbb{F}$ una sua estensione di dimensione finita. Allora $N_{\mathbb{K}}{}^{\mathbb{F}}$ e $T_{\mathbb{K}}{}^{\mathbb{F}}$, considerate come applicazioni di $\mathbb{F}$ in $\mathbb{K}$, sono suriettive.*

Dimostrazione.
Per comodità, indichiamo $N_{\mathbb{K}}^{\mathbb{F}}(u)$ con $N(u)$ e $T_{\mathbb{K}}^{\mathbb{F}}(u)$ con $T(u)$.
Vediamo che la norma è suriettiva. Poichè $\mathbb{K}$ è un campo finito ed $\mathbb{F}$ è una sua estensione di dimensione finita, consideriamo il caso particolare con $|\mathbb{K}| = p$, p primo e $|\mathbb{F}| = p^n$, con $n = [\mathbb{F} : \mathbb{K}]$. Il caso generale seguirà direttamente da questo e verrà specificato in seguito. Osserviamo che poichè $\mathbb{K}$ è un campo finito ed $\mathbb{F}$ è una sua estensione finita di grado n allora $\mathbb{F}$ è il campo di spezzamento del polinomio $x^p - x$ che è separabile. Allora, per il *Teorema 1.2.3*, $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione di Galois. Osserviamo anche che $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è generato dall'*automorfismo di Frobenius* di ordine n:

$$\varphi : \mathbb{F} \longrightarrow \mathbb{F}$$

$$x \mapsto x^p$$

Dunque $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) = \{\varphi, \varphi^2, ..., \varphi^n = id_{\mathbb{F}}\}$. Allora:

$$N(u) = \varphi(u) + \varphi^2(u) + ... + \varphi^n(u) = u + u^p + u^{p^2} + ... + u^{p^n - 1} = u^{(1+p+p^2+...+p^{n-1})}.$$

Poichè φ è un automorfismo, $N(0) = 0$, quindi per dimostrare la suriettività della norma basta considerare la sua restrizione

$$N^* : \mathbb{F}^* \longrightarrow \mathbb{K}^*.$$

Osserviamo che per il *Teorema 2.1.1*, N^* è un omomorfismo di gruppi. Per il *Teorema 1.1.4*, $\mathbb{K}^*$ è ciclico di ordine $p - 1$ e $\mathbb{F}^*$ è ciclico di ordine $p^n - 1$. Sia ora u un generatore di $\mathbb{F}^*$, $|u| = p^n - 1$. Si ha che $(N^*(u))^{(p-1)} = (N(u))^{(p-1)} = u^{(1+p+p^2+...+p^{n-1})(p-1)} = u^{p^n-1} = u$. Dunque $N^*(u)$ ha ordine $p - 1$. Poichè l'immagine $\mathrm{Im}N^*$ di N^* è un sottogruppo di $\mathbb{K}^*$, dal fatto che $\mathrm{Im}N^*$ ha ordine almeno $p - 1$ segue che $\mathrm{Im}N^* = \mathbb{K}^*$ e dunque che la norma è suriettiva. Nel caso generale con $|K| = p^n$, basta porre $q = p^n$ e si avrà $|\mathbb{F}| = q^m$ per un certo m intero positivo tale che $[\mathbb{F} : \mathbb{K}] = m$. Con lo stesso ragionamento del caso particolare si ottiene che la norma è suriettiva.

Vediamo che la traccia è suriettiva.
Vogliamo che per ogni $u \in \mathbb{K}$ esista un elemento $z \in \mathbb{F}$ tale che $T(z) = u$. Sia $|\mathrm{Gal}(\mathbb{F}/\mathbb{K})| = n$ e $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) = \{\sigma_1, ..., \sigma_n\}$. Osserviamo prima di tutto che se $u \in \mathbb{K}$ e $v \in \mathbb{F}$, allora :

$$T(uv) = \sigma_1(uv) + \sigma_2(uv) + ... + \sigma_n(uv) = \sigma_1(u)\sigma_1(v) + ... + \sigma_n(u)\sigma_n(v)$$

$$= u\sigma_1(v) + ... + u\sigma_n(v) = uT(v).$$

Per il *Lemma 2.2.1*, $\sigma_1, ..., \sigma_n$ sono linearmente indipendenti e poichè la traccia è una loro combinazione lineare con tutti i coefficienti pari a $1_{\mathbb{K}}$, possiamo sempre

trovare un elemento $v \in \mathbb{F}$ tale che $T(v) \neq 0$. A questo punto basta scegliere $z = \frac{uv}{T(v)}$ e si verifica che :

$$T(z) = T\Big(\frac{uv}{T(v)}\Big) = \frac{T(uv)}{T(v)} = \frac{uT(v)}{T(v)} = u.$$

Dunque la traccia è suriettiva.

□

2.3 Teorema di Hilbert 90

Un altro strumento necessario per lo studio delle estensioni cicliche è il *Teorema di Hilbert 90*, a cui premettiamo il seguente risultato:

Teorema 2.3.1. *Sia* $\mathbb{F}$ *un'estensione ciclica di grado* n *di un campo* $\mathbb{K}$.
Consideriamo un generatore σ *di* $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ *e sia* $u \in \mathbb{F}$*, allora :*

$$T_{\mathbb{K}}{}^{\mathbb{F}}(u) = 0 \text{ se e solo se } u = v - \sigma(v) \quad \text{per un certo } v \in \mathbb{F}.$$

Dimostrazione.
Poichè genera $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$, σ ha ordine n e $\sigma, \sigma^2, \sigma^3, ..., \sigma^n = 1_{\mathbb{F}}$ sono n automorfismi distinti di $\mathbb{F}$. Per comodità scriviamo $\sigma(x) = \sigma x$.
Dunque si ha :

$$T_{\mathbb{K}}{}^{\mathbb{F}}(u) = T(u) = u + \sigma u + \sigma^2 u ... + \sigma^{n-1} u. \tag{2.5}$$

Facciamo vedere l'implicazione ($\Leftarrow$): sia quindi $u = v - \sigma(v)$. Dal fatto che $T(v - \sigma v) = T(v) - T(\sigma v)$ e $\sigma^n(v) = v$ segue che $T(u) = 0$.
Viceversa, per dimostrare l'implicazione ($\Rightarrow$), supponiamo che $T(u) = 0$. Mostriamo che esiste $w \in \mathbb{F}$ tale che $T(w) = 1_{\mathbb{K}}$. Per il *lemma 2.2.1*, esiste $z \in \mathbb{F}$ tale che:

$$T(z) = 1_{\mathbb{F}} z + \sigma z + \sigma^2 z ... + \sigma^{n-1} z.$$

Siccome $T(z) \in \mathbb{K}$, $\sigma\big(T(z)^{-1} z\big) = T(z)^{-1} \sigma(z)$. Basta prendere $w = T(z)^{-1} z$ per avere:

$$T(w) = T(z)^{-1} z + T(z)^{-1} \sigma z + ... + T(z)^{-1} \sigma^{n-1} z = T(z)^{-1} T(z) = 1_{\mathbb{K}}.$$

Ora sia
$v = uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w) + (u + \sigma u + \sigma^2 u + \sigma^3 u)(\sigma^3 w) + ...$
$+ (u + \sigma u + ... + \sigma^{n-2} u)(\sigma^{n-2} w)$.

Dalla (2.5) otteniamo :

$$u = -(\sigma u + \sigma^2 u + ... + \sigma^{n-1} u).$$

Dunque
$v - \sigma v = uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w) + (u + \sigma u + \sigma^2 u + \sigma^3 u)(\sigma^3 w) + ...$
$+ (u + \sigma u + ... + \sigma^{n-2} u)(\sigma^{n-2} w) - \sigma u \sigma w - (\sigma u + \sigma^2 u)(\sigma^2 w) - (\sigma u + \sigma^2 u + \sigma^3 u)(\sigma^3 u) -$
$... - (\sigma u + \sigma^2 u + ... + \sigma^{n-1} u)(\sigma^{n-1} u) = uw + u\sigma w + u\sigma^2 w + ... + u\sigma^{n-1} w$
$= uT(w) = u1_{\mathbb{K}} = u.$

□

Teorema 2.3.2 (di Hilbert 90)**.** *Nelle stesse ipotesi del teorema precedente, vale:*

$$N_{\mathbb{K}}{}^{\mathbb{F}}(u) = N(u) = 1_{\mathbb{K}} \text{ se e solo se } u = v\sigma(v)^{-1}$$

per un certo $v \in \mathbb{F}, v \neq 0$.

Dimostrazione.
Sia $u = v\sigma(v)^{-1}$. Poichè σ è un automorfismo di ordine n si ha che:

(i) $\sigma^n(v^{-1}) = v^{-1}$;

(ii) $\sigma(v^{-1}) = \sigma(v)^{-1}$;

(iii) per ogni $1 \leq i \leq n-1$, $\sigma^i(v\sigma(v)^{-1}) = \sigma^i(v)\sigma^{i+1}(v)^{-1}$.

Dunque:

$$N(u) = (v\sigma(v)^{-1})(\sigma v \sigma^2(v)^{-1})(\sigma^2 v \sigma^3(v)^{-1}) \cdots (\sigma^{n-1} v \sigma^n(v)^{-1}) = 1_{\mathbb{K}}.$$

Viceversa, supponiamo che $N(u) = 1_{\mathbb{K}}$, da cui segue che $u \neq 0$.
Per il *lemma 2.2.1* , esiste $y \in \mathbb{F}$ tale che sia non nullo l'elemento :

$$v = uy + (u\sigma u)\sigma y + (u\sigma u \sigma^2 u)\sigma^2 y + ... + (u\sigma u \cdots \sigma^{n-2} u)\sigma^{n-2} y + (u\sigma u \cdots \sigma^{n-1} u)\sigma^{n-1} y. \tag{2.6}$$

Poichè l'ultimo addendo della (2.6) è $N(u)\sigma^{n-1} y = 1_{\mathbb{K}}\sigma^{n-1} y$,
si verifica facilmente che

$$u^{-1} v = \sigma v.$$

Sappiamo che $v \neq 0$, dunque per l'iniettività di σ si ha che $\sigma(v) \neq 0$.
Allora

$$u = v\sigma(v)^{-1}.$$

□

2.4 Un caso particolare di estensione ciclica

Con gli strumenti ottenuti, iniziamo l'analisi delle estensioni cicliche.

Proposizione 2.4.1. *Sia* $\mathbb{F}$ *un'estensione ciclica di* $\mathbb{K}$ *di grado* n *e supponiamo che* $n = mp^t$, *con* $0 \neq p = \text{char}\mathbb{K}$ *e* $(m, p) = 1$. *Allora esiste una catena di campi itermedi*

$$\mathbb{F} \supseteq \mathbb{E}_0 \supseteq \mathbb{E}_1 \supseteq ... \supseteq \mathbb{E}_{t-1} \supseteq \mathbb{E}_t = \mathbb{K}$$

tale che $\mathbb{F}$ *sia un'estensione ciclica di* $\mathbb{E}_0$ *di grado* m *e che per ogni* $0 \leq i \leq t-1$, $\mathbb{E}_{i-1}$ *sia un'estensione ciclica di* $\mathbb{E}_i$ *di grado* p.

Dimostrazione.
Per ipotesi $\mathbb{F}$ è di Galois su $\mathbb{K}$ e $\text{Gal}(\mathbb{F}/\mathbb{K})$ è ciclico (quindi abeliano), dunque ogni suo sottogruppo è normale e per il *Teorema 1.1.1* è anche ciclico.
Per la *Proposizione 1.1.2*, esiste un unico sottogruppo ciclico H di $\text{Gal}(\mathbb{F}/\mathbb{K})$ di ordine m. Sia $\mathbb{E}_0$ il campo fissato da H, cioè $\mathbb{E}_0 = \mathbb{F}^H$. Allora per *Teorema fondamentale di Galois 1.2.6* (*ii*), $\mathbb{F}$ è un'estensione di $\mathbb{E}_0$ di grado m e per il *Teorema della torre 1.2.1*, $\mathbb{E}_0$ è un'estensione di $\mathbb{K}$ di grado p^t. Osserviamo che entrambe sono estensioni cicliche: la prima perchè, per definizione, $\text{Gal}(\mathbb{F}/\mathbb{E}_0) = H$, la seconda perchè $\mathbb{K} \subseteq \mathbb{E}_0$ è di Galois (per il *Teorema 1.2.4*) e per il *Teorema 1.2.5*, $\text{Gal}(\mathbb{E}_0/\mathbb{K})$ è isomorfo ad un quoziente di $\text{Gal}(\mathbb{F}/\mathbb{K})$ che è ciclico, dunque per il *Teorema 1.1.1* si ha che anch'esso è ciclico e per quanto visto prima ha ordine p^t.
Allora per la corrispondenza definita dalla *Proposizione 1.1.2*, esiste una catena di sottogruppi :

$$1 = G_0 \leq G_1 \leq G_2 \leq ... \leq G_{t-1} \leq G_t = \text{Gal}(\mathbb{E}_0/\mathbb{K})$$

con $| G_i | = p^i$, $[G_i : G_{i-1}] = p$. In particolare G_i/G_{i-1} è ciclico di ordine p.
Per ogni i , sia $\mathbb{E}_i$ il campo fisso di G_i relativo a $\mathbb{E}_0$ e a $\text{Gal}(\mathbb{E}_0/\mathbb{K})$.
Per il *Teorema fondamentale di Galois 1.2.6*, si ha che:

(i) $\mathbb{E}_0 \supseteq \mathbb{E}_1 \supseteq \mathbb{E}_2 \supseteq ... \supseteq \mathbb{E}_{t-1} \supseteq \mathbb{E}_t = \mathbb{K}$;

(ii) $[\mathbb{E}_{i-1} : \mathbb{E}_i] = [G_i : G_{i-1}] = p$;

(iii) $\text{Gal}(\mathbb{E}_{i-1}/\mathbb{E}_i) \cong G_i/G_{i-1}$.

Quindi $\mathbb{E}_{i-1}$ è un'estensione ciclica di $\mathbb{E}_i$ di grado p per ogni $0 \leq i \leq t - i$.

□

Sia $\mathbb{K} \subseteq \mathbb{F}$ un'estensione ciclica di grado n.
La *Proposizione 2.4.1* ci spinge ad analizzare due specifici casi :

(i) $n = \text{char}\mathbb{K} = p \neq 0$;

(ii) $\text{char}\mathbb{K} = 0$, oppure $\text{char}\mathbb{K} = p \neq 0$ con $(p, n) = 1$, cioè $\text{char}\mathbb{K}$ non divide n.

2.5 Estensioni cicliche di grado uguale alla caratteristica del campo.

Per la dimostrazione del seguente Lemma si veda [1, Teorema 5.6, cap.V].

Lemma 2.5.1. *Dato $\mathbb{Z}_p$, campo finito con p elementi, si ha che:*

$$i^p = i, \text{ per ogni } i \in \mathbb{Z}_p.$$

Proposizione 2.5.2. *Sia $\mathbb{K}$ un campo di caratteristica $p \neq 0$. Allora valgono:*

(i) se $\mathbb{F}$ è un'estensione ciclica di $\mathbb{K}$ di grado p allora $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ di un polinomio irriducibile $f = x^p - x - a \in \mathbb{K}[x]$, per un certo $a \in \mathbb{K}$. In questo caso si ha:

$$\mathbb{F} = \mathbb{K}(u)$$

dove u è una radice di f.

(ii) se $\mathbb{F} = \mathbb{K}(u)$, con u zero di $f = x^p - x - a \in \mathbb{K}[x]$, allora o $\mathbb{F} = \mathbb{K}$ oppure $\mathbb{F}$ è un'estensione di Galois ciclica di $\mathbb{K}$ di grado p.

Dimostrazione.

(i) Sia σ un generatore di $\text{Gal}(\mathbb{F}/\mathbb{K})$. Per il *Teorema 2.1.1*, vale:

$$T_{\mathbb{K}}^{\mathbb{F}}(1_{\mathbb{K}}) = [\mathbb{F} : \mathbb{K}] = p1_{\mathbb{K}} = 0.$$

Quindi per il *Teorema 2.3.1* si ha che $1_{\mathbb{K}} = v - \sigma(v)$ per un certo $v \in \mathbb{F}$. Se $u = -v$ allora $\sigma(u) = u + 1_{\mathbb{K}} \neq u$, quindi $u \notin \mathbb{K}$. Siccome $[\mathbb{F} : \mathbb{K}] = p$, *per la corrispondenza di Galois* non ci sono campi intermedi tra $\mathbb{K}$ ed $\mathbb{F}$. Necessariamente si ha che $\mathbb{F} = \mathbb{K}(u)$. Osserviamo che :

$$\sigma(u^p) = (u + 1_{\mathbb{K}})^p = u^p + 1_{\mathbb{K}} = u^p + 1_{\mathbb{K}},$$

poichè $\mathbb{K}$ ha caratteristica p. Dunque

$$\sigma(u^p - u) = (u^p + 1_{\mathbb{K}}) - (u + 1_{\mathbb{K}}) = u^p - u.$$

Allora $a = u^p - u \in \mathbb{K}$ e u è una radice del polinomio $f = x^p - x - a \in \mathbb{K}[x]$, che è necessariamente il suo polinomio minimo su $\mathbb{K}$ in quanto il grado di u su $\mathbb{K}$ è $[\mathbb{K}(u) : \mathbb{K}] = [\mathbb{F} : \mathbb{K}] = p$. Ricordiamo che il *sottocampo fondamentale* di $\mathbb{K}$ è $\mathbb{Z}_p$ e per il *Lemma 2.5.1* si ha che $i^{|\mathbb{Z}_p|} = i$ per ogni $i \in \mathbb{Z}_p$. Allora per ogni $i \in \mathbb{Z}_p$ abbiamo che :

$$(u+i)^p - (u+i) - a = u^p + i^p - u - i - a = (u^p - u - a) + (i^p - i) = 0 + 0 = 0.$$

D'altra parte $u + i \in \mathbb{K}(u) = \mathbb{F}$ ed è una radice di f per ogni $i \in \mathbb{Z}_p$.
Dunque $\mathbb{F}$ contiene esattamente p radici distinte di f, il che implica che é il suo campo di spezzamento su $\mathbb{K}$. Basta infine osservare che se $u + i$ $(i \in \mathbb{Z}_p)$ è una radice di f, allora $\mathbb{K}(u + i) = \mathbb{K}(u) = \mathbb{F}$.

(ii) Supponiamo che $\mathbb{F}$ sia il campo di spezzamento su $\mathbb{K}$ di un polinomio $f = x^p - x - a, f \in \mathbb{K}[x]$. Se u è una radice di f, per quanto detto prima, $\mathbb{K}(u)$ contiene p radici distinte di f: $u, u + 1, ..., u + (p - 1) \in \mathbb{K}(u)$.
Ma f ha al più p radici distinte in $\mathbb{F}$ e queste radici generano $\mathbb{F}$ su $\mathbb{K}$.
Allora $\mathbb{F} = \mathbb{K}(u)$ ed essendo il campo di spezzamento per f che è separabile, per il *Teorema 1.2.3*, l'estensione $\mathbb{K} \subseteq \mathbb{F}$ è di Galois. Per l'*Osservazione 2*, ogni automorfismo $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K}) = Gal(\mathbb{K}(u)/\mathbb{K})$ è completamente determinato da $\sigma(u)$. Ma $\sigma(u) = u + i$, per un certo $i \in \mathbb{Z}_p \subseteq \mathbb{K}$. Possiamo allora definire un'applicazione :

$$\theta : \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \longrightarrow \mathbb{Z}_p$$

$$\sigma \mapsto i.$$

θ è un omomorfismo, infatti se $\sigma, \varphi \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ sono tali che $\sigma(u) = u + i$ *e* $\varphi(u) = u + j$, con i *e* $j \in \mathbb{Z}_p$, allora:

$$\sigma\varphi(u) = \sigma(u + j) = \sigma(u) + j = u + i + j.$$

Dunque $\theta(\sigma\varphi) = i + j = \theta(\sigma) + \theta(\varphi)$. Si verifica facilmente anche che θ è iniettivo e quindi $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è isomorfo ad un sottogruppo di $\mathbb{Z}_p$. Poichè gli unici sottogruppi di $\mathbb{Z}_p$ sono quelli banali, avremo $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) \cong 1$ oppure $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) \cong \mathbb{Z}_p$. Nel primo caso $[\mathbb{F} : \mathbb{K}] = 1$ e quindi $\mathbb{F} = \mathbb{K}$ e $u \in \mathbb{K}$ ed f si fattorizza in fattori lineari distinti in $\mathbb{K}[x]$; nel secondo caso $[\mathbb{F} : \mathbb{K}] = p$ e quindi f è irriducibile in $\mathbb{K}[x]$.

□

Osservazione 4. Sia $\mathbb{K}$ un campo di caratteristica p e sia $\mathbb{F}$ un'estensione ciclica di grado p di $\mathbb{K}$. Sia $f = x^p - x - a \in \mathbb{K}[x]$. Allora f è irriducibile se non ha radici in $\mathbb{K}$.

Dimostrazione.
Sia g un fattore irriducibile di f e sia u una radice di g. Allora $[\mathbb{K}(u) : \mathbb{K}]$ è uguale al grado di g. D'altra parte, u è in particolare anche una radice di f e per la *Proposizione 2.5.2* (ii) si ha che $[\mathbb{K}(u) : \mathbb{K}] = p$. Quindi g ha grado p e dunque $g = f$.

□

Corollario 2.5.3. *Se $\mathbb{K}$ è un campo di caratteristica $p \neq 0$ e $f = x^p - x - a \in |K[x]$, allora o f è irriducibile oppure si spezza completamente in $\mathbb{K}[x]$.*

Dimostrazione.
Segue direttamente dalla dimostrazione del punto (ii) della *Proposizione 2.5.2* e dall'*Osservazione 4.*

□

Vediamo ora alcune applicazioni della *Proposizione 2.5.2* :

Proposizione 2.5.4. *Sia $\mathbb{K}$ un campo di caratteristica $p \neq 0$ e sia $\mathbb{K}_p = \{u^p - u | u \in \mathbb{K}\}$. Allora esiste un'estensione ciclica $\mathbb{K} \subseteq \mathbb{F}$ di grado p se e solo se $\mathbb{F} \neq \mathbb{K}_p$.*

Dimostrazione.
Supponiamo che $\mathbb{F}$ sia un'estensione ciclica di $\mathbb{K}$ di grado p. Per la *Proposizione 2.5.2*, $\mathbb{F}$ è il campo di spezzamento di un polinomio irriducibile $f = x^p - x - a \in \mathbb{K}[x]$. Poichè f è irriducibile, l' *Osservazione 4* ci dice che f non ha radici in $\mathbb{K}$. Dunque per ogni $u \in \mathbb{K}$ si ha che $u^p - u \neq a$. Allora $a \in \mathbb{F}$ ma $a \notin \mathbb{K}_p$, cioè $\mathbb{F} \neq \mathbb{K}_p$. Viceversa, se $\mathbb{F} \neq \mathbb{K}_p$, sicuramente esiste un elemento $a \in \mathbb{K}_p$ tale che $a \neq u^p - u$ per ogni $u \in \mathbb{K}$. Dunque il polinomio $x^p - x - a$ non ha radici in $\mathbb{K}$ e basta prendere $\mathbb{F}$ uguale al suo campo di spezzamento su $\mathbb{K}$. Per la *Proposizione 2.5.2*, $\mathbb{F}$ è un estensione ciclica di $\mathbb{K}$ di grado p.

□

Prima di andare avanti, premettiamo la Proposizione 2.2 tratta da [2], che qui verrà utilizzata come Lemma per dimostrare un' altra applicazione della *Proposizione 2.5.2* .

Lemma 2.5.5. *Sia $\mathbb{F}(\alpha)$ un'estensione semplice di un campo $\mathbb{F}$ e sia $\varphi_0 : \mathbb{F} \longrightarrow \Omega$ un omomorfismo di $\mathbb{F}$ in un campo Ω. Allora se α è algebrico su $\mathbb{F}$ con polinomio minimo $f(x)$, c'è una corrispondenza biunivoca*

$$\{\varphi : \mathbb{F}[\alpha] \longrightarrow \Omega, \text{ con } \varphi \text{ estensione di } \varphi_0\} \longleftrightarrow \{ \text{ radici di } \varphi_0 f \text{ in } \Omega\};$$

che manda φ in $\varphi(\alpha)$; in particolare abbiamo tante estensioni φ quante sono le radici distinte di $\varphi_0 f$ in Ω.

Con $\varphi_0 f$ intendiamo il polinomio ottenuto applicando φ_0 ai coefficienti di f, cioè se $f = \sum a_i x^i$ allora $\varphi_0 f = \sum \varphi_0(a_i) x^i$.
Inoltre un'estensione di φ_0 a $\mathbb{F}(\alpha)$ è un omomorfismo $\varphi : \mathbb{F}(\alpha) \longrightarrow \Omega$ tale che $\varphi_{|\mathbb{F}} = \varphi_0$.

Proposizione 2.5.6. *Sia $\mathbb{K}$ un campo di caratteristica p. Se esiste un'estensione ciclica di $\mathbb{K}$ di grapo p allora esiste un'estensione ciclica di $\mathbb{K}$ di grado p^n per ogni $n \geq 1$.*

Dimostrazione.
Dimostriamo la Proposizione per induzione su n. Supponiamo che $\mathbb{E}$ sia un'estensione ciclica di $\mathbb{K}$ di grado p^{n-1}, con $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) =< \sigma >$ e proviamo che esiste un'estensione ciclica di $\mathbb{K}$ di grado p^n. Iniziamo mostrando che esistono $u, v \in \mathbb{E}$ tali che $T(v) = 1$ e $\sigma(u) - u = v^p - v$. Poichè $\sigma, \sigma^2, ..., \sigma^{p^n}$ sono automorfismi distinti di $\mathbb{E}$, per il *Lemma 2.2.1*, sono anche linearmente indipendenti. La traccia T è una combinazione lineare di $\sigma, \sigma^2, ..., \sigma^{p^n}$ con tutti i coefficienti uguali a 1, dunque esiste sicuramente un elemento $z \in \mathbb{E}$ tale che $T(z) = \sigma(z) + \sigma^2(z) + ... + \sigma^{p^n}(z) = a$ con $a \in \mathbb{K}$, $a \neq 0$. Prendiamo $v = \frac{z}{a}$, allora

$$T(v) = T\Big(\frac{z}{a}\Big) = \sigma\Big(\frac{z}{a}\Big) + \sigma^2\Big(\frac{z}{a}\Big) + ... + \sigma^{p^n}\Big(\frac{z}{a}\Big)$$

$$= \frac{\sigma(z)}{\sigma(a)} + \frac{\sigma^2(z)}{\sigma(a)} + ... + \frac{\sigma^{p^n}(z)}{\sigma(a)} = \frac{\sigma(z)}{a} + \frac{\sigma^2(z)}{a} + ... + \frac{\sigma^{p^n}(z)}{a} = \frac{T(z)}{a} = \frac{a}{a} = 1.$$

Poichè $\mathrm{char}\mathbb{K} = p$, vale anche

$$T(v^p) = v^p + \sigma(v^p) + ... + \sigma^{p^{n-1}-1}(v^p)$$

$$= (v + \sigma(v) + ... + \sigma^{p^{n-1}-1}(v))^p = T(v)^p = 1^p = 1.$$

Dunque per il *Teorema 2.1.1*(i), si ha che $T(v^p - v) = T(v^p) - T(v) = 1 - 1 = 0$. Il *Teorema 2.3.1* dice allora che esiste un elemento $u \in \mathbb{E}$ tale che $v^p - v = \sigma(u) - u$. Vediamo ora che il polinomio $f = x^p - x - u \in \mathbb{E}[x]$ è irriducibile. Per il *Corollario*

2.5.3, se f non è irriducibile in $\mathbb{E}$ allora si spezza completamente. Sia $w \in \mathbb{E}$ una sua radice : $w^p - w - u = 0$, cioè $u = w^p - w$.
Allora:

$$v^p - v = \sigma(u) - u = \sigma(w^p - w) - w^p + w$$

quindi

$$\sigma(w)^p - \sigma(w) - w^p + w = v^p - v$$

da cui

$$v^p - \sigma(w)^p + w^p = v - \sigma(w) + w$$

Dunque poichè $\mathbb{K}$ ha caratteristica p abbiamo: $(v - \sigma(w) + w)^p = v - \sigma(w) + w$, cioè l'elemento $v - \sigma(w) + w$ viene fissato dall'automorfismo $\varphi : \mathbb{K} \longrightarrow \mathbb{K}$, definito da $\varphi(x) = x^p$. Allora $v - \sigma(w) + w \in \mathbb{Z}_p$ e per un certo $i \in \mathbb{Z}_p$ vale $v - \sigma(w) + w = i$ che equivale a dire $\sigma(w) = v + w + j$ con $j \in \mathbb{Z}_p$. Dimostriamo ora che per ogni k naturale vale

$$\sigma^k(w) = v + \sigma(v) + \sigma^2(v) + ... + \sigma^{k-1}(v) + w + kj.$$

Procediamo per induzione su k: quando $k = 1$ la proprietà vale per quanto provato prima. Supponiamo che valga per $k-1$ e applicando l'ipotesi induttiva, calcoliamo:

$$\sigma^k(w) = \sigma(\sigma^{k-1}(w)) = \sigma(v + \sigma(v) + \sigma^2(v) + ... + \sigma^{k-2}(v) + w + (k-1)j)$$

$$= \sigma(v) + \sigma^2(v) + \sigma^3(v) + ... + \sigma^{k-1}(v) + \sigma(w) + (k-1)j$$

$$= v + \sigma(v) + \sigma^2(v) + ... + \sigma^{k-1}(v) + w + kj.$$

Quindi nel caso $k = p^{n-1}$ otteniamo:

$$\sigma^{p^{n-1}}(w) = v + \sigma(v) + \sigma^2(v) + ... + \sigma^{p^{n-1}-1}(v) + w + p^{n-1}j = T(v) + w = w + 1.$$

Questo è assurdo perchè σ ha periodo p^{n-1} e w è un elemento di $\mathbb{E}$. Dunque f è irriducibile in $\mathbb{E}$ e se w è una sua radice allora f è proprio il polinomio minimo di w su $\mathbb{E}$, con $[\mathbb{E}(w) : \mathbb{E}] = p$. Per il *Teorema della torre 1.2.1* si ha:

$$[\mathbb{E}(w) : \mathbb{K}] = [\mathbb{E}(w) : \mathbb{E}][\mathbb{E} : \mathbb{K}] = p \cdot p^{n-1} = p^n.$$

Dunque $\mathbb{E}(w)$ è un'estensione di $\mathbb{K}$ di grado p^n. Resta solo da provare che $\mathbb{E}(w)$ è ciclico su $\mathbb{K}$. Osserviamo che $w + v$ è una radice di σf, allora per il *Lemma 2.5.5* possiamo estendere σ a $\mathbb{E}(w)$ tramite $\sigma' : \mathbb{E}(w) \longrightarrow \mathbb{E}(w)$, con $\sigma'_{|\mathbb{E}} = \sigma$ e $\sigma'(w) = w + v$. Per quanto visto prima ${\sigma'}^{p^{n-1}}(w) = w + 1$, dunque ${\sigma'}^{p^{n-1}}$ è un automorfismo di $\mathbb{E}(w)$ che fissa $\mathbb{E}$ e che ha ordine p, cioè ${\sigma'}^{p^{n-1}}$ genera $\mathrm{Gal}(\mathbb{E}(w)/\mathbb{E})$. Segue che σ' ha ordine p^n e siccome $\sigma' \in \mathrm{Gal}(\mathbb{E}(w)/\mathbb{K})$ e

$$|\mathrm{Gal}(\mathbb{E}(w)/\mathbb{K})| = [\mathbb{E}(w) : \mathbb{K}] = p^n = | < \sigma' > |,$$

segue che $\mathrm{Gal}(\mathbb{E}(w)/\mathbb{K})$ è un gruppo ciclico generato da σ'.

□

Con queste applicazioni abbiamo concluso la caratterizzazione delle estensioni cicliche che rientrano nel *caso* (i) definito a pagina 16.
Ora focalizzeremo l'attenzione sulla struttura dell'estensioni cicliche di grado n del *caso* (ii). A tale scopo, daremo alcune importanti definizioni e aggiungeremo delle ipotesi sul campo $\mathbb{K}$.

2.6 Estensioni cicliche di grado n, in cui la caratteristica del campo non divide n

Definizione 2.5. Siano $\mathbb{K}$ un campo ed n un intero positivo. Un elemento ξ si dice **radice n-esima dell'unità** se $\xi^n = 1$, cioè se ξ è una radice del polinomio $x^n - 1_{\mathbb{K}} \in \mathbb{K}[x]$.

Osserviamo che l'insieme di tutte le radici n-esime dell'unità contenute in $\mathbb{K}$ forma un sottogruppo del gruppo moltiplicativo degli elementi non nulli di $\mathbb{K}$, che è ciclico per il *Teorema 1.1.4* . Inoltre questo sottogruppo può avere ordine al più n.

Definizione 2.6. $\xi \in \mathbb{K}$ si dice **radice n-esima primitiva dell'unità** se ξ è una radice n-esima dell'unità e ha ordine n nel gruppo moltiplicativo delle radici n-sime dell'unità.
In particolare, una radice n-esima primitiva dell'unità genera il gruppo ciclico di tutte le radici n-esime dell'unità.

Osservazione 5. Se $\mathrm{char}\mathbb{K} = p$ e $p \mid n$, allora $n = p^k m$ con $(p, m) = 1$ e $m < n$.
Dunque in caratteristica p : $x^n - 1_{\mathbb{K}} = (x^m - 1_{\mathbb{K}})^{p^k}$.
Allora in $\mathbb{K}$ le radici n-sime dell'unità coincidono con le radici m-esime dell'unità.
Poichè $m < n$, in $\mathbb{K}$ non ci possono essere radici n-esime primitive dell'unità.
Se invece $\mathrm{char}\mathbb{K}$ non divide n, in particolare se $\mathrm{char}\mathbb{K} = 0$, si ha che $nx^{n-1} \neq 0$ e dunque il polinomio $x^n - 1_{\mathbb{K}}$ è relativamente primo con la sua derivata. Per l'*Osservazione1.2.5*, $x^n - 1_{\mathbb{K}}$ è separabile, cioè ha n radici distinte nel suo campo di spezzamento $\mathbb{F}$ su $\mathbb{K}$. Il gruppo ciclico delle radici n-sime dell'unità in $\mathbb{F}$ ha ordine n e allora $\mathbb{F}$, ma non necessariamente $\mathbb{K}$, contiene almeno una radice n-sima primitiva dell'unità.
Notiamo infine che se $\mathbb{K}$ contiene una radice n-sima primitiva dell'unità, allora contiene tutte le n radici distinte del polinomio $x^n - 1_{\mathbb{K}}$ quindi $\mathbb{K} = \mathbb{F}$.

Esempi.

- $1_{\mathbb{K}}$ è una radice n-sima dell'unità nel campo $\mathbb{K}$ per ogni $n \geq 1$.
  Se char$\mathbb{K} = p \neq 0$ e $n = p^k$, allora $1_{\mathbb{K}}$ è l'unica radice n-sima dell'unità contenuta in $\mathbb{K}$;
- Il sottocampo $\mathbb{Q}(i)$ di $\mathbb{C}$ contiene entrambe le radici quarte dell'unità $\pm i$, ma non contiene radici cubiche dell'unità eccetto 1 (le altre due sono $\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$) ;
- per ogni $n > 0$, $e^{\frac{2\pi}{n}i} \in \mathbb{C}$ è una radice n-sima primitiva dell'unità.

Lemma 2.6.1. *Sia n un intero positivo e $\mathbb{K}$ un campo che contiene una radice n-sima primitiva dell'unità ξ.*

(i) se $d \mid n$, allora $\xi^{n/d} = \eta$ è una radice d-esima primitiva dell'unità in $\mathbb{K}$.

(ii) se $d \mid n$ e u è una radice non nulla del polinomio $g = x^d - a \in \mathbb{K}[x]$, allora g ha d radici distinte: $u, \eta u, \eta^2 u, ..., \eta^{d-1} u$, con $\eta \in \mathbb{K}$ radice d-esima primitiva dell'unità. Inoltre $\mathbb{K}(u)$ è il campo di spezzamento di g su $\mathbb{K}$ e $\mathbb{K} \subseteq \mathbb{K}(u)$ è un'estensione di Galois.

Dimostrazione.

(i) ξ genera un gruppo moltiplicativo di ordine n per definizione. Se $d \mid n$, allora $\eta = \xi^{n/d}$ ha ordine d ed è una radice d-esima primitiva dell'unità.

(ii) Se u è una radice del polinomio g, allora anche $\eta^i u$ lo è. Poichè η ha periodo d, gli elementi $\eta^0 = 1_{\mathbb{K}}, \eta, ..., \eta^{d-1}$ sono distinti. Dunque, essendo $\eta \in \mathbb{K}$, le radici $u, \eta u, ..., \eta^{d-1} u$ del polinomio $x^n - 1_{\mathbb{K}}$ sono elementi distinti di $\mathbb{K}(u)$. Segue che $\mathbb{K}(u)$ è il campo di spezzamento di g su $\mathbb{K}$.
I fattori irriducibili di g sono separabili poichè tutte le radici sono distinte. Allora per il *Teorema 1.2.3*, $\mathbb{K}(u)$ è un'estensione di Galois di $\mathbb{K}$.

□

Teorema 2.6.2. *Sia n un intero positivo e $\mathbb{K}$ un campo che contiene una radice n-sima primitiva dell'unità ξ.*
Allora le seguenti condizioni sull'estensione $\mathbb{K} \subseteq \mathbb{F}$ sono equivalenti:

(i) $\mathbb{F}$ è un'estensione ciclica di grado d, con $d \mid n$;

(ii) $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ di un polinomio $f = x^n - a \in \mathbb{K}[x]$. In questo caso $\mathbb{F} = \mathbb{K}(u)$, con u radice di f ;

(iii) $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ di un polinomio irriducibile $g = x^d - b \in \mathbb{K}[x]$, con $d \mid n$. In questo caso $\mathbb{F} = \mathbb{K}(v)$, con v radice di g .

Dimostrazione.
Dimostriamo prima che $(ii) \Rightarrow (i)$.
Il *Lemma 2.6.1* mostra che $\mathbb{F} = \mathbb{K}(u)$, con u radice di f, e che $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione di Galois. Se $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}(u)/\mathbb{K})$, allora per l'*Osservazione 2*, σ è completamente determinato da $\sigma(u)$ che è una radice di f. Dal *Lemma 2.6.1* segue che, $\sigma(u) = \xi^i u$ per un certo i, $0 \leq i \leq n-1$.
Si verifica che l'applicazione che manda il σ scelto nel corrispondente ξ^i, definisce un morfismo iniettivo tra $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ e il gruppo moltiplicativo ciclico di ordine n delle radici n-sime dell'unità in $\mathbb{K}$. Allora $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è un gruppo ciclico il cui ordine d divide n, dunque l'estensione $\mathbb{K} \subseteq \mathbb{F}$ è ciclica di grado d.
Mostriamo ora che $(i) \Rightarrow (iii)$:
per ipotesi $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è ciclico di ordine $d = [\mathbb{F} : \mathbb{K}]$. Sia σ un suo generatore e sia $\eta = \xi^{n/d} \in \mathbb{K}$ una radice d-esima primitiva dell'unità. Per il *Teorema 2.1.1* si ha che $N_{\mathbb{K}}{}^{\mathbb{F}}(\eta) = \eta^{[\mathbb{F}:\mathbb{K}]} = \eta^d = 1_{\mathbb{K}}$. Dunque applicando il *Teorema di Hilbert* 90, $\eta = w\sigma(w)^{-1}$, per un certo $w \in \mathbb{F}$. Posto $v = w^{-1}$ si ha che $\sigma(v) = \eta v$ e $\sigma(v^d) = (\eta v)^d = \eta^d v^d = v^d$. Poichè $\mathbb{F}$ è di Galois su $\mathbb{K}$, $v^d = b \in \mathbb{K}$, così v è una radice del polinomio $g = x^d - b \in \mathbb{K}[x]$. Sempre per il *Lemma 2.6.1* si ha $\mathbb{K}(v) \subseteq \mathbb{F}$ e $\mathbb{K}(v)$ è il campo di spezzamento su $\mathbb{K}$ del polinomio g, che ha come radici distinte $v, \eta v, ..., \eta^{d-1} v$. Inoltre per ogni i, con $0 \leq i \leq d-1$ si ha $\sigma^i(v) = \eta^i v$. Quindi σ^i stabilisce un 'isomorfismo tra $\mathbb{K}(v)$ *e* $\mathbb{K}(\eta^i v)$ per ogni i e da ciò segue che v e $\eta^i v$ sono radici di uno stesso polinomio irriducibile su $\mathbb{K}$. Allora g è irriducibile in $\mathbb{K}[x]$ e $[\mathbb{K}(v) : \mathbb{K}] = d = [\mathbb{F} : \mathbb{K}]$, quindi $\mathbb{F} = \mathbb{K}(v)$.
A questo punto basta far vedere che $(iii) \Rightarrow (ii)$ e abbiamo conluso.
Se $v \in \mathbb{F}$ è una radice di $g \in \mathbb{K}[x]$, per il *Lemma 2.6.1* si ha $\mathbb{F} = \mathbb{K}(v)$. Ora: $(\xi v)^n = \xi^n v^n = 1_{\mathbb{K}} v^{d(n/d)} = b^{n/d} \in \mathbb{K}$. Dunque ξv è una radice del polinomio $x^n - a \in \mathbb{K}[x]$, con $a = b^{n/d}$. Ancora per il *Lemma 2.6.1*, $\mathbb{K}(\xi v)$ è il campo di spezzamento di $x^n - a$ su $\mathbb{K}$. Ma $\xi \in \mathbb{K}$ quindi $\mathbb{F} = \mathbb{K}(v) = \mathbb{K}(\xi v)$.

□

E' evidente che le radici n-esime primitive dell'unità hanno un ruolo fondamentale nella dimostrazione dei nostri risultati. La caratterizzazione dei campi di spezzamento di un polinomio della forma $x^n - a \in \mathbb{K}[x]$ é notevolmente più difficile da fare se $\mathbb{K}$ non contiene almeno una radice n-sima primitiva dell'unità.
Il caso in cui $a = 1$ è costituito dalle cosiddette **estensioni ciclotomiche** .

Capitolo 3

Estensioni ciclotomiche

Definizione 3.1. Un'estensione di campi $\mathbb{K} \subset \mathbb{F}$ si dice **estensione ciclotomica di grado** n se $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ del polinomio $x^n - 1_{\mathbb{K}} \in \mathbb{K}[x]$. Ovviamente se $\mathbb{F} \neq \mathbb{K}$, deve essere $n \geq 1$.

Per quanto già visto nell' *Osservazione 5*, se char$\mathbb{K} = p \neq 0$ e il grado n dell'estensione si scrive come $n = mp^t$ con $(p, m) = 1$, allora $x^n - 1_{\mathbb{K}} = (x^m - 1_{\mathbb{K}})^{p^t}$. Dunque un'estensione ciclotomica di grado n coincide con un'estensione ciclotomica di grado m. Per questo, d'ora in poi assumeremo che la caratteristica di $\mathbb{K}$ non divida il grado n dell'estensione, vale a dire char$\mathbb{K} = 0$ oppure (char$\mathbb{K}$, n)= 1.

Osservazione 6. Se $\mathbb{F}$ è il campo di spezzamento di $x^n - 1_K \in \mathbb{K}[x]$, allora sicuramente $\mathbb{F}$ contiene tutte le sue radici, in particolare $\xi \in \mathbb{F}$ con ξ radice primitiva n-esima dell'unità. Per definizione, tutte le radici n-esime dell'unità sono $1_{\mathbb{K}}, \xi, \xi^2, ..., \xi^{n-1} \in \mathbb{K}(\xi)$. Dunque possiamo concludere che $\mathbb{F} = \mathbb{K}(\xi)$.

Prima di procedere riportiamo alcune nozioni di teoria dei numeri che, come vedremo, sono necessarie per la caratterizzazione delle estensioni ciclotomiche.

3.1 La funzione di Eulero

Definizione 3.2. La **funzione di Eulero** φ è una funzione aritmetica, vale a dire che ha come dominio $\mathbb{N}$ e fa corrispondere ad ogni naturale n il numero dei naturali coprimi con n e minori di n. Dunque $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$.
Osserviamo subito che $\varphi(0) = 0$ perchè non esistono naturali minori di 0 e $\varphi(1) = 1$ perchè 0 e 1 sono coprimi.

Osservazione 7. Sappiamo che in $\mathbb{Z}_n$ la classe di un intero i è invertibile se e solo se $(n, i) = 1$. Allora possiamo dire che il gruppo moltiplicativo delle unità di $\mathbb{Z}_n$ ha ordine $\varphi(n)$.

Per completezza vediamo ora alcune proprietà della funzione di Eulero.

Proposizione 3.1.1. *Se p è un naturale primo, allora si ha che*

$$\varphi(p) = p - 1$$
$$\varphi(p^n) = p^n(1 - \frac{1}{p}) = (p-1)p^{n-1}$$

per ogni naturale $n > 0$.

Dimostrazione.
Poichè p è primo, tutti i naturali non nulli minori di p sono coprimi con p e quindi $\varphi(p) = p-1$. Vediamo ora che vale $\varphi(p^n) = p^n(1-\frac{1}{p}) = (p-1)p^{n-1}$. I multipli di p minori di p^n sono : $p, 2p, ..., (p-1)p, p^2, (p+1)p, ..., (p^2-1)p, p^3, ..., (p^{n-1}-1)p$. Il loro numero è uguale a $p^{n-1}-1$. Il numero di tutti i naturali non nulli e minori di p^n è $p^n - 1$. Quindi $\varphi(p^n)=(p^n-1)-(p^{n-1}-1) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n(1-\frac{1}{p})$.
□

Proposizione 3.1.2. *La funzione di Eulero φ è moltiplicativa, cioè se n, m sono intei positivi tali che $(m, n) = 1$, allora $\varphi(nm) = \varphi(n)\varphi(m)$.*

Dimostrazione.
Poichè $(m, n) = 1$,vale $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$. Dunque il sottogruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_m \times \mathbb{Z}_n$ ha lo stesso ordine del sottogruppo degli elementi invertibili di $\mathbb{Z}_{mn}$. Allora l'*Osservazione 7* ci dice che

$$\varphi(mn) = \varphi(n)\varphi(m).$$

□

Proposizione 3.1.3. *Se $n = p_1^{k_1} \cdots p_r^{k_r}$ con $k_i > 0$, allora*

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}).$$

Dimostrazione.
Poichè la funzione di Eulero è moltiplicativa, si ha $\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r})$. Applichiamo la *Proposizione 3.1.1* e otteniamo :

$$\varphi(n) = p_1^{k_1}\big(1 - \frac{1}{p_1}\big)p_2^{k_2}\big(1 - \frac{1}{p_2}\big) \cdots p_r^{k_r}\big(1 - \frac{1}{p_r}\big) = n\big(1 - \frac{1}{p_1}\big)\big(1 - \frac{1}{p_2}\big) \cdots \big(1 - \frac{1}{p_r}\big).$$

□

Proposizione 3.1.4. *Sia n un naturale positivo, si dimostra che:*

$$\sum_{d|n} \varphi(d).$$

Dimostrazione.
Consideriamo la decomposizione in fattori primi di n : $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Proviamo la Proposizione per induzione su s. Sicuramente per $s = 1$ si ha che

$$\sum_{d|p^k} \varphi(d) = \varphi(1) + \varphi(p) + ... + \varphi(p^k)$$

$$= 1 + (p-1) + p(p-1) + ... + p^{k-1}(p-1)$$

$$= 1 + (p-1)(1 + p + ... + p^{k-1}) = 1 + (p-1)\frac{p^k - 1}{p-1} = p^k.$$

Sia ora $m = p_1^{k_1} p_2^{k_2} \cdot \cdot \cdot p_{s-1}^{k_{s-1}}$, dunque $n = m p_s^{k_s}$. Per ipotesi induttiva vale $\sum_{e|m} \varphi(e) = m$. Tutti i divisori di n sono tutti e soli i numeri della forma ef dove e è un divisore di m ed f è un divisore di $p_s^{k_s}$ e dunque $f = p_s^{k_j}$ con $k_j < k_s$. Applichiamo l'ipotesi induttiva anche a $p_s^{k_s}$ ed otteniamo $\sum_{f|p_s^{k_s}} \varphi(f) = \sum_{i=0}^{k_s} \varphi(p^i)$. Ricordando che la funzione di Eulero è moltiplicativa si ha che:

$$\sum_{d|n} \varphi(d) = \sum_{e|m} \sum_{f|p_s^{k_s}} \varphi(ef) = \sum_{e|m} \Big(\sum_{f|p_s^{k_s}} \varphi(e)\varphi(f) \Big)$$

$$= \sum_{e|m} \Big(\varphi(e) \sum_{f|p_s^{k_s}} \varphi(f) \Big) = \sum_{e|m} \varphi(e) p_s^{k_s}$$

$$= p_s^{k_s} \sum_{e|m} \varphi(e) = p_s^{k_s} m = n.$$

□

Utilizziamo la funzione di Eulero per dimostrare ora un'importante teorema sulle estensioni ciclotomiche, premettendo la definizione di estensione abeliana e un lemma.

Definizione 3.3. L'estensione di campi $\mathbb{K} \subseteq \mathbb{F}$ si dice **estensione abeliana** se $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ è abeliano.

Lemma 3.1.5. *Se $\mathbb{F}$ un'estensione ciclotomica di grado n di un campo $\mathbb{K}$, allora $\mathbb{F}$ è di Galois su $\mathbb{K}$.*

Dimostrazione.
Per definizione $\mathbb{F}$ è il campo di spezzamento su $\mathbb{K}$ del polinomio $x^n - 1_K$ che, per quanto visto nell' *Osservazione 5*, è separabile. Dunque per il *Teorema 1.2.3*, $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione di Galois. □

Teorema 3.1.6. *Sia n un intero positivo e $\mathbb{K}$ un campo con caratteristica che non divide n. Se $\mathbb{F}$ è un'estensione ciclotomica di $\mathbb{K}$ di grado n allora si ha che:*

(i) *$\mathbb{F}$ è un'estensione abeliana di grado d con $d \mid \varphi(n)$; in particolare se n è primo, $\mathbb{F}$ è un'estensione ciclica.*

(ii) $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$ *è isomorfo ad un sottogruppo di grado d del gruppo moltiplicativo delle unità di $\mathbb{Z}_n$.*

Dimostrazione.
Per il *Lemma 3.1.5*, $\mathbb{K} \subseteq \mathbb{F}$ è un'estensione di Galois e per quanto visto nella *Osservazione 6*, vale $\mathbb{F} = \mathbb{K}(\xi)$ con $\xi \in \mathbb{F}$ radice primitiva n-esima dell'unità. Quindi se $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, σ è completamente determinato da $\sigma(\xi)$. Per l'*Osservazione 2*, σ manda ξ in un'altra radice del polimio $x^n - 1_{\mathbb{K}}$, cioè in un'altra radice primitiva n-sima dell'unità. Dunque $\sigma(\xi) = \xi^i$, con $i \in \{1, ..., n-1\}$ fissato e per la stessa ragione anche $\sigma^{-1}(\xi) = \xi^j$, con $j \in \{1, ..., n-1\}$ fissato. Allora si ha che $\xi = \sigma^{-1}\sigma(\xi) = \xi^{ij}$ che equivale a dire $\xi^{ij-1} = 1$. Poichè ξ ha periodo n allora n divide $ij - 1$, cioè $ij \equiv 1 \bmod n$ e dunque la classe $\bar{i} \in \mathbb{Z}_n$ appartiene in realtà al gruppo moltiplicativo delle unità di $\mathbb{Z}_n$ che indichiamo con $U(\mathbb{Z}_n)$.
$U(\mathbb{Z}_n)$ è abeliano e per l'*Osservazione 7*, ha ordine $\varphi(n)$. Definiamo ora un'applicazione $f : \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \longrightarrow U(\mathbb{Z}_n)$ che manda un elemento $\gamma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ nella classe di resto modulo n dell'esponente di ξ corrispondente al valore assunto da $\gamma(\xi)$. Verifichiamo che f è un omomorfismo di gruppi. Siano $\gamma, \delta \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, con $\gamma(\xi) = \xi^h$ e $\delta(\xi) = \xi^k$ con $h, k \in \mathbb{Z}$, allora $\gamma\delta(\xi) = \xi^{kh}$. Si ha dunque che $f(\gamma\delta) = \overline{kh} = \overline{hk} = f(\gamma)f(\delta)$, cioè f è un omomorfismo. Poichè f è chiaramente iniettivo, vale $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) \cong \mathrm{Im}f$ con $\mathrm{Im}f$ abeliano in quanto sottogruppo di un gruppo abeliano e il suo ordine d divide l'ordine di $U(\mathbb{Z}_n)$ cioè $\varphi(n)$. Usando il *Teorema fondamentale di Galois* possiamo concludere che $[\mathbb{F} : \mathbb{K}] = d$. Infine, se n è primo allora $\mathbb{Z}_n$ è un campo e $U(\mathbb{Z}_n)$ è ciclico per il *Teorema 1.1.4*, dunque $\mathrm{Im}f$ è anche ciclico. Con questo abbiamo provato sia (i) che (ii).

□

3.2 Polinomi ciclotomici

Definizione 3.4. Sia $\mathbb{F}$ un'estensione ciclotomica di grado n di un campo $\mathbb{K}$ con n intero positivo. Il **polinomio ciclotomico n-esimo** su $\mathbb{K}$ è il polinomio monico $g_n = (x-\xi_1)(x-\xi_2)\cdots(x-\xi_r)$, dove $\xi_1, \xi_2, ..., \xi_r$ sono tutte le radici primitive n-sime dell'unità in $\mathbb{F}$.

Esempio. Se $\mathbb{K} = \mathbb{Q}$, vale:

$$g_1 = x - 1$$

$$g_2 = (x - (-1)) = x + 1$$

$$g_3 = (x - \Big(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\Big)(x - \Big(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\Big) = x^2 + x + 1$$

$$g_4 = (x-i)(x+i) = x^2 + 1$$

Vediamo alcune proposizioni che mostrano le proprietà più importanti dei polinomi ciclotomici.

Proposizione 3.2.1. *Sia n un intero positivo e sia $\mathbb{K}$ un campo con caratteristica che non divide n. Se g_n è l'n-simo polinomio ciclotomico su $\mathbb{K}$, allora vale*

$$x^n - 1_K = \prod_{d|n} g_d.$$

Dimostrazione.
Sia $\mathbb{F}$ un'estensione ciclotomica di $\mathbb{K}$ di grado n e $\xi \in \mathbb{F}$ una radice primitiva n-esima dell'unità. Per il *Lemma 2.6.1*, se $G =< \xi >$ è l'insieme delle radici n-esime dell'unità e d è un divisore di n, una radice primitiva d-esima dell'unità η è una potenza di ξ e dunque $\eta \in G$. Allora vale:

$$g_d = \prod_{\substack{\eta \in G \\ |\eta| = d}} (x - \eta).$$

Dunque possiamo scrivere :

$$x^n - 1_{\mathbb{K}} = \prod_{\eta \in G} (x-\eta) = \prod_{\substack{d \\ d|n}} \Big(\prod_{\substack{\eta \in G \\ |\eta| = d}} (x-\eta)\Big) = \prod_{\substack{d \\ d|n}} g_d.$$

□

Proposizione 3.2.2. *Sia $\mathbb{K} \subset \mathbb{F}$ un'estensione ciclotomica di grado n con $n \geq 1$. Se g_n è l'n-esimo polinomio ciclotomico su $\mathbb{K}$, allora i coefficienti di g_n appartengono al sottocampo fondamentale di $\mathbb{K}$. In particolare se* $\mathrm{char}\mathbb{K} = 0$ *e dunque il suo sottocampo fondamentale è $\mathbb{Q}$, i coefficienti di g_n sono interi.*

Dimostrazione.
Chiamiamo P il sottocampo fondamentale di $\mathbb{K}$ e proviamo l'enunciato per induzione su n. Sicuramente se $n = 1$, $g_1 = x - 1_{\mathbb{K}} \in P[x]$. Assumiamo che la proposizione valga per tutti i g_k con $k < n$ e proviamo che vale anche per g_n. Sia

$$f = \prod_{\substack{d \\ d|n \\ d<n}} g_d$$

e per ipotesi induttiva $f \in P$. Per la *Proposizione 3.2.1*, in $\mathbb{F}[x]$ possiamo scrivere $x^n - 1_{\mathbb{K}} = fg_n$. Se consideriamo il polinomio $x^n - 1_{\mathbb{K}} \in P[x]$, possiamo dividerlo per f applicando l'algoritmo della divisione in $P[x]$. Dunque si ha $x^n - 1_{\mathbb{K}} = fh + r$, con $h, r \in P[x] \subseteq \mathbb{F}[x]$. Per l'unicità del quoziente e del resto della divisione in $\mathbb{F}[x]$, deve essere $r = 0$ e $h = g_n$, dunque $g_n \in P[x]$.
Se char$\mathbb{K}$=0 e $P = \mathbb{Q}$, con lo stesso procedimento, applicando l'algoritmo della divisione in $\mathbb{Z}$, si dimostra che $g_n \in \mathbb{Z}[x]$.

□

Per la dimostrazione della prossima Proposizione riguardante il grado dell'n-esimo polinomio ciclotomico su un campo $\mathbb{K}$, abbiamo bisogno del Teorema 3.6, cap.I, tratto da [1], che riportiamo di seguito come lemma.

Lemma 3.2.3. *Sia $G =< a >$ un gruppo ciclico finito di ordine m. Allora a^k è un generatore di G se e solo se $(k, m) = 1$.*

Proposizione 3.2.4. *Il grado di g_n è uguale a $\varphi(n)$, dove φ è la funzione di Eulero.*

Dimostrazione.
Chiaramente il grado di g_n è pari al numero delle radici primitive n-esime dell'unità. Sia ξ una radice primitiva n-esima dell'unità, allora le altre radici primitive sono una potenza di ξ. Per il *Lemma 3.2.3*, ξ^i con $1 \leq i \leq n$, è una radice primitiva n-esima dell'unità e dunque un generatore del gruppo delle radici n-sime dell'unità che ha ordine n, se e solo se $(i, n) = 1$. Possiamo concludere che, per come è definita la funzione di Eulero, il numero di tali i è dato da $\varphi(n)$.

□

Osservazione 8. Grazie ai risultati ottenuti, possiamo ricavare una formula ricorsiva per determinare g_n :

$$g_n = \frac{x^n - 1_{\mathbb{K}}}{\prod_{\substack{d \\ d|n \\ d<n}} g_d}.$$

Inoltre se $n = p$ con p primo si ha che

$$g_p = \frac{x^p - 1_{\mathbb{K}}}{x - 1_{\mathbb{K}}} = x^{p-1} + x^{p-2} + ... + x^2 + x + 1_{\mathbb{K}}.$$

Esempio. Se $\mathbb{K} = \mathbb{Q}$, si ha :

$$\begin{aligned} g_6 &= \frac{x^6 - 1}{g_1 g_2 g_3} \\ &= \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1; \end{aligned}$$

e allo stesso modo :

$$\begin{aligned} g_{12} &= \frac{x^{12} - 1}{g_1 g_2 g_3 g_6} \\ &= \frac{x^{12} - 1}{(x-1)(x+1)(x^2+x+1)(x^2-x+1)} = x^4 - x^2 + 1. \end{aligned}$$

3.3 Estensioni ciclotomiche del campo dei razionali

In questa sezione analizzeremo le estensioni ciclotomiche di grado n del campo $\mathbb{Q}$ e alcune caratteristiche dei suoi polinomi ciclotomici. Per farlo abbiamo bisogno di richiamare alcuni enunciati tratti da [1], in ordine: Lemma 6.13, cap.III e Teorema 5.5, cap.III, opportunamente adattati al nostro caso.

Lemma 3.3.1. *Consideriamo $\mathbb{Z}$ e il suo campo dei quozienti che è $\mathbb{Q}$, allora un polinomio monico $f \in \mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$.*

Lemma 3.3.2. *Dati p primo e la proiezione canonica su quoziente $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ che manda ogni intero n in $\pi(n) = \overline{n} = [n]$ mod p, allora esite un unico omomorfismo di anelli $\overline{\pi} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ con $\overline{\pi}_{|\mathbb{Z}} = \pi$. Inoltre se $f = \sum_{i=0}^{t} b_i x^i \in \mathbb{Z}[x]$, allora $\overline{\pi}(f) = \sum_{i=0}^{t} \overline{b_i} x^i$.*

Proposizione 3.3.3. *Sia $\mathbb{F}$ un'estensione ciclotomica di grado n del campo $\mathbb{Q}$ e sia g_n l'n-esimo polinomio ciclotomico su $\mathbb{Q}$. Allora g_n è irriducibile in $\mathbb{Q}[x]$.*

Dimostrazione.
Per il *Lemma 3.3.1*, basta provare che g_n è irriducibile in $\mathbb{Z}[x]$. Supponiamo che g_n non sia irriducibile in $\mathbb{Z}[x]$ e sia $h \in \mathbb{Z}[x]$ un suo fattore irriducibile con deg $h \geq 1$. Allora sarà $g_n = fh$ con $f, h \in \mathbb{Z}[x]$ necessariamente monici. Siano ξ una radice di h e p un primo tale che $(p, n) = 1$. Vogliamo mostrare che ξ^p è ancora una radice di h. Essendo una radice di g_n, ξ è una radice primitiva n-esima dell'unità e per il *Lemma 3.2.3*, anche ξ^p lo è. Dunque ξ^p è una radice di f oppure è una radice di h. Supponiamo che sia una radice di $f = \sum_{i=0}^{r} a_i x^i$, si deduce che ξ è una radice del polinomio $f_p = f(x^p) = \sum_{i=0}^{r} a_i x^{ip}$. Il *Lemma 3.3.1* ci dice che h è irriducibile anche in $\mathbb{Q}[x]$ ed essendo monico, è il polinomio minimo di ξ su $\mathbb{Q}$. Dunque h deve dividere f_p e si ha $f_p = hk$ con $k \in \mathbb{Q}[x]$. Ora dividiamo f_p per h in $\mathbb{Z}[x]$ applicando l'algoritmo euclideo della divisione : $f_p = hk_1 + r_1$ con $k_1, r_1 \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$. A questo punto l'unicità del quoziente e del resto della divisione in $\mathbb{Q}[x]$ ci dice che $k_1 = k \in \mathbb{Z}[x]$ e $r_1 = 0$.
Consideriamo ora l'omomorfismo di anelli $\psi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ che esiste sempre per il *Lemma 3.3.2* e che manda l'elemento $g = \sum_{i=0}^{t} b_i x^i \in \mathbb{Z}[x]$ in $\psi(g) = \sum_{i=0}^{t} \overline{b_i} x^i$. Allora in $\mathbb{Z}_p[x]$ si ha $\overline{f_p} = \overline{hk}$ ma in caratteristica p si ha pure $\overline{f_p} = \overline{f}^{\,p}$. Dunque

$$\overline{f}^{\,p} = \overline{h}\ \overline{k} \in \mathbb{Z}_p[x].$$

Si ha che in $\mathbb{Z}_p[x]$, un fattore irriducibile di $\overline{h}$ deve dividere $\overline{f}^{\,p}$ e di conseguenza $\overline{f}$. D'altra parte in $\mathbb{Z}[x]$ vale $x^n - 1 = g_n r$ per un certo polinomio r.
Allora $\psi(x^n - 1) = \overline{f}\ \overline{h}\overline{r}$, ma $\overline{f}$ e $\overline{h}$ hanno un fattore comune in $\mathbb{Z}_p[x]$, dunque $x^n - \overline{1}$ ha una radice multipla. Questo è assurdo perchè contraddice quanto detto nell' *Osservazione 5*. Dunque ξ^p è una radice di h.
Se prendiamo un intero $m < n$ e tale che $(m, n) = 1$, vale $m = p_1 p_2 \cdots p_s$, con p_i primi non necessariamente distinti tali che $(p_i, n) = 1$. Applichiamo più volte il fatto che per ogni ξ radice di h e per ogni primo p tale che $(p, n) = 1$, ξ^p è ancora una radice di h, all'espressione $\xi^m = \xi^{\,p_1 p_2 \cdots p_s}$ e si verifica che ξ^m è ancora una radice di h. Per il *Lemma 3.2.3* e per quanto visto nella dimostrazione della *Proposizione 3.2.4*, il numero di tali m è uguale al numero delle radici primitive n-esime dell'unità. Questo ci dice che g_n divide h ma per definizione, h divide g_n, dunque $g_n = h$ ed è irriducibile.

□

Proposizione 3.3.4. *Sia $\mathbb{F}$ un'estensione ciclotomica di $\mathbb{Q}$ di grado n. Allora:*

(i) $[\mathbb{F} : \mathbb{Q}] = \varphi(n)$, *dove φ è la funzione di Eulero.*

(ii) $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ *è isomorfo al gruppo moltiplicativo delle unità di $\mathbb{Z}_n$.*

Dimostrazione.

(i) Per il *Lemma 2.6.1*, $\mathbb{F} = \mathbb{Q}(\xi)$ dove ξ è una radice primitiva n-esima dell'unità contenuta in $\mathbb{F}$. Per quanto visto fin'ora, g_n è irriducibile ed essendo anche monico allora è il polinomio minimo di ξ su $\mathbb{Q}$ e si ha

$$[\mathbb{F} : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] = \deg g = \varphi(n).$$

(ii) Per il punto (ii) del *Teorema 3.1.6* abbiamo che $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ è isomorfo ad un sottogruppo di ordine d del gruppo moltiplicativo delle unità di $\mathbb{Z}_n$ che per l'*Osservazione 7* ha ordine $\varphi(n)$ e quindi in particolare d deve dividere $\varphi(n)$. Poichè $\mathbb{F}$ è un'estensione ciclotomica di $\mathbb{Q}$ di grado n, per il *Lemma 3.1.5*, $\mathbb{Q} \subseteq \mathbb{F}$ è un'estensione di Galois e dunque $|\mathrm{Gal}(\mathbb{F}/\mathbb{Q})| = [\mathbb{F} : \mathbb{Q}]$ che, per il punto (i), è uguale a $\varphi(n)$. Quindi $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ è isomorfo proprio al sottogruppo moltiplicativo delle unità di $\mathbb{Z}_n$.

□

Esempio. Sia $\mathbb{F}_5$ un'estensione ciclotomica di $\mathbb{Q}$ di grado 5, vale a dire che $\mathbb{F}_5$ è un campo di spezzamento del polinomio $x^5 - 1$ su $\mathbb{Q}$. Analizziamo $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q})$ e tutti campi intermedi.
In questo caso $g_5 = x^4 + x^3 + x^2 + x + 1$, dunque $[\mathbb{F}_5 : \mathbb{Q}] = \varphi(5) = \deg g_5 = 4$. Inoltre $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q})$ è isomorfo al gruppo moltiplicativo delle unità di $\mathbb{Z}_5$ e vale $|\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q})| = 4$. Quindi $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ oppure $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q}) \cong \mathbb{Z}_4$. Il *Teorema 3.1.6*, ci dice che poichè 5 è primo, $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q})$ è ciclico e allora possiamo affermare che $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q}) \cong \mathbb{Z}_4$.
Vediamo quali sono i campi intermedi tra $\mathbb{Q}$ ed $\mathbb{F}_5$. Ricordando che $\mathbb{Q} \subset \mathbb{F}_5$ è un'estensione di Galois, basta applicare la corrispondenza di Galois ed analizzare i sottogruppi di $\mathbb{Z}_4$ che sono $1, \mathbb{Z}_2, \mathbb{Z}_4$. Poichè il campo fissato da $\mathrm{Gal}(\mathbb{F}_5/\mathbb{Q}) \cong \mathbb{Z}_4$ è tutto $\mathbb{Q}$ e quello fissato dall'identità è tutto $\mathbb{F}_5$, resta da considerare solo il sottogruppo $\mathbb{Z}_2$. Sia ξ una radice primitiva quinta dell'unità tale che $\mathbb{F} = \mathbb{Q}(\xi)$, allora $\mathbb{Z}_2 \cong \{id, \sigma\} = H$ dove $\sigma : \mathbb{Q}(\xi) \longrightarrow \mathbb{Q}(\xi)$ ha ordine 2 ed è definito da $\sigma(\xi) = \xi^4$. Si ha che

$$\mathbb{F}_5^H = \{u \in \mathbb{Q}(\xi) \text{ tale che } \sigma(u) = u\}.$$

Dunque, preso $u \in \mathbb{Q}(\xi)$ che si può scrivere come $q_0 + q_1\xi + q_2\xi^2 + q_3\xi^3$ con $q_i \in \mathbb{Q}$, vale che

$$\sigma(u) = q_0 + q_1\xi^4 + q_2\xi^8 + q_3\xi^{12} = q_0 + q_1\xi^4 + q_2\xi^3 + q_3\xi^2. \tag{3.1}$$

Poichè ξ è radice di g_5, si ha che $\xi^4 = -\xi^3 - \xi^2 - \xi - 1$. Sostituiamo nella (3.1) e otteniamo:

$$\sigma(u) = q_0 - q_1 - q_1\xi + (q_3 - q_1)\xi^2 + (q_2 - q_1)\xi^3.$$

Allora affinchè $u \in \mathbb{F}_5^H$ deve valere che $q_1 = 0$ e $q_2 = q_3$, cioè

$$F_5^H = \{u \in \mathbb{Q}(\xi) \text{ tale che } u = q_0 + q(\xi^2 + \xi^3) \text{ con } q_0, q \in \mathbb{Q}\} = \mathbb{Q}(\xi^2 + \xi^3).$$

Bibliografia

[1] Thomas W. Hungerford, *Algebra*. Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

[2] J. S. Milne, *Fields and Galois Theory*, Note versione 4.22, 126 pagine, Marzo 2011. Sito: www.jmilne.org/math/CourseNotes/ft.html

[3] David A. Cox, *Galois Theory*, Wiley-Interscience [John Wiley and Sons], Hoboken, NJ, 2004.

[4] Irving Kaplansky, *Fields and Rings*. Second edition. Chicago Lectures in Mathematics. The University of Chicago Press, Chicago, Ill.-London, 1972.

Ringraziamenti

Quando ho scelto di lasciare la mia città e iniziare il mio percorso di studi universitari a Bologna, sono partita con l'appoggio e la presenza seppur non fisica ma comunque costante, di alcune persone a cui, durante il cammino, se ne sono aggiunte altre. Oggi è come se tutte loro avessero tagliato insieme a me questo importante traguardo accademico e quindi mi sembra doveroso ringranziarle.
Desidero ringraziare la Professoressa Marta Morigi, non solo per la sua disponibilità, professionalità e pazienza di relatrice ma anche per l'interesse che ha suscitato in me il suo corso di complementi di algebra.
Vorrei poi ringraziare la mia famiglia, che mi ha permesso di scegliere liberamente la mia strada e mi ha sempre sostenuta in ogni decisione, aiutandomi con l'amore a superare i momenti bui e difficili che in questi tre anni non sono mancati. In particolare voglio dire grazie a mia madre perchè con il suo esempio e il suo credo mi ha spinta a fare sempre meglio, a lottare, a non accontentarmi e ad essere diversa. A mia sorella Sara voglio dire che mi è mancato molto vivere la nostra quotidianeità in questi anni ma sicuramente la lontananza può anche avvicinare.
Ringrazio la mia amica Serena con cui ho conosciuto l'amore per la matematica, quello stesso amore che ci ha portate a percorrere strade diverse ma che ci ha fatto crescere e maturare con la certezza che ci saremo sempre l'una per l'altra.
Voglio dire grazie a mia nonna Dora e avrei voluto che anche mio nonno Guido fosse stato presente in questo giorno per poterlo rendere fiero di me.
Non posso certo dimenticare Gianluca e Ida che anche se considero parte della mia famiglia, meritano un ringraziamento speciale per l'affetto che mi hanno sempre dimostrato e per avermi insegnato tanto. A loro voglio fare anche un augurio particolare per la nascita del piccolo Jaco.
Desidero ringraziare la mia squadra di pallavolo, il mio allenatore, i TUG e in particolare la famiglia Bonetti che sono la mia grande famiglia bolognese in cui ho trovato un punto di riferimento e di sostegno.
Infine dico grazie alla persona senza la quale non sarei mai arrivata fin qui,
Gianluca, mio compagno di studio e di vita che non mi ha mai fatta sentire sola,

che ha creduto in me senza mai avere incertezze, che ha condiviso con me non solo successi e gioie ma anche fallimenti e dolori, restandomi sempre accanto con il suo ottimismo e il suo sorriso. Come si dice, finchè la matematica non ci separi.