Scheda riassuntiva di Teoria dei campi e di Galois

Campi e omomorfismi

Si dice **campo** un anello commutativo non banale K che è contemporaneamente anche un corpo. Si dice **omomorfismo di campo** tra due campi K ed L un omomorfismo di anelli. Dal momento che un omomorfismo φ è tale per cui $\operatorname{Ker}\varphi$ è un ideale di K con $1 \notin \operatorname{Ker}\varphi$, deve per forza valere $\operatorname{Ker}\varphi = \{0\}$, e quindi ogni omomorfismo di campi è un'immersione.

Caratteristica di un campo

Dato l'omomorfismo $\zeta : \mathbb{Z} \to K$ completamente determinato dalla relazione $1 \overset{\zeta}{\mapsto} 1_K$, si definisce **caratteristica di** K, detta $\operatorname{char} K$, il generatore non negativo di $\operatorname{Ker}\zeta$. In particolare $\operatorname{char} K$ è 0 o un numero primo. Se $\operatorname{char} K$ è zero, ζ è un'immersione, e quindi K è un campo infinito, e in particolare vi si immerge anche $\mathbb{Q}$.

Tuttavia non è detto che $\operatorname{char} K = p$ implichi che K è finito. In particolare $\mathbb{Z}_p(x)$, il campo delle funzioni razionali a coefficienti in $\mathbb{Z}_p$, è un campo infinito a caratteristica p.

Proprietà dei campi a caratteristica p

Se $\operatorname{char} K = p$, per il Primo teorema di isomorfismo per anelli, $\mathbb{Z}/p\mathbb{Z}$ si immerge su K tramite la proiezione di ζ; pertanto K contiene una copia isomorfa di $\mathbb{Z}/p\mathbb{Z}$. Per campi di caratteristica p, vale il Teorema del binomio ingenuo, ossia:

$$(a+b)^p = a^p + b^p,$$

estendibile anche a più addendi. In particolare, per un campo K di caratteristica p, la mappa $\mathcal{F} : K \to K$ tale per cui $a \overset{\mathcal{F}}{\mapsto} a^p$ è un omomorfismo di campi, ed in particolare è un'immersione di K in K, detta **endomorfismo di Frobenius**. Se K è un campo finito, $\mathcal{F}$ è anche un isomorfismo. Si osserva che per gli elementi della copia $K \supseteq \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ vale $\mathcal{F}|_{\mathbb{F}_p} = \mathrm{Id}_{\mathbb{F}_p}$, e quindi $\mathcal{F}$ è un elemento di $\operatorname{Gal}(K/\mathbb{F}_p)$.

Campi finiti

Per ogni p primo e $n \in \mathbb{N}^+$ esiste un campo finito di ordine p^n. In particolare, tutti i campi finiti di ordine p^n sono isomorfi tra loro, possono essere visti come spazi vettoriali di dimensione n sull'immersione di $\mathbb{Z}/p\mathbb{Z}$ che contengono, e come campi di spezzamento di $x^{p^n} - x$ su tale immersione. Tali campi hanno obbligatoriamente caratteristica p, dove $|K| = p^n$. Esiste sempre un isomorfismo tra due campi finiti che manda la copia isomorfa di $\mathbb{Z}/p\mathbb{Z}$ di uno nell'altra.

Poiché i campi finiti di medesima cardinalità sono isomorfi, si indicano con $\mathbb{F}_p$ e $\mathbb{F}_{p^n}$ le strutture algebriche di tali campi. In particolare con $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si intende che esiste un'immersione di un campo con p^n elementi in uno con p^m elementi, e analogamente si farà con altre relazioni (come l'estensione di campi) tenendo bene in mente di star considerando tutti i campi di tale ordine.

Vale la relazione $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{q^m}$ se e solo se $p = q$ e $n \mid m$. Conseguentemente, l'estensione minimale per inclusione comune a $\mathbb{F}_{p^{n_1}}$, ..., $\mathbb{F}_{p^{n_i}}$ è $\mathbb{F}_{p^m}$ dove $m := \operatorname{mcm}(n_1, \ldots, n_i)$. Pertanto se $p \in \mathbb{F}_{p^n}[x]$ si decompone in fattori irriducibili di grado n_1, ..., n_i, il suo campo di spezzamento è $\mathbb{F}_{p^m}$. Inoltre, $x^{p^n} - x$ è in $\mathbb{F}_p$ il prodotto di tutti gli irriducibili di grado divisore di n.

Proprietà dei polinomi di $K[x]$

Per il Teorema di Lagrange sui campi, ogni polinomio di $K[x]$ ammette al più tante radici quante il suo grado. Come conseguenza pratica di questo teorema, ogni sottogruppo moltiplicativo finito di K è ciclico. Pertanto $\mathbb{F}_{p^n}^* = \langle\alpha\rangle$ per $\alpha \in \mathbb{F}_{p^n}$, e quindi $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, ossia $\mathbb{F}_{p^n}$ è sempre un'estensione semplice su $\mathbb{F}_p$. Si dice **campo di spezzamento** di una famiglia $\mathcal{F}$ di polinomi di $K[x]$ un sovracampo minimale per inclusione di K che fa sì che ogni polinomio di $\mathcal{F}$ si decomponga in fattori lineari. I campi di spezzamento di $\mathcal{F}$ sono sempre K-isomorfi tra loro.

Un polinomio irriducibile si dice separabile se ammette radici distinte. Per il criterio della derivata, $p \in K[x]$ ammette radici multiple se e solo se $\operatorname{MCD}(p, p')$ non è invertibile, dove p' è la derivata formale di p. Se $p \in K[x]$ e $n := \deg p$, il campo di spezzamento L di p è tale per cui $[L : K] \leq n!$. Se p è irriducibile e separabile, vale anche che $n \mid [L : K] \mid n!$, come conseguenza dell'azione del relativo gruppo di Galois sulle radici.

Se p è irriducibile in $K[x]$, (p) è un ideale massimale, e $K[x]/(p)$ è un campo che ne contiene una radice, ossia $[x]$. In particolare K si immerge in $K[x]/(p)$, e quindi tale campo può essere identificato come un'estensione di K che aggiunge una radice di p. Se K è finito, detta α la radice aggiunta all'estensione, $L := K[x]/(p) \cong K(\alpha)$ contiene tutte le radici di p (ed è dunque il suo campo di spezzamento). Infatti detto $[L : \mathbb{F}_p] = n$, $[x]$ annulla $x^{p^n} - x$ per il Teorema di Lagrange sui gruppi, e quindi p deve dividere $x^{p^n} - x$; in tal modo p deve spezzarsi in fattori lineari, e quindi ogni radice deve già appartenere ad L. In particolare, ogni estensione finita e semplice di un campo finito è normale, e quindi di Galois.

Estensioni di campo

Si dice che L è un'estensione di K, e si indica con L/K, se L è un sovracampo di K, ossia se $K \subseteq L$. Si indica con $[L : K] = \dim_K L$ la dimensione di L come K-spazio vettoriale. Si dice che L è un'estensione finita di K se $[L : K]$ è finito, e infinita altrimenti. Un'**estensione finita** di un campo finito è ancora un campo finito. Un'estensione è finita se e solo se è finitamente generata da elementi algebrici. Una K-immersione è un omomorfismo di campi iniettivo da un'estensione di K in un'altra estensione di K che agisce come l'identità su K. Un K-isomorfismo è una K-immersione che è isomorfismo.

Composto di estensioni e teorema delle torri algebriche

Date estensioni L e M su K, si definisce $LM = L(M) = M(L)$ come il **composto** di L ed M, ossia come la più piccola estensione di K che contiene sia L che M. In particolare, LM può essere visto come L-spazio vettoriale con vettori in M, o analogamente come M-spazio con vettori in L.

Per il Teorema delle torri algebriche, L/K è un'estensione finita se e solo se L/F e F/K lo sono (ossia la finitezza vale strettamente per torri). Inoltre, se $\mathcal{B}_{L/F}$ e $\mathcal{B}_{F/K}$ sono basi di L/F e F/K, allora $\mathcal{B}_{L/F}\mathcal{B}_{F/K}$ è una base di L/K, dove i suoi elementi sono i prodotti tra i vari elementi delle due basi. Infine se L/K è finita, allora anche LM/M è finita, e vale che $[LM : M] \leq [L : K]$ (infatti una base di L/K può essere trasformata in un insieme di generatori di LM/M), e quindi la finitezza vale per *shift*. Sempre per il Teorema delle torri algebriche, se L/K è finito, allora vale che:

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

Se L/K e M/K sono finite, anche LM/K lo è (infatti la finitezza vale sia per torri che per *shift*). In particolare, vale che:

$$\operatorname{mcm}([L : K], [M : K]) \mid [LM : K].$$

Se $[L : K]$ ed $[M : K]$ sono coprimi tra loro, allora vale proprio l'uguaglianza $[LM : K] = [L : K][M : K]$. Infatti, in tal caso, si avrebbe $[L : K][M : K] \leq [LM : K]$ e $[LM : K] = [LM : M][M : K] \leq [L : K][M : K]$.

Omomorfismo di valutazioni, elementi algebrici e trascendenti e polinomio minimo

Dato α, si definisce $K(\alpha)$ il più piccolo sovracampo di K che contiene α. Si definisce l'**omomorfismo di valutazione** $\varphi_{\alpha,K} : K[x] \to K[\alpha]$, detto φ_α se K è noto, l'omomorfismo completamente determinato dalla relazione $p \overset{\varphi_\alpha}{\longmapsto} p(\alpha)$. Si verifica che φ_α è surgettivo. Se φ_α è iniettivo, si dice che α è **trascendentale** su K e $K[x] \cong K[\alpha]$, da cui $[K[\alpha] : K] = [K[x] : K] = \infty$. Se invece φ_α non è iniettivo, si dice che α è **algebrico** su K. Si definisce μ_α, detto il **polinomio minimo** di α su K, il generatore monico di $\operatorname{Ker}\varphi_\alpha$. IDal momento che K è in particolare un dominio di integrità, μ_α è sempre irriducibile.

Si definisce $\deg_K \alpha := \deg \mu_\alpha$. Se α è algebrico su K, $K[x]/(\mu_\alpha) \cong K[\alpha]$, e quindi $K[\alpha]$ è un campo. Dacché $K[\alpha] \subseteq K(\alpha)$, vale allora $K[\alpha] = K(\alpha)$. Inoltre, poiché $\dim_K K[x]/(\mu_\alpha) = \deg_K \alpha$, vale anche che $[K(\alpha) : K] = \deg_K \alpha$. Infine, si verifica che α è algebrico se e solo se $[K(\alpha) : K]$ è finito.

Estensioni semplici, algebriche

Si dice che L è un'**estensione semplice** di K se $\exists\,\alpha \in L$ tale per cui $L = K(\alpha)$. In tal caso si dice che α è un **elemento primitivo** di K. Si dice che L è un'**estensione algebrica** di K se ogni suo elemento è algebrico su K. Ogni estensione finita è algebrica. Non tutte le estensioni algebriche sono finite (e.g. $\overline{\mathbb{Q}}$ su $\mathbb{Q}$).

L'insieme degli elementi algebrici di un'estensione di K su K è un estensione algebrica di K. Pertanto se α e β sono algebrici, $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ e $\alpha^{-1}\beta$ (a patto che o $\alpha \neq 0$ o $\beta \neq 0$) sono algebrici.

Campi perfetti, estensioni separabili e coniugati

Si dice che un'estensione algebrica L è un'**estensione separabile** di K se per ogni elemento $\alpha \in L$, μ_α ammette radici distinte. Si dice che K è un **campo perfetto** se ogni polinomio irriducibile ammette radici distinte, ossia se ogni polinomio irriducibile è separabile. In un campo perfetto, ogni estensione algebrica è separabile. Si definiscono i coniugati di α algebrico su K come le radici di μ_α. Se $K(\alpha)$ è separabile su K, α ha esattamente $\deg_K \alpha$ coniugati, altrimenti esistono al più $\deg_K \alpha$ coniugati.

Un campo è perfetto se e solo se ha caratteristica 0 o altrimenti se l'endomorfismo di Frobenius è un automorfismo. Equivalentemente, un campo è perfetto se le derivate dei polinomi irriducibili sono sempre non nulle. Esempi di campi perfetti sono allora tutti i campi di caratteristica 0 e tutti i campi finiti.

Campi algebricamente chiusi e chiusura algebrica di K

Un campo K si dice **algebricamente chiuso** se ogni $p \in K[x]$ ammette una radice in K. Equivalentemente K è algebricamente chiuso se ogni $p \in K[x]$ ammette tutte le sue radici in K. Si dice **chiusura algebrica** di K una sua estensione algebrica e algebricamente chiusa. Le chiusure algebriche di K sono K-isomorfe tra loro, e quindi si identifica con $\overline{K}$ la struttura algebrica della chiusura algebrica di K.

Se L è una sottoestensione di K algebricamente chiuso, allora $\overline{L}$ è il campo degli elementi algebrici di K su L. Infatti se $p \in L[x]$, p ammette una radice α in K, essendo algebricamente chiuso. Allora α è un elemento di K algebrico su L, e quindi $\alpha \in \overline{L}$. Per il Teorema fondamentale dell'algebra, $\overline{\mathbb{R}} = \mathbb{C}$.

Estensioni normali e di Galois, K-immersioni di un'estensione finita di K

Sia α un elemento algebrico su K. Allora $[K(\alpha) : K] = \deg_K \alpha$. Le K-immersioni da $K(\alpha)$ in $\overline{K}$ sono esattamente tante quanti sono i coniugati di α e sono tali da mappare α ad un suo coniugato. Se K è perfetto, esistono esattamente $\deg_K \alpha$ K-immersioni da $K(\alpha)$ in $\overline{K}$.

Se L/K è un'estensione separabile finita su K, allora esistono esattamente $[L : K]$ K-immersioni da L in $\overline{K}$. Per quanto detto prima, tali immersioni mappano gli elementi L nei loro coniugati.

Se L è un'estensione separabile finita, allora per ogni $\varphi : K \to \overline{K}$ esistono esattamente $[L : K]$ estensioni $\varphi_i : L \to \overline{K}$ di φ, ossia omomorfismi tali per cui $\varphi_i|_K = \varphi$.

Per quanto detto prima, per calcolare dunque tutti i coniugati di $\alpha \in L$ su K, è sufficiente calcolare i distinti valori delle K-immersioni di L su α. Infatti, ogni K-immersione da $K(\alpha)$ può estendersi a K-immersione di L, e viceversa ogni K-immersione di L può restringersi a K-immersione di $K(\alpha)$. In particolare, una volta computati tutti i coniugati, è semplice trovare il polinomio minimo di α su K (è sufficiente considerare il prodotto dei vari $x - \alpha_i$ dove gli α_i sono tutti i coniugati di α).

Si dice che un'estensione algebrica L/K è un'**estensione normale** se per ogni K-immersione φ da L in $\overline{K}$ vale che $\varphi(L) = L$. Equivalentemente un'estensione è normale se è il campo di spezzamento di una famiglia di polinomi (in particolare è il campo di spezzamento di tutti i polinomi irriducibili che hanno una radice in L). Ancora, un'estensione L è normale se e solo se per ogni $\alpha \in L$, i coniugati di L appartengono ancora ad L. Per un'estensione normale, per ogni K-immersione $\varphi : L \to \overline{K}$ si può restringere il codominio ad un campo isomorfo a $L \subseteq \overline{K}$, e quindi considerare φ come un automorfismo di L che fissa K.

Un'estensione finita L/K di grado 2 è sempre normale, ed in particolare può sempre scriversi come $L = K(\sqrt{\Delta})$, dove Δ non è un quadrato in K.

Si indica con $\mathrm{Aut}_K(L) = \mathrm{Aut}(L/K)$ l'insieme degli automorfismi di L che fissano K. Se L è normale e separabile, si dice **estensione di Galois**, e si definisce il suo **gruppo di Galois** $\mathrm{Gal}(L/K)$ come $(\mathrm{Aut}_K L, \circ)$, ossia come il gruppo $\mathrm{Aut}_K L$ con l'operazione di composizione.

Azione di $\mathrm{Gal}(L/K)$ sulle radici di L campo di spezzamento

Sia $p \in K[x]$ irriducibile e separabile. Allora si definisce il **gruppo di Galois di** p come il gruppo di Galois $\mathrm{Gal}(L/K)$, dove L è un campo di spezzamento di p su K. Se $\deg p = n$ e a_1, ..., a_n sono le radici di p, $\mathrm{Gal}(L/K)$ agisce su $\{a_1, \ldots, a_n\}$ mediante Ξ, in modo tale che:

$$\Xi : \mathrm{Gal}(L/K) \to S(\{a_1, \ldots, a_n\}) \cong S_n,$$
$$\varphi_i \overset{\Xi}{\longmapsto} [a_j \mapsto \varphi_i(a_j)].$$

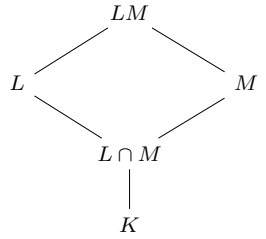
In particolare tale azione è transitiva (dunque $\mathrm{Orb}(a_i) = \{a_j\}_{j=1-n}$)e fedele. Poiché Ξ è fedele, vale che $\mathrm{Gal}(L/K) \hookrightarrow S_n$. Se $\mathrm{Gal}(L/K)$ è abeliano (e in tal caso si dice che L è un'**estensione abeliana**), Ξ è anche transitiva, e quindi $\mathrm{Gal}(L/K)$ si identifica come un sottogruppo abeliano transitivo di S_n, e in quanto tale deve valere che $|\mathrm{Gal}(L/K)| = n$.

Dal momento che Ξ è un'immersione, vale che $|\mathrm{Gal}(L/K)| \mid n!$. Dacché allora $[K(a_1) : K] = n$, vale in particolare che:

$$n \mid |\mathrm{Gal}(L/K)| = [L : K] \mid n!.$$

Diagrammi di campo e proprietà

Si definisce **diagramma di campo** un diagramma della seguente forma:



In particolare il precedente diagramma rappresenta lo studio dell'estensione di LM su K, e rappresenta L, M e $L \cap M$ come sottoestensioni di LM. Un estremo superiore di una freccia è sempre, per definizione, un'estensione dell'estremo inferiore della stessa freccia.

Sia $\mathcal{P}$ una proprietà. Allora si studia la proprietà $\mathcal{P}$ secondo le seguenti tre modalità:

- validità per **torri**: se $\mathcal{P}$ vale in due estensioni in $K \subseteq F \subseteq L$, allora vale anche per la terza estensione, ossia vale per tutta la torre di estensioni,
- validità per ***shift*** (o per il **traslato**): se $\mathcal{P}$ vale per F/K, allora vale anche per LF/F, ossia vale sul ramo parallelo a quello di F/K,
- validità per il **composto**: se $\mathcal{P}$ vale per L/K ed M/K, allora vale anche per LM/K.
- validità per l'**intersezione**: se $\mathcal{P}$ vale per L/K ed M/K, allora vale anche per $L \cap M/K$.

Si dice che $\mathcal{P}$ vale *debolmente* per torri, se $\mathcal{P}$ vale per L/K solo se vale per L/F sottoestensione. Si dice che $\mathcal{P}$ vale *strettamente* per torri, se è $\mathcal{P}$ vale per L/K se e solo se vale per L/F e F/K. Se $\mathcal{P}$ vale strettamente per torri, allora $\mathcal{P}$ vale anche per l'intersezione.

Si dice che $\mathcal{P}$ vale *inversamente* per *shift* se $\mathcal{P}$ vale su LF/F solo se vale su L/K. Si dice che $\mathcal{P}$ vale *inversamente* per il composto se $\mathcal{P}$ vale su LF/K implica che $\mathcal{P}$ valga anche su L/K e F/K. Si dice che $\mathcal{P}$ vale *completamente* per *shift* o composto se $\mathcal{P}$ vale *inversamente* e normalmente per *shift* o composto. Se $\mathcal{P}$ vale per torri e per *shift*, allora vale anche per il composto.

La seguente tabella raccoglie le proprietà delle estensioni sui diagrammi di campo:

$\mathcal{P}$	Torri	*Shift*	Composto	Intersez.
Est. fin.	Strett.	Normal.	Complet.	Sì
Est. alg.	Strett.	Complet.	Complet.	Sì
Est. sep.	Strett.	Normal.	Normal.	Sì
Est. nor.	Debolm.	Normal.	Normal.	Sì
Est. Gal.	Debolm.	Normal.	Normal.	Sì

Teorema dell'elemento primitivo

Se L/K è un'estensione finita e separabile, L è in particolare un'estensione semplice di K, per il **Teorema dell'elemento primitivo**. In campi finiti, un tale elemento primitivo è un generatore di L^*. In campi infiniti, per $L = K(a, b)$, si può invece considerare il seguente polinomio:

$$p(x) = \prod_{i<j} (\varphi_i(a) + x\varphi_i(b) - \varphi_j(b) - x\varphi_j(b)),$$

dove le varie φ_i sono le K-immersioni di L su $\overline{K}$. Si verifica che $p(x)$ è non nullo, e pertanto ha supporto non vuoto. Pertanto esiste un $t \in K$ tale per cui $p(t) \neq 0$, da cui si ricava che $L = K(a + bt)$. Reiterando questo algoritmo su tutti i generatori dell'estensione, si ottiene un elemento primitivo desiderato.

Teorema di corrispondenza di Galois

Se L/K è di Galois, detto $H \leq \mathrm{Gal}(L/K)$, si definisce L^H come la sottoestensione di L fissata da tutte le K-immersioni di H. In particolare vale che $L^H = K \iff H = \mathrm{Gal}(L/K)$. Conseguentemente, vale il **Teorema di corrispondenza di Galois**, di seguito descritto:

Teorema. Sia $\mathcal{E}$ l'insieme delle sottoestensioni di L/K estensione di Galois. Sia $\mathcal{G}$ l'insieme dei sottogruppi di $\mathrm{Gal}(L/K)$. Allora $\mathcal{E}$ è in bigezione con $\mathcal{G}$ attraverso la mappa $\alpha : \mathcal{E} \to \mathcal{G}$ tale per cui:

$$F \overset{\alpha}{\mapsto} \mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K),$$

la cui inversa $\beta : \mathcal{G} \to \mathcal{E}$ è tale per cui:

$$H \overset{\beta}{\mapsto} L^H \subseteq L.$$

Inoltre, una sottoestensione F/K di L/K è normale su K se e solo se il corrispondente sottogruppo di $\mathrm{Gal}(L/K)$ è normale. Infine, se F/K è normale, F è in particolare di Galois e vale che:

$$\mathrm{Gal}(F/K) \cong {}^{\mathrm{Gal}(L/K)}\!/_{\mathrm{Gal}(L/F)}.$$

Pertanto, a partire dal Teorema di corrispondenza di Galois, valgono le seguenti proprietà:

- il numero di sottogruppi di $\mathrm{Gal}(L/K)$ di un certo ordine n è uguale al numero di sottoestensioni di L tali per cui L abbia grado n su di esse (infatti $[L : F] = |\mathrm{Gal}(L/F)|$),
- il numero di sottogruppi di $\mathrm{Gal}(L/K)$ di un certo indice n è uguale al numero di sottoestensioni di L che hanno grado n su K (infatti $[F : K] = [L : K]/[L : F] = |\mathrm{Gal}(L/K)|/|\mathrm{Gal}(L : F)| = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)]$),
- $L^H \subset L^Q \iff Q < H$,
- $L^H L^Q = L^H(L^Q) = L^{H \cap Q}$,
- $L^{\langle H,Q \rangle} = L^H \cap L^Q$,

In particolare, un diagramma di campi – a patto che il suo estremo superiore sia di Galois – può essere collegato ad un diagramma di gruppi, "invertendo" le inclusioni. Se $G = \mathrm{Gal}(L/K)$ e $H \subseteq G$, allora il diagramma:

$$\begin{array}{c} L \\ \Big| H \\ L^H \\ \Big| G/H \\ K \end{array} \qquad G$$

si relaziona tramite corrispondenza al diagramma:

$$\begin{array}{c} \{e\} \\ \Big| \\ H \\ \Big| \\ G \end{array}$$

Gruppi di Galois noti

Campi finiti

Il campo finito $\mathbb{F}_{p^n}$ è sempre normale su $\mathbb{F}_p$, dal momento che può essere costruito come campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$ stesso. Equivalentemente, poiché un omomorfismo di campi è sempre iniettivo (e dunque conserva sempre la cardinalità), una $\mathbb{F}_p$-immersione deve mandare $\mathbb{F}_{p^n}$ in un campo della stessa cardinalità, e quindi necessariamente un campo isomorfo a $\mathbb{F}_{p^n}$.

Per un campo finito, $\mathcal{F}$ è un automorfismo che fissa $\mathbb{F}_p$. Allora $\mathcal{F} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Inoltre $\mathrm{ord}\,\mathcal{F} = n = |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p|$ (altrimenti $\mathbb{F}_{p^n}$ non sarebbe campo di spezzamento di $x^{p^n} - x$), e quindi vale che:

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathcal{F} \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Pertanto se $\alpha \in \mathbb{F}_{p^n} \setminus \mathbb{F}_p$, tutti i suoi coniugati si ottengono reiterando al più p^n volte $\mathcal{F}$ su α.

Polinomi biquadratici

Sia $p(x) = x^4 + ax^2 + b$ irriducibile su $\mathbb{Q}$. Allora, se L è un suo campo di spezzamento e $\Delta = a^2 - 4b$ è l'usuale discriminante di p visto come polinomio in x^2, vale che:

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{se } b \text{ è quadrato in } \mathbb{Q}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{se } b\Delta \text{ è quadrato in } \mathbb{Q}, \\ D_4 & \text{altrimenti.} \end{cases}$$

Radici di primi in $\mathbb{Q}$

Siano p_1, ..., p_n numeri primi distinti. Allora vale che:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

I polinomi ciclotomici $\Phi_n(x)$

Sia $\Phi_n(x)$ l'n-esimo polinomio ciclotomico, così definito:

$$\Phi_n(x) = \prod_{\substack{1 \leq d \leq n \\ \mathrm{MCD}(d,n)=1}} (x - \zeta_n^d),$$

dove ζ_n è una radice primitiva n-esima dell'unità.

Tale polinomio è sempre a coefficienti interi ed è inoltre primitivo su $\mathbb{Z}[x]$. Vale inoltre che:

$$x^n - 1 = \prod_{m|n} \Phi_m(x).$$

Il campo di spezzamento di $\Phi_n(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\zeta_n)$, che è un'estensione normale, separabile e finita, e pertanto di Galois.

Inoltre vale che:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

e dunque $\Phi_n(x)$ è sempre irriducibile su $\mathbb{Q}$.

Ad opera di Gabriel Antonio Videtta,
https://poisson.phc.dm.unipi.it/~videtta/.
Reperibile su https://notes.hearot.it, nella sezione *Secondo anno → Algebra 1 → 3. Teoria delle estensioni di campo e di Galois → Scheda riassuntiva di Teoria dei campi e di Galois.*