Università di Pisa
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

Tesi di Laurea

Il problema della classificazione delle estensioni locali: le estensioni di grado p^2 su $\mathbb{Q}_p$

Candidato
Luca Caputo

Relatore
Prof. Roberto Dvornicich

Controrelatore
Prof.ssa Ilaria Del Corso

Anno Accademico 2003/2004

Indice

Introduzione e ringraziamenti

Lo scopo di questa tesi è classificare le estensioni di grado p^2 di $\mathbb{Q}_p$ in base al numero dei loro coniugati, al gruppo di Galois della loro chiusura normale e alla valutazione del loro differente. L'intento è raggiunto solo in parte (per questioni di tempo, essenzialmente): proponiamo infatti una classificazione di tutte le estensioni di Galois di grado p^2 di $\mathbb{Q}_p$ e di alcune estensioni di grado p^2 di $\mathbb{Q}_p$ che hanno p coniugati. Per quanto riguarda queste ultime, trattiamo solo i casi in cui contengono una sottoestensione normale su $\mathbb{Q}_p$ di grado p. Più precisamente, data un'estensione $\mathbf{L}$ di grado p^2 di $\mathbb{Q}_p$ con chiusura normale $\mathbf{F}$ con gruppo di Galois $G(\mathbf{F}|\mathbb{Q}_p) = G$, studiamo i casi in cui la sottoestensione di $\mathbf{L}$ corrispondente al normalizzatore del sottogruppo di G relativo a $\mathbf{L}$ ha indice p (questo dipende unicamente dal fatto che $\mathbf{L}$ ha p coniugati) ed è normale in G.

L'idea di classificare le estensioni locali, cioè le estensioni di un dato campo completo rispetto ad un valore assoluto non archimedeo, prende le mosse dalla fondamentale considerazione che esse sono, fissato un grado, in numero finito. Questo risultato, dovuto a Krasner e risalente al 1962, è stato poi seguito da diversi lavori: primo fra tutti quello di Serre del 1978, nel quale è proposto un nuovo modo, più elegante, di contare le estensioni che si basa sull'introduzione di una misura sull'insieme dei polinomi che generano tali estensioni. Contemporaneamente partiva un altro tipo di tentativo, quello di classificare certe particolari estensioni, quelle più difficili, cioè quelle il cui grado è una potenza di p. In questi casi infatti, quelli in cui la ramificazione può essere *wild*, molti metodi falliscono e si hanno poche informazioni. D'altra parte si tratta anche del caso più interessante sotto molti punti di vista. Il risultato più notevole in questo senso è quello di Amano, del 1971: una classificazione completa e dettagliata delle estensioni di grado p di un campo p-adico (vale a dire un'estensione finita di $\mathbb{Q}_p$). Più recentemente si è poi tentato un approccio computazionale: sono stati messi appunto diversi algoritmi in grado di determinare quando due polinomi di uguale grado danno vita alla stessa estensione. Utilizzando questi metodi, Jones e Roberts, nel 2003, hanno pubblicato un database delle estensioni finite di $\mathbb{Q}_p$. In esso sono presenti le estensioni di grado n primo con p (anche per n molto grande), le estensioni di grado p di $\mathbb{Q}_p$ (fino a un certo valore di p) e, per $p = 2, 3$, le estensioni di grado p^2 di $\mathbb{Q}_p$. Come si vede dunque, il problema di classificare le estensioni di grado p^2 resta aperto.

Il tentativo di classificare le estensioni locali nasce dalla necessità di conoscere informazioni sui campi di numeri (cioè le estensioni finite di $\mathbb{Q}$). Infatti, completando un campo di numeri rispetto ad un opportuno valore assoluto, si ottiene un campo locale. I campi locali sono più semplici: l'anello degli interi è un anello di valutazione discreta (quindi in particolare è un dominio a ideali principali ed ha un unico ideale primo). Le estensioni di un campo locale $\mathbf{K}$ hanno poi il grande vantaggio di avere un anello degli

interi che può essere generato da un solo elemento come algebra sull'anello degli interi di $\mathbf{K}$. Inoltre il processo di completamento conserva alcune informazioni, ad esempio la valutazione della componente p-esima del differente, e l'utilizzo di diversi completamenti può dare informazioni generali sulla traccia e la norma del campo di numeri di partenza.

I metodi utilizzati in questa tesi sono molto semplici. Essenzialmente data un'estensione ne determiniamo il gruppo di Galois della chiusura normale; poi contiamo quante estensioni essa contenga dello stesso tipo di quella di partenza e, ricavando il numero delle estensioni con un dato gruppo di Galois dalla formula di Šafarevič, riusciamo a dedurre il numero di estensioni del tipo analizzato. A questo punto resta da determinare il differente: sfruttando la teoria della ramificazione molte informazioni sono immedatamente disponibili. Nei casi più complicati tuttavia è necessario passare ad analizzare il gruppo di Galois della chiusura normale del composto di due estensioni non coniugate. Questo metodo fornisce un oggetto unico, per l'appunto il gruppo di Galois, che racchiude informazioni su quasi tutte le estensioni. In un certo senso, questa è la giustificazione dell'approccio da noi scelto: cercare di capire, con l'ausilio della teoria dei gruppi, come si dispongono le estensioni, avere cioè, piuttosto che un lungo elenco di estensioni, un metodo algebrico per ricordarsi le loro caratteristiche. Il risultato forse più interessante è quello inerente alle estensioni di grado p^2 di $\mathbb{Q}_p$ la cui chiusura normale ha ordine p^4: c'è infatti, a questo livello, una differenza tra il caso $p = 3$ e il caso $p \neq 3$ che deriva (o si può pensare che derivi) dalla diversa struttura del gruppo di Galois nei due casi.

Nello spirito che ci ha mosso in questo tentativo di classificazione, e cioè, come dicevo prima, ottenere oggetti algebrici che descrivano le estensioni, forniamo, nell'ultimo capitolo, una classificazione delle estensioni cicliche di grado p^n di $\mathbb{Q}_p$ (si tratta di un risultato già noto o comunque facilmente deducibile). Lo strumento utilizzato è la teoria dei corpi di classe: il risultato principale è che il gruppo di Galois del composto di tutte le estensioni cicliche di grado p^n è isomorfo a $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. Questo è esattamente il tipo di oggetti algebrici che cercavamo. Sempre nell'ultimo capitolo c'è un piccolo risultato originale: sfuttando la teoria dei p-gruppi si riesce a concludere che un'estensione totalmente ramificata di Galois deve necessariamente essere ciclica.

Mi preme ringraziare in primo luogo il professor Roberto Dvornicich: da lui ho imparato molte delle idee e delle tecniche che spesso permettono di risolvere questo tipo di problemi. La mia curiosità è stata stimolata dalla sua e, acquisita grazie a lui una certa agilità nei calcoli, mi sono divertito a scoprire, passo dopo passo, la disposizione e la forma degli oggetti che abbiamo studiato.
Voglio ringraziare poi la mia famiglia: papà, mamma, Matteo, Davide e Sara. Forse per loro la ramificazione è un termine botanico e, se poi è selvaggia, sarà per via di una mancata potaura, ma non mi è mai mancato il loro appoggio e gran parte della mia tranquillità la devo a loro.
E che dire allora dei compagni di questi anni di università? Abramo, Angelo, Carlo, David e Jessika, Fulvia, Gianandrea, Michele, Piotr, Riccardo e Valentina: un supporto che non è quantificabile. Per quanto tempo mi avranno ascoltato pronunciare oscure frasi piene di strani aggettivi, quante volte mi avranno fatto compagnia dopo una lunga giornata di studio e sopportato nelle mie ore di stanchezza? In ultimo, ringrazio Giulio e Maurizio e, ancora, Gianandrea, Michele e Valentina per gli utili suggerimenti tecnici.

Capitolo 1

Gli strumenti: definizioni, notazioni, risultati

1.1 Valutazioni e valori assoluti

La teoria delle valutazioni e dei valori assoluti su campi è piuttosto ampia: tuttavia il caso che interessa questa trattazione è piuttosto semplice e intuitivo.

Definizione 1.1.1 *Sia* $(\Gamma, +)$ *un gruppo abeliano. Un* ordine *su* Γ *è un sottosemigruppo* S *di* Γ *tale che*

$$\Gamma = S \cup \{0\} \cup S^{-1}$$

Un ordine S *su* Γ *definisce una* relazione d'ordine $<_S$ *nel modo seguente:*

$$a <_S b \quad \textit{se e solo se} \quad a - b \in S \quad \textit{per ogni } a, b \in \Gamma$$

Con la notazione $(\Gamma, +, <)$ *intenderemo quindi un gruppo abeliano* $(\Gamma, +)$ *su cui è dato un ordine che definisce* $<$*.*

Definizione 1.1.2 *Siano* $(\Gamma, +, <)$ *un gruppo abeliano ordinato e* $\Lambda \subset \Gamma$ *un suo sottogruppo.* Λ *si dice* convesso *se ha la seguente proprietà:*

$$b \in \Lambda,\ a \in \Gamma,\ -b < a < b \ \Rightarrow a \in \Gamma$$

Definizione 1.1.3 *Siano* $\mathbf{K}$ *un campo e* $(\Gamma, +, <)$ *un gruppo abeliano ordinato. Una* valutazione *su* $\mathbf{K}$ *è una funzione*

$$v : \mathbf{K} \to \Gamma \cup \{\infty\}$$

tale che

1. $v(x) = \infty \ \Rightarrow\ x = 0$*;*
2. $v(xy) = v(x) + v(y)$*;*
3. $v(x + y) \geq \min\{v(x),\, v(y)\}$

Esempio Siano $\mathbf{K}$ un campo e $\Gamma = \{0\}$ il gruppo con un unico elemento. L'unica valutazione v possibile su $\mathbf{K}$ a valori in Γ (cioè $v(x) = 0$ per ogni $x \in \mathbf{K}^*$ e $v(0) = \infty$) è detta banale. Non si terrà mai conto di questa valutazione, nel senso che d'ora in poi per valutazione intenderemo valutazione non banale.

Esempio Sia $\mathbf{K} = \mathbb{Q}$ il campo dei numeri razionali e $\Gamma = \mathbb{Z}$ il gruppo degli interi ordinato rispetto all'ordine usuale di $\mathbb{R}$. Sia p un numero primo e siano $a = p^{k_a}a_1$ e $b = p^{k_b}b_1$ (con $(p,\, a_1) = (p,\, b_1) = 1$) due numeri interi diversi da zero. Allora poniamo

$$v_p\left(\frac{a}{b}\right) = k_a - k_b \qquad \text{e} \qquad v_p(0) = \infty$$

La funzione su $\mathbb{Q}$ così definita è una valutazione a valori in $\mathbb{Z} \cup \{\infty\}$, detta valutazione p-adica.

Definizione 1.1.4 *Siano* $\mathbf{K}$ *un campo e* $(\Gamma, +, <)$ *un gruppo abeliano ordinato. Il* rango *di* Γ *è la cardinalità dell'insieme dei sottogruppi convessi di* Γ *diversi da* Γ. *Se inoltre* v *è una valutazione su* $\mathbf{K}$ *a valori in* $\Gamma \cup \{\infty\}$, *allora il* rango *di* v *è il rango di* Γ.

Esempio La valutazione introdotta nell'esempio precedente ha rango 1.

Definizione 1.1.5 *Sia* $\mathbf{K}$ *un campo. Un* valore assoluto *su* $\mathbf{K}$ *è una funzione*

$$|\ |\, : \mathbf{K} \to \mathbb{R}$$

tale che per ogni $x,\, y \in \mathbf{K}$

1. *se* $x \in \mathbf{K}^*$ *allora* $|x| > 0$ *e* $|0| = 0$;
2. $|xy| = |x||y|$;
3. $|x + y| \leq |x| + |y|$

Un valore assoluto è detto non archimedeo *se per ogni* $x,\, y \in \mathbf{K}$ *si ha*

4. $|x + y| \leq \max\{|x|,\, |y|\}$

Se invece esistono $x,\, y \in \mathbf{K}$ *tali che* $|x + y| > \max\{|x|,\, |y|\}$ *il valore assoluto è detto* archimedeo.

Definizione 1.1.6 *Sia* $\mathbf{K}$ *un campo. Due valori assoluti,* $|\ |_1$ *e* $|\ |_2$, *su di esso si dicono* equivalenti *se esiste* $c \in \mathbb{R}$, $c > 0$ *tale che* $|\ |_1^c = |\ |_2$.

Esempio Analogamente al caso delle valutazioni, anche per i valori assoluti c'è un caso banale. D'ora in avanti, non terremo conto di questo caso e i valori assoluti considerati saranno tacitamente assunti non banali.

Esempio Sia $\mathbf{K} = \mathbb{Q}$ il campo dei numeri razionali e sia p un numero primo. Siano $a = p^{k_a}a_1$ e $b = p^{k_b}b_1$ (con $(p,\, a_1) = (p,\, b_1) = 1$) due numeri interi diversi da zero. Allora poniamo

$$\left|\frac{a}{b}\right|_p = p^{k_b - k_a} \qquad \text{e} \qquad |0|_p = 0$$

La funzione su $\mathbb{Q}$ così definita è una valore assoluto non archimedeo, detto valore assoluto p-adico.

Esempio Il valore assoluto usuale indotto da $\mathbb{R}$ su $\mathbb{Q}$, che indicheremo con $|\ |_\infty$, è un valore assoluto archimedeo.

Tra i valori assoluti non archimedei e le valutazioni di rango 1 non c'è differenza, come illustrano le seguenti proposizioni. È di questi valori assoluti che ci interesseremo nel seguito.

Proposizione 1.1.1 *Siano* $\mathbf{K}$ *un campo e* $|\ |$ *un valore assoluto non archimedeo su di esso. Allora l'immagine* Γ *di* $|\ |$ *è un sottogruppo di* $(\mathbb{R}^*, \cdot)$*. Inoltre la funzione* $v_{|\ |} : \mathbf{K} \to \mathbb{R} \cup \{\infty\}$ *(*$\mathbb{R}$ *è considerato con la relazione d'ordine* $<_{\mathbb{R}}$ *che è quella usuale), definita da* $v_{|\ |}(x) = -\log_e(|x|)$ *se* $x \neq 0$ *e* $v_{|\ |}(0) = \infty$*, è una valutazione di rango* 1 *su* $\mathbf{K}$*.*[1]

Dimostrazione (vedi [Ba]). □

Proposizione 1.1.2 *Sia* $(\Gamma, +, <)$ *un gruppo abeliano ordinato di rango* 1*. Allora c'è un isomorfismo che conserva gli ordini tra* Γ *e un sottogruppo di* $(\mathbb{R}, +, <_{\mathbb{R}})$*.*

Dimostrazione (vedi [Ba]). □

Proposizione 1.1.3 *Siano* $\mathbf{K}$ *un campo,* $(\Gamma, +, <)$ *un gruppo abeliano ordinato di rango* 1 *(che pensiamo come un sottogruppo di* $(\mathbb{R}, +, <_{\mathbb{R}})$*) e* $v : \mathbf{K} \to \Gamma \cup \{\infty\}$ *una valutazione su* $\mathbf{K}$*. Allora la funzione* $|\ |_v : \mathbf{K} \to \mathbb{R}$ *definita da* $|x|_v = e^{-v(x)}$ *se* $x \neq 0$ *e* $|0|_v = 0$ *è un valore assoluto non archimedeo su* $\mathbf{K}$*.*

Dimostrazione (vedi [Ba]). □

Osservazione 1.1.1 *Siano* $\mathbf{K}$ *un campo,* $(\Gamma, +, <)$ *un gruppo abeliano ordinato di rango* 1 *(che al solito pensiamo come un sottogruppo di* $(\mathbb{R}, +, <_{\mathbb{R}})$*),* $v : \mathbf{K} \to \Gamma \cup \{\infty\}$ *una valutazione su* $\mathbf{K}$ *e* $|\ |$ *un valore assoluto non archimedeo su* $\mathbf{K}$*. Con riferimento alle notazioni introdotte nelle precedenti proposizioni, si ha*

$$v_{|\ |_v} = v \qquad e \qquad |\ |_{v_{|\ |}} = |\ |$$

Dimostrazione (vedi [Ba]). □

D'ora in poi si dirà anche che $|\ |$ è *indotto* da v o che è *associato* a v e viceversa. I concetti e le nuove definizioni saranno spesso date in un solo caso ed estese in maniera ovvia all'altro.

Osservazione 1.1.2 *Il valore assoluto p-adico è equivalente a quello associato alla valutazione p-adica.*

[1] e denota il numero di Nepero.

Dimostrazione (vedi [Ba]). □

Nel seguito faremo largo uso della seguente proprietà delle valutazioni.

Osservazione 1.1.3 *Sia* **K** *un campo su cui è definita una valutazione. Siano* x_1, x_2, ..., x_n *elementi di* **K**. *Supponiamo che* $v(x_1) < v(x_i)$ *per ogni* $i = 2, \ldots, n$. *Allora* $v(x_1 + x_2 + \ldots + x_n) = v(x_1)$.

Dimostrazione (vedi [Ba]). □

Definizione 1.1.7 *Siano* **K** *un campo e* $(\Gamma, +, <)$ *un gruppo abeliano ordinato. Una valutazione* v *su* **K** *a valori in* Γ *si dice* discreta *se* $v(\Gamma)$ *è ciclico infinito.*

Si vede facilmente che, se v è una valutazione discreta a valori in Γ gruppo abeliano ordinato, allora, se pensiamo $v(\Gamma) = \mathbf{Z}$, l'ordine su $v(\Gamma)$ deve essere quello indotto dall'ordine usuale di $\mathbb{R}$. In particolare questo implica che v ha rango 1. Nel seguito porremo sempre $v(\Gamma) = \mathbf{Z}$, se v è discreta.

Esempio v_p è una valutazione discreta.

Il seguente risultato illustra come i valori assoluti p-adici siano gli unici valori assoluti non archimedei su $\mathbb{Q}$.

Teorema 1.1.1 (Ostrowski) *Sia* $|\ |$ *un valore assoluto su* $\mathbb{Q}$*: se è archimedeo allora è equivalente a* $|\ |_\infty$*; se è non archimedeo, allora esiste p primo tale che* $|\ |$ *è equivalente a* $|\ |_p$.

Dimostrazione (vedi [CF]). □

Una valutazione **K** può essere definita anche in modo diverso, a partire da un particolare sottoanello di **K**.

Definizione 1.1.8 *Sia* $\mathcal{O}$ *un dominio di integrità e* **K** *il suo campo quoziente.* $\mathcal{O}$ *è un* anello di valutazione *di* **K** *se per ogni* $x \in \mathbf{K}^*$*, si ha* $x \in \mathcal{O}$ *oppure* $x^{-1} \in \mathcal{O}$.

Osservazione 1.1.4 *Sia* $\mathcal{O}$ *un anello di valutazione di* **K** *campo. Allora*

1. $\mathcal{O}$ *è un anello locale;*
2. *se* $\mathcal{O}'$ *è un sottoanello di* **K** *che contiene* $\mathcal{O}$*, allora* $\mathcal{O}'$ *è un anello di valutazione di* **K***;*
3. $\mathcal{O}$ *è integralmente chiuso.*

Dimostrazione (vedi [AMc]). □

Proposizione 1.1.4 *Sia $\mathcal{O}$ un anello di valutazione di un campo $\mathbf{K}$. Sia $\Gamma = \mathbf{K}^*/\mathcal{O}^*$ con l'ordine $<$ dato da*

$$[x] < [y] \quad \Leftrightarrow \quad xy^{-1} \in \mathcal{O} \qquad ([x],\, [y] \in \Gamma)$$

Sia $v_{\mathcal{O}} : \mathbf{K} \to \Gamma \cup \{\infty\}$ l'omomorfismo di proiezione esteso con $v_{\mathcal{O}}(0) = \infty$. Allora $v_{\mathcal{O}}$ è una valutazione su $\mathbf{K}$ a valori in Γ.

Dimostrazione (vedi [AMc]). □

Proposizione 1.1.5 *Siano $\mathbf{K}$ un campo, $(\Gamma, +, <)$ un gruppo abeliano ordinato e v una valutazione su $\mathbf{K}$ a valori in Γ. Allora*

$$\mathcal{O}_v = \{x \in \mathbf{K}^* \,|\, v(x) \geq 0\}$$

è un anello di valutazione di $\mathbf{K}$.

Dimostrazione (vedi [AMc]). □

Osservazione 1.1.5 *Con riferimento alle notazioni introdotte nelle proposizioni precedenti si ha*

$$\mathcal{O}_{v_{\mathcal{O}}} = \mathcal{O} \qquad e \qquad v_{\mathcal{O}_v} = v$$

Dimostrazione (vedi [AMc]). □

Esempio $\mathcal{O}_{v_p} = \mathbb{Z}_{(p)}$, il localizzato di $\mathbb{Z}$ alla parte moltiplicativa $S = \mathbb{Z} \setminus (p)$.

Le valutazioni discrete hanno il vantaggio di avere degli anelli di valutazione associati con una struttura più semplice.

Definizione 1.1.9 *Sia $\mathcal{O}$ un anello. $\mathcal{O}$ è un* anello di valutazione discreta *di $\mathbf{K}$ se è un dominio a ideali principali con un unico ideale primo diverso da* (0)*. Un generatore π dell'ideale primo di $\mathcal{O}$ è detto elemento* uniformizzante*.*

Si può dimostrare (vedi [Se]) che gli unici ideali di un anello di valutazione discreta sono le potenze del suo ideale primo.

Osservazione 1.1.6 *Siano $\mathbf{K}$ un campo, $(\Gamma, +, <)$ un gruppo abeliano ordinato e v una valutazione su $\mathbf{K}$ a valori in Γ. v è discreta se e solo se $\mathcal{O}_v$ è un anello di valutazione discreta e in questo caso, se π è un uniformizzante di $\mathcal{O}_v$, $v(\pi)$ genera $v(\Gamma)$ (per le nostre convenzioni quindi, $v(\pi) = 1$). Inoltre, dato un anello di valutazione discreta $\mathcal{O}$, esso è un anello di valutazione e $v_{\mathcal{O}}$ è una valutazione discreta.*

Dimostrazione (vedi [AMc]). □

Esempio Un elemento uniformizzante per $\mathbb{Z}_{(p)}$ è p.

Definizione 1.1.10 *Siano v una valutazione discreta su un campo $\mathbf{K}$ e $\mathcal{O}$ l'anello associato a v con uniformizzante π. Il campo $\mathcal{O}/(\pi)$ è detto* campo residuo*.*

Esempio Nel caso di v_p, il campo residuo è $\mathbb{Z}/p\mathbb{Z}$.

1.2 Topologia: distanze e completamenti

Un valore $|\ |$ assoluto su un campo $\mathbf{K}$ induce una distanza d nel modo seguente:

$$d(x,y) = |x-y| \qquad \forall x,\, y \in \mathbf{K}$$

Proposizione 1.2.1 *Due valori assoluti su un campo* $\mathbf{K}$ *sono equivalenti se e solo se inducono la stessa topologia su* $\mathbf{K}$*.*

Dimostrazione (vedi [Ca]). □

In virtù della proposizone precedente, non faremo distinzione tra valori assoluti (o valutazioni) equivalenti.

Con la topologia indotta da d, $\mathbf{K}$ diviene uno spazio metrico: in particolare, poiché le operazioni sono continue in questa topologia, $\mathbf{K}$ diviene un campo topologico. Indichiamo con $\widehat{\mathbf{K}}$ il suo completamento[2].

Proposizione 1.2.2 *Il completamento di* $\widehat{\mathbf{K}}$ *di* $\mathbf{K}$ *è un campo ed esiste un unico valore assoluto* $\widehat{|\ |}$ *su* $\widehat{\mathbf{K}}$ *che estende* $|\ |$*. Inoltre, se* $|\ |$ *è non archimedeo (risp. archimedeo), anche* $\widehat{|\ |}$ *è non archimedeo (risp. archimedeo). Infine se la valutazione* v *associata a* $|\ |$ *è discreta, anche la valutazione* $\widehat{v}$ *associata a* $\widehat{|\ |}$ *è discreta.*

Dimostrazione (vedi [Ba]). □

Rispetto alla topologia indotta da $\widehat{|\ |}$, $\mathbf{K}$ è denso in $\widehat{\mathbf{K}}$.

Esempio Nel caso v_p, il completamento di $\mathbb{Q}$ si indica con $\mathbb{Q}_p$: tale campo è detto campo dei razionali p-adici.

Osservazione 1.2.1 *Siano* $\mathbf{K}$ *un campo,* v *una valutazione discreta su di esso e* π *un elemento uniformizzante per* $\mathcal{O}_v = \mathcal{O}$*.* $\mathcal{O}_{\widehat{v}} = \widehat{\mathcal{O}}$ *è la chiusura di* $\mathcal{O}$ *in* $\widehat{\mathbf{K}}$*. Inoltre la topologia indotta da* v *su* $\mathcal{O}$ *ha per base di intorni di zero la famiglia* $\{(\pi^n\}_{n\in\mathbb{N}}$ *(cioè è la topologia naturale di* $\mathcal{O}$ *come anello locale). Infine,* π *è un uniformizzante anche per* $\widehat{\mathcal{O}}$ *e*

$$\widehat{\mathcal{O}} = \varprojlim \mathcal{O}/\pi^n\mathcal{O} \quad \textit{(limite proiettivo)} \qquad \widehat{\mathcal{O}}/\pi^n\widehat{\mathcal{O}} = \mathcal{O}/\pi^n\mathcal{O} \quad (n \in \mathbb{N})$$

Dimostrazione (vedi [Se]). □

Esempio Nel caso v_p, l'anello di valutazione di $\mathbb{Q}_p$ si indica con $\mathbb{Z}_p$ (l'anello degli interi p-adici) che spesso è definito come

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

Osservazione 1.2.2 *Sia* $\mathcal{O}$ *un anello di valutazione su un campo* $\mathbf{K}$*.* $\mathbf{K}$ *è localmente compatto rispetto alla topologia indotta dalla valutazione se e solo se è completo e il suo campo residuo è finito. In questo caso* $\mathcal{O}$ *e* $\mathcal{O}^*$ *sono compatti con la topologia indotta.*

[2] Per la definizione di completamento vedi [La1].

Dimostrazione (vedi [Se], [La]). □

Esempio La proposizione si applica al caso v_p, quindi $\mathbb{Q}_p$ è localmente compatto, $\mathbb{Z}_p$ e $\mathbb{Z}_p^*$ sono compatti.

Osservazione 1.2.3 *Sia* $\mathbf{K}$ *un campo completo rispetto ad una valutazione discreta con anello di valutazione* $\mathcal{O}$ *e sia* π *un uniformizzante. Sia* $R \subset \mathcal{O}$ *un insieme di rappresentanti per* $\mathcal{O}/(\pi)$ *che contiene* 0*. Allora ogni* $a \in \mathbf{K}$ *si può scrivere in maniera unica come serie di Laurent convergente nelle potenze di* π *a coefficienti in* R*, cioè*

$$a = \sum_{n=-n_0}^{\infty} a_n \pi^n \qquad (a_n \in R)$$

per un certo $n_0 \in \mathbb{N}$*. Viceversa una tale serie converge sempre ad un elemento di* $\mathbf{K}$*. Inoltre un elemento appartiene a* $\mathcal{O}$ *se e solo se il suo sviluppo in serie non ha termini con potenze negative di* π *(cioè* $n_0 = 0$*).*

Dimostrazione (vedi [Se]). □

Esempio Nel caso v_p, possiamo scegliere $R = \{0, 1, \ldots, p-1\}$. Tuttavia, come si vedrà più avanti, altre scelte potrebbero essere più convenienti, anche se meno familiari.

1.3 Il lemma di Hensel e il lemma di Krasner

A partire da ora, le valutazioni considerate saranno tutte discrete.

Dato un campo $\mathbf{K}$ con una valutazione, abbiamo costruito un nuovo campo $\widehat{\mathbf{K}}$ completo rispetto ad una valutazione che estende quella data. Di quest'ultimo campo, per ora, conosciamo la definizione e una descrizione dei suoi elementi come certe serie di potenze. Siamo interessati allo studio delle sue estensioni algebriche finite, quindi è estremamente utile conoscere dei criteri per l'esistenza in $\widehat{\mathbf{K}}$ di radici di polinomi in $\widehat{\mathbf{K}}[X]$. A questa esigenza risponde in maniera abbastanza esaustiva il lemma di Hensel.

Proposizione 1.3.1 (Lemma di Hensel) *Sia* $\mathbf{K}$ *un campo completo rispetto ad una valutazione* v *e sia* $\mathcal{O}$ *l'anello di valutazione associato. Sia* $f(X)$ *un polinomio a coefficienti in* $\mathcal{O}[X]$*. Sia* α_0 *un elemento di* $\mathcal{O}$ *tale che*

$$v(f(\alpha_0) > v(f'(\alpha_0)$$

(dove f' *denota la derivata formale di* f*). Allora la sequenza*

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

converge ad una radice α *di* $f(X)$ *in* $\mathcal{O}$*. Inoltre*

$$v(\alpha - \alpha_0) \geq v(\frac{f(\alpha_0)}{f'(\alpha_0)^2}) > 1$$

Dimostrazione (vedi [La]). □

Esempio Il lemma di Hensel è spesso applicato al caso in cui, detto π un uniformizzante, $f(\alpha_0) \equiv 0\ (mod\,(\pi))$ ma $f'(\alpha_0) \notin (\pi)$. Con questo tipo di applicazione si scopre, per esempio, che $\mathbb{Q}_p$ contiene le radici $(p-1)$-esime dell'unità (considerando il polinomio $X^{p-1}-1$).

Proposizione 1.3.2 (Lemma di Krasner) *Sia* $\mathbf{K}$ *un campo completo rispetto ad una valutazione* v *e siano* α, β *due elementi della chiusura algebrica di* $\mathbf{K}$ *tali che* α *sia separabile su* $\mathbf{K}(\beta)$. *Supponiamo che per tutti gli automorfismo* $\sigma \neq \mathrm{id}$ *di* $\mathbf{K}(\alpha)$ *si abbia*

$$v(\beta-\alpha) > v(\sigma\alpha-\alpha)$$

Allora $\mathbf{K}(\alpha) \subseteq \mathbf{K}(\beta)$.

Dimostrazione (vedi [La]). □

Il lemma di Krasner è l'ingrediente fondamentale nella dimostrazione che le estensioni di grado n di un campo p-adico (cioè un'estensione finita di $\mathbb{Q}_p$) sono in numero finito: se i generatori di due estensioni sono sufficientemente vicini, le estensioni coincidono.

1.4 Estensioni di campi completi: ramificazione e inerzia

Un'estensione finita di un campo completo, in particolare, è uno spazio vettoriale di dimensione finita su un campo completo: non sorprende allora il seguente risultato.

Proposizione 1.4.1 *Sia* $\mathbf{K}$ *un campo completo rispetto ad una valutazione* $v_{\mathbf{K}}$ *e sia* $\mathbf{E}$ *un'estensione di* $\mathbf{K}$ *di grado* n. *Allora esiste un'unica valutazione* $v_{\mathbf{E}}$ *su* $\mathbf{E}$ *che estende* $v_{\mathbf{K}}$ *(si scrive anche* $v_{\mathbf{E}}|v_{\mathbf{K}}$*) che risulta essere, per un certo numero naturale* $m \in \mathbb{N}$,

$$v_{\mathbf{E}} = \frac{m}{n}\left(v_{\mathbf{K}} \circ N_{\mathbf{K}}^{\mathbf{E}}\right)$$

In particolare se $\sigma : \mathbf{E} \to \sigma\mathbf{E} = \mathbf{E}$ *è un isomorfismo su* $\mathbf{K}$, *allora* $v_{\mathbf{E}}(\sigma(\alpha)) = v_{\mathbf{E}}(\alpha)$ *per ogni* $\alpha \in \mathbf{E}$. *Inoltre, con la topologia indotta da* $v_{\mathbf{E}}$, $\mathbf{E}$ *è completo.*

Dimostrazione (vedi [La]). □

La topologia indotta da $v_{\mathbf{E}}$ su $\mathbf{E}$ è ovviamente indotta da altre valutazioni (quelle eqivalenti a $v_{\mathbf{E}}$): $v_{\mathbf{E}}$ è l'unica tra queste che estenda $v_{\mathbf{K}}$. Vedremo che il fattore m nella sua definizione (che dipende strettamente dal fatto che $v_{\mathbf{E}}|v_{\mathbf{K}}$) ha un significato ben preciso.

Nel seguito considereremo solo campi completi $\mathbf{K}$ rispetto ad una valutazione $v_{\mathbf{K}}$ e loro estensioni $\mathbf{E}$, considerate con la topologia indotta dall'unica estensione $v_{\mathbf{E}}$ di $v_{\mathbf{K}}$: in questo caso diremo semplicemente $\mathbf{E}$ un'estensione finita di $\mathbf{K}$. $\mathcal{O}_{\mathbf{K}}$ e $\mathcal{O}_{\mathbf{E}}$ saranno gli anelli di valutazione corrispondenti, con ideali primi, rispettivamente, $\mathfrak{p}_{\mathbf{K}}$ e $\mathfrak{p}_{\mathbf{E}}$.

Proposizione 1.4.2 *Sia* $\mathbf{E}$ *un'estensione di grado* n *di un campo completo* $\mathbf{K}$. *Allora valgono le seguenti affermazioni:*

1. *$\mathcal{O}_{\mathbf{E}}$ è la chiusura integrale di $\mathcal{O}_{\mathbf{K}}$ in $\mathbf{E}$;*

2. *$\mathcal{O}_{\mathbf{E}}$ è un $\mathcal{O}_{\mathbf{K}}$-modulo libero di rango n;*

3. *esiste un certo numero naturale $e \in \mathbb{N}$ tale che $\mathfrak{p}_{\mathbf{K}}\mathcal{O}_{\mathbf{E}} = (\mathfrak{p}_{\mathbf{E}})^e$*

4. *c'è un'inclusione di campi (residui) $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}_{\mathbf{K}} \hookrightarrow \mathcal{O}_{\mathbf{E}}/\mathfrak{p}_{\mathbf{E}}$ e il grado di $\mathcal{O}_{\mathbf{E}}/\mathfrak{p}_{\mathbf{E}}$ su $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}_{\mathbf{K}}$ è finito.*

Dimostrazione (vedi [Se]). □

Nel seguito ci riferiremo spesso a $\mathcal{O}_{\mathbf{E}}$ come all'anello degli interi di $\mathbf{E}$ su $\mathcal{O}_{\mathbf{K}}$.

Definizione 1.4.1 *L'*indice di ramificazione $e(\mathbf{E}|\mathbf{K})$ *di* $\mathbf{E}$ *su* $\mathbf{K}$ *è* [3]

$$e(\mathbf{E}|\mathbf{K}) = v_{\mathbf{E}}(\mathfrak{p}_{\mathbf{K}}\mathcal{O}_{\mathbf{E}})$$

*L'*indice di inerzia $f(\mathbf{E}|\mathbf{K})$ *di* $\mathbf{E}$ *su* $\mathbf{K}$ *è*

$$f(\mathbf{E}|\mathbf{K}) = [\mathcal{O}_{\mathbf{E}}/\mathfrak{p}_{\mathbf{E}} : \mathcal{O}_{\mathbf{K}}/\mathfrak{p}_{\mathbf{K}}]$$

Se il contesto non dà adito ad ambiguità, indicheremo semplicemente con e e f rispettivamente l'indice di ramificazione e l'indice di inerzia.

Esempio Se $\mathbf{E}$ è un'estensione finita di $\mathbb{Q}_p$ con indice di inerzia f allora il campo residuo di $\mathbf{E}$ è isomorfo a $\mathbb{F}_{p^f}$.

Proposizione 1.4.3 *Sia $\mathbf{E}$ un'estensione di grado n di un campo completo $\mathbf{K}$. Allora ef=n.*

Dimostrazione (vedi [Se]). □

Definizione 1.4.2 *Diremo che $\mathbf{E}$ è* totalmente ramificata *su $\mathbf{K}$ se $e(\mathbf{E}|\mathbf{K}) = n$, mentre sarà* non ramificata *se $f(\mathbf{E}|\mathbf{K}) = n$.*

Osservazione 1.4.1 *Se $v_{\mathbf{E}}$ è l'unica estensione di $v_{\mathbf{K}}$, allora*

$$v_{\mathbf{E}} = \frac{e}{n}\left(v_{\mathbf{K}} \circ N_{\mathbf{K}}^{\mathbf{E}}\right)$$

Dimostrazione (vedi [Se]). □

In particolare, se $x \in \mathbf{K}$, $v_{\mathbf{E}}(x) = ev_{\mathbf{K}}(x)$.

[3] Conveniamo di porre $v_{\mathbf{E}}(\mathfrak{p}_{\mathbf{E}}^n) = n$.

1.5 I campi p-adici e la struttura delle loro estensioni

Veniamo ora a studiare più da vicino le estensioni di $\mathbb{Q}_p$. Molto di quello che si dirà a partire da ora, tuttavia, vale più in generale per le estensioni di campi completi rispetto ad una valutazione discreta.

Definizione 1.5.1 *Un* campo p-adico *è un'estensione algebrica finita di $\mathbb{Q}_p$. Un'estensione di un campo p-adico è detta un'estensione* locale.

D'ora in poi $\mathbf{K}$ sarà un campo p-adico con anello degli interi $\mathcal{O}_\mathbf{K}$ e ideale primo $\mathfrak{p}_\mathbf{K}$. L'immagine di un elemento x tramite la proiezione canonica dall'anello degli interi al campo residuo si indicherà con $\overline{x}$.

Proposizione 1.5.1 *Sia $\mathbf{E}$ un'estensione finita non ramificata di $\mathbf{K}$. Se $\alpha \in \mathcal{O}_\mathbf{E}$ è tale che $\mathcal{O}_\mathbf{E}/\mathfrak{p}_\mathbf{E} = \mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}(\overline{\alpha})$, allora $\mathbf{E} = \mathbf{K}(\alpha)$ e il polinomio minimo di α su $\mathbf{K}$ è irriducibile in $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}[X]$ (e quindi è il polinomio minimo di $\overline{\alpha}$ su $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}$).*

Dimostrazione (vedi [La]). □

Proposizione 1.5.2 *Sia $\mathbf{E} = \mathbf{K}(\alpha)$ un'estensione finita di $\mathbf{K}$ ($\alpha \in \overline{\mathbf{K}}$). Supponiamo che α appartenga a $\mathcal{O}_\mathbf{E}$ e che il suo polinomio minimo su $\mathbf{K}$ non abbia radici multiple considerato come polinomio a coefficienti in $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}$. Allora $\mathbf{E}$ è non ramificata e $\mathcal{O}_\mathbf{E}/\mathfrak{p}_\mathbf{E} = \mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}(\overline{\alpha})$.*

Dimostrazione (vedi [La]). □

Proposizione 1.5.3 *Siano $\mathbf{E}$ e $\mathbf{F}$ due estensioni finite di $\mathbf{K}$.*

1. *Se $\mathbf{E} \supset \mathbf{F} \supset \mathbf{K}$, allora $\mathbf{E}$ è non ramificata su $\mathbf{K}$ se e solo se $\mathbf{E}$ è non ramificata su $\mathbf{F}$ e $\mathbf{F}$ è non ramificata su $\mathbf{K}$;*
2. *se $\mathbf{E}$ è non ramificata su $\mathbf{K}$, allora $\mathbf{EF}$ è non ramificata su $\mathbf{F}$;*
3. *se $\mathbf{E}$ e $\mathbf{F}$ sono non ramificate su $\mathbf{K}$, allora $\mathbf{EF}$ è non ramificata su $\mathbf{K}$.*

Dimostrazione (vedi [La]). □

Teorema 1.5.1 *La seguente corrispondenza tra le estensioni finite non ramificate di $\mathbf{K}$ e le estensioni del campo residuo $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}$*

$$\mathbf{E} \quad \longmapsto \quad \mathcal{O}_\mathbf{E}/\mathfrak{p}_\mathbf{E}$$

è biunivoca e conserva i gradi.

Dimostrazione (vedi [La]). □

Osserviamo in particolare che c'è, quindi, un'unica estensione non ramificata su $\mathbf{K}$ di grado n. Se $\mathbf{K} = \mathbb{Q}_p$, non è difficile rendersi conto che si tratta del campo di spezzamento del polinomio $X^{p^n} - X$ (che è quello che genera $\mathbb{F}_{p^n}$ su $\mathbb{F}_p$). Le estensioni non ramificate sono dunque molto semplici da studiare: un corollario dei precedenti risultati è la seguente osservazione.

Osservazione 1.5.1 *Sia* $\mathbf{E}$ *un'estensione finita non ramificata su* $\mathbf{K}$*. Ogni elemento di* $\mathcal{O}_{\mathbf{K}}^*$ *è la norma di un elemento di* $\mathcal{O}_{\mathbf{E}}^*$*.*

Dimostrazione (vedi [La]). □

Veniamo ora alle estensioni che hanno un indice di ramificazione diverso da 1.

Definizione 1.5.2 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$*.* $\mathbf{E}$ *è* debolmente ramificata [4] *su* $\mathbf{K}$ *se*

$$(e(\mathbf{E}|\mathbf{K}), p) = 1$$

Se questo non accade, $\mathbf{E}$ *si dice* fortemente ramificata [5]*.* $\mathbf{E}$ *si dice invece* selvaggiamente ramificata[6] *su* $\mathbf{K}$ *se*

$$e(\mathbf{E}|\mathbf{K}) = p^k$$

per un certo $k \in \mathbb{N}$*.*

Proposizione 1.5.4 *Sia* $\mathbf{E}$ *un'estensione finita totalmente ramificata su* $\mathbf{K}$*. Sia* Π *un uniformizzante per* $\mathcal{O}_{\mathbf{E}}$*. Allora* Π *è radice di un polinomio di Eisenstein, cioè*

$$X^e + a_{e-1}X^{e-1} + \ldots + a_0$$

con $a_i \in \mathfrak{p}_{\mathbf{K}}$ *e* $a_0 \notin \mathfrak{p}_{\mathbf{K}}^2$*. Viceversa un tale polinomio è iriducibile in* $\mathbf{K}[X]$ *e una sua radice genera un'estensione totalmente ramificata di* $\mathbf{K}$*.*

Dimostrazione (vedi [La]). □

Proposizione 1.5.5 *Sia* $\mathbf{E}$ *un'estensione finita totalmente e debolmente ramificata di* $\mathbf{K}$ *di grado* e*. Allora esiste un uniformizzante* Π *di* $\mathcal{O}_{\mathbf{E}}$ *che è radice di un polinomio del tipo* $X^e - \pi$*, con* π *uniformizzante per* $\mathcal{O}_{\mathbf{K}}$*.*

Dimostrazione (vedi [La]). □

Proposizione 1.5.6 *Sia* $\alpha \in \overline{\mathbf{K}}$ *un elemento algebrico su* $\mathbf{K}$ *che è radice di un polinomio del tipo* $X^e - a$ *per un certo* $a \in \mathcal{O}_{\mathbf{K}}$ *ed un certo* $e \in \mathbb{N}$ *tale che* $(e, p) = 1$*. Allora* $\mathbf{K}(\alpha)$ *è debolmente ramificata su* $\mathbf{K}$ *ed è anche totalmente ramificata se* $v(a) = r$ *con* $(r, p) = 1$*.*

Dimostrazione (vedi [La]). □

Proposizione 1.5.7 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$*.*

1. *Se* $\mathbf{E} \supset \mathbf{F} \supset \mathbf{K}$*, allora* $\mathbf{E}$ *è debolmente ramificata su* $\mathbf{K}$ *se e solo se* $\mathbf{E}$ *è debolmente ramificata su* $\mathbf{F}$ *e* $\mathbf{F}$ *è debolmente ramificata su* $\mathbf{K}$*;*

[4] L'espressione inglese è *tamely ramified*.
[5] L'espressione inglese è *strongly ramified*.
[6] L'espressione inglese è *wildly ramified*: in questo caso la preferiremo sempre a quella italiana, per motivi estetici.

2. *se* $\mathbf{E}$ *è debolmente ramificata su* $\mathbf{K}$*, allora* $\mathbf{EF}$ *è debolmente ramificata su* $\mathbf{F}$*;*
3. *se* $\mathbf{E}$ *e* $\mathbf{F}$ *sono debolmente ramificate su* $\mathbf{K}$*, allora* $\mathbf{EF}$ *è debolmente ramificata su* $\mathbf{K}$*.*

Dimostrazione (vedi [La]). □

Il seguente teorema è noto anche come teorema di struttura delle estensioni finite di campi p-adici: grazie ad esso, si possono studiare separatamente ramificazione e inerzia.

Teorema 1.5.2 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$ *con indice di inerzia* f *e indice di ramificazione* $e = e_0 p^r$ *(*$(e_0, p) = 1$*,* $r \in \mathbb{N}_0$*). Allora esistono due sottoestensioni di* $\mathbf{E}$ *su* $\mathbf{K}$*,* $\mathbf{E}_u$ *e* $\mathbf{E}_t$*, tali che*

1. $\mathbf{E}_u$ *è non ramificata di grado* f *su* $\mathbf{K}$ *e qualsiasi sottoestensione non ramificata di* $\mathbf{E}$ *su* $\mathbf{K}$ *è contenuta in* $\mathbf{E}_u$ *(*$\mathbf{E}_u$ *è il composto di tutte le sottoestensioni di* $\mathbf{E}$ *su* $\mathbf{K}$ *non ramificate);*
2. $\mathbf{E}_t$ *è debolmente e totalmente ramificata di grado* e_0 *su* $\mathbf{E}_u$*;*
3. $\mathbf{E}$ *è totalmente ramificata wild di grado* p^r *su* $\mathbf{E}_t$*.*

Dimostrazione (vedi [La]). □

Con questi risultati, possiamo dimostrare il seguente teorema che è quello che dà senso al tentativo di classificare le estensioni locali. La dimostrazione sfrutta un argomento di compattezza e il lemma di Krasner.

Teorema 1.5.3 *Sia* $n \in \mathbb{N}$*. Esistono solo un numero finito di estensioni di grado* n *di un campo p-adico.*

Dimostrazione (vedi [La]). □

1.6 L'anello degli interi

Richiamiamo in questa sottosezione due risultati importanti riguardo all'anello degli interi di un'estensione di un campo p-adico. Il secondo è una delle più importanti differenze tra il caso locale (quello che stiamo analizzando) e quello globale (quello dei campi di numeri, ossia delle estensioni finite di $\mathbb{Q}$). Manteniamo le notazioni della sezione precedente.

Teorema 1.6.1 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$*. Sia* $\beta \in \mathcal{O}_\mathbf{E}$ *un elemento la cui immagine tramite la proiezione canonica genera* $\mathcal{O}_\mathbf{E}/\mathfrak{p}_\mathbf{E}$ *su* $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}$ *e* $\Pi \in \mathcal{O}_\mathbf{E}$ *un uniformizzante. Allora*

$$\mathcal{O}_\mathbf{E} = \mathcal{O}_\mathbf{K}[\beta, \Pi]$$

Dimostrazione (vedi [La]). □

Teorema 1.6.2 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$*. Esiste un elemento* $\alpha \in \mathcal{O}_\mathbf{E}$ *tale che*

$$\mathcal{O}_\mathbf{E} = \mathcal{O}_\mathbf{K}[\alpha]$$

Dimostrazione vedi [La]). □

1.7 Il differente e il discriminante

In questa sezione costruiamo due invarianti che ci serviranno nella classificazione delle estensioni che intendiamo studiare. Questi due invarianti sono collegati fra loro e li utilizzeremo nel seguito in maniera diffusa. Le notazioni sono sempre quelle della precedente sezione.

Definizione 1.7.1 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$ *e sia* L *un sottogruppo di* $(\mathbf{E}, +)$. *Il* modulo complementare *(relativo alla traccia)* L' *di* L *è*

$$L' = \left\{ x \in \mathbf{E} \,|\, Tr_{\mathbf{E}}^{\mathbf{K}}(xL) \subseteq \mathcal{O}_{\mathbf{K}} \right\}$$

Osservazione 1.7.1 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$ *e sia* L *un sottogruppo di* $(\mathbf{E}, +)$. L' *è un sottogruppo di* $(\mathbf{E}, +)$ *e se* $L = L\mathcal{O}_{\mathbf{K}}$ *allora* $L' = L'\mathcal{O}_{\mathbf{K}}$.

Dimostrazione (vedi [La]). □

Definizione 1.7.2 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$. *Il* differente $\mathcal{D}_{\mathbf{K}}^{\mathbf{E}}$ *di* $\mathbf{E}$ *su* $\mathbf{K}$ *è*

$$\mathcal{D}_{\mathbf{K}}^{\mathbf{E}} = (\mathcal{O}'_{\mathbf{E}})^{-1}$$

Proposizione 1.7.1 *Sia* $\mathbf{E} \subseteq \mathbf{F} \subseteq \mathbf{K}$ *una torre di estensioni finite su* $\mathbf{K}$. *Allora*

$$\mathcal{D}_{\mathbf{K}}^{\mathbf{E}} = \mathcal{D}_{\mathbf{F}}^{\mathbf{E}} \mathcal{D}_{\mathbf{K}}^{\mathbf{F}}$$

Dimostrazione (vedi [La]). □

Proposizione 1.7.2 *Siano* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$ *e* $\alpha \in \mathcal{O}_{\mathbf{E}}$ *tale che* $\mathcal{O}_{\mathbf{E}} = \mathcal{O}_{\mathbf{K}}[\alpha]$. *Se* $f(X) \in \mathbf{K}[X]$ *è il polinomio minimo di* α *su* $\mathbf{K}$, *allora*

$$\mathcal{D}_{\mathbf{K}}^{\mathbf{E}} = (f'(\alpha))$$

In particolare il differente è un ideale di $\mathcal{O}_{\mathbf{E}}$ *(e quindi è una potenza di* $\mathfrak{p}_{\mathbf{E}}$*).*

Dimostrazione (vedi [La]). □

Vediamo ora come il differente possa dare informazioni sulla ramificazione.

Teorema 1.7.1 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$ *con indice di ramificazione* e. *Allora*

1. $\mathfrak{p}_{\mathbf{E}}^{e-1}$ *divide* $\mathcal{D}_{\mathbf{K}}^{\mathbf{E}}$;
2. *se* $\mathbf{E}$ *è fortemente ramificata su* $\mathbf{K}$, *allora* $\mathfrak{p}_{\mathbf{E}}^{e}$ *divide* $\mathcal{D}_{\mathbf{K}}^{\mathbf{E}}$;
3. *se* $\mathbf{E}$ *è non ramificata su* $\mathbf{K}$, *allora* $\mathfrak{p}_{\mathbf{E}}$ *non divide* $\mathcal{D}_{\mathbf{K}}^{\mathbf{E}}$ *(e quindi* $\mathcal{D}_{\mathbf{K}}^{\mathbf{E}} = \mathcal{O}_{\mathbf{E}}$*).*

Dimostrazione (vedi [La]). □

Definizione 1.7.3 *Sia* $\mathbf{E}$ *un'estensione finita di grado* n *di* $\mathbf{K}$ *e siano* $\sigma_1, \sigma_2 \ldots, \sigma_n$ *le immersioni di* $\mathbf{E}$ *nella chiusura algebrica* $\overline{\mathbf{K}}$ *di* $\mathbf{K}$. *Sia infine* $W \subseteq \mathbf{E}^n$ *una* n*-upla di elementi di* $\mathbf{E}$, $W = (w_1, w_2, \ldots, w_n)$. *Allora il* discriminante $D_{\mathbf{K}}^{\mathbf{E}}(W)$ *di* W *è*

$$D_{\mathbf{K}}^{\mathbf{E}}(W) = \det(\sigma_i w_j)^2$$

Osservazione 1.7.2 *Nelle notazioni della definizione precedente,* $D_{\mathbf{K}}^{\mathbf{E}}(W)$ *è un elemento di* $\mathbf{K}$ *e, se* $W \in \mathcal{O}_{\mathbf{E}}^n$, *allora* $D_{\mathbf{K}}^{\mathbf{E}}(W) \in \mathcal{O}_{\mathbf{K}}$. *Inoltre* $D_{\mathbf{K}}^{\mathbf{E}}(W)$ *è diverso da zero se e solo se* W *è una base di* $\mathbf{E}$ *su* $\mathbf{K}$.

Dimostrazione (vedi [La]). □

Osservazione 1.7.3 *Sia* $\mathbf{E}$ *un'estensione finita di grado* n *di* $\mathbf{K}$. *Sia* M *un modulo libero di rango* n *su* $\mathcal{O}_{\mathbf{K}}$ *contenuto in* $\mathbf{E}$ *e siano* W_1 *e* W_2 *due basi per* M *su* $\mathcal{O}_{\mathbf{K}}$. *Allora esiste un elemento* $u \in \mathcal{O}_{\mathbf{K}}^*$ *tale che*

$$D_{\mathbf{K}}^{\mathbf{E}}(W_1) = u^2 D_{\mathbf{K}}^{\mathbf{E}}(W_2)$$

Dimostrazione (vedi [La]). □

Definizione 1.7.4 *Sia* $\mathbf{E}$ *un'estensione finita di grado* n *di* $\mathbf{K}$. *Sia* M *un modulo libero di rango* n *su* $\mathcal{O}_{\mathbf{K}}$ *contenuto in* $\mathbf{E}$. *Allora il* discriminante *di* $D_{\mathbf{K}}^{\mathbf{E}}(M)$ *di* M *è l'ideale generato dal discriminante di una qualsiasi base di* M *su* $\mathcal{O}_{\mathbf{K}}$.

Definizione 1.7.5 *Sia* $\mathbf{E}$ *un'estensione finita di grado* n *di* $\mathbf{K}$. *Allora il* discriminante $D_{\mathbf{K}}^{\mathbf{E}}$ *di* $\mathbf{E}$ *su* $\mathbf{K}$ *è*

$$D_{\mathbf{K}}^{\mathbf{E}} = D_{\mathbf{K}}^{\mathbf{E}}(\mathcal{O}_{\mathbf{E}})$$

Definizione 1.7.6 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$ *con indice d'inerzia* f. *Sia inoltre* $n \in \mathbb{N}$. *Allora la* norma *di* $\mathfrak{p}_{\mathbf{E}}^n \subseteq \mathcal{O}_{\mathbf{E}}$ *è*

$$N_{\mathbf{K}}^{\mathbf{E}}(\mathfrak{p}_{\mathbf{E}}^n) = (\mathfrak{p}_{\mathbf{K}}^f)^n$$

Teorema 1.7.2 *Sia* $\mathbf{E}$ *un'estensione finita di* $\mathbf{K}$. *Allora*

$$N_{\mathbf{K}}^{\mathbf{E}}(\mathcal{D}_{\mathbf{K}}^{\mathbf{E}}) = D_{\mathbf{K}}^{\mathbf{E}}$$

Dimostrazione (vedi [La]). □

Riassumendo: il differente è un ideale di $\mathcal{O}_{\mathbf{E}}$, il discriminante è un ideale di $\mathcal{O}_{\mathbf{K}}$ e uno è la norma dell'altro.

Il seguente risultato è spesso utile per calcolare il differente di estensioni composte: tuttavia nei casi che analizzeremo risulta inefficace, perché non sono verificate le ipotesi. Lo riportiamo per sottolineare che il caso delle estensioni di grado una potenza di p (che sono quelle di cui ci occuperemo) è il più complicato.

Proposizione 1.7.3 *Siano* $\mathbf{E}$ *e* $\mathbf{F}$ *due estensioni finite disgiunte di* $\mathbf{K}$, *rispettivamente di grado* m *e* n. *Supponiamo che i loro discriminanti siano relativamente primi. Allora*

$$\mathcal{O}_{\mathbf{EF}} = \mathcal{O}_{\mathbf{E}}\mathcal{O}_{\mathbf{F}} \qquad e \qquad D_{\mathbf{K}}^{\mathbf{EF}} = (D_{\mathbf{K}}^{\mathbf{E}})^n (D_{\mathbf{K}}^{\mathbf{F}})^m$$

Dimostrazione (vedi [La]). □

1.8 Le unità

Le unità di un'estensione $\mathbf{E}$ sono gli elementi invertibili dell'anello degli interi $\mathcal{O}_{\mathbf{E}}$: spesso si indicano con $U_{\mathbf{E}}$ oppure semplicemente con $\mathcal{O}_{\mathbf{E}}^*$. C'è un'interessante teorema di struttura delle unità: ecco il risultato nel caso di $\mathbb{Q}_p$.

Teorema 1.8.1

$$\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times U_1$$

dove $U_1 = \{x \in \mathbb{Z}_p \,|\, x \equiv 1 \ (p)\}$ *è un sottogruppo di* $\mathbb{Z}_p^*$. *Inoltre, se* p *è un primo dispari,*

$$U_1 \cong \mathbb{Z}_p$$

mentre, se $p = 2$,

$$U_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$$

Dimostrazione (vedi [FV]).

Il fattore $(\mathbb{Z}/p\mathbb{Z})^*$ rappresenta le radici $(p-1)$-esime dell'unità (che abbiamo già visto appartenere a $\mathbb{Q}_p$). Ogni elemento di $\mathbb{Z}_p^*$ si può scrivere come un prodotto tra una radice $(p-1)$-esima dell'unità ed un elemento di U_1. L'isomorfismo di U_1 con $\mathbb{Z}_p$ (se $p \neq 2$) è dato da un esponenziale: ogni elemento di U_1 si può scrivere come $(1+p)^a$ per qualche $a \in \mathbb{Z}_p$. Una mappa simile dà anche l'isomorfismo nel caso $p = 2$. Inoltre l'esponenziale dota U_1 di una struttura di $\mathbb{Z}_p$-modulo. Nel caso di $\mathbb{Q}_p$ ($p \neq 2$), questo modulo è libero di rango 1. Nel caso più generale (sempre per $p \neq 2$) di un'estensione finita di grado n $\mathbf{K}$ di $\mathbb{Q}_p$, $U_1^{\mathbf{K}}$ è uno $\mathbb{Z}_p$-modulo libero di rango n (l'isomorfismo è ancora una specie di esponenziale ,vedi [FV]). In generale, inoltre ($p \neq 2$),

$$U_{\mathbf{K}} \cong W \times U_1$$

dove W è il gruppo delle radici dell'unità contenute in $\mathbf{K}$.

Per quanto riguarda la struttura del gruppo degli invertibili di $\mathbb{Q}_p$ si ha il seguente risultato:

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p^*$$

Questo risultato è conseguenza del fatto, di immediata verifica, che tutti gli elementi di $\mathbb{Q}_p^*$ si possono scrivere come $p^n u$, per un certo $n \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^*$.

1.9 La teoria della ramificazione: le filtrazioni

Per tutta questa sezione, oltre a mantenere le notazioni della sezione 1.7, supporremo che $\mathbf{E}$ sia un'estensione finita di Galois su $\mathbf{K}$ con gruppo di Galois $G(\mathbf{E}|\mathbf{K}) = G$ e che $\alpha \in \mathcal{O}_{\mathbf{E}}$ sia un generatore di $\mathcal{O}_{\mathbf{E}}$ come $\mathcal{O}_{\mathbf{K}}$-algebra. Vedremo come l'ipotesi di Galois renda lo studio della ramificazione più semplice. Il gruppo di Galois G agisce sull'anello $\mathcal{O}_{\mathbf{E}}$.

Osservazione 1.9.1 *Sia* $s \in G$ *e sia* $i \in \mathbb{Z}$, $i \geq -1$. *Allora le seguenti condizioni sono equivalenti:*

1. *s agisce banalmente sull'anello quoziente $\mathcal{O}_{\mathbf{E}}/\mathfrak{p}_{\mathbf{E}}^{i+1}$;*

2. $v_{\mathbf{E}}(s(a) - a) \geq i + 1$ *per tutti gli* $a \in \mathcal{O}_{\mathbf{E}}$;

3. $v_{\mathbf{E}}(s(\alpha) - \alpha) \geq i + 1$

Dimostrazione (vedi [Se]). □

Proposizione 1.9.1 *Per ogni intero* $i \geq -1$, *sia* G_i *è l'insieme degli elementi* $s \in G$ *che soddisfano le tre condizioni dell'osservazione precedente. Allora i* G_i *formano una successione decrescente (rispetto all'inclusione) di sottogruppi normali di* G. *Inoltre* $G = G_{-1}$, G_0 *corrisponde alla massima sottoestensione non ramificata di* $\mathbf{E}$ *su* $\mathbf{K}$ *e* $G_i = \{1\}$ *per i abbastanza grande.*

Dimostrazione (vedi [Se]). □

Definizione 1.9.1 *Sia* $i \in \mathbb{Z}$, $i \geq -1$. *L'*i-esimo gruppo di ramificazione G_i *è*

$$G_i = \{s \in G \mid v_{\mathbf{E}}(s(a) - a) \geq i + 1 \ \forall\, a \in \mathcal{O}_{\mathbf{E}}\}$$

G_0 *è detto* gruppo d'inerzia *di* $\mathbf{E}$ *su* $\mathbf{K}$.

I G_i definiscono quindi una *filtrazione* di G, cioè semplicemente una catena discendente di sottogruppi di G.

Definizione 1.9.2 *Denotando ancora con* α *un generatore di* $\mathcal{O}_{\mathbf{E}}$ *come* $\mathcal{O}_{\mathbf{K}}$*-algebra, definiamo la funzione* $i_G : G \to \mathbb{Z} \cup \{\infty\}$ *con la formula*

$$i_G(s) = v_{\mathbf{E}}(s(\alpha) - \alpha)$$

Osservazione 1.9.2 *La funzione* i_G *soddisfa le seguenti proprietà (per tutti gli* s,$t \in G$*):*

1. $i_G(s)$ *è un intero non negativo se* $s \neq 1$ *e* $i_G(1) = \infty$;

2. $i_G(s) \geq i + 1 \Leftrightarrow s \in G_i$;

3. $i_G(tst)^{-1} = i_G(s)$;

4. $i_G(st) \geq \min\{i_G(s), i_G(t)\}$.

Dimostrazione (vedi [Se]). □

La filtrazione dei G_i si trasferisce bene ai sottogruppi di G. Non così bene si comporta con i quozienti di G, motivo per cui si introduce solitamente un'altra filtrazione[7], della quale però non ci occuperemo. Fortunatamente se H è un sottogruppo di ramificazione, i sottogruppi di ramificazione di G/H sono deducibili in modo semplice da quelli di G.

Proposizione 1.9.2 *Sia* H *un sottogruppo di* G. *Per ogni* $s \in H$, $i_H(s) = i_G(s)$ *e* $H_i = G_i \cap H$ *(si sono indicati con* H_i *i sottogruppi di ramificazione di* H*).*

[7] Si tratta della *upper numbering filtration* (vedi [Se]).

Dimostrazione (vedi [Se]). □

Per esempio, se $H = G_0$, dalla proposizione precedente si vede che si può ridurre lo studio di un'estensione generica alla parte totalmente ramificata di essa.

Proposizione 1.9.3 *Sia H un sottogruppo normale di G e sia $\mathbf{K}'$ la sottoestensione di $\mathbf{E}$ ad esso corrispondente. Allora, detto e' l'indice di ramificazione di $\mathbf{K}'$ su $\mathbf{K}$, si ha, per ogni $\sigma \in G/H$,*

$$i_{G/H} = \frac{1}{e'} \sum_{s \to \sigma} i_G(s)$$

(la somma è presa sugli $s \in G$ la cui proiezione è σ).

Dimostrazione (vedi [Se]). □

Osservazione 1.9.3 *Sia $j \in \mathbb{Z}$, $j \geq 0$. Allora*

$$(G/G_j)_i = G_i/G_j \quad \textit{se } i \leq j \qquad e \qquad (G/G_j)_i = \{1\} \quad \textit{se } i \geq j$$

Dimostrazione (vedi [Se]). □

Veniamo ora alla relazione che intercorre tra differente e gruppi di ramificazione. Della seguente proposizione faremo largo uso nel seguito: essa lega la valutazione della derivata del polinomio minimo di α calcolata in α (cioè la valutazione di un generatore del differente) alla cardinalità dei gruppi di ramificazione.

Proposizione 1.9.4 *Sia $f(X) \in \mathbf{K}[X]$ il polinomio minimo di α su $\mathbf{K}$. Allora*

$$v_{\mathbf{E}}(f'(\alpha)) = v_{\mathbf{E}}(\mathcal{D}_{\mathbf{K}}^{\mathbf{E}}) = \sum_{s \neq 1} i_G(s) = \sum_{i=0}^{\infty} (|G_i| - 1)$$

Dimostrazione (vedi [Se]). □

Introduciamo adesso una seconda filtrazione, questa volta sulle unità di $\mathcal{O}_{\mathbf{E}}$.

Definizione 1.9.3 *Sia $U_{\mathbf{E}}$ il gruppo delle unità di $\mathbf{E}$. Poniamo*

$$\begin{aligned} U_{\mathbf{E}}^{(0)} &= U_{\mathbf{E}} \\ U_{\mathbf{E}}^{(i)} &= 1 + \mathfrak{p}_{\mathbf{E}}^{i} \quad \textit{se } i \geq 1 \end{aligned}$$

È chiaro che gli $U_{\mathbf{E}}^{(i)}$ costiutiscono una filtrazione di $U_{\mathbf{E}}$: le seguenti proposizioni spiegano perché è utile per lo studio della ramificazione. Denotiamo con Π un uniformizzante per $\mathcal{O}_{\mathbf{E}}$.

Proposizione 1.9.5 *Sia i un intero non negativo. Affinché un elemento $s \in G_0$ appartenga a G_i, è necessario e sufficiente che*

$$s(\Pi)/\Pi \equiv 1 \pmod{\mathfrak{p}_{\mathbf{E}}^{i}}$$

Dimostrazione (vedi [Se]). □

Proposizione 1.9.6 *1.* $U_{\mathbf{E}}^{(0)}/U_{\mathbf{E}}^{(1)} \cong (\mathcal{O}_{\mathbf{E}}/\mathfrak{p}_{\mathbf{E}})^*$*;*

2. per $i \geq 1$*, il gruppo* $U_{\mathbf{E}}^{(i)}/U_{\mathbf{E}}^{(i+1)}$ *è canonicamente isomorfo al gruppo* $\mathfrak{p}_{\mathbf{E}}^i/\mathfrak{p}_{\mathbf{E}}^{i+1}$*, il quale a sua volta è isomorfo (non canonicamente) a* $(\mathcal{O}_{\mathbf{E}}/\mathfrak{p}_{\mathbf{E}}, +)$

Dimostrazione (vedi [Se]). □

Proposizione 1.9.7 *La mappa che, ad ogni* $s \in G_i$*, assegna* $s(\Pi)/\Pi$*, induce passando ai quozienti un isomorfismo* θ_i *tra* G_i/G_{i+1} *e un sottogruppo di* $U_{\mathbf{E}}^{(i)}/U_{\mathbf{E}}^{(i+1)}$*. Questo isomorfismo è indipendente dalla scelta dell'uniformizzante* Π*.*

Dimostrazione (vedi [Se]). □

Proposizione 1.9.8 *1.* G_0/G_1 *è ciclico e ha ordine primo con p;*

2. se $i \geq 1$*,* G_i/G_{i+1} *è isomorfo a un prodotto diretto di gruppi ciclici di ordine p;*

3. G_1 *è un p-gruppo;*

4. G_0 *è il prodotto semidiretto di un gruppo ciclico di ordine primo con p con un sottogruppo normale il cui ordine è una potenza di p;*

5. G *e* G_0 *sono gruppi risolubili;*

6. gli interi $i \geq 1$ *tali che* $G_i \neq G_{i+1}$ *sono congruenti uno all'altro modulo p.*

Dimostrazione (vedi [Se]). □

La lista delle proprietà della filtrazione dei G_i potrebbe continuare ma diverrebbe più tecnica. Ci limitiamo ad elencare alcune proprietà che useremo spesso nel computo dei gruppi di ramificazione.

Proposizione 1.9.9 *Sia* $e = v_{\mathbf{E}}(p)$ *l'indice di ramificazione assoluto.*

1. $G_i = \{1\}$ *se* $i > e/(p-1)$*;*

2. se $i = e/(p-1)$*,* G_i *è banale oppure ciclico di ordine p (quest'ultima eventualità potendosi verificare solo se* $i \equiv 0 \,(mod\ p)$*);*

3. se $i < e/(p-1)$ *e* $i \equiv 0 \,(mod\ p)$*,* G_i/G_{i+1} *è banale oppure ciclico di ordine p (quest'ultima eventualità potendosi verificare solo se esiste un certo numero intero* $h > 0$ *tale che* $p^h i = e/(p-1)$*);*

4. se $i < e/(p-1)$ *e* $p \nmid i$*,* G_{pi+1} *contiene la p-esima potenza di un elemento di* G_i*;*

5. se gli interi $i \geq 1$ *tali che* $G_i \neq G_{i+1}$ *sono tutti divisibili per p, allora questi interi hanno la forma*

$$p^k i_0, \qquad 1 \leq k \leq h$$

dove $p^h i_0 = e/(p-1)$ *e* G_1 *ha ordine* p^h*.*

Dimostrazione (vedi [Se]). □

1.10 La corrispondenza della teoria dei corpi di classe locale

Questa sezione è dedicata ad enunciare il risultato fondamentale della teoria dei corpi di classe locale, del quale faremo uso nel capitolo 4. Con la teoria dei corpi di classe si classificano le estensioni abeliane finite.

Teorema 1.10.1 *Sia* $\mathbf{K}$ *un campo p-adico. La mappa*

$$\mathbf{E} \longmapsto \mathcal{N}_{\mathbf{E}} = N_{\mathbf{K}}^{\mathbf{E}}(\mathbf{E}^*)$$

fornisce una corrispondenza biunivoca tra le estensioni abliane finite $\mathbf{E}$ *di* $\mathbf{K}$ *e i sottogruppi aperti di indice finito* $\mathcal{N}$ *di* $\mathbf{K}^*$*. Inoltre*

$$\begin{aligned} \mathbf{E}_1 \subset \mathbf{E}_2 &\Leftrightarrow \mathcal{N}_{\mathbf{E}_1} \supseteq \mathcal{N}_{\mathbf{E}_2} \\ \mathcal{N}_{\mathbf{E}_1\mathbf{E}_2} &= \mathcal{N}_{\mathbf{E}_1} \cap \mathcal{N}_{\mathbf{E}_2} \\ \mathcal{N}_{\mathbf{E}_1 \cap \mathbf{E}_2} &= \mathcal{N}_{\mathbf{E}_1} \cdot \mathcal{N}_{\mathbf{E}_2} \end{aligned}$$

Infine

$$G(\mathbf{E}|\mathbf{K}) \cong \mathbf{K}^*/\mathcal{N}_{\mathbf{E}}$$

Dimostrazione (vedi [Ne], [Mi]).

Si può dimostrare che, poiché $\mathbf{K}$ ha caratteristica zero, ogni sottogruppo di indice finito di $\mathbf{K}^*$ è aperto (vedi [Mi]).

1.11 Il numero di automorfismi di una estensione

In questa sezione introduciamo un altro invariante: non è tipico della teoria dei numeri, si tratta del numero di automorfismi di un'estensione. Tuttavia per comodità fissiamo alcune notazioni. Studiamo solo il caso particolare delle estensioni di grado p^2 di $\mathbb{Q}_p$ ma è chiaro che discorsi analoghi valgono anche in casi più generali.

Sia p un numero primo e $q(X) \in \mathbb{Q}_p[X]$ un polinomio irriducibile di grado p^2. Siano $\{\alpha_i\}_{i=1}^{p^2}$ le radici di $q(X)$. Poniamo

$$\mathbf{L}_i \;=\; \mathbb{Q}_p(\alpha_i)$$

Sarà chiaramente possibile che $\mathbf{L}_i = \mathbf{L}_j$ anche se $i \neq j$ (si pensi ad esempio al caso in cui $\mathbf{L}_i$ è di Galois su $\mathbb{Q}_p$). Più precisamente, se poniamo $\Lambda = \{\mathbf{L}_i\}_{i=1}^{p^2}$, si avrà $Card(\Lambda) \leq p^2$. Indichiamo con $w_i = w(\mathbf{L}_i)$ il numero di $\mathbb{Q}_p$-automorfismi di $\mathbf{L}_i$.
Non è difficile riconoscere che in realtà $w_i = w_j$ per ogni i e j compresi tra 1 e p^2 (e quindi denoteremo semplicemente con w il numero di $\mathbb{Q}_p$-automorfismi di una qualsiasi estensione di $\mathbb{Q}_p$ ottenuta aggiungendo una radice di $q(X)$). Infatti sia $\mathbf{F}$ il campo di spezzamento di $q(X)$, in particolare dunque $\mathbf{L}_i \subseteq \mathbf{F}$. Poniamo per semplicità $G = G(\mathbf{F}|\mathbb{Q}_p)$ e $G_i = G(\mathbf{F}|\mathbf{L}_i)$. Denotiamo inoltre con A_i il gruppo dei $\mathbb{Q}_p$-automorfismi di $\mathbf{L}_i$: si avrà perciò $Card(A_i) = w_i$. Sia $\sigma \in G$ tale che $\sigma(\alpha_i) = \alpha_j$ per due indici fissati i e j compresi tra 1 e p^2 (tale σ esiste perchè il gruppo di Galois del campo di spezzamento

di un polinomio agisce transitivamente sulle radici del polinomio). Definiamo allora la funzione

$$\varphi : A_i \to A_j$$

$$\varphi(\tau) = \sigma_{|\mathbf{L}_i}\tau(\sigma^{-1})_{|\mathbf{L}_i}$$

È chiaro che effettivamente $\varphi(\tau) \in A_j$. Inoltre φ è un isomorfismo (come facilmente si verifica). Allora $w_i = w_j$.
Sia ora $S = \{\alpha \in \overline{\mathbb{Q}_p} \,|\, q(\alpha) = 0\}$ l'insieme delle radici di $q(X)$. Su S mettiamo la seguente relazione di equivalenza

$$\alpha\,,\ \beta \in S \qquad \alpha \sim \beta \Leftrightarrow \mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$$

Sia $\Sigma = S/\sim$ l'insieme quoziente e si ha $Card(\Lambda) = Card(\Sigma)$. Poniamo inoltre

$$H_i = \{\sigma \in G \,|\, \mathbb{Q}_p(\sigma(\alpha_i)) = \mathbb{Q}_p(\alpha_i)\}$$

Non è difficile verificare che H_i è un sottogruppo di G che contiene G_i e in realtà H_i è il normalizzatore di G_i in G, ovvero il più grande sottogruppo di G contenente G_i in cui G_i sia normale. Indichiamo come di consueto con $G/H_i = \{\sigma H_i, \sigma \in G\}$ $H_i/G_i = \{\tau G_i, \tau \in H_i\}$ gli insiemi delle classi laterali sinistre (il secondo è anche un gruppo essendo $G_i \triangleleft H_i$). Allora si avrà

$$|G/H_i| \cdot |H_i/G_i| = |G/G_i| = p^2$$

Allora l'applicazione

$$\psi : G/H_i \to \Sigma$$

$$\psi(\sigma H_i) = [\sigma(\alpha_i)]$$

(è effettivamente una funzione e) definisce una biiezione tra G/H_i e Σ: la verifica è immediata, basta provare l'iniettività perché entrambi gli insiemi hanno cardinalità finita (del resto anche la suriettività è semplice).
Similmente l'applicazione

$$\gamma : H_i/G_i \to A_i$$

$$\gamma(\sigma G_i) = \sigma_{|\mathbf{L}_i}$$

(è effettivamente una funzione e) definisce una biiezione tra H_i/G_i e A_i: anche qui come sopra le verifiche sono semplici.
Abbiamo così mostrato che $w \,|\, p^2$ (e quindi w può assumere i valori 1, p o p^2) e si ha $Card(\Lambda) = p^2/w$.
Studiando con maggiore attenzione i sottogruppi H_i si riconosce che sono fra di loro coniugati, cioè che, scelti i e j, esiste $\sigma_{ij} \in G$ tale che $\sigma_{ij}^{-1} H_i \sigma_{ij} = H_j$. Basterà infatti scegliere σ_{ij} in modo che $\sigma_{ij}(\alpha_j) = \alpha_i$. Per quanto segue ci conviene utilizzare la seguente notazione

$$\mathbf{K}_i = Fix(H_i)$$

Osserviamo allora che $\mathbf{K}_i \subseteq \mathbf{L}_i$.

1.11.1 Il caso $w = p^2$

Questo è il caso più semplice (e anche il più raro ...): si tratta infatti della situazione in cui tutte le estensioni $\mathbf{L}_i$ coincidono (fra loro e dunque anche) con il campo di spezzamento $\mathbf{F}$ che risulta essere perciò una estensione di Galois di grado p^2 di $\mathbb{Q}_p$. Inoltre $G = H_i$ e $G_i = \{id\}$ e (quindi) anche $\mathbf{K}_i = \mathbb{Q}_p$. Non rimane molto da aggiungere, se non che G, essendo un gruppo di ordine p^2, sarà abeliano, in particolare ciclico o p-elementare di rango 2.

1.11.2 Il caso $w = p$

Possiamo analizzare separatamente un sottocaso particolare per coglierne le differenze rispetto alla situazione generale:

- H_i è un sottogruppo normale.
  In questo caso, siccome gli H_i sono tutti coniugati, si ha che $H_i = H_j$ per ogni i e j compresi tra 1 e p^2. Da questo segue anche che tutti gli $\mathbf{K}_i$ coincidono. Conveniamo di denotare con $\mathbf{K}$ uno qualsiasi degli $\mathbf{K}_i$ e con H uno qualsiasi degli H_i: si avrà pertanto $\mathbf{K} = Fix(H)$. La situazione è allora la seguente: $\mathbf{F}$ contiene p estensioni di grado p^2 su $\mathbb{Q}_p$ (che sono le $\mathbf{L}_i$, considerato che $Card(\Lambda) = p$) la cui intersezione a due a due risulta essere $\mathbf{K}$. Le $\mathbf{L}_i$ sono cicliche di grado p su $\mathbf{K}$. Quest'ultima è normale di grado p (quindi ciclica) su $\mathbb{Q}_p$. Vedremo, per quanto riguarda questo sottocaso, cioè $w = p$ e H_i sottogruppo normale di G, che (se $p \neq 2$) G è un p-gruppo di ordine p^3 o p^4 (ci sono solo tre possibilità, tutte effettivamente realizzate, per G).

- Caso generale.
  Le $\mathbf{L}_i$ (che sono in tutto p) sono cicliche di grado p sulle $\mathbf{K}_i$ e queste ultime sono estensioni di grado p di $\mathbb{Q}_p$. Osserviamo esplicitamente che basta che una sola delle $\mathbf{E}_i$ sia normale perchè tutte lo siano, visto che sono fra loro coniugate (in tal caso si ricade nella situazione analizzata sopra). Se $p = 2$, H_i sarà necessariamente un sottogruppo normale di G, perché è un sottogruppo di indice 2. Non è detto, se p è dispari, che G sia un p-gruppo.

1.11.3 Il caso $w = 1$

Si tratta del caso più complicato: se $p = 2$, coincide con il caso che nessuna delle $\mathbf{L}_i$ abbia una sottoestensione propria. Infatti supponiamo che esista un indice i tale che $\mathbf{L}_i$ ha una sottoestensione propria $\mathbf{E}_i$. Allora $[\mathbf{L}_i : \mathbf{E}_i] = 2$ quindi $\mathbf{L}_i$ è normale su $\mathbf{E}_i$ e $G(\mathbf{K}|\mathbf{E}_i)$ è contenuto nel normalizzatore di G_i, che avevamo indicato con H_i. Ma allora

$$|H_i/G_i| \geq |G(\mathbf{K}|\mathbf{F}_i)/G_i| = 2$$

ossia $w = |H_i/G_i| \geq 2$, contro le ipotesi. In generale, per p qualsiasi, il caso $w = 1$ ha per sottocaso quello in cui $\mathbf{L}_i$ le sono prive di sottoestensioni.

1.12 La classificazione

Veniamo ora a introdurre, per comodità del lettore, alcuni degli strumenti specifici che utilizzeremo per classificare alcune delle estensioni di grado p^2 di $\mathbb{Q}_p$.

1.12.1 La formula di Krasner e la formula di Serre

Abbiamo già visto che, utilizzando il lemma di Krasner, si arriva a dire che le estensioni di grado fissato di un campo p-adico sono in numero finito. Proprio Krasner le ha poi contate ottenendo il seguente risultato.

Teorema 1.12.1 (Krasner) *Sia* $\mathbf{K}$ *un campo p-adico di grado* n_0 *su* $\mathbb{Q}_p$. *Sia* $n = hp^m$ $((h,p) = 1)$ *un numero naturale. Definiamo la funzione* $\epsilon : \mathbb{N} \cup \{-1\} \to \mathbb{Q} \cup \{-\infty\}$ *come*

$$\epsilon(s) = \sum_{i=1}^{s} p^{-i}$$

se $s > 1$ *e*

$$\epsilon(1) = 0 \qquad \epsilon(-1) = -\infty$$

Allora il numero $\mathfrak{N}_n^{\mathbf{K}}$ *delle estensioni di grado* n *di* $\mathbf{K}$ *è*

$$\mathfrak{N}_n^{\mathbf{K}} = \left(\sum_{d|h} d \right) \left[\sum_{s=0}^{m} \frac{p^{m+s+1} - p^{2s}}{p-1} \left(p^{\epsilon(s) n n_0} - p^{\epsilon(s-1) n n_0} \right) \right]$$

Inoltre il numero $\mathfrak{N}_{n,\,ram}^{\mathbf{K}}$ *delle estensioni totalmente ramificate di grado* n *di* $\mathbf{K}$ *è*

$$\mathfrak{N}_{n,\,ram}^{\mathbf{K}} = n \sum_{s=0}^{m} p^s \left(p^{\epsilon(s) n n_0} - p^{\epsilon(s-1) n n_0} \right)$$

Dimostrazione (vedi [Kr 62]).

È noto anche il numero di estensioni totalmente di grado fissato la valutazione del cui discriminante è fissata. Sia $\mathbf{E}$ un'estensione totalmente di grado n di $\mathbf{K}$: indichiamo con $d(\mathbf{E})$ la valutazione del discriminante di $\mathbf{E}$ ($d(\mathbf{E}) = v_{\mathbf{K}}(D_{\mathbf{K}}^{\mathbf{E}})$ e poniamo

$$c(\mathbf{E}) = d(\mathbf{E}) - n + 1$$

(vedi [Se 78]). In primo luogo, valgono allora le condizioni di Ore: l'insieme delle estensioni totalmente $\mathbf{E}$ di grado n di $\mathbf{K}$, tali che $c(\mathbf{E}) = c$, è non vuoto se e solo se

$$v_{\mathbf{K}}(l) \leq c/n \leq v_{\mathbf{K}}(n)$$

dove l è l'intero compreso tra 1 e n tale che $c \equiv l \ (mod\ n)$ (vedi [Se 78]). In questo caso vale il seguente risultato.

Teorema 1.12.2 (Serre) *Sia* $\mathbf{K}$ *un campo p-adico il cui campo residuo ha* $q = p^f$ *elementi. Sia* c *un intero che soddisfa le condizioni di Ore. Allora il numero* $\mathfrak{N}_{n,\,c}^{\mathbf{K}}$ *di estensioni* $\mathbf{E}$ *di* $\mathbf{K}$ *di grado* n *con* $c(\mathbf{E}) = c$ *è*

$$\mathfrak{N}_{n,\,c}^{\mathbf{K}} = n\alpha(c) q^{c - \beta(c)}$$

dove

$$\begin{aligned} \alpha(c) &= \begin{cases} 1 & \text{se } l = n \\ q - 1 & \text{se } l \neq n \end{cases} \\ \beta(c) &= \sum_{1 \leq i \leq n-1} \sup\{0,\, [(c+i)/n] - v_{\mathbf{K}}(n-i)\} \end{aligned}$$

Dimostrazione (vedi [Se 78]).

1.12.2 La formula di Šafarevič

Una p-estensione di un campo p-adico $\mathbf{K}$ è un'estensione di Galois di grado una potenza di p. Šafarevič ha pubblicato nel 1947 un articolo nel quale dava risposta, fra l'altro, alle seguenti domande, nel caso in cui $\mathbf{K}$ non contenga le radici p-esime dell'unità:

1. sotto quali condizioni, dato un p-gruppo G, esiste una p-estensione di $\mathbf{K}$ con gruppo isomorfo a G;
2. quale è il numero di p-estensioni di $\mathbf{K}$ con un dato gruppo di Galois;
3. sotto quali condizioni una p-estensione è contenuta in un'altra p-estensione più grande.

Le risposte sono nel seguente teorema.

Teorema 1.12.3 (Šafarevič) *Sia* $\mathbf{K}$ *un campo p-adico di grado* n_0 *su* $\mathbb{Q}_p$ *che non contiene le radici p-esime dell'unità. Allora*

1. *un dato p-gruppo finito è realizzato come gruppo di Galois di un'estensione di* $\mathbf{K}$ *se e solo se il numero d dei suoi generatori non supera* $n_0 + 1$*;*
2. *se* $d \leq n_0 + 1$*, se* p^n *è l'ordine del p-gruppo e* α *è il numero dei suoi automorfismi, allora il numero delle estensioni, il cui gruppo di Galois è isomorfo a tale gruppo è*
$$\frac{1}{\alpha} p^{(n_0+1)(n-d)} \left(p^{(n_0+1)} - 1\right) \left(p^{(n_0+1)} - p\right) \dots \left(p^{(n_0+1)} - p^{d-1}\right)$$
3. *dati due p-gruppi* G *e* $\overline{G}$*, in modo che* $\overline{G}$ *sia immagine omomorfa di* G *tramite un fissato omomorfismo e che il numero di generatori per* G *non superi* $n_0 + 1$*, per ogni estensione di Galois* $\mathbf{L}$ *su* $\mathbf{K}$ *con gruppo di Galois* $\overline{G}$ *esiste un'estensione di Galois* $\mathbf{F}$ *su* $\mathbf{K}$ *che contiene* $\mathbf{L}$ *in modo che l'omomorfismo fissato coincida con quello di restrizione.*

Dimostrazione (vedi [Ša 56]).

Risulta chiaro, a questo punto, che il caso delle estensioni di $\mathbb{Q}_2$ andrà trattato con altri metodi perché $\mathbb{Q}_2$ contiene le radici quadrate dell'unità. Questo comporterà uno sforzo maggiore e una perdita di eleganza nella trattazione. In realtà, nel 1995, Yamagishi (vedi [Ya 95]) ha pubblicato un articolo analogo a quello di Šafarevič, in cui viene studiato il caso in cui le radici dell'unità sono contenute nel campo di partenza. Non faremo tuttavia ricorso a questa pubblicazione, se non come riferimento, perché non risulta essere necessaria.

Capitolo 2

Le estensioni di grado p su $\mathbb{Q}_p$

2.1 Il caso $p = 2$

Osservazione 2.1.1 *Sia* $\mathbf{K}$ *un'estensione di grado* 2 *su* $\mathbb{Q}_2$*. Allora* $\mathbf{K} = \mathbb{Q}_2(\sqrt[2]{\delta})$*, con* $\delta \in \mathbb{Z}_2$ *non quadrato.*

Dimostrazione Per ipotesi esiste $\gamma \in \overline{\mathbb{Q}_2}$ tale che $\mathbf{K} = \mathbb{Q}_2(\gamma)$. A patto eventualmente di moltiplicare per un opportuna potenza di 2 si può supporre γ intero su $\mathbb{Z}_2$. Infatti γ soddisfa una equazione monica di secondo grado irriducibile a coefficienti in $\mathbb{Q}_2$, cioè

$$\gamma^2 + a\gamma + b = 0 \qquad a, b \in \mathbb{Q}_2$$

Usando la scrittura che evidenzia la potenza di 2 negli elementi di $\mathbb{Q}_2$

$$\gamma^2 + 2^{k_a} u_a \gamma + 2^{k_b} u_b = 0 \qquad k_a, k_b \in \mathbb{Z} \quad u_a, u_b \in \mathbb{Z}_2^*$$

Se $k_a,\ k_b \geq 0$, allora $a,\ b \in \mathbb{Z}_2$ e allora γ è intero su $\mathbb{Z}_2$. Altrimenti scegliamo $k = \min\{k_a, k_b\}$. Moltiplicando per 2^{-k} si ottiene una equazione a coefficienti in $\mathbb{Z}_2$

$$2^{-k}\gamma^2 + 2^{k_a - k} u_a \gamma + 2^{k_b - k} u_b = 0$$

Moltiplichiamo ulteriormente per 2^{-k}

$$2^{-2k}\gamma^2 + 2^{k_a - 2k} u_a \gamma + 2^{k_b - 2k} u_b = 0$$

Allora $2^{-k}\gamma$ è una soluzione del polinomio monico a coefficienti in $\mathbb{Z}_2$ (che ovviamente è irriducibile)

$$X^2 + 2^{k_a - k} u_a X + 2^{k_b - 2k} u_b$$

Quindi $2^{-k}\gamma$ è intero su $\mathbb{Z}_2$ e chiaramente $\mathbb{Q}_2(2^{-k}\gamma) = \mathbb{Q}_2(\gamma)$. Supponiamo dunque che γ sia intero su $\mathbb{Z}_2$, cioè γ è radice di un polinomio monico a coefficienti in $\mathbb{Z}_2$ irriducibile, diciamo

$$f(X) = X^2 + aX + b \qquad a, b \in \mathbb{Z}_2 \qquad f(\gamma) = 0$$

Sia δ il discriminante di $f(X)$, cioè $\delta = a^2 - 4b$. Essendo chiaro, dalla formula per le radici di $f(X)$ in funzione di $\sqrt[2]{\delta}$, che $\mathbb{Q}_2(\gamma) = \mathbb{Q}_2(\sqrt[2]{\delta})$, si ha la tesi.□

Per studiare le estensioni di grado 2 è utile dunque avere una descrizione dei quadrati di $\mathbb{Z}_2$.

Osservazione 2.1.2 *Sia $\delta = 2^k u \in \mathbb{Z}_2$ con $k \in \mathbb{N}_0$ e $u \in \mathbb{Z}_2^*$. Allora δ è un quadrato in $\mathbb{Z}_2$ se e solo se $k \equiv 0\,(mod\ 2)$ ed esiste $b \in \mathbb{Z}_2$ tale che $u = 1 + 4b(b+1)$.*

Dimostrazione Osserviamo innazitutto che, scegliendo come insieme di rappresentanti per $\mathbb{Z}_2/2\mathbb{Z}_2 = \mathbf{F}_2$ l'insieme $\{0, 1\}$, esiste $a \in \mathbb{Z}_2$ tale che $u = 1 + 2a$ perché $u \in \mathbb{Z}_2^*$. Ora, u è un quadrato in $\mathbb{Z}_2$ se e solo esiste $v \in \mathbb{Z}_2$ tale che $v^2 = u$ ma chiaramente tale v andrà cercato in $\mathbb{Z}_2^*$, dato che $u \in \mathbb{Z}_2^*$. Scriviamo allora $v = 1 + 2b$ e imponiamo $u = v^2$:

$$1 + 2a \;=\; (1 + 2b)^2 \quad \Leftrightarrow \quad a \;=\; 2b(b+1)$$

È chiaro quindi che, se la condizione della tesi è soddisfatta, δ è un quadrato in $\mathbb{Z}_2$. Viceversa, se δ è un quadrato, sarà il quadrato di un elemento di $\mathbb{Z}_2^*$. Sia allora $\epsilon = 2^h(1 + 2b)$ e supponiamo $2^k(1 + 2a) \;=\; \delta \;=\; \epsilon^2 \;=\; 2^{2h}(1 + 4b(b + 1))$. Quindi per l'unicità della scrittura (ossia per la fattorizzazione unica) si ha

$$k = 2h \qquad a = 2b(b+1)$$

che è quello che volevamo. □

Osservazione 2.1.3 *Sia $a \in \mathbb{Z}_2$. Allora $a \in (2)^2$ se e solo se esiste $b \in \mathbb{Z}_2$ tale che $a = 2b(b+1)$*

Dimostrazione Se un tale b esiste, cioè si ha $a = 2b(b+1)$, dalla semplice osservazione che (esattamente) uno tra b e $b + 1$ deve essere in $2\mathbb{Z}_2$, si ottiene la tesi. Viceversa supponiamo che $a = 4c$ per un qualche $c \in \mathbb{Z}_2$. Osserviamo che il polinomio

$$g(X) \;=\; X^2 + X - 2c$$

ha soluzioni in $\mathbb{Z}_2$ per il lemma di Hensel. Quindi se b è una soluzione di $g(X)$, si ha $a = 2b(b + 1)$. □

Considerazione
Combinando le osservazioni precedenti si ha che $\delta = 2^k(1 + 2a)$ è un quadrato in $\mathbb{Z}_2$ se è solo se $k \;\equiv\; 0\,(mod\ 2)$ e $a \in (2)^2$.

Osservazione 2.1.4 *Siano α , $\beta \in \overline{\mathbb{Q}_2} \setminus \mathbb{Q}_2$ due elementi tali che α^2, $\beta^2 \in \mathbb{Z}_2$. Allora*

$$\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\beta) \qquad \Leftrightarrow \qquad \alpha\beta \;\in\; \mathbb{Z}_2$$

Dimostrazione
($\Rightarrow$) Possiamo scrivere $\alpha = s + t\beta$ con s, $t \in \mathbb{Q}_2$. Elevando entrambe i membri di questa identità al quadrato si ha $\alpha^2 = s^2 + t^2\beta^2 + 2st\beta$, ossia $s^2 + t^2\beta^2 - \alpha^2 + 2st\beta = 0$. Poiché α^2, $\beta^2 \in \mathbb{Z}_2$ e $\{1, \beta\}$ costituisce una base per $\mathbb{Q}_2(\beta)$, si deve avere $s^2 + t^2\beta^2 = \alpha^2$ e $2st = 0$. Da quest'ultima si ha che almeno uno tra s e t deve essere 0 (la caratteristica di $\mathbb{Q}_2$ è 0!). Supponiamo che $t = 0$: allora $\alpha = s \in \mathbb{Q}_2$ che è contro le ipotesi. Allora deve essere $s = 0$ e quindi, dalla prima delle due equazioni precedenti, $t^2 = \alpha/\beta$. Moltiplicando entrambi i membri per β^2, si ha che $\alpha\beta = t^2\beta^2 \in \mathbb{Q}_2$. Quindi $\alpha\beta$ è un elemento di $\mathbb{Q}_2$ che è intero su $\mathbb{Z}_2$ (perché prodotto di elementi interi). Quindi $\alpha\beta \in \mathbb{Z}_2$.
($\Leftarrow$) $\alpha\beta \in \mathbb{Q}_2 \subset \mathbb{Q}_2(\alpha)$. Allora $\beta \in \mathbb{Q}_2(\alpha)$ e dall'uguaglianza dei gradi $\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\beta)$. □

Considerazione
Osserviamo esplicitamente che la condizione dell'osservazione precedente è a sua volta evidentemente equivalente alla condizione che $\alpha^2\beta^2$ sia un quadrato in $\mathbb{Z}_2$.

Osservazione 2.1.5 *Sia $2^k(1+2u) = \delta \in \mathbb{Z}_2$, con $u \in \mathbb{Z}_2$ e $k \in \mathbb{N}_0$. Allora esiste $2^h(1+2v) = \epsilon \in \mathbb{Z}$, con $v \in \mathbb{Z}$ e $h \in \mathbb{N}_0$, tale che $\mathbb{Q}_2(\sqrt[2]{\delta}) = \mathbb{Q}_2(\sqrt[2]{\epsilon})$.*

Dimostrazione Alla luce della considerazione precedente, ci basta di trovare un $\epsilon \in \mathbb{Z}$ tale che $\delta\epsilon$ sia un quadrato in $\mathbb{Z}_2$. Se $\epsilon = 2^h(1+2c)$, con $v \in \mathbb{Z}$ e $h \in \mathbb{N}_0$, per la descrizione dei quadrati di $\mathbb{Z}_2$, bisogna richiedere che $h+k \equiv 0\ (mod\, 2)$ e $2uv+u+v \in (2)^2$. Scegliamo allora $h \in \mathbb{N}_0$, tale che $h+k \equiv 0\ (mod\, 2)$, cosa che è chiaramente sempre possibile. Se $u = 1+2t$ con $t \in \mathbb{Z}_2$ e $t \notin (2)$, scegliendo $v = 3$ otteniamo quanto voluto, mentre se $t \in (2)$, una scelta possibile è $v = 1$. Se invece $u = 2t$ con $t \in \mathbb{Z}_2$ e $t \notin (2)$, possiamo prendere $v = 2$ e se $t \in (2)$, scegliamo $v = 4$. □

Sia $E = \{\delta \in \mathbb{Z} \mid \delta \text{ non è un quadrato}\}$. Mettiamo su E la seguente relazione d'equivalenza

$$\delta_1 \sim \delta_2 \qquad \Leftrightarrow \qquad \mathbb{Q}_2(\sqrt[2]{\delta_1}) = \mathbb{Q}_2(\sqrt[2]{\delta_2})$$

e sia $\mathcal{E}$ l'insieme quoziente. Allora $\mathcal{E}$, per quanto fin qui mostrato, è in corrispondenza biunivoca con l'insieme delle estensioni di grado 2 su $\mathbb{Q}_2$. Proviamo ad esibire dei rappresentanti per gli elementi di $\mathcal{E}$. Cerchiamo dunque elementi $\delta \in \mathbb{Z}$ tali che $\delta = 2^k(1+2s)$ con $k \in \mathbb{N}_0$ e $s \in \mathbb{Z}$ e $2 \nmid k$ oppure $4 \nmid s$ e prendendo uno solo tra δ e $\delta' = 2^h(1+2t)$ se $k+h \equiv 0\,(mod\, 2)$ e $s+t+2st \equiv 0\,(mod\, 4)$. Allora è chiaro che basta, per quanto riguarda k, considerare i casi $k = 0$, 1. Inoltre, fissato $k = h$, $\delta \sim \delta'$ se e solo se $s \equiv t\ (mod\, 4)$. Infatti

$$s+t+2st \equiv 0 \pmod 4 \qquad \Leftrightarrow \qquad t \equiv -s(2s+1)^{-1} \pmod 4$$

ma, qualunque sia s, si ha

$$s \equiv -s(2s+1)^{-1} \pmod 4$$

Quindi, fissato k, basta considerare i casi $s = 0$, 1, 2, 3. Allora, se $k = 0$, poiché deve essere $4 \nmid s$, i casi che ci interessano sono $s = 1$, 2, 3, cioè $\delta = 3$, 5, 7. Se invece $k = 1$, non ci sono condizioni su s e quindi $\delta = 2$, 6, 10, 14. Per avere dei rappresentanti più comodi da ricordare, possiamo osservare che $3 \sim -5$, $7 \sim -1$, $6 \sim -10$ e $14 \sim -2$. Raccogliamo quanto finora provato in un unico risultato.

Proposizione 2.1.1 *Ci sono esattamente sette estensioni $\mathbf{K}$ di grado 2 di $\mathbb{Q}_2$. Ognuna di esse è del tipo $\mathbf{K} = \mathbb{Q}_2(\sqrt[2]{\delta})$ con δ un elemento di $\mathcal{E} = \{-1, 2, -2, 5, -5, 10, -10\}$. L'estensione non ramificata di grado 2 è $\mathbb{Q}_2(\sqrt[2]{5}) = \mathbb{Q}_2(\zeta)$ dove ζ è una radice terza primitiva dell'unità. Infine, se indichiamo con $\mathcal{D}_{\mathbf{K}}$ il differente di $\mathbf{K} = \mathbb{Q}_2(\sqrt[2]{\delta})$ su $\mathbb{Q}_2$, si avrà che*

$$\begin{array}{lcll} v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) & = & 3 & \text{se } \delta = 2, -2, 10, -10 \\ v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) & = & 2 & \text{se } \delta = -1, -5 \\ v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) & = & 0 & \text{se } \delta = 5 \end{array}$$

Dimostrazione Le uniche cose da dimostrare sono le ultime affermazioni. L'estensione non ramificata di grado 2 di $\mathbb{Q}_2$ si ottiene aggiungendo a $\mathbb{Q}_2$ una radice terza primitiva dell'unità, cioè una soluzione del polinomio X^2+X+1 oppure equivalentemente la radice del suo discriminante che è $\sqrt[2]{-3}$. È facile osservare che $-3 \sim 5$, quindi si ottiene la tesi.
Le considerazioni sul differente sono conseguenza della formula che lega il differente alla

derivata prima del polinomio minimo $f(X)$ su $\mathbb{Q}_2$ di un elemento intero x su $\mathbb{Z}_2$ che generi l'anello degli interi di $\mathbf{L}$ come $\mathbb{Z}_2$-algebra.

$$v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) = v_{\mathbf{K}}(f'(x))$$

Nei casi $\delta = 2, -2, 10, -10$ si sceglie semplicemente $x = \delta$; nel caso $\delta = -1$ si prende $f(X) = X^2 + 2X + 2$ (e $x = \sqrt[2]{-1} + 1$) mentre se $\delta = -5$ si prende $f(X) = X^2 + 2X - 2$ (e $x = \sqrt[2]{3} + 1$, ricordando che $-5 \sim 3$). □

2.2 Il caso $p \neq 2$

Osservazione 2.2.1 *Le estensioni* $\mathbf{K}$ *di grado* p *su* $\mathbb{Q}_p$ *sono* $p^3 - p^2 + p + 1$. *Tra queste,* $p + 1$ *sono di Galois.*

Dimostrazione Ponendo, nella formula di Krasner, $m = h = 1$ e $N = p$, si ottiene la prima parte della tesi. Osserviamo che una estensione di Galois di grado p su $\mathbb{Q}_p$ non può che avere gruppo di Galois isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Utilizzando allora la formula di Šafarevič (e ricordando che $|Aut(\mathbb{Z}/p\mathbb{Z})| = p - 1$), si ottiene la tesi. □

Tabella 2.1: *estensioni di Galois di grado* p *su* $\mathbb{Q}_p$

Numero di estensioni $\mathbf{K}$	$e(\mathbf{K}\|\mathbb{Q}_p)$	$f(\mathbf{K}\|\mathbb{Q}_p)$	$G(\mathbf{K}/\mathbb{Q}_p)$	$v_{\mathbf{K}}(\mathcal{D})$
1	1	p	$\mathbb{Z}/p\mathbb{Z}$	0
p	p	1	$\mathbb{Z}/p\mathbb{Z}$	$2p-2$

Tabella 2.2: *estensioni di grado* p *su* $\mathbb{Q}_p$*: classificazione in base al differente*

Numero di estensioni $\mathbf{K}$	$e(\mathbf{K}\|\mathbb{Q}_p)$	$f(\mathbf{K}\|\mathbb{Q}_p)$	$v_{\mathbf{K}}(\mathcal{D})$
1	1	p	0
$p(p-1)$	p	1	p
$p(p-1)$	p	1	$p+1$
$p(p-1)$	p	1	$p+2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
p^2	p	1	$2p-1$

Osservazione 2.2.2 *Sia* $\mathbf{K}$ *un'estensione di grado* p *su* $\mathbb{Q}_p$ *totalmente ramificata. Allora* $p \leq v_{\mathbf{K}}(\mathcal{D}) \leq 2p-1$. *Inoltre il numero di estensioni* $\mathbf{K}$ *con un certo* $v_{\mathbf{K}}(\mathcal{D})$ *è quello riportato nella tabella.*

Dimostrazione Sia $c(\mathbf{K}) = v_{\mathbf{K}}(\mathcal{D}) - p + 1$. Le condizioni di Ore forniscono la seguente limitazione su $c(\mathbf{K})$

$$pv_p(l) \leq c(\mathbf{K}) \leq pv_p(p) = p$$

dove l è l'intero compreso tra 1 e p tale che $c(\mathbf{K}) \equiv l \,(mod\, p)$. I possibili valori per $c(\mathbf{K})$ sono allora gli interi compresi tra 1 e p. Di conseguenza i possibili valori per $v_{\mathbf{K}}(\mathcal{D})$

sono quelli della tesi. Dalla formula di Serre, si ricava che il numero di estensioni con $c = p$ è p^2; per ogni $c < p$ ci sono invece $p(p-1)$ estensioni. Questo risultato conferma il computo del numero delle estensioni di grado p su $\mathbb{Q}_p$: infatti, ricordandosi di contare anche l'unica estensione non ramificata,

$$p^3 - p^2 + p + 1 = \left(\sum_{c=1}^{p-1} \mathfrak{N}_{p,\,c}^{\mathbb{Q}_p} \right) + p^2 + 1$$

□

Cerchiamo di capire quale sia il gruppo di Galois della chiusura normale di una certa estensione di grado p su $\mathbb{Q}_p$. Siamo interessati in modo particolare alle estensioni totalmente ramificate di grado p, giacché l'unica estensione non ramificata (di grado p) è di Galois ciclica. Richiamiamo a tal proposito, per comodità del lettore, alcune notazioni e convenzioni presenti in [Am 71].
Le estensioni totalmente ramificate di grado p di $\mathbb{Q}_p$ si ottengono aggiungendo a $\mathbb{Q}_p$ una radice di un polinomio di Eisenstein di grado p, cioè un polinomio del tipo

$$f(X) = X^p - \sum_{i=1}^{p-1} a_i X^i - p a_0$$

$$v(a_0) = 0 \qquad \text{e} \qquad v(a_i) \geq 1 \quad \text{se} \quad 1 \leq i \leq p-1$$

(abbiamo indicato con v la valutazione su $\mathbb{Q}_p$ per cui $v(p) = 1$, cioè quella che fin qui era v_p). Sia Π una radice di $f(X)$ e poniamo $\mathbf{K} = \mathbb{Q}_p(\Pi)$. Per ragioni tecniche, in [Am 71], si suppone inoltre che

$$\Pi^p \equiv N_{\mathbf{K}}(\Pi) \equiv p \pmod{p^2}$$

(rimpiazzando Π con $\xi\Pi$ per un opportuno $\xi \in \mathbb{Q}_p$). In particolare questo implica $a_0 \equiv 1 \pmod{p}$.
Per un polinomio della forma di $f(X)$ possiamo definire il *tipo* come segue:

1. se $\min_{1 \leq i \leq p-1} v(a_i) = 1$, denotiamo con λ il minimo intero tale che $v(a_\lambda) = 1$ e scegliamo $\omega \neq 0$ nel campo residuo di $\mathbb{Q}_p$ (cioè in $\mathbb{F}_p$)[1] tale che $a_\lambda \equiv \omega p \pmod{p^2}$. In questo caso diremo che $f(X)$ è di tipo $<\lambda, \omega>$;

2. se $v(a_i) \geq 2$ per ogni $1 \leq i \leq p-1$ diremo che $f(X)$ è di tipo $<0>$ (convenendo di porre in questo caso $\lambda = 0$)[2].

Non è difficile verificare che nel caso $<\lambda, \omega>$ si ha

$$v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) = p v(f'(\Pi)) = p \min\{v(p\Pi^{p-1}),\, v(a_{p-1}\Pi^{p-2}),\, \ldots,\, 1\} = p(1 + \frac{\lambda - 1}{p}) = p + \lambda - 1$$

[1] ω sarà indifferentemente considerato come un elemento del campo residuo oppure un elemento di $\mathbb{Z} \subset \mathbb{Z}_p$. Conveniamo a tal proposito che sia $1 \leq \omega \leq p-1$.

[2] La notazione in [Am 71] è leggermente diversa: studiando estensioni di grado p di un'estensione k di $\mathbb{Q}_p$ è utile considerare l'indice i ramificazione $e = e(k|\mathbb{Q}_p)$: se $\min_{1 \leq i \leq p-1} v(a_i) = m \leq e$ si ha il tipo $<\lambda,\, m,\, \omega>$; se invece $v(a_i) \geq e+1 \quad \forall\, 1 \leq i \leq p-1$ si ha il tipo $<0>$ (in questo caso si sceglie $m = e+1$). Nel nostro caso $k = \mathbb{Q}_p$ e in particolare $e = 1$, quindi l'indice m nel primo tipo è sempre 1 e dunque si può omettere. Anche in alcune definizioni successive verrà utilizzata la stessa semplificazione.

(la seconda uguaglianza vale perché $v(i) = 0$ se $1 \leq i \leq p-1$ e i valori tra i quali si cerca il minimo sono tutti diversi fra loro), mentre nel caso $<0>$

$$v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) = pv(f'(\Pi)) = p(1 - \frac{p-1}{p}) = 2p-1$$

(si ragiona come nel caso precedente). In questo modo ritroviamo parzialmente quanto dimostrato nell'osservazione 2.2.2: in particolare le estensioni di tipo $<0>$ sono tutte e sole quelle con $v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}}) = 2p-1$. Mettiamoci per un attimo nel caso $<\lambda, \omega>$ e poniamo $I = \{i \in \mathbb{Z} \mid 1 \leq i \leq [\frac{\lambda}{p-1}],\ p \nmid i+\lambda\}$ e definiamo, sempre seguendo [Am 71], $\mathfrak{M}(\lambda)$ come l'insieme degli elementi di $\mathbb{Z}_p$ che si possono scrivere nella forma

$$1 + \sum_I \alpha_i p^i \quad \alpha_i \in \mathbb{F}_p$$

Non è difficile riconoscere che in ogni caso $I = \emptyset$ e quindi $\mathfrak{M}(\lambda) = \{1\}$. Per i λ tali che $p-1 \nmid \lambda$ (cioè $\lambda \neq p-1$, essendo $1 \leq \lambda \leq p-1$) c'è una corrisondenza biunivoca tra $\mathfrak{M}(\lambda)$ e l'insieme delle classi di estensioni coniugate di tipo $<\lambda, \omega>$ e tale corrispondenza è data da

$$a \longleftrightarrow [\mathbb{Q}_p(\Pi)] \quad \text{con } \Pi \text{ radice di } X^p - \omega p X^\lambda - pa$$

Inoltre, nel caso in cui $\lambda \equiv 0\ (mod\,(p-1))$ (cioè $\lambda = p-1$) ma $\sqrt[p-1]{\lambda\omega} \notin \mathbb{Q}_p$, vale ancora tale corrispondenza biunivoca.
Possiamo calcolare a questo punto, facendo opportunamente variare λ e ω il numero di estensioni di tipo $<\lambda, \omega>$

Tabella 2.3: *estensioni di tipo* $<\lambda, \omega>$

Caratteristiche	Numero
$\lambda \neq p-1$	$p(p-2)(p-1)$
$\lambda = p-1$ e $\sqrt[p-1]{\lambda\omega} \notin \mathbb{Q}_p$	$p(p-2)$
$\lambda = p-1$ e $\sqrt[p-1]{\lambda\omega} \in \mathbb{Q}_p$	p

Non è difficile riconoscere che i dati della tabella sono corretti: in primo luogo, dimostreremo più avanti che solo nell'ultimo caso (cioè $\lambda = p-1$ e $\sqrt[p-1]{\lambda\omega} \in \mathbb{Q}_p$) le estensioni sono di Galois (cicliche). Quindi nei primi due casi ogni classe di estensioni coniugate contiene esattamente p estensioni (e questa è la ragione del fattore p nella prima e seconda riga della seconda colonna). Vediamo ora per quali ω il polinomio

$$g(X) = X^{p-1} - (p-1)\omega$$

ha una radice in $\mathbb{Q}_p$ (ossia $\sqrt[p-1]{\lambda\omega} \in \mathbb{Q}_p$ nel caso $\lambda = p-1$). Riducendo modulo p si osserva che $\overline{g(X)}$ ha radici se e solo se $\omega = \overline{-1}$. Siamo d'altra parte nella ipotesi del lemma di Hensel (perché $\omega \neq 0$). Quindi $g(X)$ ha una radice in $\mathbb{Q}_p$ se e solo se $\omega = p-1$. In questo modo si completa la giustificazione del computo del numero di estensioni con $\lambda = p-1$ e $\sqrt[p-1]{\lambda\omega} \notin \mathbb{Q}_p$. L'ultimo caso si presenta p volte perché si tratta delle estensioni totalmente ramificate di Galois (che sappiamo essere in tutto p) e non vi sono (come dimostriamo subito) estensioni di Galois di tipo $<0>$.
Per quanto riguarda invece il caso $<0>$, possiamo distinguere due casi: quello in cui tutte le radici di $f(X)$ siano in un'unica estensione di grado p (cioè il caso di Galois) e quello in cui questo non accade. Il primo caso in realtà non si verifica perché le estensioni

di Galois hanno valutazione del differente pari a $2p-2$ mentre per quelle di tipo $<0>$ la valutazione del differente è $2p-1$; inoltre le estensioni la valutazione del cui differente è $2p-1$ sono tutte e sole quelle di tipo $<0>$ quindi ci sono p^2 estensioni di tipo $<0>$ (perché ce ne sono esattamente p^2 con valutazione del differente pari a $2p-1$).

Tabella 2.4: *estensioni di tipo* $<0>$

Caratteristiche	Numero
di Galois	0
non di Galois	p^2

Veniamo ora ad alcune considerazioni sul campo di spezzamento $\mathbf{L}$ di una estensione $\mathbf{K} = \mathbb{Q}_p(\Pi)$ (al solito, Π è una radice del polinomio $f(X)$) di grado p su $\mathbb{Q}_p$ e sulla struttura di $G = G(\mathbf{L}|\mathbb{Q}_p)$. Anche qui c'è una caratterizzazione che dipende dal tipo di $f(X)$:

- tipo $<\lambda, \omega>$: $\mathbf{L} = \mathbb{Q}_p(\Gamma, \Pi)$ con $\Gamma \in \overline{\mathbb{Q}_p}$ tale che $\Gamma^{p-1} = \lambda\omega p^{\lambda}$;
- tipo $<0>$: $\mathbf{L} = \mathbb{Q}_p(\Gamma_0, \Pi)$ con $\Gamma_0 \in \overline{\mathbb{Q}_p}$ tale che $\Gamma_0^{p-1} = -p$

Osserviamo in primo luogo che il polinomio $Y^{p-1} + p$ è irriducibile per il criterio di Eisenstein, quindi $[\mathbb{Q}_p(\Gamma_0) : \mathbb{Q}_p] = p-1$ e dunque, essendo $(p, p-1) = 1$, nel caso $<0>$ si ha $[\mathbf{L} : \mathbb{Q}_p] = p(p-1)$.

Analogamente, nel caso $<\lambda, \omega>$ si ha $[\mathbf{L} : \mathbb{Q}_p] = pd$ con $d = [\mathbb{Q}_p(\Gamma) : \mathbb{Q}_p]$, solo che adesso d può essere minore di $p-1$ (in generale dipenderà da λ e da ω). Nel caso in cui $\mathbf{K}$ sia ottenuta aggiungendo una radice di un polinomio con $\lambda = p-1$ e $\sqrt[p-1]{\lambda\omega} \in \mathbb{Q}_p$, si vede subito che $[\mathbf{L} : \mathbb{Q}_p] = p$ e quindi $\mathbf{K}$ sarà un'estensione di Galois. Viceversa se $\mathbf{K}$ è un'estensione di Galois, deve essere $d = 1$ e quindi $\sqrt[p-1]{\lambda\omega} \in \mathbb{Q}_p$. Questo è possibile solo se $\lambda = p-1$ (vedi [Am 71]). Quindi le estensioni di Galois totalmente ramificate di grado p sono tutte e sole quelle con $\lambda = p-1$ e $\sqrt[p-1]{\lambda\omega} \in \mathbb{Q}_p$.

Per quanto riguarda, più in generale, il gruppo di Galois di $\mathbf{L}$ sappiamo, sia nel caso $<0>$ che nel caso $<\lambda, \omega>$, che deve essere un sottogruppo transitivo di S_p di ordine minore o uguale a $p(p-1)$ e divisibile per p. Inoltre G è il gruppo di Galois di un'estensione di campi locali, quindi è risolubile (cfr. [Se]). Molto è noto riguardo a questa situazione: richiamiamo alcune definizioni (per quanto segue cfr. [Ar]).

Definizione 2.2.1 *Una permutazione σ dei numeri $1, 2, \ldots, p$ (cioè $\sigma \in S_p$) si dice una* sostituzione lineare (s. l.) modulo p *se esistono due numeri interi b e c con $p \nmid b$ tali che $\sigma(i) \equiv bi + c \pmod p$, $i = 1, 2, \ldots, p$.*

Osserviamo esplicitamente che una funzione τ da $\{1, 2, \ldots, p\}$ in sé tale che esistano due numeri b e c con $p \nmid b$ tali che $\tau(i) \equiv bi + c \pmod p$, $i = 1, 2, \ldots, p$ è necessariamente una permutazione, cioè $\tau \in S_p$. Inoltre due permutazioni, σ_1 e σ_2, che soddisfino la stessa regola (vale a dire $\sigma_1(i) \equiv \sigma_2 \equiv bi + c \pmod p$, $i = 1, 2, \ldots, p$), sono uguali. È immediato osservare che le s. l. modulo p costituiscono un sottogruppo L_p di S_p di ordine $p(p-1)$ che contiene il p-ciclo $(1\,2 \ldots p)$ che è il sottogruppo di tutte le sostituzioni del tipo $\sigma(i) \equiv i + c \pmod p$, $c = 1, 2, \ldots, p$ che è effettivamente un sottogruppo di ordine p (un generatore è σ tale che $\sigma(i) \equiv i + 1$). Vale allora il seguente teorema.

Teorema 2.2.1 *Sia $f(X)$ un polinomio irriducibile di grado p primo a coefficienti in un campo $\mathbf{F}$. Il gruppo G di $f(X)$ (che è un gruppo di permutazioni delle radici o equivalentemente dei numeri $i = 1, 2, \ldots, p$) è risolubile se e solo se, eventualmente dopo un opportuno cambio nella numerazione delle radici di $f(X)$, G è un gruppo di sostituzioni lineari modulo p e in G sono presenti tutte le sostituzioni lineari del tipo $\sigma(i) \equiv i + c \ (mod\, p)$, $c = 1, 2, \ldots, p$ (cioè $b = 1$).*

Dimostrazione (vedi [Ar]). □

Avendo a disposizione questo teorema, riusciamo a dire quale è il gruppo di Galois di $\mathbf{L}$. Nel caso $< 0 >$ si ha $G = L_p$, perché $[\mathbf{L} : \mathbb{Q}_p] = p(p-1)$. Nel caso $< \lambda, \omega >$, G sarà un sottogruppo proprio di L_p, risolubile e transitivo rispetto all'azione di S_p. Quindi sarà un gruppo di s. l. modulo p che contiene tutte le permutazioni del tipo $\sigma(i) \equiv i + c \ (mod\, p)$, $c = 1, 2, \ldots, p$ (cioè $b = 1$). Vediamo come possono essere fatti tali sottogruppi di L_p. Osserviamo che vale la seguente regola di composizione

$$\sigma(i) \equiv b_\sigma i + c_\sigma \ (mod\, p) \qquad \tau(i) \equiv b_\tau i + c_\tau \ (mod\, p)$$

$$\sigma\tau(i) \equiv b_\sigma b_\tau i + b_\sigma c_\tau + c_\sigma \ (mod\, p) \tag{2.1}$$

Osservazione 2.2.3 *Sia β un generatore di $(\mathbb{Z}/p\mathbb{Z})^*$. Allora i sottogruppi di L_p che contengono tutte le permutazioni del tipo $\sigma(i) \equiv i + c \ (mod\, p)$ per $c = 1, 2, \ldots, p$, sono del tipo*

$$L_{p,\,s} = \{\sigma \in L_p | \sigma(i) \equiv \beta^{sh} i + c \ (mod\, p),\ h = 0, 1, \ldots, p-1,\ c = 1, 2, \ldots, p\}$$

al variare di $s = 0, 1 \ldots p-1$, e quindi sono in corrispondenza biunivoca con i sottogruppi di $(\mathbb{Z}/p\mathbb{Z})^*$ la corrispondenza essendo data da

$$L_{p,\,s} \quad \longleftrightarrow \quad C_{p,\,s} = < \beta^s > \subseteq (\mathbb{Z}/p\mathbb{Z})^*$$

Infine, $L_{p,\,s}$ ha $p\frac{p-1}{(p-1,s)}$ elementi e, se poniamo

$$K_s = \{\sigma \in L_p | \sigma(i) \equiv \beta^{sh} i \ (mod\, p),\ h = 0, 1, \ldots, p-1\}$$

si ha che K_s è un sottogruppo di $L_{p,\,s}$ e

$$L_{p,\,s} \cong L_{p,\,0} \ltimes K_s$$

Dimostrazione Intanto, in virtù di (2.1), è chiaro che $L_{p,\,s}$ è effettivamente un sottogruppo e naturalmente contiene anche

$$L_{p,\,0} = \{\sigma \in L_p \,|\, \sigma(i) \equiv i + c \ (mod\, p), c = 1, 2, \ldots, p\}$$

e K_s, che fra l'altro è un sottogruppo ciclico generato da $\sigma(i) \equiv \beta^s i \ (mod\, p)$. Non è difficile verificare che $L_{p,\,0}$ è un sottogruppo normale in $L_{p,\,s}$ che ha intersezione banale con K_s e con quest'ultimo genera $L_{p,\,s}$. Quindi otteniamo l'ultima affermazione.
Sia ora L un sottogruppo di L_p nelle ipotesi. Una permutazione σ in L_p è individuata univocamente da c e da s: più precisamente indicheremo con $\sigma_{s,\,c}$ la permutazione tale che $\sigma_{s,\,c}(i) \equiv \beta^s i + c$. Sia $E = \{s \neq 0 | \exists\, c_0 \text{ tale che } \sigma_{s,\,c_0} \in L\}$ e sia $s_0 = \min_{s \in E} s$. Dico allora che $L = L_{p,\,s_0}$. In primo luogo $\sigma_{s_0,\,0} \in L$ (come si vede componendo $\sigma_{s_0,\,c}$ per

un opportuno $\tau \in L_{p,0}$). Quindi $L_{p,s_0} =< L_{p,0}, K_{s_0} >\subseteq L$. Se per assurdo ci fosse un elemento di L non contenuto in L_{p,s_0}, esso sarebbe della forma $\sigma_{s,c}$ con $s > s_0$ e $s_0 \nmid s$. Possiamo inoltre suppore, come prima, che anche $\sigma_{s,0} \in L$. Sia allora $d = (s, s_0)$ (in particolare $d < s_0$) e siano t e r tali che $ts + rs_0 = d$: $\sigma_{rs_0,0}\sigma_{ts,0} = \sigma_{d,0} \in L$, contro l'ipotesi di minimalità di s_0. A questo punto, la verifica della corrispondenza è banale. L'affermazione sulla cardinalità segue dalle considerazioni fatte prima dell'enunciato del teorema. □

È necessario a questo punto tornare allo studio di **L**. Studiamo con più attenzione il caso $< \lambda, \omega >$. Poniamo (cfr. [Am 71]) $d = (p-1, \lambda)$ e $p - 1 = \alpha(\lambda, \omega)d$. Si prova facilmente allora che esiste $\theta \in \mathbf{L}$ tale che $\theta^d = \lambda\omega$. Se inoltre poniamo $\mathbf{V} = \mathbb{Q}_p(\Gamma)$ e $\mathbf{T} = \mathbb{Q}_p(\theta)$, non è difficile verificare che **T** è la massima sottoestensione non ramificata di **L** su $\mathbb{Q}_p$ e che **V** è la massima sottoestensione debolmente ramificata di **L** su $\mathbb{Q}_p$. Inoltre, in particolare, $\mathbf{T} \subseteq \mathbf{V}$ e $[\mathbf{V} : \mathbf{T}] = \alpha(\lambda, \omega)$. Se allora poniamo $\beta(\lambda, \omega) = [\mathbf{T} : \mathbb{Q}_p]$, si ha che $[\mathbf{L} : \mathbb{Q}_p] = p\beta(\lambda, \omega)\alpha(\lambda, \omega)$.

Lemma 2.2.1 *Sia $a \in \mathbb{Z}_p$ e indichiamo con $[a]$ la classe resto modulo (p) di a. Supponiamo che $[a] \neq [0]$ e sia $n \in \mathbb{N}$ tale che $n \mid (p-1)$. Indichiamo inoltre con m l'ordine di $[a]$ in $(\mathbb{Z}/p\mathbb{Z})^*$ e $mt = p - 1$. Allora il polinomio $X^n - a$ si spezza completamente in $\mathbb{Q}_p[X]$ se e solo se $n \mid t$.*

Dimostrazione Osserviamo in primo luogo che, poiché $n \mid (p-1)$, il polinomio $X^n - a$ si spezza completamente in $\mathbb{Q}_p[X]$ se e solo se ha una radice in $\mathbb{Q}_p$, perché $\mathbb{Q}_p$ contiene le radici $(p-1)$-esime (e di conseguenza quelle n-esime).
Supponiamo ora che $X^n - a$ abbia una radice in $\mathbb{Q}_p$, ossia che esista $\gamma \in \mathbb{Q}_p$ tale che $\gamma^n = a$. Ovviamente allora $\gamma \notin (p)$, altrimenti $a \equiv 0 \ (mod\, p)$. Il primo termine dello sviluppo in serie di potenze di γ è allora un elemento b_0 che appartiene a $\mathbb{F}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^*$ e vale $b_0^n \equiv a \ (mod\, p)$: in particolare $[a]$ è una potenza n-esima in $(\mathbb{Z}/p\mathbb{Z})^*$. Allora $n \mid t$. Infatti, sia β un generatore per $(\mathbb{Z}/p\mathbb{Z})^*$: possiamo scrivere per un opportuno k che $b_0 \equiv \beta^k$ e quindi $a \equiv \beta^{kn}$. Quindi $m = \frac{p-1}{(p-1,kn)}$, quindi in particolare, essendo $n \mid (p-1)$, si ha che $n \mid t$. Viceversa supponiamo che $n \mid t$. Riduciamo modulo p il polinomio $X^n - a$. Sappiamo che esiste h tale che $m = \frac{p-1}{hn}$. Scegliendo un generatore β per $(\mathbb{Z}/p\mathbb{Z})^*$ possiamo scrivere che $[a] = \beta^{hn}$. Quindi $X^n - [a]$ ha una radice in $(\mathbb{Z}/p\mathbb{Z})^*$. Possiamo allora applicare il criterio di Hensel, perché $X^n - [a]$ non ha radici in comune con la sua derivata (se n è uguale a 1, la tesi è banale) e concludere. □

Osservazione 2.2.4 *Sia m l'ordine di $\lambda\omega$ in $(\mathbb{Z}/p\mathbb{Z})^*$ e $mt = p - 1$. Il grado di **T** su $\mathbb{Q}_p$ è $\beta(\lambda, \omega) = \frac{d}{(t,d)}$.*

Dimostrazione Analizziamo il polinomio $X^d - \lambda\omega$. In primo luogo **T** è il campo di spezzamento di tale polinomio perché le radici d-esime dell'unità sono contenute in $\mathbb{Q}_p$. Poniamo $r = (t, d)$, $r_d r = d$ e $r_t r = t$ (in particolare $(r_d, r_t) = 1$): allora per il lemma precedente (con $n = t$) le radici t-esime di $\lambda\omega$ sono in $\mathbb{Q}_p$ e quindi la seguente fattorizzazione

$$X^d - \lambda\omega = \left(X^{r_d} - (\sqrt[t]{\lambda\omega})^{r_t}\right)\left(X^{r_d} - \xi_r(\sqrt[t]{\lambda\omega})^{r_t}\right)\ldots\left(X^{r_d} - \xi_r^{r-1}(\sqrt[t]{\lambda\omega})^{r_t}\right)$$

è in $\mathbb{Q}_p[X]$ (ξ_r indica una radice r-esima primitiva dell'unità). Il primo fattore della precedente fattorizzazione è irriducibile. Infatti, poniamo per semplicità $a = (\sqrt[t]{\lambda\omega})^{r_t}$.

Si tratta dunque di mostrare che il polinomio $f(X) = X^{r_d} - a$ è irriducibile. Supponiamo che $g(X) \in \mathbb{Q}_p[X]$ sia un fattore non costante presente nella fattorizzazione di $f(X)$. Il termine noto di $g(X)$ sarà il prodotto di certe radici di $f(X)$, diciamo di h di esse. Quindi sarà della forma $\xi_{r_d}^k a^{h/r_d}$ per un certo $k \in \mathbb{N}$ e abbiamo indicato come al solito con ξ_{r_d} una radice r_d-esima primitiva dell'unità. Poichè $\xi_{r_d} \in \mathbb{Q}_p$ (perché $r_d \mid p-1$), si ha che a^{h/r_d} deve appartenere a $\mathbb{Q}_p$. Questo significa che l'equazione $X^{r_d} - a^h = 0$ ha soluzioni in $\mathbb{Q}_p$. Poniamo $k_t = \frac{p-1}{r_t}$ ($t \mid (p-1)$ e quindi $r_t \mid (p-1)$). Poiché l'ordine della classe di a^h è $\frac{k_t}{(k_t,h)}$, dal lemma precedente si ha che $r_d \mid (k_t, h) r_t$ ed, essendo $(r_d, r_t) = 1$, $r_d \mid (k_t, h)$. Quindi, in particolare, $r_d \mid h$. Allora $r_d = h$, di conseguenza $g(X)$ ha per radici tutte le radici di $f(X)$ e quindi $g(X) = f(X)$. Il campo di spezzamento di $f(X)$ contiene i campi di spezzamento degli altri fattori (perché $\xi_r^{1/r_d} = \xi_{r r_d} \in \mathbb{Q}_p$). Quindi il campo di spezzamento di $X^d - \lambda\omega$ è quello di $f(X)$. Più precisamente, detta α una radice di $f(X)$ si ha che

$$\mathbf{T} = \text{c. di s. di}\,(X^d - \lambda\omega) = \text{c. di s. di}\, f(X) = \mathbb{Q}_p(\alpha)$$

Quindi $[\mathbf{T} : \mathbb{Q}_p] = \deg f(X) = r_d = \frac{d}{(d,t)}$. □

Rimettendo insieme tutti i pezzi, si riconosce che il gruppo di Galois di un'estensione di tipo $<\lambda, \omega>$ è $L_{p,\,s}$ con $s = (t, d)$. Inoltre il sottogruppo d'inerzia di $L_{p,\,s}$ è $L_{p,\,\lambda}$ (dall'osservazione (2.2.3), ricordando che il sottogruppo d'inerzia di $L_{p,\,s}$ contiene $L_{p,\,0}$, è risolubile e ha cardinalità $p\alpha(\lambda, \omega) = p\frac{p-1}{(p-1,\lambda)}$).
Per quanto riguarda il caso $<0>$, sappiamo che $G = L_p = L_{p,\,1}$ (ancora una conferma che non ci sono estensioni di Galois di tipo $<0>$). Soffermiamoci un attimo a studiare la forma dei polinomi che danno origine ad estensioni di tipo $<0>$ (vedi [Am 71], anche per ciò che segue): si dimostra che i polinomi del tipo $X^p - pa$ ($a \in \mathbb{Q}_p$) generano questo tipo di estensioni e che $X^p - pa$ e $X^p - pb$ generano la stessa estensione se e solo se esiste un elemento $u \in \mathbb{Q}_p$ tale che $b = au^p$. Da questo si deduce che l'insieme dei polinomi che generano le estensioni di tipo $<0>$ è in corrispondenza biunivoca con $U_1/U_1^p \cong \mathbb{Z}/p\mathbb{Z}$ dove, come nel capitolo 1, U_1 indica il sottogruppo di $\mathbb{Z}_p^*$ costituito dagli elementi u tali che $u \equiv 1\,(mod\,p)$. Quindi i polinomi che cerchiamo sono quelli del tipo $X^p - p(1 + ap)$ per $a = 0, 1, \ldots, p-1$. È chiaro a questo punto che, se $\mathbf{K}$ è di tipo $<0>$, la sua chiusura normale $\mathbf{L}$ è totalmente ramificata su $\mathbb{Q}_p$, quindi il sottogruppo d'inerzia di G è G stesso (se ζ_p come al solito è una radice p-esima primitiva dell'unità, $\mathbb{Q}_p(\zeta_p)$ è totalmente ramificata di grado $p-1$, vedi [Se], e $\mathbf{L}$ è totalmente ramificata di grado p su $\mathbb{Q}_p(\zeta_p)$).
Un'analoga ricerca dei polinomi generatori può essere condotta anche per le estensioni di Galois totalmente ramificate, cioè quelle del tipo $<\lambda, \omega>$ con $\lambda = p-1$ e $\omega = p-1$. Anche qui, con ragionamenti simili a quelli che hanno portato a determinare i polinomi nel caso $<\lambda, \omega>$ generico, si arriva a dire che i polinomi che ci interessano sono quelli del tipo $X^p - p(p-1)X^{p-1} - p(1 + ap)$ per $a = 0, 1, \ldots, p-1$.

Siamo ora pronti a sistemare questi risultati nella seguente tabella. Essa conclude la trattazione delle estensioni di grado p di $\mathbb{Q}_p$: richiamiamo le notazioni. $\mathbf{K}$ è l'estensione di grado p, $\mathbf{L}$ è la sua chiusura normale che ha gruppo di Galois $G(\mathbf{L}|\mathbb{Q}_p) = G$ e G_0 è il sottogruppo d'inerzia di G, w è il numero di automorfismi di $\mathbf{K}$ su $\mathbb{Q}_p$ (e quindi p/w è il numero di estensioni coniugate a $\mathbf{K}$ su $\mathbb{Q}_p$), e e f sono rispettivamente l'indice di ramificazione e l'indice d'inerzia di $\mathbf{K}$ su $\mathbb{Q}_p$. Infine $v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}})$ è la valutazione del differente

di $\mathbf{K}$ su $\mathbb{Q}_p$ ($v_{\mathbf{K}} = pv$ e $v = v_p$).

Tabella 2.5: *estensioni di grado p di* $\mathbb{Q}_p$

Polinomio generatore	w	Parametri	e	f	$v_{\mathbf{K}}(\mathcal{D}_{\mathbf{K}})$	G	G_0	Numero
$X^{p^p-1}-1$	p		1	p	0	$\mathbb{Z}/p\mathbb{Z}$	$\{0\}$	1
$X^p-\omega pX^\lambda-p$	1	$1\leq\lambda<p-1$ $0<\omega\leq p-1$	p	1	$p+\lambda-1$	$L_{p,\,s}$	$L_{p,\,\lambda}$	$p(p-2)(p-1)$
$X^p-\omega pX^\lambda-p$	1	$\lambda=p-1$ $0<\omega<p-1$	p	1	$2p-2$	$L_{p,\,s}$	$L_{p,\,\lambda}$	$p(p-2)$
$X^p-p(p-1)X^{p-1}-p(1+ap)$	p	$0\leq a\leq p-1$	p	1	$2p-2$	$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}$	p
$X^p-p(1+ap)$	1	$0\leq a\leq p-1$	p	1	$2p-1$	$L_{p,\,1}$	$L_{p,\,1}$	p^2

Capitolo 3

Le estensioni di grado p^2 di $\mathbb{Q}_p$

3.1 Il caso $p = 2$

Dalla formula di Krasner si deduce che ci sono 107 estensioni di grado 4 su $\mathbb{Q}_2$ e tra queste 92 sono quelle totalmente ramificate. Sia $\mathbf{L}$ una di esse. Se indichiamo, come nel primo capitolo, con $d(\mathbf{L})$ la valutazione del discriminante di $\mathbf{L}$ rispetto alla valutazione standard di $\mathbb{Q}_2$ e poniamo $c(\mathbf{L}) = d(\mathbf{L}) - 4 + 1$ come Serre, si ha che, per le condizioni di Ore, i possibili valori di $c(\mathbf{L})$ sono 1, 3, 5, 6, 7 e 8. Inoltre, con la formula di Serre, si ottiene il numero di estensioni totalmente ramificate $\mathbf{L}$ con un fissato $c(\mathbf{L})$ che risulta essere quello riportato nella seguente tabella.

Tabella 3.1: *estensioni totalmente ramificate di grado* 4 *su* $\mathbb{Q}_2$

$c(\mathbf{L})$	Numero di estensioni
1	4
3	8
5	16
6	16
7	16
8	32

Osservazione 3.1.1 *Ci sono esattamente* 7 *estensioni di Galois* $\mathbf{L}$ *di grado* 4 *su* $\mathbb{Q}_2$ *con gruppo di Galois isomorfo a* $(\mathbb{Z}/2\mathbb{Z})^2$*. Tra queste* 4 *sono totalmente ramificate, con valutazione del discriminante pari a* 8*, e* 3 *sono miste (cioè* $e(\mathbf{L}|\mathbb{Q}_2) = f(\mathbf{L}|\mathbb{Q}_2) = 2$*), con valutazione del discriminante pari a* 4 *in un caso, pari a* 6 *nei rimanenti due.*

Dimostrazione Osserviamo in primo luogo che richiedere che una estensione $\mathbf{L}$ di grado 4 su $\mathbb{Q}_2$ abbia (almeno) due sottoestensioni proprie (quindi di grado 2 su $\mathbb{Q}_2$) equivale a richiedere che sia di Galois di grado 4 su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$. Infatti supponiamo di avere una estensione $\mathbf{L}$ di grado 4 su $\mathbb{Q}_2$ e siano $\mathbf{K}_1$ e $\mathbf{K}_1$ due sottoestensioni di $\mathbf{L}$ di grado 2 su $\mathbb{Q}_2$. Allora $\mathbf{K}_1\mathbf{K}_2 \subseteq \mathbf{L}$ ma $[\mathbf{K}_1\mathbf{K}_2 : \mathbb{Q}_2] = 4$ ($\mathbf{K}_1\mathbf{K}_2$ è di Galois su $\mathbb{Q}_2$ perché lo sono $\mathbf{K}_1$ e $\mathbf{K}_2$ e $G(\mathbf{K}_1\mathbf{K}_2|\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$ perché $\mathbf{K}_1 \cap \mathbf{K}_2 = \mathbb{Q}_2$). Quindi $\mathbf{K}_1\mathbf{K}_2 = \mathbf{L}$ e $\mathbf{L}$ è di Galois con $G(\mathbf{L}|\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Quindi, in particolare, per la corrispondenza di Galois $\mathbf{L}$ ha esattamente 3 sottoestensioni. Viceversa se $\mathbf{L}$

è di Galois di grado 4 su $\mathbb{Q}_2$ con $G(\mathbf{L}|\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$ è chiaro che ha almeno due sottoestensioni (ne ha esattamente tre).
Analizziamo in primo luogo quali devono essere le caratteristiche delle estensioni di Galois di grado 4 su $\mathbb{Q}_2$ con $G(\mathbf{L}|\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$ che sono totalmente ramificate su $\mathbb{Q}_2$ (cioè $e(\mathbf{L}|\mathbb{Q}_2) = 4$). Denotiamo ora le tre sottoestensioni di $\mathbf{L}$ con $\mathbf{K}_1$, $\mathbf{K}_2$ e $\mathbf{K}_3$, allora (a meno di rinumerarle) si avrà che $d(\mathbf{K}_1) = 2$ e $d(\mathbf{K}_2) = 3$. Infatti, ovviamente non tutte le tre estensioni possono avere valutazione del discriminante pari a 2 perché ci sono solo 2 estensioni di questo tipo (vedi la classificazione delle estensioni di grado 2 di $\mathbb{Q}_2$). D'altra parte se avessero tutte valutazione del discriminante pari a 3 allora non è difficile notare (sempre dalla classificazione delle estensioni di grado 2 di $\mathbb{Q}_2$) che $\mathbf{L}$ dovrebbe contenere anche la sottoestensione non ramificata di grado 2. Questo è impossibile poiché avevamo supposto che $\mathbf{L}$ fosse totalmente ramificata. Con un discorso analogo si riesce anche a dire che in realtà $d(\mathbf{K}_3) = 3$. Allora, ricordando che si ha

$$d(\mathbf{L}|\mathbb{Q}_2) \;=\; d(\mathbf{L}|\mathbf{K}_i) \;+\; 2d(\mathbf{K}_i|\mathbb{Q}_2) \tag{3.1}$$

si ottiene che

$$d(\mathbf{L}|\mathbb{Q}_2) \;=\; d(\mathbf{L}|\mathbf{K}_1) \;+\; 2d(\mathbf{K}_1|\mathbb{Q}_2) \;=\; d(\mathbf{L}|\mathbf{K}_2) \;+\; 2d(\mathbf{K}_2|\mathbb{Q}_2)$$

cioè

$$d(\mathbf{L}|\mathbb{Q}_2) \;=\; d(\mathbf{L}|\mathbf{K}_1) \;+\; 4 \;=\; d(\mathbf{L}|\mathbf{K}_2) \;+\; 6$$

Possiamo allora scrivere, passando ai c , che

$$c(\mathbf{L}|\mathbf{K}_1) \;-\; c(\mathbf{L}|\mathbf{K}_2) \;=\; 2$$

Le condizioni di Ore impongono che i possibili valori per $c(\mathbf{L}|\mathbf{K}_i)$ siano 1, 3 o 4 ($\mathbf{K}_i$ è totalmente ramificata per ogni i). Quindi si dovrà avere $c(\mathbf{L}|\mathbf{K}_1) = 3$ e $c(\mathbf{L}|\mathbf{K}_2) = 1$ e in particolare $c(\mathbf{L}|\mathbb{Q}_2) = 5$ ossia $d(\mathbf{L}|\mathbb{Q}_2) = 8$.
Notiamo ora che ci sono effettivamente solo 4 estensioni come $\mathbf{L}$ cioè totalmente ramificate di Galois su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$. Per l'analisi portata avanti fin qui infatti tali estensioni risultano coincidere con i composti di una estensione totalmente ramificata di grado 2 su $\mathbb{Q}_2$ con valutazione del discriminante pari a 2 e di una estensione totalmente ramificata di grado 2 su $\mathbb{Q}_2$ con valutazione del discriminante pari a 3. Poiché ci sono 2 estensioni del primo tipo e 4 estensioni del secondo, si ottiene quanto affermato.
Contiamo ora tutte le estensioni $\mathbf{L}$ di $\mathbb{Q}_2$ che sono di Galois con $G(\mathbf{L}|\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$: ricordando che ci sono 7 estensioni di grado 2 di $\mathbb{Q}_2$, non è difficile riconoscere che ci sono ancora una volta 7 estensioni del tipo di $\mathbf{L}$ (tutti i possibili composti). Allora le tre rimanenti saranno necessariamente miste (perché le non ramificate sono cicliche). Una estensione $\mathbf{L}$ di grado 4 di $\mathbb{Q}_2$ che abbia $e(\mathbf{L}|\mathbf{Q_2}) = f(\mathbf{L}|\mathbb{Q}_2) = 2$ deve contenere necessariamente una sottoestensione (propria) di grado due, segnatamente la massima sottoestensione non ramificata. Supponiamo ora che $\mathbf{L}$ sia di Galois su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$ e mista. Siano $\mathbf{K}_1$ la sottoestensione non ramificata e $\mathbf{K}_2$ e $\mathbf{K}_3$ le altre due sottoestensioni (totalmente ramificate). Allora per le proprietà del discriminate rispetto alle torri e delle estensioni non ramificate rispetto alle traslazioni

$$2d(\mathbf{K_i}|\mathbb{Q}_2) \;=\; d(\mathbf{L}|\mathbb{Q}_2) \qquad i \;=2,\,3 \tag{3.2}$$

Sappiamo che le estensioni $\mathbf{L}$ di Galois di grado 4 su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$ che non sono totalmente ramificate sono 3. Poichè ci sono precisamente 2

estensioni di grado 2 di $\mathbb{Q}_2$ con valutazione del discriminante pari a 2 e 4 estensioni di grado 2 di $\mathbb{Q}_2$ con valutazione del discriminante pari a 3, considerato che $(\mathbb{Z}/2\mathbb{Z})^2$ ha 3 sottogruppi di ordine 2 (e quindi 3 quozienti di ordine 2), si ottiene, sfruttando (3.2), che c'è un'unica estensione di Galois di grado 4 su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$ che abbia valutazione del discriminante pari a 4 (che contiene le due di grado 2 la valutazione del cui discriminante è pari a 2) e che ci sono 2 estensioni di Galois di grado 4 su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$ che abbiano valutazione del discriminante pari a 6 (ciascuna delle quali contiene due estensioni di grado 2 la valutazione del cui discriminante è pari a 3). □

Osservazione 3.1.2 *Ci sono esattamente* 16 *estensioni* $\mathbf{L}$ *di grado* 4 *su* $\mathbb{Q}_2$ *sprovviste di sottoestensioni. Queste ultime sono tutte totalmente ramificate e fra di esse sono presenti tutte le estensioni* $\mathbf{L}$ *di grado* 4 *su* $\mathbb{Q}_2$ *con* $d(\mathbf{L}|\mathbb{Q}_2) = 1$ *(che sono in numero di* 4*).*

Dimostrazione È chiaro che se una estensione di grado 4 è priva di sottoestensioni, allora non può che essere totalmente ramificata, altrimenti la massima sottoestensione non ramificata sarebbe una sottoestensione propria. Dalla formula di Krasner risulta che, fissata una estensione $\mathbf{K}$ di grado 2 su $\mathbb{Q}_2$, ci sono 15 estensioni di grado 2 su $\mathbf{K}$. Ricordando che ci sono 7 estensioni di grado 2 di $\mathbb{Q}_2$ e che, per quanto appena visto, ci sono precisamente 7 estensioni di grado 4 di $\mathbb{Q}_2$ che hanno più di una sottoestensione propria (e quindi ne hanno esattamente 3), si ottiene che ci sono $7 \cdot 15 - 7 \cdot 3 + 7 = 91$ estensioni di grado 4 di $\mathbb{Q}_2$ con almeno una sottoestensione (propria). Di conseguenza ci sono $107 - 91 = 16$ estensioni di grado 4 sprovviste di sottoestensioni. Sicuramente tra queste ci sono le 4 estensioni totalmente ramificate $\mathbf{L}$ con $c(\mathbf{L}) = 1$. Infatti, per un calcolo simile a quello che è stato in precedenza condotto a partire dall'equazione (3.1) (e che sfrutta le condizioni di Ore), si vede facilmente che 1 non può essere il valore che assume c per una estensione di grado 4 totalmente ramificate su $\mathbb{Q}_2$ che abbia almeno una sottoestensione. □

Osservazione 3.1.3 *Vale la seguente tabella*

Tabella 3.2: *estensioni totalmente ramificate di grado* 4 *su* $\mathbb{Q}_2$ *con al più una sottoestensione*

$c(\mathbf{L})$	Numero estensioni con una sottoestensione	Numero estensioni prive di sottoestensioni
1	0	4
3	4	4
5	4	8
6	16	0
7	16	0
8	32	0

Dimostrazione Introduciamo per comodità alcune nuove notazioni. Sia $\mathbf{K}$ una estensione totalmente ramificata di grado 2 di $\mathbb{Q}_2$ e $\mathbf{L}$ una estensione totalmente ramificata di grado 2 di $\mathbf{K}$. Poniamo

$$c(\mathbf{K}|\mathbb{Q}_2) = c_1 \qquad c(\mathbf{L}|\mathbf{K}) = c_2 \qquad c(\mathbf{L}|\mathbb{Q}_2) = c$$

Allora vale che

$$2c_1 + c_2 = c \tag{3.3}$$

Inoltre con la formula di Serre e le condizioni di Ore (**K** è totalmente ramificata su $\mathbb{Q}_2$) si ottiene la seguente tabella. Ricordiamo ancora una volta che ci sono 2 estensioni di

Tabella 3.3: *estensioni totalmente ramificate di grado* 2 *su* **K**

c_2	Numero di estensioni
1	2
3	4
4	8

grado 2 su $\mathbb{Q}_2$ che hanno $c_1 = 1$ e 4 che hanno $c_1 = 2$.
Se $c_2 = 4$ sicuramente **L** non è di Galois su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$ (questo deriva dal computo precedentemente svolto sul valore di c per tali estensioni e dall'equazione (3.3)). Allora sappiamo che ci sono almeno $8 \cdot 4 = 32$ estensioni con $c_2 = 4$ e $c_1 = 2$ (e quindi $c = 8$) e $8 \cdot 2 = 16$ estensioni con $c_2 = 4$ e $c_1 = 1$ (e quindi $c = 6$). Si esauriscono così, rispettivamente, tutte le estensioni totalmente ramificate di grado 4 con $c = 8$ e tutte le estensioni totalmente ramificate di grado 4 con $c = 6$ (vedi tabella 3.1).
Ancora: se $c_1 = 1$ e $c_2 = 1$ allora **L** non è di Galois su $\mathbb{Q}_2$ con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$. Quindi sappiamo che ci sono almeno $2 \cdot 2 = 4$ estensioni con $c = 3$. In realtà queste 4 sono tutte le estensioni **L** di grado 4 su $\mathbb{Q}_2$ con $c(\mathbf{L}) = 3$ che hanno esattamente una sottoestensione. Infatti se una estensione ha $c = 3$ non può avere più di una sottoestensione, perché se ne avesse più d'una allora ne avrebbe 3 e quindi avrebbe $c = 5$. D'altra parte se ha una sottoestensione allora è sicuramente una delle 4 che abbiamo contato prima perché la (3.3) dà risultato 3 se e solo se $c_1 = 1$ e $c_2 = 1$. Da questo si ricava che ci sono 4 estensioni con $c = 3$ che sono prive di sottoestensioni (quindi delle 8 con $c = 3$, 4 hanno una sola sottoestensione e 4 sono prive di sottoestensioni).
Considerazioni analoghe quando $c_1 = 2$ e $c_2 = 3$ portano a dire che ci sono almeno $4 \cdot 4 = 16$ estensioni con $c = 7$ (e quindi quelle contate in questo modo sono tutte quelle con $c = 7$).
A questo punto abbiamo terminato: in primo luogo le restanti 8 estensioni senza sottoestensioni che non abbiano ancora contato (delle 16 prive di sottoestensioni sappiamo già che 4 hanno $c = 1$ e 4 hanno $c = 3$) non possono che avere $c = 5$ (perché abbiamo già contato tutte le estensioni quando c assume un altro valore). Mancano allora solo altre 4 estensioni con $c = 5$ che, per esclusione, avranno necessariamente una sottoestensione (questo dato può anche essere ricavato in maniera diretta e altrettanto semplice utilizzando la (3.3) e un'analisi più dettagliata delle estensioni di Galois con gruppo di Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$). □

Ancora una volta utilizzando le formule di Krasner e Serre e i risultati dell'osservazione 3.1.1 si ottiene la seguente tabella

Ovviamente l'unica estensione **L** di grado 4 su $\mathbb{Q}_2$ con $d(\mathbf{L}) = 0$ è quella non ramificata (che è di Galois con gruppo di Galois ciclico).

Tabella 3.4: *estensioni non totalmente ramificate di grado* 4 *su* $\mathbb{Q}_2$

$d(\mathbf{L})$	Con tre sottoestensioni	Con una sottoestensione	Totale estensioni
0	0	1	1
4	1	5	6
6	2	6	8

Passiamo ora ad analizzare il gruppo di Galois della chiusura normale $\mathbf{F}$ di una estensione $\mathbf{L}$ di grado 4 su $\mathbb{Q}_2$ (ovviamente nei casi in cui $\mathbf{L}$ non sia di Galois, cioè $w(\mathbf{L}) \neq p^2$) e poniamo $G = G(\mathbf{F}|\mathbb{Q}_2)$.

Osservazione 3.1.4 *Se* $w(\mathbf{L}) = 2$*, allora* $G = G(\mathbf{F}|\mathbb{Q}_2) \cong D_4$*.*

Dimostrazione Per ipotesi $\mathbf{L}$ ha un solo altro coniugato, che chiameremo $\mathbf{L}'$. Poiché $w = 2$ per un'osservazione fatta in precedenza (durante lo studio di w), si ha che esiste un'estensione normale $\mathbf{K}$ di grado 2 su $\mathbb{Q}_2$ che coincide con il campo lasciato fisso dal normalizzatore di $G(\mathbf{F}|\mathbf{L})$. Inoltre tale normalizzatore coincide (essendo a sua volta un sottogruppo normale di G, vedi ancora la trattazione cui si fa riferimento prima) con il normalizzatore di $G(\mathbf{F}|\mathbf{L}')$ e si ha $\mathbf{L} \cap \mathbf{L}' = \mathbf{K}$. È chiaro dunque che $[\mathbf{F} : \mathbb{Q}_2] = 8$. Quindi G è un gruppo di ordine 8. Poiché $\mathbf{F}$ possiede delle sottoestensioni che non sono normali su $\mathbb{Q}_2$, G non può essere abeliano e quindi restano solo due possibilità per la sua struttura: può essere isomorfo a D_4 oppure a Q, il gruppo dei quaternioni. Tuttavia quest'ultima possibilità non si concretizza: ci sono almeno due modi per vederlo. In primo luogo non esistono sottogruppi transitivi di S_4 isomorfi a Q. In modo più diretto, Q ha un solo sottogruppo di ordine 2, mentre la presenza di $\mathbf{L}$ e $\mathbf{L}'$ ne richiede almeno 2. Infine, poiché D_4 ha esattamente 4 sottogruppi di ordine 2 non normali (suddivisi in due coppie di sottogruppi coniugati), si ottiene che $\mathbf{F}$ è la chiusura normale di 4 estensioni di grado 4 su $\mathbb{Q}_2$ (suddivise in due coppie di estensioni coniugate) con $w = 2$. □

Studiamo più in dettaglio le estensioni cicliche di grado 4.

Osservazione 3.1.5 *Ci sono esattamente* 12 *estensioni cicliche di grado* 4 *su* $\mathbb{Q}_2$ *e vale la seguente tabella*

Tabella 3.5: *estensioni cicliche di grado* 4 *su* $\mathbb{Q}_2$

$e(\mathbf{L}\|\mathbb{Q}_2)$	$f(\mathbf{L}\|\mathbb{Q}_2)$	$d(\mathbf{L}\|\mathbb{Q}_2)$	Numero di estensioni
1	4	0	1
2	2	4	1
2	2	6	2
4	1	11	8

Dimostrazione In primo luogo il composto delle estensioni cicliche di grado 4 su $\mathbb{Q}_2$ è un'estensione abeliana di $\mathbb{Q}_2$ di grado 32 il cui gruppo di Galois è isomorfo a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Ciò è una conseguenza dei risultati più generali ottenuti nel capitolo 4. È possibile comunque, utilizzando [Ya 95], dimostrarlo direttamente, in modo analogo a come si farà più avanti per le estensioni cicliche di grado p^2 su $\mathbb{Q}_p$ per

$p \neq 2$ (qui si utilizzerà però [Ša 56]).
Dimostriamo dapprima che tutte le estensioni $\mathbf{L}$ totalmente ramificate cicliche di grado 4 su $\mathbb{Q}_2$ sono 8 e hanno $d = 11$. Analizziamo il gruppo di Galois G del composto di tutte le estensioni cicliche, ossia $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Esso possiede esattamente 3 sottogruppi di ordine 16 isomorfi a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. La loro intersezione è il sottogruppo abeliano elementare di ordine 8 di G. Ciascuno di questi sottogruppi inoltre ha 7 sottogruppi di ordine 8: 3 di questi 7 considerati come sottogruppi di G hanno quoziente non ciclico, per i restanti 4 il quoziente è invece ciclico. Quindi le 12 estensioni cicliche di grado 4 su $\mathbb{Q}_2$ sono suddivise in 3 famiglie composte ciascuna da 4 elementi: fissata una famiglia, tutte le estensioni ad essa appartenenti hanno a stessa sottoestensione di grado 2 su $\mathbb{Q}_2$. Ad esempio c'è la famiglia delle 4 estensioni cicliche non totalmente ramificate (perché c'è l'estensione ciclica di grado 4 non ramificata) e quindi le totalmente ramficate cicliche sono 8. Le due famiglie composte da estensioni totalmente ramificate hanno rispettivamente, diciamo, $\mathbf{K}_1$ e $\mathbf{K}_2$ come sottoestensione di grado 2. Il sottogruppo di G corrispondente a $\mathbf{K}_1\mathbf{K}_2$ (che è l'unico abeliano elementare di ordine 8) è contenuto nel sottogruppo che corrisponde all'unica estensione non ramificata di $\mathbb{Q}_2$. Quindi $\mathbf{K}_1\mathbf{K}_2$ non è totalmente ramificata e dunque $d(\mathbf{K}_1) = d(\mathbf{K}_2)$ (vedi la trattazione delle estensioni di Galois con gruppo di Galois $(\mathbb{Z}/2\mathbb{Z})^2$). Da questo si deduce che $d(\mathbf{K}_1) = d(\mathbf{K}_2) = 3$ e $d(\mathbf{L}) = 11$: vediamo come. In primo luogo è facile vedere, utilizzando le possibili filtrazioni dei sottogruppi di ramificazione, che per un'estensione ciclica totalmente ramificata gli unici valori di d possibili sono 8 e 11. Supponiamo per assurdo che sia $d(\mathbf{K}_1) = d(\mathbf{K}_2) = 2$ (che è l'unica altra possibilità). Ci sono 4 estensioni $\mathbf{L}$ di grado 4 di $\mathbf{K}_1$ con $d(\mathbf{L}) = 8$ e nessuna con $d = 11$ (e lo stesso accade per $\mathbf{K}_2$). Esattamente 2 di queste 4 sono di Galois con gruppo di Galois $(\mathbb{Z}/2\mathbb{Z})^2$, come già si è visto. Allora rimangono solo 2 estensioni che potrebbero essere cicliche e che hanno come sottoestensione $\mathbf{K}_1$ e altrettante che hanno come sottoestensione $\mathbf{K}_2$: in tutto 4 estensioni, quindi. Ma ce ne sono 8 cicliche totalmente ramificate: allora le altre dovrebbero avere una sottoestensione che non è né $\mathbf{K}_1$ né $\mathbf{K}_2$, il che è assurdo. Quindi $d(\mathbf{K}_1) = d(\mathbf{K}_2) = 3$ e poiché non ci sono estensioni cicliche di grado 4 con $d = 8$ che hanno una sottoestensione di grado 2 con $d = 3$ (le uniche sono quelle di Galois con gruppo di Galois $(\mathbb{Z}/2\mathbb{Z})^2$), le estensioni cicliche totalmente ramificate devono avere $d = 11$.
Ci resta di classificare le estensioni cicliche non totalmente ramificate di grado 4. Di queste una è sicuramente quella non ramificata. Dalla tabella 3.1 risulta che ci sono 5 estensioni non totalmente ramificate con $d = 4$ e 6 con $d = 6$: tra queste, alcune avranno $w = 2$ (cioè 2 coniugati) e altre saranno di Galois cicliche. È chiaro comunque che quelle che hanno $w = 2$ compaiono (perché ci sono solo 3 estensioni cicliche miste) e compaiono in coppia (una estensione e la sua coniugata). Allora ci sono 2 possibilità: le tre estensioni cicliche miste hanno tutte $d = 4$ oppure due hanno $d = 6$ e una ha $d = 4$. Tuttavia esiste almeno una estensione ciclica $\mathbf{L}$ di grado 4 su $\mathbb{Q}_2$ con $d = 6$. Infatti, se $\zeta \in \overline{\mathbb{Q}_2}$ è una radice terza primitiva dell'unità, $\mathbf{L} = \mathbb{Q}_2(\alpha)$ con $\alpha = \sqrt[2]{2(1+4\zeta)}$ è ciclica di grado 4 su $\mathbb{Q}_2$ e $d(\mathbf{L}) = 6$. Dimostriamolo: al solito è utile una descrizione dei quadrati di $\mathbf{K} = \mathbb{Q}_2(\zeta)$ (l'estensione non ramificata di grado 2 di $\mathbb{Q}_2$). Un elemento generico di $\mathbf{K}^*$ si può scrivere come $2^k x(1+2y)$ con $k \in \mathbb{Z}$, $x \in \mathbb{F}_4^*$ e $y \in \mathbb{Z}_2$. Esso è un quadrato se e solo se esitono $h \in \mathbb{Z}$, $z \in \mathbb{F}_4^*$ e $w \in \mathbb{Z}_2$ tali che

$$2^k x(1+2y) = 2^{2h} z^2 (1+2w)^2 = 2^{2h} z^2 (1+4w^2+4w)$$

e questo accade se e solo se k è pari ed esiste $t \in \mathbb{Z}_2$ tale che $y = 2t$ e $t \equiv 0$ oppure $t \equiv 1$ $(mod\ 2\mathcal{O}_{\mathbf{K}})$ (si tratta degli unici casi in cui il polinomio $W^2 + W + t \in \mathbb{F}_4[W]$ ha soluzione). Allora è possibile scrivere una lista dei rappresentanti delle 15 estensioni di grado 2 di $\mathbf{K}$, similmente a quanto si è fatto nel caso delle estensioni di grado 2 di $\mathbb{Q}_2$. Inoltre $2(1 + 4\zeta)$ non è un quadrato, quindi $\mathbf{L} = \mathbb{Q}_2(\sqrt[2]{2(1 + 4\zeta)})$ ha grado 4 su $\mathbb{Q}_2$ e $d(\mathbf{L}) = 6$ (come si vede usando la formula che lega la derivata del polinomio minimo di α su $\mathbf{K}$ calcolata in α al differente di $\mathbf{L}$ su $\mathbf{K}$). È un'estensione di Galois: se estendiamo l'automorfismo non banale di $\mathbf{K}$ (che è quello indotto dal Frobenius di $\mathbb{F}_4$) a $\mathbf{L}$ otteniamo un automorfismo φ di $\mathbf{L}$ (perché $2(1 + 4\zeta)$ e $2(1 + 4\zeta^2)$ differiscono per un quadrato). Quindi il gruppo degli automorfismi di $\mathbf{L}$ su $\mathbb{Q}_2$ ha almeno 3 elementi (φ, l'identità e quello dato da $\alpha \mapsto -\alpha$) ma poiché l'ordine di tale gruppo deve dividere il grado di $\mathbf{L}$, si ha che $|Aut(\mathbf{L}|\mathbb{Q}_2)| = [\mathbf{L} : \mathbb{Q}_2]$ e quindi $\mathbf{L}$ è di Galois. Inoltre

$$(2(1 + 4\zeta))(2(1 + 4\zeta^2)) = 4 \cdot 13$$

Allora $\varphi(\alpha) = \sqrt[2]{2(1 + 4\zeta^2)}$ ma $\varphi(\sqrt[2]{2(1 + 4\zeta^2)}) \neq \alpha$ perché $\sqrt[2]{13} \in \mathbf{K} \setminus \mathbb{Q}_2$ e φ non lascia fisso $\mathbf{K}$. Quindi φ ha ordine 4 e $G(\mathbf{L}|\mathbb{Q}_2)$ è ciclico. □

Combinando i risultati di quest'ultima osservazione e della precedente, sappiamo che ci sono in tutto 72 estensioni $\mathbf{L}$ di grado 4 su $\mathbb{Q}_2$ con $w(\mathbf{L}) = 2$: 8 non totalmente ramificate (di cui 4 con $d = 4$ e 4 con $d = 6$) e 64 totalmente ramificate (di cui 4 con $c = 3$, 4 con $c = 5$, 16 con $c = 6$, 16 con $c = 7$ e 24 con $c = 8$). Inoltre ciascuna di esse ha chiusura normale con gruppo D_4.

Rimangono da studiare le estensioni $\mathbf{L}$ con $w(\mathbf{L}) = 1$: è chiaro che $\mathbf{F}$ in questo caso non può avere grado 8 su $\mathbb{Q}_2$ (in tal caso G sarebbe isomorfo a D_4 oppure a Q ma nessuno di questi gruppi possiede 4 sottogruppi di ordine 2 tutti coniugati fra di loro). Per cui le possibilità restanti per G, considerato che deve essere isomorfo ad un sottogruppo di S_4, sono $G \cong A_4$ oppure $G \cong S_4$.

Osservazione 3.1.6 *C'è una estensione* $\mathbf{L}$ *di grado* 4 *su* $\mathbb{Q}_2$ *tale che* $G = G(\mathbf{F}|\mathbb{Q}_2) \cong A_4$ *(*$\mathbf{F}$ *denota al solito la chiusura normale di* $\mathbf{L}$*).*

Dimostrazione Vogliamo costruire intanto una estensione $\mathbf{F}$ che sia di Galois su $\mathbb{Q}_2$ con gruppo di Galois $G(\mathbf{F}|\mathbb{Q}_2) \cong A_4$. Verificheremo poi che $\mathbf{F}$ non può non essere la chiusura normale di una estensione di grado 4 su $\mathbb{Q}_2$.
Studiamo allora quale possa essere la ramificazione di $\mathbf{F}$ su $\mathbb{Q}_2$ attraverso i gruppi di ramificazione di G se $G \cong A_4$. L'osservazione fondamentale è che G_0, ovverosia il sottogruppo d'inerzia, è V, il sottogruppo normale di ordine 4 (isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$) di A_4. È chiaro intanto che $G_0 \neq \{1\}$ altrimenti $\mathbf{F}$ sarebbe non ramificata e quindi ciclica. Inoltre G_0 deve essere un sottogruppo normale di A_4, quindi le possibilità sono $G_0 \cong V$ oppure $G_0 \cong A_4$. Mettiamoci per assurdo in quest'ultima situazione. Allora si ha che $e(\mathbf{F}|\mathbb{Q}_2) = 12$, cioè $\mathbf{F}$ è totalmente ramificata su $\mathbb{Q}_2$. Detta $\mathbf{E}$ la sottoestensione che corrisponde a V (cioè $G(\mathbf{F}|\mathbf{E}) = V$), si ha che $\mathbf{E}$ è normale di grado 3 su $\mathbb{Q}_2$ (e quindi è ciclica) ed è totalmente ramificata (perché contenuta in $\mathbf{F}$ che è totalmente ramificata). Dalla formula di Krasner si deduce che ci sono esattamente 3 estensioni totalmente ramificate di grado 3 su $\mathbb{Q}_2$. Consideriamo ora per esempio il polinomio $h(X) = X^3 - 2 \in \mathbb{Q}_2[X]$. Il suo discriminante è -108 che non è un quadrato in $\mathbb{Q}_2$[1].

[1] L'abbiamo già dimostrato in una sottosezione precedente: basta vedere che 3 non è un quadrato in $\mathbb{Q}_2$, il che è vero perché la forma $Y^2 + 3$ è priva di zeri già in $\mathbb{Z}/4\mathbb{Z}$.

Quindi il campo di spezzamento di $h(X)$ ha grado 6 e gruppo di Galois isomorfo a S_3. Per cui le uniche 3 estensioni di grado 3 totalmente ramificate di $\mathbb{Q}_2$ sono quelle ottenute aggiungendo le 3 radici di $h(X)$ e dunque non sono normali su $\mathbb{Q}_2$. Di conseguenza $\mathbf{E}$ non può essere totalmente ramificata, contro l'ipotesi. Allora si avrà $G_0 = V$ e quindi $e(\mathbf{F}|\mathbb{Q}_2) = 4$.
Guidati da queste considerazioni proviamo a costruire $\mathbf{F}$ a partire dall'unica estensione non ramificata di grado 3 di $\mathbb{Q}_2$, che denotiamo con $\mathbf{E}$. Allora $\mathbf{E} = \mathbb{Q}_2(\zeta)$ dove ζ è un radice settima primitiva dell'unità. Dunque ζ soddisfa il polinomio $X^6+X^5+\ldots+X+1$ (che non è il suo polinomio minimo su $\mathbb{Q}_2$). Si ha

$$X^6 + X^5 + \ldots + X + 1 \equiv (X^3 + X + 1)(X^3 + X^2 + 1) \qquad (mod\ 2\mathcal{O}_{\mathbf{E}}[X])$$

Scegliamo allora ζ in modo che sia $\zeta^3 + \zeta + 1 \equiv 0$ $(mod\ 2\mathcal{O}_{\mathbf{E}})$. Notiamo esplicitamente che le altre radici settime dell'unità che soddisfano questa condizione sono ζ^2 e ζ^4.
Ora, qualche considerazione sugli elementi di $U_1^{\mathbf{E}} = \{u \in \mathcal{O}_{\mathbf{E}} \,|\, u \equiv 1\,(mod\ 2\mathcal{O}_{\mathbf{E}})\}$ che sono quadrati. Scriviamo $u = 1 + 2x$.

$$\begin{aligned} u = v^2 \quad &\Leftrightarrow \quad v = 1 + 2y \text{ e } x = 2y(y + 1) \text{ oppure } v = -1 + 2y \text{ e } x = 2y(y - 1) \\ &\Leftrightarrow \quad x = 2z \text{ e } z = y(y + 1) \text{ oppure } x = 2z \text{ e } z = y(y - 1) \end{aligned}$$

Allora u è un quadrato se e solo se esiste $z \in \mathcal{O}_{\mathbf{E}}$ tale che $u = 1 + 4z$ e almeno uno dei polinomi Y^2+Y-z e Y^2-Y-z ammette soluzioni in $\mathbb{Q}_2$. Non è difficile vedere (usando il lemma di Hensel e la relazione di annullamento su ζ) che uno dei due polinomi ha soluzioni se e solo se $z \equiv 0, \zeta, \zeta^2, \zeta^4$ $(mod\ 2\mathcal{O}_{\mathbf{E}})$.
Con questa descrizione dei quadrati possiamo allora scegliere un elemento $\alpha \in \mathbf{E}$ che non è un quadrato e considerare $\mathbf{E}(\sqrt[2]{\alpha})$ che ha grado 6 su $\mathbb{Q}_2$. Vorremmo inoltre che $\mathbf{E}(\sqrt[2]{\alpha})$ non fosse normale su $\mathbb{Q}_2$ e che la sua chiusura normale avesse grado 12 su $\mathbb{Q}_2$. Scegliamo allora $\alpha = 1 + 2\zeta + 4\zeta)$ e poniamo $\mathbf{E}_0 = \mathbf{E}(\sqrt[2]{\alpha})$. In primo luogo è chiaro, in base alle considerazioni precedenti, che $\mathbf{E}_0$ ha grado 6 su $\mathbb{Q}_2$. Inoltre non è normale: dico che le altre due estensioni coniugate a $\mathbf{E}_0$ su $\mathbb{Q}_2$ sono $\mathbf{E}_1 = \mathbf{E}(\sqrt[2]{1 + 2\zeta^2 + 4\zeta^2})$ e $\mathbf{E}_2 = \mathbf{E}(\sqrt[2]{1 + 2\zeta^4 + 4\zeta^4}))$. Infatti, dalla descrizione dei quadrati, si vede che sono distinte: sono inoltre coniugate perché sono mandate l'una nell'altra dalle stensioni dei due automorfismi non banali di $\mathbf{E}$ su $\mathbb{Q}_2$ (che sono dati da $\zeta \mapsto \zeta^2$ e $\zeta \mapsto \zeta^4$, che corrispondono all'automorfismo di Frobenius e al suo quadrato nel campo residuo). Inoltre $\mathbf{E}_2 \subseteq \mathbf{E}_0\mathbf{E}_1$ perché $(1 + 2\zeta + 4\zeta)(1 + 2\zeta^2 + 4\zeta^2)(1 + 2\zeta^4 + \zeta^4) \equiv 1$ $(mod\ 8\mathcal{O}_{\mathbf{E}})$ è un quadrato in $\mathbf{E}$. Quindi la chiusura normale $\mathbf{F}$ di $\mathbf{E}(\sqrt[2]{\alpha})$ su $\mathbb{Q}_2$ ha grado 12 su $\mathbf{Q}_2$ e $G = G(\mathbf{F}|\mathbb{Q}_2)$ è un sottogruppo transitivo di S_6 di ordine 12 che possiede un sottogruppo normale di ordine 4 isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$. Ci sono quindi solo 2 possibilità per G: che esso sia isomorfo a D_6 oppure che sia isomorfo ad A_4 (cfr. [BMc 83]). Ma D_6 non ha sottogruppi normali di ordine 4, quindi $G \cong A_4$.
Abbiamo dunque trovato una estensione $\mathbf{F}$ di Galois su $\mathbb{Q}_2$ con $G = G(\mathbf{F}|\mathbb{Q}_2) \cong A_4$. A_4 possiede 4 sottogruppi di ordine 3 (quelli generati dai 3-cicli) ciascuno dei quali non è normale: in particolare il loro normalizzatore è A_4. Questi sottogruppi inoltre sono tutti coniugati fra di loro e generano A_4: allora, passando ai campi con la corrispondenza di Galois, si ha quanto voluto. □

Si può fare a questo punto un'utile distinzione, sempre nel caso $w(\mathbf{L}) = 1$: se $c(\mathbf{L}) \neq 3$ (ossia $c(\mathbf{L}) = 1$ oppure $c(\mathbf{L}) = 5$) allora G non può essere isomorfo a A_4. Studiamo infatti la ramificazione di $\mathbf{F}$ su $\mathbb{Q}_2$ attraverso i gruppi di ramificazione di G nell'ipotesi

$G \cong A_4$. Abbiamo già visto nel corso della dimostrazione precedente che $G_0 \cong V$. Poiché $(|G_0/G_1|, 2) = 1$, risulta essere $G_1 = V$. Inoltre si ha che $G_i = \{0\}$ per ogni $i > e = 4$. Poiché nessun G_i può avere ordine 2 perché A_4 non ha sottogruppi normali di ordine 2 (e i gruppi di ramificazione sono tutti normali in G), si ricava (vedi proposizione 1.9.4) che $v(\mathcal{D}_{\mathbf{F}})$ può assumere i valori 6, 9, 12 o 15. Ma si ha $v(\mathcal{D}_{\mathbf{F}}) = v(\mathcal{D}_{\mathbf{L}})$ (perché, per le regole sul comportamento delle estensioni non ramificate rispetto alla traslazione, $\mathbf{F}/\mathbf{L}$ è non ramificata) e quindi, poiché i valori 9, 12 o 15 non sono possibili per $v(\mathcal{D}_{\mathbf{L}})$ (vedi tabella 3.1.3), deve essere $v(\mathcal{D}_{\mathbf{L}}) = d(\mathbf{L}) = 6$ cioè $c(\mathbf{L}) = 3$ (in realtà i casi $v(\mathcal{D}_{\mathbf{K}}) = 9, 15$ possono essere esclusi a priori, vedi [Se]). Possiamo allora concludere che le 4 estensioni con $c = 3$ e $w = 1$ devono avere gruppo di Galois isomorfo ad A_4 (esso si realizza almeno una volta come chiusura normale di certe estensioni ma queste per il ragionamento appena fatto possono solo avere $c = 3$), mentre le 4 con $c = 1$ e le 8 con $c = 5$ hanno chiusura normale con gruppo di Galois S_4 (ogni estensione con gruppo S_4 contiene 4 estensioni coniugate con $w = 1$).
Eccoci dunque pronti a organizzare i nostri risultati in una tabella.

Tabella 3.6: *estensioni di grado* 4 *su* $\mathbb{Q}_2$

Quantità	$e(\mathbf{L})$	$f(\mathbf{L})$	$d(\mathbf{L})$	$w(\mathbf{L})$	$G(\mathbf{F}\|\mathbb{Q}_2)$	Sottoestensioni
1	1	4	0	4	$\mathbb{Z}/4\mathbb{Z}$	1
1	2	2	4	4	$\mathbb{Z}/4\mathbb{Z}$	1
1	2	2	4	4	$(\mathbb{Z}/2\mathbb{Z})^2$	3
4	2	2	4	2	D_4	1
4	4	1	4	1	S_4	0
2	2	2	6	4	$\mathbb{Z}/4\mathbb{Z}$	1
2	2	2	6	4	$(\mathbb{Z}/2\mathbb{Z})^2$	3
4	2	2	6	2	D_4	1
4	4	1	6	2	D_4	1
4	4	1	6	1	A_4	0
4	4	1	8	4	$(\mathbb{Z}/2\mathbb{Z})^2$	3
4	4	1	8	2	D_4	1
8	4	1	8	1	S_4	0
16	4	1	9	2	D_4	1
16	4	1	10	2	D_4	1
8	4	1	11	4	$\mathbb{Z}/4\mathbb{Z}$	1
24	4	1	11	2	D_4	1

3.2 Il caso $p \neq 2$

3.2.1 Estensioni cicliche di grado p^2 su $\mathbb{Q}_p$

Proposizione 3.2.1 *Le estensioni* $\mathbf{L}$ *di Galois con* $G(\mathbf{L}|\mathbb{Q}_p) \cong \mathbb{Z}/p^2\mathbb{Z}$ *sono* $p(p+1)$*: tra queste esattamente* p^2 *sono totalmente ramificate.*

Dimostrazione[2] Dalla formula di Šafarevič risulta che le estensioni $\mathbf{L}$ di Galois con $G(\mathbf{L}|\mathbb{Q}_p) \cong \mathbb{Z}/p^2\mathbb{Z}$ sono $p(p+1)$ (gli automorfismi di $\mathbb{Z}/p^2\mathbb{Z}$ sono $p(p-1)$) mentre c'è

[2]Vedi anche i risultati del capitolo 4.

una sola estensione $\mathbf{L_0}$ di Galois con $G(\mathbf{L_0}|\mathbb{Q}_p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (gli automorfismi di $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sono $(p^2-1)(p^2-p)$). Quest'ultima non può che essere il composto delle $p+1$ estensioni di Galois grado p su $\mathbb{Q}_p$. Quindi si ha $e(\mathbf{L_0}|\mathbb{Q}_p) = f(\mathbf{L_0}|\mathbb{Q}_p) = p$.

Tra le rimanenti estensioni (quelle del tipo $\mathbf{L}$ con $G(\mathbf{L}|\mathbb{Q}_p) \cong \mathbb{Z}/p^2\mathbb{Z}$), c'è l'unica estensione $\mathbf{N}$ di grado p^2 su $\mathbb{Q}_p$ con $f(\mathbf{N}|\mathbb{Q}_p) = p^2$. D'altra parte, per Šafarevič, il gruppo $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ si realizza come gruppo di Galois di una estensione $\mathbf{M}$ di $\mathbb{Q}_p$. Tale gruppo possiede esattamente $p(p+1)+1$ sottogruppi di indice p^2, ovvero $\mathbf{M}$ ha esattamente $p(p+1)+1$ sottoestensioni (normali) di grado p^2 e, dall'analisi dei quozienti, si ricava che (come in realtà già sappiamo) una sola di esse ha gruppo di Galois isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Quindi $\mathbf{M}$ contiene tutte le estensioni di grado p^2 di Galois su $\mathbb{Q}_p$ e dunque è l'unica con questo gruppo di Galois.

Denotiamo con $\mathbf{K_0}$ l'unica estensione di grado p su $\mathbb{Q}_p$ non ramificata. Allora si ha $G(\mathbf{M}|\mathbf{K_0}) \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Infatti $G(\mathbf{M}|\mathbf{K_0})$ è un sottogruppo (abeliano) di $G(\mathbf{M}|\mathbb{Q}_p) \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$: quest'ultimo ha solo p^2-1 elementi di ordine p e nessuno di ordine p^3. $G(\mathbf{M}|\mathbf{K_0})$ ha dunque $p+1$ sottogruppi di ordine p^2. Questi sono in particolare anche sottogruppi di $G(\mathbf{M}|\mathbb{Q}_p)$ e considerati in questo modo solo uno di essi può avere quoziente isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$. Gli altri quozienti definiscono quindi p estensioni cicliche $\mathbf{L}$ di $\mathbb{Q}_p$ tali che $[\mathbf{L} : \mathbb{Q}_p] = p^2$ e $\mathbf{K_0} \subset \mathbf{L}$. È chiaro che queste sono tutte e sole le estensioni con questa proprietà e tra di esse è chiaramente compresa anche $\mathbf{N}$. Quindi ci sono esattamente $p-1$ estensioni cicliche $\mathbf{L}$ con $e(\mathbf{L}|\mathbb{Q}_p) = f(\mathbf{L}|\mathbb{Q}_p) = p$. □

Proposizione 3.2.2 *Sia* $\mathbf{L}$ *una estensione ciclica totalmente ramificata di grado* p^2 *su* $\mathbb{Q}_p$. *Allora* $v_{\mathbf{L}}(\mathcal{D}) = 3p^2 - p - 2$

Dimostrazione Sia $G(\mathbf{L}|\mathbb{Q}_p)$ il gruppo di Galois di $\mathbf{L}$ su $\mathbb{Q}_p$. Utilizzando le notazioni usuali per i sottogruppi di ramificazione si ha $G_{-1} = G(\mathbf{L}|\mathbb{Q}_p)$. Essendo inoltre $\mathbf{L}$ totalmente ramificata, risulta $G_0 = G(\mathbf{L}|\mathbb{Q}_p)$. Ma la ramificazione è wild quindi anche $G_1 = G(\mathbf{L}|\mathbb{Q}_p)$. Inoltre G_i $(i \in \mathbb{N})$ è banale se $i > \frac{e}{p-1}$, dove e indica l'indice di ramificazione assoluto, che in questo caso è $e(\mathbf{L}|\mathbb{Q}_p) = p^2$. Quindi G_i è banale se $i \geq p+2$. Inoltre i quozienti G_i/G_{i+1} sono p-gruppi abeliani elementari: in questo caso dunque, se G_i/G_{i+1} è non banale, è isomorfo a $\mathbb{Z}/p\mathbb{Z}$. I *salti* nella filtrazione data dai G_i, cioè gli indici i per cui $G_i \neq G_{i+1}$, sono congrui fra di loro modulo p. È facile dunque riconoscere che la filtrazione risulta essere la seguente

$$G_0 = G_1 \cong \mathbb{Z}/p^2\mathbb{Z} \qquad G_i = G_{i+1} \cong \mathbb{Z}/p\mathbb{Z} \quad \text{se} \quad 1 < i \leq p+1 \qquad G_i = 0 \quad \text{se } i > p+1.$$

Allora utilizzando la formula che mette in relazione la valutazione del differente con i sottogruppi di ramificazione

$$v_{\mathbf{L}}(\mathcal{D}) = \sum_{i=0}^{\infty} (|G_i| - 1)$$

si ottiene la tesi. □

Proposizione 3.2.3 *Sia* $\mathbf{L}$ *una estensione di Galois di grado* p^2 *su* $\mathbb{Q}_p$ *mista, cioè tale che risulti* $e(\mathbf{L}|\mathbb{Q}_p) = f(\mathbf{L}|\mathbb{Q}_p) = p$. *Allora* $v_{\mathbf{L}}(\mathcal{D}) = 2p - 2$.

Dimostrazione Se $\mathbf{L}$ è mista, allora l'indice di ramificazione assoluto vale p. Quindi, se $i > 1$, G_i è banale. D'altra parte $G_0 = G_1 \cong \mathbb{Z}/p\mathbb{Z}$ perché la ramificazione è wild. Utilizzando ancora la formula per $v_{\mathbf{L}}(\mathcal{D})$ si ottiene la tesi. □

Tabella 3.7: *estensioni di Galois di grado p^2 su $\mathbb{Q}_p$*

Numero di estensioni $\mathbf{L}$	$e(\mathbf{L}\|\mathbb{Q}_p)$	$f(\mathbf{L}\|\mathbb{Q}_p)$	$G(\mathbf{L}\|\mathbb{Q}_p)$	$v_{\mathbf{L}}(\mathcal{D})$
1	1	p^2	$\mathbb{Z}/p^2\mathbb{Z}$	0
1	p	p	$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	$2p-2$
$p-1$	p	p	$\mathbb{Z}/p^2\mathbb{Z}$	$2p-2$
p^2	p^2	1	$\mathbb{Z}/p^2\mathbb{Z}$	$3p^2-p-2$

3.2.2 Estensioni la cui chiusura normale ha gruppo di Galois isomorfo a $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$

Sia $\mathbf{L}_1$ una estensione di grado p^2 su $\mathbb{Q}_p$ tale che $w(\mathbf{L}_1) = p$. Indichiamo con $\mathbf{F}$ la chiusura normale di $\mathbf{L}_1$ e con $G = G(\mathbf{F}|\mathbb{Q}_p)$ il gruppo di Galois di $\mathbf{F}$ su $\mathbb{Q}_p$. Le estensioni come $\mathbf{F}$ sono i campi di spezzamento di certi polinomi irriducibili $q(X) \in \mathbb{Q}_p[X]$ di grado p^2. In questa sottosezione e nelle due successive analizzeremo quelle estensioni $\mathbf{L}_1$ tali che il normalizzatore del sottogruppo di G che lascia fisso $\mathbf{L}_1$ è normale in G. È facile rendersi conto che sotto queste ipotesi G ha ordine p^3 o p^4: è chiaro altresì che esso non sarà un gruppo abeliano[3]. Inoltre, essendo $w(\mathbf{L}_1) = p$, si ha che ci sono esattamente p estensioni coniugate a $\mathbf{L}_1$ su $\mathbb{Q}_p$ (tra cui $\mathbf{L}_1$ stessa), diciamo $\{\mathbf{L}_j\}_{j=1}^p$. Quindi $[\mathbf{L}_j : \mathbb{Q}_p] = p^2$ per ogni $1 \leq j \leq p$ ed inoltre $\bigcap_{j=1}^p \mathbf{L}_j = \mathbf{K}$ con $\mathbf{K}$ normale di grado p su $\mathbb{Q}_p$. Le estensioni $\mathbf{L}_j$ sono tutte normali di grado p su $\mathbf{K}$.

In questa e nella successiva sottosezione studieremo in dettaglio il caso in cui G ha ordine p^3. Richiedere che $[\mathbf{F} : \mathbb{Q}_p] = p^3$ equivale a richiedere che si abbia

$$G(\prod_{j=1}^{p} \mathbf{L}_i|\mathbf{K}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

In particolare G contiene un sottogruppo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Ci sono due gruppi di ordine p^3 non abeliani (vedi [Bu]): le notazioni abituali per indicarli sono $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ e $(\mathbb{Z}/p\mathbb{Z})^2 \ltimes \mathbb{Z}/p\mathbb{Z}$. Entrambi possiedono dei sottogruppi isomorfi a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In questa sottosezione ci occuperemo del caso $G \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$.

Indicheremo con $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ o equivalentemente con $G(4)$ il gruppo dato dalla seguente presentazione

$$G(4) = < P, Q >$$
$$P^{p^2} = E \qquad Q^p = E \qquad Q^{-1}PQ = P^{p+1}$$

La notazione $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ non risulta essere ambigua perché $G(4)$ è l'unico gruppo non abeliano di ordine p^3 isomorfo al prodotto semidiretto di due suoi sottogruppi H_1 e H_2 con $H_1 \cong \mathbb{Z}/p^2\mathbb{Z}$ e $H_2 \cong \mathbb{Z}/p\mathbb{Z}$. Osserviamo che $G(4)$ si realizza come gruppo di Galois di certe estensioni $\mathbf{L}$ di $\mathbb{Q}_p$: sono soddisfatte infatti le condizioni di Šafarevič.

Notazione Denotiamo con H e K rispettivalmente il sottogruppo generato da P e quello generato da Q, con riferimento a questa presentazione.

[3]Si può anche dimostrare che, nel caso in cui il normalizzatore del sottogruppo di G che lascia fisso $\mathbf{L}_1$ non sia normale in G, G non è un p-gruppo. Infatti il normalizzatore in questione avrebbe comunque indice p in G perché $w(\mathbf{L}_1) = p$. Se G fosse un p-gruppo tale normalizzatore dovrebbe essere normale in quanto sottogruppo massimale (vedi la sottosezione su w).

Osservazione 3.2.1 $|Aut(G(4))| = p^3(p-1)$

Dimostrazione Sia $A = \{f \in Aut(G(4)) | f(H) = H\} \leq Aut(G(4))$. È facile verificare che $[Aut(G(4)) : A] = p$. D'altra parte, se $f \in A$, allora

$$f(P) = P^i \quad 0 \leq i \leq p^2 - 1 \quad (i, p^2) = 1 \tag{3.4}$$

$$f(Q) = P^j Q^l \quad 0 \leq j \leq p^2 - 1 \quad 1 \leq l \leq p - 1 \tag{3.5}$$

Si osservi anche che, essendo $1 \leq l \leq p-1$

$$(P^j Q^l)^p = P^{j(\sum_{s=0}^{p-1}(p+1)^{sl})} = P^{j(\sum_{s=0}^{p-1}(p+1)^s)}$$

$$= P^{j(\sum_{s=0}^{p-1}(1+sp))} = P^{j(p+p^2)} = P^{jp}$$

Allora, poiché f è un automorfismo, si deve avere $j \equiv 0 \, (mod\, p)$. Si può allora scrivere $f(Q) = P^{pm}Q^l$ con $0 \leq m \leq p-1$ e $pm = j$. Inoltre, imponendo che

$$f(Q^{-1}PQ) = f(P^{p+1}) \quad \Leftrightarrow \quad P^{pm}Q^l P^i Q^{-l} P^{-pm} = P^{i(p+1)}$$

poiché $P^{pm}Q^l P^i Q^{-l} P^{-pm} = P^{pi-pil}$ (come si riconosce facilmente) si ottiene la condizione

$$pi - pil \equiv pi + i \quad (mod\, p^2)$$

che è soddisfatta se e solo se $l = 1$ ancora una volta perché $1 \leq l \leq p-1$. Dunque $f \in A$ se e solo se (con le notazioni di (3.4) e (3.5)) le seguenti condizioni sono soddisfatte

$$(i, p^2) = 1 \qquad j \equiv 0 \quad (mod\, p) \qquad l = 1$$

Per cui $|A| = p^2(p-1)$ e di conseguenza $|Aut(G(4))| = p|A| = p^3(p-1)$. □

Conseguenza Dalla formula di Šafarevič si ricava che ci sono esattamente $p^2 - 1$ estensioni $\mathbf{F}$ di Galois su $\mathbb{Q}_p$ tali che $G(\mathbf{F}|\mathbb{Q}_p) \cong G(4)$.

Osserviamo esplicitamente che una estensione di Galois su $\mathbb{Q}_p$ con gruppo di Galois isomorfo a $G(4)$ è la chiusura normale di p estensioni di grado p^2 fra loro coniugate: è una semplice conseguenza della struttura di $G(4)$ e della corrispondenza di Galois.

Indichiamo ora con $\{\mathbf{K}_i\}_{i=0}^p$ le $p+1$ estensioni di grado p di Galois di $\mathbb{Q}_p$ e tra queste denotiamo con $\mathbf{K}_0$ l'unica non ramificata. Ci proponiamo allora di determinare, fissato $i \in \{0, 1, ..., p\}$, per quante delle estensioni $\mathbf{F}$ con $G(\mathbf{F}|\mathbb{Q}_p) \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ si ha $\bigcap_{j=1}^p \mathbf{L}_j = \mathbf{K}_i$.

Notazione Siano $\mathbf{F}$ e $\{\mathbf{L}_j\}_{j=1}^p$ come nelle convenzioni iniziali e $\bigcap_{j=1}^p \mathbf{L}_j = \mathbf{K}_i$. Diremo allora che $\mathbf{F}$ è *relativa* a $\mathbf{K}_i$.

Notazione Indicheremo con $G(8)$ il gruppo di ordine p^4 dato con la seguente presentazione

$$G(8) = < P, Q >$$

$$P^{p^2} = E \qquad Q^{p^2} = E \qquad Q^{-1}PQ = P^{p+1}$$

Notazione Indicheremo con $G(10)$ il gruppo di ordine p^4 dato con la seguente presentazione

$$G(10) = < P, Q, R >$$

$$P^{p^2} = E \qquad Q^p = E \qquad R^p = E \qquad Q^{-1}PQ = P \qquad Q^{-1}RQ = R \qquad R^{-1}PR = PQ$$

Osservazione 3.2.2 *$G(8)$ ha centro isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In particolare ha p sottogruppi $\{H_m\}_{m=1}^p$ normali di ordine p tali che $G(8)/H_m \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$. Inoltre ciascuno degli H_m è contenuto esattamente in p sottogruppi $\{K_{mt}\}_{t=1}^p$ di ordine p^2 non normali in $G(8)$. Infine, se $< K_{mt}$, $t = 1, 2, ..., p >= G_m$, si ha che $|G_m| = p^3$ e $G_{m_1} = G_{m_2}$ se e solo se $m_1 = m_2$.*

Dimostrazione In primo luogo, si verifica facilmente per induzione su n che

$$(P^j Q^k)^n \; = \; Q^{nk} P^{j(n+kp\frac{n(n+1)}{2})} \tag{3.6}$$

L'affermazione sul centro è dimostrata verificando direttamente che i soli sottogruppi di ordine p (che peraltro sono tutti normali) di G sono del tipo $H_m =< P^{mp} Q^p >$ al variare di m in $\{1, 2, ..., p\}$ ai quali si aggiunge $N =< P^p >$. Quest'ultimo in particolare è l'unico che ha quoziente non isomorfo a $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ (infatti $G/N \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$), mentre $G/H_m \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ (verifica diretta). Da (3.6) si ricava che $< P^j Q^k >$ è ciclico di ordine p^2 se e solo se $p \nmid k$ oppure $p \nmid j$. Inoltre, sotto queste ipotesi, $H_m \subseteq < P^j Q^k >$ se e solo se esiste $l \in \{1, 2, ..., p-1\}$ tale che

$$lk \equiv 1 \pmod p \quad e \quad lj \equiv m \pmod p$$

che equivale a

$$lk \equiv 1 \pmod p \quad e \quad mk \equiv j \pmod p \tag{3.7}$$

Fissato m ci sono allora esattamente p sottogruppi ciclici di ordine p^2 che contengono H_m: infatti, scelto $k = 1$ nella (3.7), si ha $H_m \subseteq < P^{m+tp} Q >$ per ogni $0 \leq t \leq p-1$. Osserviamo ora che si ha

$$< P^{m+t_1 p} Q >=< P^{m+t_2 p} Q > \quad \Leftrightarrow \quad t_1 = t_2$$

e d'altra parte scelto $k \in \{1, 2, ..., p^2 - 1\}$ tale che $p \nmid k$ si ha che per ogni $0 \leq t_1 \leq p-1$ esiste t_2 con $0 \leq t_2 \leq p-1$ tale che $< P^{km+t_1 p} Q^k >=< P^{m+t_2 p} Q >$ (basterà prendere $2t_2 \equiv mk(k-1) + 2t_1 \, (mod\, p)$). Allora ogni H_m è contenuto in p sottogruppi distinti, segnatamente $\left\{K_{mt} =< P^{m+tp} Q >\right\}_{t=0}^{p-1}$. Verifichiamo che, oltre ai K_{mt} non ci sono altri sottogruppi non normali in $G(8)$ di ordine p^2 che contengano H_m. Se ce ne fossero altri di ordine p^2 sicuramente non saranno ciclici, perché gli unici ciclici sono i K_{mt}. Inoltre utilizzando ancora la (3.6), risulta che l'unico sottogruppo non ciclico di ordine p^2 in $G(8)$ è il centro: esso contiene H_m ma è normale in $G(8)$.
Verifichiamo adesso l'ultima affermazione. Consideriamo

$$G_m =< P^{m+tp} Q, \, t = 0, 1, ..., p-1 >$$

È immediato riconoscere che $G_m =< P^m Q, P^p >$ e, poiché $P^p \in Z(G(8))$, si ha che $G_m \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Supponiamo $m_1 \neq m_2$. Allora, se per assurdo fosse $G_{m_1} = G_{m_2}$, si avrebbe che $P^{m_1 - m_2} \in G_{m_1}$ e quindi, poiché $p \nmid (m_1 - m_2)$, $P \in G_{m_1}$. Ma allora $Q = P^{-m_1}(P^{m_1} Q) \in G_{m_1}$ e quindi $G_{m_1} = G$, che è una contraddizione. □

Osservazione 3.2.3 *Si ha $Z(G(10)) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e $G(10)$ ha un unico sottogruppo K tale che $K \cong (\mathbb{Z}/p\mathbb{Z})^3$. Inoltre ha esattamente $p-1$ sottogruppi $\{H_m\}_{m=1}^{p-1}$ normali di ordine p tali che $G(10)/H_m \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$: in particolare, ciascuno degli H_m è contenuto in esattamente p sottogruppi $\{K_{mt}\}_{t=1}^{p}$ di ordine p^2 non normali in $G(10)$. Infine, scelti comunque $1 \leq m_1, m_2 \leq p-1$ e $1 \leq t_1, t_2 \leq p$, si ha $< K_{m_1 t_1}, K_{m_1 t_2} >= K$.*

Dimostrazione Sicuramente $< P^p\, Q > \subset Z(G(10))$. D'altra parte $|Z(G(10))| \leq p^2$ perché $G(10)$ non è abeliano. Quindi $Z(G(10)) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Inoltre non è difficile riconoscere che $K =< P^p,\, Q,\, R >$: è chiaro che K è un p-gruppo abeliano elementare di rango 3. Osserviamo ora che

$$(P^i Q^j R^k)^n = P^{in} Q^{nj-ikn} \tag{3.8}$$

Quindi gli elementi di ordine p sono solo quelli in K. Inoltre il sottogruppo delle p-esime potenze è $< P^p >$.
Quindi $G(10)$ ha in tutto $p+1$ sottogruppi normali di ordine p (che sono quelli contenuti nel centro). Poniamo $H_m =< P^{mp} Q >$ per $m = 1,\, 2,\, \ldots,\, p-1$. Non è difficile verificare che $G(10)/H_m \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$. Inoltre gli altri due sottogruppi normali di ordine p sono $< P^p >$ e $< Q >$ e non hanno quoziente isomorfo a $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$. Poniamo ora, per ogni $m = 1,\, 2,\, \ldots,\, p-1$, $K_{mt} =< P^{mp} Q,\, RQ^t >$. È facile riconoscere che, fissato m, si ha $K_{mt_1} = K_{mt_2}$ se e solo se $t_2 = t_1$. Infatti $RQ^{t_1} \in K_{mt_2}$ se e solo se esistono $0 \leq a,\, b < p$ tali che $RQ^{t_1} = P^{amp} Q^{a+bt_2} R^b$ e questo è possibile se e solo se $t_2 = t_1$. Dunque, fissato m, al variare di t tra 1 e p, i K_{mt} costituiscono una famiglia di p sottogruppi (distinti) di $G(10)$ di ordine p^2 (isomorfi a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$) che contengono H_m. I K_{mt} sono tutti non normali: ciò è conseguenza del fatto che

$$P^{-1} RQ^t P = RQ^{t-1}$$

e (per quanto osservato prima) $RQ^{t-1} \notin K_{mt}$. I K_{mt} sono i soli sottogruppi di ordine p^2 non normali in $G(10)$ che contengano H_m. Infatti, in primo luogo non c'è nessun sottogruppo ciclico di ordine p^2 che contiene H_m perché il sottogruppo delle p-esime potenze è $< P >$. Se H è un sottogruppo di ordine p^2 non ciclico di $G(10)$, di sicuro è contenuto in K (è il caso ad esempio dei K_{mt}). Fissato un sottogruppo H_m, in particolare esso è un sottogruppo di ordine p di $K \cong (\mathbb{Z}/p\mathbb{Z})^3$ ed è quindi contenuto in esattamente $p+1$ sottogruppi di ordine p^2 di K (e quindi è contenuto in esattamente $p+1$ sottoggruppi non ciclici di ordine p^2 di $G(10)$). L'unico che non è compreso nei K_{mt} è il centro che però è normale.
Infine è immediato convincersi dell'ultima affermazione. □

Osservazione 3.2.4 $|Aut(G(10)| = p^5(p-1)^2$

Dimostrazione Sia f un automorfismo di $G(10)$. Poniamo

$$f(P) = P^a Q^b R^c \qquad 0 \leq a \leq p^2 - 1 \quad 0 \leq b, c \leq p-1$$

$$f(Q) = P^i Q^j \qquad 0 \leq i \leq p^2 - 1 \quad i \equiv 0\,(mod\, p) \quad 0 \leq j \leq p-1$$

$$f(R) = P^s Q^t R^u \qquad 0 \leq s \leq p^2 - 1 \quad 0 \leq t, u \leq p-1$$

la seconda posizione essendo giustificata dal fatto che $Z(G(10)) =< P^p, Q >$ è caratteristico. Inoltre $\mathrm{ord}(f(P)) = p^2$. Questo impone che $(a, p) = 1$. Infatti utilizzando l'identità

$$P^a R^c = Q^{ac} R^c P^a$$

si ottiene che $f(P)^p = P^{ap}$. Inoltre si ha che (utilizzando ancora l'identità precedente)

$$f(R^{-1}PR) = P^a Q^{b-cs-au} R^c$$

Dovendo essere $f(R^{-1}PR) = f(PQ) = P^{a+i}Q^{b+j}R^c$, si ottengono allora le condizioni $i \equiv 0 \ (mod\, p^2)$ e $b - cs + au \equiv b + j \ (mod\, p)$. Notiamo infine che, poiché deve essere $ord(f(R)) = p$, si deve avere $s \equiv 0 \ (mod\, p)$. L'osservazione fondamentale è che le condizioni necessarie fin qui trovate sono anche sufficienti, ossia $f \in Aut(G(10))$ se e solo se

$$(j, p) = 1\,; \qquad i \equiv 0 \pmod{p^2}\,; \qquad s \equiv 0 \pmod{p}\,; \qquad au \equiv j \pmod{p} \tag{3.9}$$

(in particolare queste condizioni implicano $(a, p) = 1$). Infatti condizione necessaria e sufficiente affinché f sia un automorfismo è che $Ker(f) = \{E\}$. La condizione di banalità del nucleo si può scrivere anche

$$f(P^h Q^k R^l) = E \qquad \Rightarrow \qquad h \equiv 0 \pmod{p^2}\,; \quad k \equiv 0 \pmod{p}\,; \quad l \equiv 0 \pmod{p}$$

Utilizzando la solita identità si riconosce che $f(P^h Q^k R^l) = Q^\beta R^\gamma P^\alpha$ con

$$\alpha = sl + ha \qquad \beta = bh + kj + tl + \sum_{n=1}^{h} acn + \sum_{m=1}^{l} msu + ulha \qquad \gamma = hc + ul \tag{3.10}$$

Se vale la (3.10), f è un automorfismo quindi vale la (3.9). Viceversa se vale la (3.9), non è difficile riconoscere che la (3.10) implica $h \equiv 0 \, (mod\, p^2)$, $k \equiv 0 \, (mod\, p)$ e $l \equiv 0 \, (mod\, p)$ cioè f è un automorfismo. Quindi per contare gli automorfismi di $G(10)$ possiamo contare quante possibilità ci sono per a, b, c, i, j, s, t, u in relazione alla (3.9). Un rapido calcolo porta allora alla tesi. □

Osservazione 3.2.5 *$G(10)$ può essere generato con due elementi.*

Dimostrazione In un p-gruppo (finito) G il quoziente $G/\phi(G)$ (dove con $\phi(G)$ si denota al solito il sottogruppo di Frattini) è un p-gruppo abeliano elementare il cui rango corrisponde al numero (minimale) di generatori per G. Inoltre sotto queste ipotesi è noto che $\phi(G)$ è generato dalle p-esime potenze e dai commutatori. Non è difficile verificare, utilizzando l'identità più volte sfruttata nella dimostrazione precedente, che $\phi(G(10)) = Z(G(10))$, quindi si ha la tesi considerando la cardinalità del quoziente. □

Conseguenza Per il criterio di Šafarevič $G(8)$ e $G(10)$ si realizzano come gruppi di Galois di certe estensioni di $\mathbb{Q}_p$.

Conseguenza Dalla formula di Šafarevič si ricava che ci sono esattamente $p+1$ estensioni $\mathbf{E}$ di $\mathbb{Q}_p$ tali che $G(\mathbf{E}|\mathbb{Q}_p) \cong G(10)$.

Proposizione 3.2.4 *Siano $\mathbf{F}'$ e $\mathbf{F}''$ estensioni distinte relative entrambe a $\mathbf{K}_i$. Allora $G = G(\mathbf{F}'\mathbf{F}''|\mathbb{Q}_p) \cong G(10)$.*

Dimostrazione In primo luogo certamente G non sarà un gruppo abeliano, quindi con riferimento alla classificazione di Burnside, G non sarà di tipo (i), (ii), (iii), (iv) e (v). Inoltre G si realizza come gruppo di Galois di una estensione di $\mathbb{Q}_p$, quindi deve avere un numero (minimale) di generatori inferiore a 3. Vengono allora scartati i gruppi (vii), (ix), (xiv) e (xv). G deve avere (almeno) due sottogruppi normali H' e H'' di ordine p tali che

$$G/H' \cong G/H'' \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$$

In particolare $H' = G(\mathbf{F}'\mathbf{F}''|\mathbf{F}')$ e $H'' = G(\mathbf{F}'\mathbf{F}''|\mathbf{F}'')$. Dunque, poichè i sottogruppi normali di ordine p in un p-gruppo sono contenuti nel centro, il centro di G dovrà contenere almeno due (e quindi almeno $p+1$) sottogruppi di ordine p. Si può inoltre verificare che allora $Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In ogni caso verrano scartati a causa di questa seconda condizione i gruppi (vi), (xi), (xii) e (xii). Inoltre l'ipotesi che $\mathbf{F}'$ e $\mathbf{F}''$ siano relative ad una stessa estensione $\mathbf{K}_i$ implica che H' e H'' siano contenuti ciascuno in p sottogruppi (non normali) di ordine p^2 (nella notazione fin qui usata questi sottogruppi sono rispettivamente $G(\mathbf{F}'\mathbf{F}''|\mathbf{L}'_j)$ e $G(\mathbf{F}'\mathbf{F}''|\mathbf{L}''_j)$ con $j = 1, 2, ..., p$) e infine che tutti questi $2p$ sottogruppi siano contenuti tutti in uno stesso sottogruppo di indice p (che è $G(\mathbf{F}'\mathbf{F}''|\mathbf{K}_i)$). Questa condizione esclude, in virtù dell'osservazione precedente, il gruppo (viii) e conclude la dimostrazione. Si può peraltro verificare direttamente senza troppa difficoltà che (x) verifica tutte le condizioni richieste. □

Proposizione 3.2.5 *Siano $\mathbf{F}'$ e $\mathbf{F}''$ estensioni con $\mathbf{F}'$ relativa a $\mathbf{K}_{i'}$ e $\mathbf{F}''$ relativa a $\mathbf{K}_{i''}$ con $i' \neq i''$. Allora $G = G(\mathbf{F}'\mathbf{F}''|\mathbb{Q}_p) \cong G(8)$.*

Dimostrazione Per gli stessi motivi addotti nella dimostrazione della proposizione precedente, G non potrà essere di tipo (i), (ii), (iii), (iv), (v), (vi), (vii), (ix), (xi), (xii), (xii), (xiv) e (xv). Anche qui dunque rimangono il tipo (viii) e quello (x). G deve avere (almeno) due sottogruppi normali H' e H'' di ordine p tali che

$$G/H' \cong G/H'' \cong \mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$$

In particolare $H' = G(\mathbf{F}'\mathbf{F}''|\mathbf{F}')$ e $H'' = G(\mathbf{F}'\mathbf{F}''|\mathbf{F}'')$. Inoltre l'ipotesi che $\mathbf{F}'$ e $\mathbf{F}''$ siano relative ad estensioni distinte $\mathbf{K}'_i$ e $\mathbf{K}''_i$ implica che ci sono due famiglie distinte costituite ciascuna da p sottogruppi (non normali) di ordine p^2 (nella notazione fin qui usata questi sottogruppi sono rispettivamente $G(\mathbf{F}'\mathbf{F}''|\mathbf{L}'_j)$ e $G(\mathbf{F}'\mathbf{F}''|\mathbf{L}''_j)$ con $j = 1, 2, ..., p$), la prima che contiene sottogruppi contenenti H' e la seconda sottogruppi contenenti H''. Queste due famiglie di sottogruppi infine sono contenute in due diversi sottogruppi di indice p (che sono $G(\mathbf{F}'\mathbf{F}''|\mathbf{K}'_i)$ e $G(\mathbf{F}'\mathbf{F}''|\mathbf{K}''_i)$). Questa condizione esclude, in virtù dell'osservazione precedente, il gruppo (x) e conclude la dimostrazione. Si può peraltro verificare direttamente senza troppa difficoltà che (viii) verifica tutte le condizioni richieste. □

Proposizione 3.2.6 *Fissato $i \in \{0, 1, ..., p\}$, ci sono esattamente $p-1$ estensioni distinte relative a $\mathbf{K}_i$.*

Dimostrazione In primo luogo $G(10)$ si realizza come gruppo di Galois di una estensione di $\mathbb{Q}_p$, quindi ci sono p estensioni $\mathbf{F}_i$ con $i = 0, 1, \ldots, p-1$ relative ciascuna ad una diversa estensione normale di grado p di $\mathbb{Q}_p$, diciamo che queste siano $\mathbf{K}_i$ con $i = 0, 1, \ldots, p-1$ e $\mathbf{F}_i$ relativa a $\mathbf{K}_i$. Allora ci sono p famiglie distinte $\{\mathcal{F}_i\}_{i=0}^{p-1}$ di

estensioni di Galois con gruppo di Galois isomorfo a $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ e ciascuna famiglia contiene $p-1$ di queste estensioni tutte relative ad una stessa estensione di grado p su $\mathbb{Q}_p$. Inoltre per il criterio di Šafarevič c'è un'estensione di Galois con gruppo $G(8)$. Supponiamo per assurdo che l'estensione $\mathbf{K}_p$ sia priva di estensioni ad essa relative. La famiglia $\mathcal{F}_p$ che è quella dell'ultimo gruppo $G(8)$ che non abbiamo ancora contato sarà dunque relativa diciamo all'estensione $\mathbf{K}_{i_0}$. Componendo un membro della famiglia $\mathcal{F}_0$ con uno della famiglia $\mathcal{F}_p$ si ottiene allora una estensione con gruppo $G(8)$ nuova, che non può cioè essere una di quelle che contengono una delle famiglie $\mathcal{F}_i$. Questo è impossibile e quindi la famiglia $\mathcal{F}_p$ deve essere relativa a $\mathbf{K}_p$. Quindi due famiglie distinte sono relative ad estensioni distinte e si conclude. □

Osservazione 3.2.6 *Sia* $\mathbf{L}$ *è un estensione di grado* p^2 *su* $\mathbb{Q}_p$ *tale che detta* $\mathbf{F}$ *la sua chiusura normale, si abbia che* $\mathbf{F}$ *è relativa ad una estensione normale di grado* p *di* $\mathbb{Q}_p$ *totalmente ramificata. Allora* $v_{\mathbf{F}}(\mathcal{D}) = v_{\mathbf{K}}(\mathcal{D}) = 3p^2 - p - 2$.

Dimostrazione Per ipotesi, $G(\mathbf{F}|\mathbb{Q}_p)$ è isomorfo a $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$. È facile verificare, considerando la struttura di $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ e sfruttando l'ipotesi che $\mathbf{F}$ è relativa ad una estensione totalmente ramificata, che il gruppo di inerzia $G_0(\mathbf{F}|\mathbb{Q}_p)$ dell'estensione $\mathbf{F}$ su $\mathbb{Q}_p$ è isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$. L'affermazione su $v_{\mathbf{F}}(\mathcal{D})$ segue allora dal solito criterio che stabilisce che i gruppi di ramificazione G_i sono banali se $i > \frac{e}{p-1}$, dove e indica l'indice di ramificazione assoluto, che in questo caso è $e(\mathbf{F}|\mathbb{Q}_p) = p^2$. Quindi $G_{p+2} = \{1\}$: ricordando che gli indici i tali che $G_i \neq G_{i+1}$ devono essere congrui tra di loro modulo p e che G_i/G_{i+1} per $i \geq 1$ è isomorfo ad un prodotto diretto di gruppi ciclici di ordine p, si ha $v_{\mathbf{F}}(\mathcal{D}) = 3p^2 - p - 2$. D'altra parte, poiché $\mathbf{F}$ è non ramificata su $\mathbf{K}$, si ottiene anche l'altra uguaglianza. □

Tabella 3.8: *estensioni di grado* p^2 *su* $\mathbb{Q}_p$ *la cui chiusura normale ha gruppo* $G(4)$

Numero di estensioni $\mathbf{L}$	$e(\mathbf{L}\|\mathbb{Q}_p)$	$f(\mathbf{L}\|\mathbb{Q}_p)$	$G_0(\mathbf{F}\|\mathbb{Q}_p)$	$v_{\mathbf{L}}(\mathcal{D})$
$p^2 - p$	p^2	1	$\mathbb{Z}/p^2\mathbb{Z}$	$3p^2 - p - 2$
$p - 1$	p	p	$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	

3.2.3 Estensioni la cui chiusura normale ha gruppo di Galois isomorfo a $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \ltimes \mathbb{Z}/p\mathbb{Z}$

Con riferimento alle notazioni introdotte nella sottosezione precedente (e che saranno mantenute in questa), in questa sottosezione ci occuperemo del caso in cui si ha $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \ltimes \mathbb{Z}/p\mathbb{Z}$.

Indichiamo con $G(5)$ o equivalentemente con $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \ltimes \mathbb{Z}/p\mathbb{Z}$ il gruppo dato dalla seguente presentazione

$$G(5) = < P, Q, R >$$

$$P^p = E \qquad Q^p = E \qquad R^p = E \qquad R^{-1}QR = QP \qquad R^{-1}PR = P \qquad Q^{-1}PQ = P$$

Anche qui, come nel caso di $\mathbb{Z}/p^2\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$, la notazione non è ambigua, perché c'è un solo gruppo non abeliano di ordine p^3 che sia prodotto semidiretto di un sottogruppo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e di uno ciclico di ordine p.

Osservazione 3.2.7 *$G(5)$ può essere generato da due elementi.*

Dimostrazione Per dimostrare la tesi, basta controllare che $\phi(G(5))$, il sottogruppo di Frattini di $G(5)$, ha cardinalità p. Infatti, di certo non consiste della sola identità perché $G(5) \ncong (\mathbb{Z}/p\mathbb{Z})^3$. Se fosse $|\phi(G(5))| = p^2$, allora $G(5)$ sarebbe ciclico, il che è chiaramente falso. Poiché infine, per definizione, $\phi(G(5)) \neq G(5)$ (il sottogruppo di Frattini è l'intersezione dei sottogruppi massimali), si ha la tesi. □

Conseguenza Per il criterio di Šafarevič $G(5)$ si realizza come gruppo di Galois di (almeno) una estensione di $\mathbb{Q}_p$.

Osservazione 3.2.8 $|Aut(G(5))| = p^3(p-1)^2(p+1)$.

Dimostrazione Sia $f \in Aut(G(5))$. È facile osservare che $Z(G(5)) =< P >$: quindi, essendo il centro un sottogruppo caratteristico, possiamo scrivere

$$\begin{aligned} f(P) &= P^i \qquad 0 \leq i \leq p-1 \\ f(Q) &= P^a R^c Q^b \qquad 0 \leq a, b, c \leq p-1 \\ f(R) &= P^s R^u Q^t \qquad 0 \leq s, t, u \leq p-1 \end{aligned}$$

Osserviamo che vale la seguente identità

$$Q^h R^k = P^{hk} R^k Q^h$$

Imponendo che $f(Q^{-1}RQ) = f(QP)$ e utilizzando la precedente identità, si ottiene che

$$i \equiv bu - ct \pmod{p}$$

Inoltre, poiché f è un automorfismo, si deve avere che $(i, p) = 1$ e almeno uno tra b e c non è divisibile per p, cioè $(bc, p^2) \neq p^2$. Anche qui, l'osservazione fondamentale è che le condizioni necessarie fin qui trovate sono anche sufficienti, ossia $f \in Aut(G(5))$ se e solo se

$$(i, p) = 1\,; \qquad i \equiv bu - ct \pmod{p} \tag{3.11}$$

(in particolare queste condizioni implicano $(bc, p^2) \neq p^2$). Infatti condizione necessaria e sufficiente affinché f sia un automorfismo è che $Ker(f) = \{E\}$. La condizione di banalità del nucleo si può scrivere anche

$$f(P^h Q^k R^j) = E \qquad \Rightarrow \qquad h \equiv 0 \pmod{p}\,; \quad k \equiv 0 \pmod{p}\,; \quad j \equiv 0 \pmod{p}$$

Utilizzando la solita identità si riconosce che $f(P^h Q^k R^j) = P^\alpha R^\gamma Q^\beta$ con

$$\alpha = ih + ak + sj + \sum_{n=1}^{h} cbn + \sum_{m=1}^{l} mut + kbju \qquad \beta = kb + jt \qquad \gamma = ju + ck \tag{3.12}$$

Se vale la (3.12), f è un automorfismo quindi vale la (3.11). Viceversa se vale la (3.11), non è difficile riconoscere che la (3.12) implica $h \equiv 0\,(mod\,p)$, $k \equiv 0\,(mod\,p)$ e $j \equiv 0\,(mod\,p)$ cioè f è un automorfismo. Quindi per contare gli automorfismi di $G(5)$ possiamo contare quante possibilità ci sono per a, b, c, i, s, t, u in relazione alla (3.11). Un rapido calcolo porta allora alla tesi. □

Conseguenza Dalla formula di Šafarevič si ricava che c'è un'unica estensione $\mathbf{F}$ di $\mathbb{Q}_p$ tale che $G(\mathbf{F}|\mathbb{Q}_p) \cong G(5)$.

Osservazione 3.2.9 *$G(5)$ ha esattamente p^2+p+1 sottogruppi di ordine p, uno solo dei quali è normale, segnatamente quello generato da P. Cascun sottogruppo di ordine p non normale è contenuto in un solo sottogruppo di ordine p^2 che risulta essere non ciclico ed ovviamente normale (perché massimale). Ci sono esattamente $p+1$ sottogruppi di ordine p^2 non ciclici e $<P>$ è contenuto in ciascuno di essi. Inoltre due sottogruppi di ordine p non normali che siano contenuti nello stesso sottogruppo di ordine p^2 sono coniugati.*

Dimostrazione Tutti gli elementi di $G(5)$ hanno ordine p (tranne E), quindi è chiaro che ci sono $(p^3-1)/(p-1) = p^2+p+1$ sottogruppi di ordine p. Sappiamo già che $Z(G(5)) =< P >$ e gli altri sottogruppi di ordine p non sono normali altrimenti dovrebbero essere contenuti nel centro. Inoltre è chiaro che nessun sottogruppo di ordine p^2 di $G(5)$ sarà ciclico e che ogni sottogruppo di ordine p è contenuto in (almeno) un sottogruppo di ordine p^2 (sempre perché $G(5)$ è un p-gruppo). Inoltre ogni sottogruppo di ordine p^2 (cioè massimale) contiene $<P>$ (perché esso è anche il sottogruppo di Frattini di $G(5)$). Se fosse allora che un certo sottogruppo di ordine p non normale, diciamo quello generato da X (e quindi $X \notin < P >$), è contenuto in due sottogruppi distinti di ordine p^2, diciamo H e K, si avrebbe che $<X, P>\subset H \cap K$ e quindi $<X, P>= H \cap K$. In particolare $H = K$, assurdo. Allora è anche chiaro che ci sono $(p^2+p)/p = p+1$ sottogruppi di ordine p^2.
Veniamo all'ultima affermazione. Fissiamo i, j, k $(0 \leq i, j, k \leq p-1)$ in modo che $P^iQ^jR^k$ sia un elemento di $G(5)$ che genera un sottogruppo di ordine p non normale, cioè $j \neq 0$ oppure $k \neq 0$. Allora i sottogruppi di ordine p contenuti in $<P, P^iQ^jR^k>$ sono $<P>$ e $\{<P^{i+s}Q^jR^k>\}_{s=0}^{p-1}$. Per dimostrare l'ultima affermazione della tesi basta verificare allora che, preso un s tra 0 e $p-1$, esiste un elemento $X \in G(5)$ tale che $XP^{i+s}Q^jR^kX^{-1} = P^iQ^jR^k$. Sia $X = P^aQ^bR^c$. Si ha

$$XP^{i+s}Q^jR^kX^{-1} = P^{i+s}Q^bR^cQ^jR^{k-c}Q^{-b} = P^{i+s-cj+bk}Q^jR^k$$

Se $j \neq 0$, scegliamo a e b qualsiasi e $c = j^{-1}(bk-s)$. Se $k \neq 0$, scegliamo a e c qualsiasi e $b = k^{-1}(cj+s)$. In questo modo abbiamo quanto voluto. □

Osservazione 3.2.10 *L'unica estensione $\mathbf{F}$ di $\mathbb{Q}_p$ tale che $G(\mathbf{F}|\mathbb{Q}_p) \cong G(5)$ possiede esattamente p^2+p+1 sottoestensioni $\mathbf{L}_i$ di grado p^2 su $\mathbb{Q}_p$ e una sola di queste è normale. Inoltre ciascuna delle estensioni non normali $\mathbf{L}_i$ ha una sottoestensione normale su $\mathbb{Q}_p$ di grado p e due estensioni che hanno la stessa sottoestensione sono coniugate su $\mathbb{Q}_p$. Infine $\mathbf{F}$ contiene tutte le $p+1$ estensioni normali di grado p su $\mathbb{Q}_p$ e ciascuna di esse è contenuta in esattamente p estensioni non normali $\mathbf{L}_i$.*

Dimostrazione Tutte le affermazioni sono facile conseguenza dell'osservazione precedente in virtù della corrispondenza di Galois. □

3.2.4 Estensioni la cui chiusura normale ha ordine p^4

Continuiamo a utilizzare le notazioni delle due sottosezioni precedenti: in queste ultime abbiamo analizzato in dettaglio quelle estensioni $\mathbf{L}$ tali che il normalizzatore del sottogruppo di G che lascia fisso $\mathbf{L}$ è normale in G e $[\mathbf{F} : \mathbb{Q}_p] = p^3$. In questa sottosezione analizziamo invece le estensioni $\mathbf{L}$ tali che ancora il normalizzatore del sottogruppo di G

Tabella 3.9: *estensioni di grado p^2 su $\mathbb{Q}_p$ la cui chiusura normale ha gruppo $G(5)$*

Numero di estensioni $\mathbf{L}$	$e(\mathbf{L}\|\mathbb{Q}_p)$	$f(\mathbf{L}\|\mathbb{Q}_p)$	$G_0(\mathbf{F}/\mathbb{Q}_p)$	$v_{\mathbf{L}}(\mathcal{D})$
p^2	p^2	1	$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	
p	p	p	$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	

che lascia fisso $\mathbf{L}$ è normale in G ma $[\mathbf{F} : \mathbb{Q}_p] = p^4$. Richiedere che $[\mathbf{F} : \mathbb{Q}_p] = p^4$ equivale a richiedere che si abbia

$$G(\prod_{j=1}^{p} \mathbf{L}_i|\mathbf{K}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

In particolare G contiene un sottogruppo isomorfo a $(\mathbb{Z}/p\mathbb{Z})^3$. Ci sono diversi gruppi di ordine p^4 non abeliani (vedi [Bu]) ma uno solo fa al caso nostro. Per dimostrarlo concentriamo l'attenzione su questo particolare gruppo di ordine p^4.

Il gruppo $G(11)$ è un gruppo di ordine p^4 (p primo, $p \neq 2$) definibile nel modo seguente

$$G(11) =< P, Q, R >$$

$$P^{p^2} = E \qquad Q^p = E \qquad R^p = E \qquad Q^{-1}PQ = P^{p+1}$$

$$R^{-1}PR = PQ \qquad Q^{-1}RQ = R$$

Notazione Nel seguito di questa sottosezione indicheremo semplicemente con $\mathcal{G}$ il gruppo $G(11)$.

Osservazione 3.2.11 *Sia $\phi(\mathcal{G})$ il sottogruppo di Frattini di $\mathcal{G}$. Allora si ha che $\phi(\mathcal{G}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione È facile riconoscere che $< P^p >$ è contenuto nel sottogruppo $\mathcal{G}^p$ generato dalle p-esime potenze, mentre $< Q >$ è contenuto nel sottogruppo $\mathcal{G}'$ generato dai commutatori. Poiché $\mathcal{G}$ è un p-gruppo finito allora $\phi(\mathcal{G}) = \mathcal{G}^p\mathcal{G}'$. Per cui $|\phi(\mathcal{G})| \geq p^2$ e quindi $|\mathcal{G}/\phi(\mathcal{G})| \leq p^2$. $\mathcal{G}/\phi(\mathcal{G})$ è un p-gruppo abeliano elementare e quindi uno spazio vettoriale su $\mathbb{Z}/p\mathbb{Z}$, la cui dimensione coincide con il numero minimale di generatori per $\mathcal{G}$; riconoscendo che $\mathcal{G}$ non è ciclico (non è abeliano!), tale numero, e quindi $\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{G}/\phi(\mathcal{G}))$, deve essere maggiore o uguale a 2. Ma allora $|\phi(\mathcal{G})| = p^2$ e quindi $\phi(\mathcal{G}) =< P^p, Q >$. Allora necessariamente si ha la tesi perché un gruppo di ordine p^2 è abeliano e $< P^p, Q >$ contiene più di $p-1$ elementi di ordine p (non può essere quindi isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$). □

Osservazione 3.2.12 $< P^p >= Z(\mathcal{G})$.

Dimostrazione Il centro è l'intersezione dei centralizzatori degli elementi: in particolare è contenuto nel centralizzatore di $< P >$, che denotiamo con $Z(< P >)$. Quest'ultimo sottogruppo è $< P >$: infatti il centralizzatore è sempre contenuto nel normalizzatore,

cioè $Z(<P>) \subset N(<P>)$. Il normalizzatore del sottogruppo generato da P è $<P, Q>$: infatti quest'ultimo è chiaramente un sottogruppo normale (è massimale) e sicuramente $P, Q \in N(<P>)$. Inoltre il normalizzatore e il centralizzatore non possono coincidere, perché ci sono elementi $X \in \mathcal{G}$ tali che $X^{-1}PX = P^a$ con $a \neq 1$ (per esempio Q). Quindi $Z(<P>)$ è un sottogruppo proprio di $N(<P>)$ che contiene $<P>$, quindi coincide con $<P>$. Allora $Z(\mathcal{G}) \subseteq Z(<P>)$ ma è chiaro, ancora una volta, che non possono coincidere perché, ad esempio, P non commuta con Q. Quindi, poiché l'unico sottogruppo non banale (il centro di un p-gruppo è sempre non banale) di $<P>$ è $<P^p>$, si ha la tesi. □

Osservazione 3.2.13 *$\mathcal{G}$ ha un unico sottogruppo H_0 di ordine p^3 isomorfo a $(\mathbb{Z}/p\mathbb{Z})^3$*

Dimostrazione $H_0 =< P^p, Q, R >$. Essendo $[Q, R] = E$, è chiaro, in virtù dell'osservazione 3.2.12, che $H_0 \cong (\mathbb{Z}/p\mathbb{Z})^3$. Sia ora K un altro sottogruppo di questo tipo e $P^hQ^kR^s \in K$. K è massimale quindi contiene il sottogruppo di Frattini, in particolare $Q \in K$. È immediato inoltre verificare che

$$[P^hQ^kR^s, Q] = P^{hp} = E \qquad \Leftrightarrow \qquad h \equiv 0 \pmod{p} \tag{3.13}$$

Essendo K abeliano, per (3.13), $h \equiv 0 \,(mod\, p)$. Ma allora $P^hQ^kR^s \in H_0$. Quindi $K \subseteq H_0$ e, considerate le cardinalità, $H_0 = K$. □

Osservazione 3.2.14 *Se $p \neq 3$, $|Aut(\mathcal{G})| = p^5(p-1)$.*

Dimostrazione Sia φ un automorfismo di $\mathcal{G}$. Allora $\varphi(H_0) = H_0$. Infatti gli elementi di $\varphi(H_0)$ costituiscono un sottogruppo abeliano elementare di ordine p^3 e questo, per l'osservazione (3.2.13), non può essere che H_0. Inoltre osservando che

$$P^hQ^iR^j = Q^iP^{hip+h}R^j = P^{hip}Q^iP^hR^j = P^{hip}Q^iR^j(PQ^j)^h = P^{p(hi+\frac{h(h+1)}{2}j)}Q^{i+jh}R^jP^h \tag{3.14}$$

non è difficile verificare (ad esempio per induzione su n) che

$$(P^hQ^iR^j)^n = P^\alpha Q^\beta R^\gamma P^{hn} \tag{3.15}$$

$$\alpha = \sum_{k=1}^{n}\left[khip + \frac{kh(kh+1)}{2}jp\right] = p\left(\frac{n(n+1)}{2}hi + \frac{n(n+1)}{4}hj + \frac{n(n+1)(2n+1)}{12}h^2j\right) \tag{3.16}$$

$$\beta = \left(\sum_{k=1}^{n} jkh\right) + ni = \frac{n(n+1)}{2}jh + ni \qquad \gamma = nj \tag{3.17}$$

Ponendo nella (3.16) $n = p$, si ha $\alpha \equiv 0 \ (mod\ p^2)$. Quindi un elemento $P^hQ^iR^j$ ha ordine p^2 se e solo se $(h, p) = 1$. Si riconosce dunque che $\mathcal{G}$ ha p^3 elementi di ordine p. Vediamo quali sono le condizioni affinché, assegnando le immagini dei generatori, si ottenga effettivamente un automorfismo di $\mathcal{G}$. Intanto porremo, in virtù del fatto che $\varphi(H_0) = H_0 =< P^p, Q, R >$ e della condizione sugli elementi di ordine p^2,

$$P \mapsto P^hQ^iR^j \quad (h,p) = 1 \qquad Q \mapsto P^{ap}Q^bR^c \qquad R \mapsto P^{sp}Q^rR^t$$

e indicheremo con φ la funzione che manda i generatori in queste immagini. Perché φ si estenda ad un omomorfismo è necessario e sufficiente che le immagini dei generatori rispettino le relazioni. Sfruttando le regole di commutazione di $\mathcal{G}$ si ottiene che

$$\varphi(Q^{-1}PQ) = P^{hpb+\frac{h(h+1)}{2}cp+h(1-hcp)}Q^{ch+i}R^j$$
$$\varphi(P^{p+1}) = P^{hp+h}Q^iR^j$$
$$\varphi(R^{-1}PR) = P^{hpr+\frac{h(h+1)}{2}tp+h(1-htp)}Q^{th+i}R^j$$
$$\varphi(PQ) = P^{h+ap}Q^{i+b}R^{j+c}$$

Allora le relazioni sono rispettate dalle immagini se e solo se

$$hpb + \frac{h(h+1)}{2}cp + h(1-hcp) \equiv hp + h \pmod{p^2} \qquad ch \equiv 0 \pmod{p}$$

$$hpr+\frac{h(h+1)}{2}tp+h(1-htp) \equiv h+ap \pmod{p^2} \qquad th \equiv b \pmod{p} \qquad 0 \equiv c \pmod{p}$$

(la relazione di commutazione tra $\varphi(Q)$ e $\varphi(R)$ e le relazioni sulle potenze dei generatori che danno E sono automaticamente rispettate per come abbiamo definito φ). Riscriviamo queste condizioni in maniera più semplice

$$c \equiv 0 \pmod{p} \qquad b \equiv 1 \pmod{p} \qquad th \equiv b \pmod{p} \qquad 2hr + h - 1 \equiv 2a \pmod{p}$$

Quindi φ è definisce un omomorfismo se e solo se valgono queste condizioni.
Vediamo ora quali siano le condizioni necessarie e sufficienti perché φ sia iniettivo (e quindi surgettivo). Indichiamo con g un generico elemento di H_0. Allora un elemento di $\mathcal{G}$ si può scrivere, per opportuni $n \in \mathbb{N}$ e $g \in H_0$, come $P^n g$. Supponiamo che $\varphi(P^n g) = E$, allora $\varphi(P^n) \in H_0$ (sempre perché H_0 è invariante per φ). In particolare $\varphi(P^n)$ ha ordine (al più) p. Per come abbiamo definito $\varphi(P)$, deve essere allora $n \equiv 0 \pmod{p}$, cioè $P^n \in H_0$. In sostanza abbiamo mostrato che se un elemento è mandato in E allora deve appartenere a H_0. Supponiamo allora che $\varphi(g) = E$ con $g = P^{px}Q^yR^z$. Questo significa che

$$\begin{aligned} hx + ay + sz &\equiv 0 \pmod{p} \\ by + rz &\equiv 0 \pmod{p} \\ cy + tz &\equiv 0 \pmod{p} \end{aligned}$$

Se vogliamo che l'unico elemento che viene mandato in E sia E stesso, cioè che φ sia iniettivo, dovremo porre

$$p \nmid \det \begin{pmatrix} h & a & s \\ 0 & b & r \\ 0 & c & t \end{pmatrix} = h(bt - cr)$$

Considerato che $(h, p) = 1$, questa condizione equivale a $p \nmid bt - cr$. Inoltre è chiaro che si tratta di una condizione necessaria e sufficiente affinché l'omomorfismo φ sia un automorfismo.
Allora, rimettendo insieme tutte le condizioni, ci si rende conto che, fissato h (il che si può fare in $p(p-1)$ modi), restano fissati c, b e t. Inoltre fissato a indipendentemente da h (il che si può fare in p modi), resta fissato r. Infine non ci sono condizioni sulla scelta di s, i e j, quindi ciascuno di essi può essere scelto in p modi. Quindi si ha la tesi. □

Osservazione 3.2.15 *Se $p = 3$, $|Aut(\mathcal{G})| = 324$.*

Dimostrazione Come nell'osservazione precedente, se $\varphi \in Aut(\mathcal{G})$, allora deve essere $\varphi(H_0) = H_0$. Valgono ancora le (3.14), (3.15), (3.16), (3.17) con $p = 3$. Ponendo $n = 3$ nella (3.16) si ha $\alpha \equiv 3h^2j + 3h \pmod 9$. Quindi un elemento $P^hQ^iR^j \in \mathcal{G}$ ha ordine minore di 9 se e solo se $h^2j+h \equiv 0 \pmod 3$, ossia $h \equiv 0 \pmod 3$ oppure $hj \equiv -1 \pmod 3$. Quindi ci sono esattamente 36 elementi di ordine 9.
Vediamo quali sono le condizioni affinché, assegnando le immagini dei generatori, si ottenga effettivamente un automorfismo di $\mathcal{G}$. Intanto porremo, in virtù del fatto che $\varphi(H_0) = H_0 =< P^3, Q, R >$ e della condizione sugli elementi di ordine 9,

$$P \mapsto P^hQ^iR^j \quad (h, 3) = 1,\ 3 \nmid (hj - 1) \qquad Q \mapsto P^{3a}Q^bR^c \qquad R \mapsto P^{3s}Q^rR^t$$

e indicheremo con φ la funzione che manda i generatori in queste immagini. Perché φ si estenda ad un omomorfismo è necessario e sufficiente che le immagini dei generatori rispettino le relazioni. Sfruttando le regole di commutazione di $\mathcal{G}$ si ottiene che

$$\varphi(Q^{-1}PQ) = P^{3hb+3\frac{h(h+1)}{2}c+h(1-3hc)}Q^{ch+i}R^j$$

$$\varphi(P^{3+1}) = P^{3h^2j+h}Q^iR^j$$

$$\varphi(R^{-1}PR) = P^{3hr+3\frac{h(h+1)}{2}t+h(1-3ht)}Q^{th+i}R^j$$

$$\varphi(PQ) = P^{h+3a}Q^{i+b}R^{j+c}$$

Allora le relazioni sono rispettate dalle immagini se e solo se

$$3hb + 3\frac{h(h+1)}{2}c + h(1 - 3hc) \equiv 3h^2j + h \pmod 9 \qquad ch \equiv 0 \pmod 3$$

$$3hr+3\frac{h(h+1)}{2}t+h(1-3ht) \equiv h+3a \pmod 9 \qquad th \equiv b \pmod 3 \qquad 0 \equiv c \pmod 3$$

(la relazione di commutazione tra $\varphi(Q)$ e $\varphi(R)$ e le relazioni sulle potenze dei generatori che danno E sono automaticamente rispettate per come abbiamo definito φ). Riscriviamo queste condizioni in maniera più semplice

$$c \equiv 0 \pmod 3 \qquad th \equiv b \pmod 3 \qquad b \equiv hj \pmod 3 \qquad 2h(r+b)+b \equiv 2a \pmod 3$$

Quindi φ è definisce un omomorfismo se e solo se valgono queste condizioni.
È chiaro che la condizione necessaria e sufficiente affinché l'omomorfismo φ sia un automorfismo è, anche per $p = 3$, che 3 non divida $bt - cr$.
Allora, rimettendo insieme tutte le condizioni, ci si rende conto che, fissati h (il che si può fare in 6 modi) e j (il che si può fare in 2 modi), restano fissati c, b e t. Inoltre fissato a indipendentemente da h (il che si può fare in 3 modi), resta fissato r. Infine non ci sono condizioni sulla scelta di s e i , quindi ciascuno di essi può essere scelto in 3 modi. Quindi si ha la tesi. □

Conseguenza Come conseguenza della formula di Šafarevič ricaviamo che, se $p \neq 3$, ci sono esattamente $(p + 1)(p - 1)^2$ estensioni di Galois su $\mathbb{Q}_p$ il cui gruppo di Galois è isomorfo a $\mathcal{G}$, mentre nel caso $p = 3$, il numero di estensioni di questo tipo è $12 = 4 \cdot 3$ (abbiamo mostrato in precedenza che il numero minimale di generatori per $\mathcal{G}$ è 2).

Osservazione 3.2.16 *Il gruppo di Galois di* **F** *su* $\mathbb{Q}_p$ *è isomorfo a* $\mathcal{G}$*, cioè* $G \cong \mathcal{G}$*. Inoltre una estensione di Galois su* $\mathbb{Q}_p$ *di grado* p^4 *che abbia gruppo di Galois isomorfo a* $\mathcal{G}$ *è la chiusura normale di* p^2 *estensioni del tipo di* **L** *(cioè del tipo considerato in questa sottosezione), che possono essere suddivise in p famiglie, ciascuna composta da p estensioni coniugate su* $\mathbb{Q}_p$*.*

Dimostrazione G è un gruppo non abeliano di ordine p^4 che si realizza come gruppo di Galois di un'estensione di $\mathbb{Q}_p$. Deve quindi avere per [Ša 56] due generatori (non meno perché non è abeliano). Vengono scartati dunque, con riferimento alla clasificazione di Šafarevič i gruppi (i), (ii), (iii), (iv), (v), (vii), (ix), (xiv) e (xv). Inoltre G deve contenere un sottogruppo isomorfo a $(\mathbb{Z}/p\mathbb{Z})^3$. Questa ulteriore condizione fa sì che vengano scartati i gruppi (viii) (ha solo p^2 elementi di ordine p), (xii) e (xiii) (l'insieme degli elementi di ordine al più p è un sottogruppo di ordine p^3 ma non è abeliano). Restano dunque i gruppi (x) (che è quello che nelle sottosezioni precedenti abbiamo denotato con $G(10)$) e (xi). Vediamo che anche (x) non fa al caso nostro. Sappiamo che G deve contenere almeno p sottogruppi di ordine p^2 non normali e che non contengono sottogruppi normali di ordine p. Non è difficile verificare che questa richiesta non è soddisfatta dal gruppo (x). Infatti, da quanto osservato nella dimostrazione dell'osservazione 3.2.3, il sottogruppo delle p-esime potenze di $G(10)$ è $< P^p >$ che è normale. Quindi i sottogruppi di ordine p^2 ciclici contengono un sottogruppo di ordine p normale. Inoltre, se un sottogruppo di ordine p^2 abeliano elementare avesse intersezione banale con il centro, ci sarebbero almeno p^4 elementi di ordine p, il che è falso. Quindi, poiché la descrizione di (xi) coincide con quella di $\mathcal{G}$, si ha $G \cong \mathcal{G}$.
Per dimostrare la seconda parte di questa osservazione, andiamo in cerca delle famiglie di sottogruppi, ciascuna delle quali possieda p sottogruppi di ordine p^2 coniugati che non contengono alcun sottogruppo normale di ordine p. Dobbiamo mostrare che ci sono esattamente $p + 1$ di queste famiglie. Studiamo dapprima il caso $p \neq 3$. Osserviamo innazitutto che il sottogruppo delle p-esime potenze di $\mathcal{G}$ è $< P^p >$ che è un sottogruppo normale (è l'unico perché coincide con il centro): quindi non ci sono sottogruppi ciclici di ordine p^2 che non contengono sottogruppi normali di ordine p. Andiamo quindi alla ricerca di sottogruppi di ordine p^2 isomorfi a $(\mathbb{Z}/p\mathbb{Z})^2$ che non contengono il centro di $\mathcal{G}$ e che non sono normali. Tali sottogruppi sono dunque contenuti in H_0. Possiamo pensare questo sottogruppo come un p-spazio vettoriale su $\mathbb{Z}/p\mathbb{Z}$ la cui base è $\{P^p, Q, R\}$. Più precisamente identifichiamo un elemento del tipo $P^{xp}Q^yR^z$ con la terna (x, y, z). Allora un sottogruppo di ordine p^2 è un piano ed è dunque dato da un equazione del tipo

$$ax + by + cz = 0$$

per una certa terna $(a, b, c) \in (\mathbb{Z}/p\mathbb{Z})^3$. La condizione che un sottogruppo di ordine p^2 non contenga il centro si esprime richiedendo che a sia diverso da 0 (e quindi possiamo supporlo 1). Allora una base di questo piano è

$$\{(b, -1, 0), (c, 0, -1)\}$$

Osserviamo adesso che il coniugio per P è un'applicazione lineare invertibile di questo spazio vettoriale e la matrice ad essa associata è

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Fissiamo un sottogruppo di ordine p^2 che non contenga il centro, cioè una terna $(1, b, c)$ (il sottogruppo determina univocamente questa terna e viceversa). La sua immagine mediante il coniugio per P è il piano la cui base è

$$\{(b-1, -1, 0), (c-1, -1, -1)\}$$

Si tratta quindi del sottogruppo $(1, b-1, c-b)$. Sia ora $(1, b', c')$ un altro sottogruppo: esso coincide con l'immagine di $(1, b, c)$ tramite il coniugio per P se

$$\begin{cases} b' &= b-1 \\ c' &= c-b \end{cases}$$

Allora $(1, b, c)$ non è normale. Inoltre non può avere più di p coniugati perché il suo normalizzatore è un sottogruppo normale di indice p (si tratta di H_0), quindi ne ha esattamente p. Dunque, poiché ci sono p^2 sottogruppi di ordine p^2 in H_0 che non contengono il centro (o equivalentemente p^2 terne del tipo $(1, b, c)$), ci sono esattamente p famiglie ciscuna composta da p sottogruppi coniugati del tipo che cercavamo.
Nel caso $p = 3$ rimane vero che il sottogruppo delle terze potenze è normale (è ancora $Z(\mathcal{G}) =< P^p >$), quindi non ci sono sottogruppi ciclici di ordine 9 che non contengono sottogruppi normali di ordine 3. Inoltre supponiamo che K sia un sottogruppo abeliano elementare di ordine 9 che non è contenuto in H_0. Allora $< P^3 > \subset K$. Infatti, se così non fosse, ci sarebbe un sottogruppo abeliano elementare di ordine 27 diverso da H_0 (cioè $< K, P^3 >$. Quindi ci si può ricondurre al caso precedente (cioè analizzare cosa succede per i sottogruppi di ordine 9 di H_0) ed ottenere un risultato analogo. □

Conseguenza Da quest'ultima osservazione e dalla considerazione precedente si ricava che, se $p \neq 3$, ci sono $p^2(p+1)(p-1)^2$ estensioni del tipo considerato in questa sottosezione. Se $p = 3$, le estensioni sono 108.

Capitolo 4

Le p-estensioni cicliche di $\mathbb{Q}_p$

4.1 Le p-estensioni di Galois totalmente ramificate

Proposizione 4.1.1 *Sia p un primo dispari. Sia $\mathbf{K}$ una estensione di Galois di grado p^n su $\mathbb{Q}_p$ totalmente ramificata con gruppo di Galois $G(\mathbf{K}|\mathbb{Q}_p)$. Allora $G(\mathbf{K}|\mathbb{Q}_p)$ è un gruppo ciclico.*

Dimostrazione Le estensioni di Galois di grado p su $\mathbb{Q}_p$ sono esattamente $p+1$. Due estensioni di questo tipo, distinte fra di loro, hanno per intersezione $\mathbb{Q}_p$ e quindi il gruppo di Galois del composto di esse è isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Dunque tale campo composto contiene tutte le estensioni di Galois di grado p su $\mathbb{Q}_p$ (per la corrispondenza di Galois). Sia dunque $\mathbf{K}$ una estensione con le proprietà richieste. Supponiamo che $G(\mathbf{K}|\mathbb{Q}_p)$ abbia almeno due sottogruppi di ordine p^{n-1}. Tali sottogruppi sono dunque normali perché massimali. Allora, per la corrispondenza di Galois, $\mathbf{K}$ contiene almeno due sottoestensioni di grado p su $\mathbb{Q}_p$ che risultano essere normali. Ma allora contiene tutte le estensioni di Galois di grado p su $\mathbb{Q}_p$ e quindi anche quella non ramificata, contro le ipotesi. Allora necessariamente $\mathbf{K}$ deve avere meno di due sottogruppi di ordine p^{n-1}. Tuttavia un p-gruppo ha sempre almeno un sottogruppo per ogni divisore dell'ordine. Quindi $G(\mathbf{K}|\mathbb{Q}_p)$ ha un solo sottogruppo di ordine p^{n-1} e un p-gruppo con una tale proprietà è un gruppo ciclico. □

4.2 Il composto di tutte le estensioni cicliche

In questa sezione ci proponiamo di ottenere delle informazioni sul composto delle estensioni cicliche di grado p^n su $\mathbb{Q}_p$ mediante la teoria dei corpi di classe locale (*class field theory*). Gli stessi risultati possono essere ottenuti con metodi più elementari (formula di Šafarevič e teoria della ramificazione, per esempio) ma l'utilizzo della teoria dei corpi di classe sembra fornire un metodo più generale (eventualmente sfruttando la variante non abeliana) utilizzabile anche in casi più complicati.

4.2.1 Il caso $p \neq 2$

Proposizione 4.2.1 *Sia $\mathbf{F}$ il composto di tutte le estensioni $\mathbf{L}$ cicliche di grado p^n su $\mathbb{Q}_p$. Allora $\mathbf{F}$ è un'estensione abeliana finita di grado p^{2n} su $\mathbb{Q}_p$ con*

$$G(\mathbf{F}|\mathbb{Q}_p) \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$$

Inoltre si ha $N_{\mathbb{Q}_p}^{\mathbf{F}}(\mathbf{F}^*) = (\mathbb{Q}_p^*)^{p^n}$.

Dimostrazione Osserviamo in primo luogo che, se $\mathbf{L}$ è ciclica di grado p^n su $\mathbb{Q}_p$, allora $(\mathbb{Q}_p^*)^{p^n} \subseteq N_{\mathbb{Q}_p}^{\mathbf{L}}(\mathbf{L}^*)$. Inoltre se $\mathbf{L'}$ è un'altra estensione di questo tipo si ha

$$N_{\mathbb{Q}_p}^{\mathbf{LL'}}((\mathbf{LL'})^*) = N_{\mathbb{Q}_p}^{\mathbf{L}}(\mathbf{L}^*) \cap N_{\mathbb{Q}_p}^{\mathbf{L'}}(\mathbf{L'}^*)$$

Questo significa che $(\mathbb{Q}_p^*)^{p^n} \subseteq N_{\mathbb{Q}_p}^{\mathbf{F}}(\mathbf{F}^*)$.
Osserviamo esplicitamente che $(\mathbb{Q}_p^*)^{p^n}$ è un sottogruppo di $\mathbb{Q}_p^*$ di indice finito (e quindi aperto[1]). Sia allora $\mathbf{F'}$ il campo di classe relativo a $(\mathbb{Q}_p^*)^{p^n}$. In particolare si ha $N_{\mathbb{Q}_p}^{\mathbf{F'}}(\mathbf{F'}^*) = (\mathbb{Q}_p^*)^{p^n}$ e $G(\mathbf{F'}|\mathbb{Q}_p) \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ perché $G(\mathbf{F'}|\mathbb{Q}_p) \cong \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^{p^n}$ e

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p$$

Inoltre

$$N_{\mathbb{Q}_p}^{\mathbf{F'}}(\mathbf{F'}^*) = (\mathbb{Q}_p^*)^{p^n} \subseteq N_{\mathbb{Q}_p}^{\mathbf{F}}(\mathbf{F}^*) \quad \Rightarrow \quad \mathbf{F} \subseteq \mathbf{F'}$$

Tuttavia vale anche l'altro contenimento: dalla corrispondenza di Galois si ha che $\mathbf{F'}$ è il composto delle sue sottoestensioni che sono cicliche di grado p^n su $\mathbb{Q}_p$ e dunque, poiché tutte le estensioni di questo tipo sono contenute in $\mathbf{F}$, si ha $\mathbf{F'} \subseteq \mathbf{F}$ e quindi $\mathbf{F'} = \mathbf{F}$. □

Considerazione

- Il caso $n = 1$: abbiamo già visto che le estensioni cicliche di grado p su $\mathbb{Q}_p$ sono in tutto $p+1$ e infatti i sottogruppi di $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ che hanno quoziente (ciclico) di ordine p sono $p+1$.

- Il caso $n = 2$: le estensioni cicliche di grado p^2 su $\mathbb{Q}_p$ corrispondono ai sottogruppi di $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ che hanno quoziente ciclico di ordine p^2 e quindi sono in tutto $p(p+1)$. Otteniamo così il risultato già dimostrato nell'osservazione 3.2.1.

4.2.2 Il caso $p = 2$

Proposizione 4.2.2 *Sia* $\mathbf{F}$ *il composto di tutte le estensioni* $\mathbf{L}$ *cicliche di grado* 2^n *su* $\mathbb{Q}_2$. *Allora* $\mathbf{F}$ *è un'estensione abeliana finita di grado* 2^{2n} *su* $\mathbb{Q}_p$ *con*

$$G(\mathbf{F}|\mathbb{Q}_p) \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$$

Inoltre si ha $N_{\mathbb{Q}_2}^{\mathbf{F}}(\mathbf{F}^*) = (\mathbb{Q}_2^*)^{2^n}$.

Dimostrazione La dimostrazione è identica a quella del caso $p \neq 2$ a parte il fatto che

$$\mathbb{Q}_2^* \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$$

e quindi $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^{2^n} \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$. □

Considerazione

[1] Vedi [Mi].

- Il caso $n = 1$: le estensioni cicliche di grado 2 su $\mathbb{Q}_2$ sono semplicemente le estensioni di grado 2 su $\mathbb{Q}_2$. Abbiamo già visto che sono in tutto 7 e infatti i sottogruppi di $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ che hanno quoziente di ordine 2 sono 7. Lo stesso risultato può essere ottenuto con la teoria di Kummer, perché $\mathbb{Q}_2$ contiene le radici quadrate dell'unità: le estensioni abeliane di esponente 2 di $\mathbb{Q}_2$ sono in corrispondenza biunivoca con i sottogruppi di $\mathbb{Q}_2^*$ che contengono $(\mathbb{Q}_2^*)^2$, ossia con i sottogruppi di $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.
- Il caso $n = 2$: le estensioni cicliche di grado 4 su $\mathbb{Q}_2$ corrispondono ai sottogruppi di $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ che hanno quoziente ciclico di ordine 4 e quindi sono in tutto 12. Otteniamo così il risultato preannunciato nell'osservazione 3.1.5.

Bibliografia

[Ba] G. Bachman *Introduction to p-adic numbers and valuation theory*, Academic Press, 1964

[CF] AA. VV. *Algebraic Number Theory. Proceedings of an instructional conference organized by the London Mathemathical Society (a NATO advanced institute) with the support of the international mathematical union*, edito da J. W. S. Cassels e A. Frölich, Academic Press, 1967

[Ca] J. W. S. Cassels *Local Fields*, Cambridge University Press, 1986

[La] S. Lang *Algebraic Number Theory*, Addison-Wesley, 1970

[La1] S. Lang *Algebra (revised third edition)*, GTM **211**, Springer-Verlag, 2002

[AMc] M. Atiyah e I. McDonald *Introduction to commutative algebra*, Addison-Wesley, 1969

[FV] I. B. Fesenko e S. V. Vostokov *Local fields and their extensions. A constructive approach*, AMS Transl. Monographs **121**, 1993

[Se] J. P. Serre, *Local fields*, GTM **7**, Springer-Verlag, 1979

[Bu] W. Burnside, *Theory of groups of finite orders*, Dover 1955

[Ar] E. Artin, *Galois Theory (second edition with additions and revisions)*, Notre Dame Mathematical Lecture Number **2**, University of Notre Dame Press, 1985

[Ne] J. Neukirch *Class field theory*, Springer Verlag , 1986

[Mi] J. Milne *Class field theory* (elettronico), http://www.jmilne.org/math/coursenote/math776.pdf

[Se 78] J. P. Serre, *Une formule de masse pour les estensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Série A, **286** (1978), 1031-1036

[Am 71] S. Amano, *Eisenstein equations of degree p in a $\mathfrak{p}$-adic field*, J. Fasc. Sci. Univ. Tokyo Sect. IA Math **18** (1971), 1-22

[Kr 62] M. Krasner, *Nombre d'estensions d'un degré donné d'un corps $\mathfrak{p}$-adique*, CR **254** (1962) 3470-3472, *ibidem* **255** (1962), 224-226, 2342-2344, 3095-3097

[Ša 56] I. R. Šafarevič, *On p-extensions*, Mat. Sb. **20** (**62**) (1947), 351-363 (in Russo); trad. inglese, Amer. Math. Soc. Transl. Ser. 2 **4** (1956), 59-72

[JR 03] J. W. Jones e D. P. Roberts, *A database of local fields* (elettronico), http://math.la.asu.edu/∼jj/localfields (ultimo aggiornamento settembre 2003)

[Ya 95] M. Yamagishi *On the number of Galois p-extensions of a local field*, Proc. Amer. Math Soc. **123** (1995), 2373-2380

[BMc 83] G. Butler e J. McKay *Transitive groups of degree up to eleven*, Comm. Alg. **11** (1983)