Appunti di Teoria Algebrica dei Numeri 2

Giacomo Mezzedimi Carlo Sircana

25 giugno 2016

Indice

1 Valori assoluti

1.1 Valori assoluti su un campo

Nel seguito indicheremo con K un generico campo.

Definizione 1.1.1. Un **valore assoluto** $|\cdot| : K \to \mathbb{R}$ è una funzione con le seguenti proprietà:

1. $|x| \geq 0 \ \forall x \in K$ e $|x| = 0 \iff x = 0$;
2. $|xy| = |x||y| \ \forall x, y \in K$;
3. $\exists C > 0$ tale che $|1 + x| \leq C \ \forall x \in K$ tale che $|x| \leq 1$.

Osservazione. La proprietà 3. precedente è equivalente a una versione più debole della disuguaglianza triangolare:

3'. $\exists C' > 0$ tale che $|x + y| \leq C'(|x| + |y|) \ \forall x, y \in K$.

Quest'equivalenza è molto facile da provare, in quanto, supposto per simmetria che $|x| \leq |y| \neq 0$ e posto $\alpha = \frac{x}{y}$, si ha:

$$|x + y| = |y||1 + \alpha| \leq C|y| \leq C(|x| + |y|),$$

mentre viceversa:

$$|1 + \alpha| = \frac{|x + y|}{|y|} \leq C'(1 + |\alpha|) \leq 2C'.$$

Osservazione. É troppo restrittivo chiedere che un valore assoluto soddisfi la disuguaglianza triangolare standard, poichè ad esempio con tale definizione la norma quadra $\| \cdot \|^2 : \mathbb{C} \to \mathbb{R}$ non rientra nella categoria dei valori assoluti.

Osservazione. Dalla definizione di valore assoluto, più precisamente dalla moltiplicatività, si ottiene che $|\zeta| = 1$ per ogni ζ radice dell'unità; in particolare $|1| = |-1| = 1$.
Il valore assoluto su K tale che $|x| = 1 \ \forall x \in K^*$ è detto **valore assoluto banale**.

Osservazione. Un valore assoluto $|\cdot|$ su un campo K induce una topologia su K: un sistema fondamentale di intorni per $x \in K$ è dato dalle palle $B(x, \varepsilon) = \{y \in K \mid |x - y| < \varepsilon\}$ al variare di $\varepsilon > 0$.
Ad esempio, il valore assoluto banale induce sul campo la topologia discreta, mentre la norma euclidea su $\mathbb{C}$ induce la topologia euclidea standard su $\mathbb{C}$ stesso.

Definizione 1.1.2. Due valori assoluti $|\cdot|_v$ e $|\cdot|_w$ su K si dicono equivalenti se esiste $\gamma > 0$ tale che $|x|_v = |x|_w^\gamma \ \forall x \in K$.

É del tutto evidente che due valori assoluti equivalenti inducono la stessa topologia sul campo. Inoltre, scegliendo un opportuno $\gamma > 0$, è immediato osservare che ogni valore assoluto è equivalente ad un altro valore assoluto con $C = 2$.

Proposizione 1.1.1. *Se $|\cdot|$ è un valore assoluto su K con $C = 2$, allora $|\cdot|$ soddisfa la disuguaglianza triangolare standard.*

Dimostrazione. Supponiamo per simmetria che $|x| \geq |y|$; poniamo inoltre $\alpha = \frac{y}{x}$. $|\alpha| \leq 1$, perciò:

$$|x + y| = |x + \alpha x| = |1 + \alpha||x| \leq 2|x|,$$

da cui deduciamo la disuguaglianza $|x+y| \leq 2 \max\{|x|, |y|\}$ valida $\forall x, y \in K$. A questo punto, con una semplice induzione otteniamo che:

$$\left| \sum_{i=1}^{2^r} x_i \right| \leq 2^r \max_i |x_i|$$

(ad esempio basta spezzare la somma in due metà e applicare il passo base); se inoltre $n \in \mathbb{N}$ è tale che $2^{r-1} < n \leq 2^r$, aggiungendo $2^r - n$ zeri alla somma ricaviamo la disuguaglianza:

$$\left| \sum_{i=1}^{n} x_i \right| \leq 2^r \max_i |x_i| < 2n \max_i |x_i|.$$

In particolare, ponendo $x_1 = \cdots = x_n = 1$, si ha che $|n| < 2n$. Ma adesso:

$$|x+y|^n = \left| \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j} \right| \leq 2(n+1) \max_j \left| \binom{n}{j} x^j y^{n-j} \right| <$$
$$< 4(n+1) \max_j \binom{n}{j} |x^j||y^{n-j}| \leq 4(n+1)(|x|+|y|)^n,$$

(in quanto $\max_j \binom{n}{j} |x^j||y^{n-j}|$ è solo uno dei termini di $(|x|+|y|)^n$), e la tesi si ottiene estraendo la radice n-esima e facendo tendere $n \to \infty$. □

Corollario 1.1.2. *Ogni valore assoluto su un campo è equivalente ad un altro valore assoluto che soddisfa la disuguaglianza triangolare.*

Osserviamo quindi che la restrizione a cui portava l'imposizione della disuguaglianza triangolare nella definizione di valore assoluto era solamente apparente, in quanto, volendo studiare i valori assoluti a meno di equivalenza, posso chiedere che la disuguaglianza triangolare sia effettivamente soddisfatta.
Nel seguito potremmo dire che un valore assoluto è **normalizzato** se soddisfa la disuguaglianza triangolare.

Osservazione. Se $|\cdot|$ è un valore assoluto normalizzato, vale l'altra disuguaglianza triangolare:

$$||x| - |y|| \leq |x - y|.$$

Infatti $x = y + (x - y)$ e $y = x + (y - x)$, dunque per la disuguaglianza triangolare:

$$|x| \leq |y| + |x - y| \quad \text{e} \quad |y| \leq |x| + |y - x|,$$

e la tesi segue notando che $|x - y| = |y - x|$ (in quanto $|-1| = 1$).

Proposizione 1.1.3. *Due valori assoluti $|\cdot|_v$ e $|\cdot|_w$ su K danno la stessa topologia su K $\iff$ sono equivalenti.*

Dimostrazione. L'implicazione facile $\Leftarrow$ è già stata vista; per l'altra, supponiamo che i due valori assoluti siano non banali, in quanto se uno dei due lo fosse, il teorema sarebbe evidentemente vero.
Per l'ipotesi appena fatta, sia $\alpha \in K$ tale che $|\alpha|_v < 1$. Per moltiplicatività del valore assoluto, si ha:

$$\lim_{n \to \infty} |\alpha^n|_v = 0,$$

cioè $\alpha^n \to 0$ nella topologia indotta da $|\cdot|_v$. Visto che le topologie indotte sono uguali, $\alpha^n \to 0$ anche nella topologia indotta da $|\cdot|_w$, cioè $|\alpha|_w < 1$.
Detti perciò:

$$A_v := \{x \in K \mid |x|_v < 1\} \subseteq \{x \in K \mid |x|_w < 1\} =: A_w,$$

e:

$$B_v := \{x \in K \mid |x|_v > 1\} \subseteq \{x \in K \mid |x|_w > 1\} =: B_w,$$

($B_v \subseteq B_w$ in quanto se $x \in B_v$, $x^{-1} \in A_v$, dunque $x^{-1} \in A_w$ e cioè $x \in B_w$), fissiamo un elemento $x \in B_v$.
Sia $y \in B_v$; $|y|_v = |x|_v^\gamma$ per un certo $\gamma > 0$. Sia inoltre $\frac{m}{n} \in \mathbb{Q}$, $\frac{m}{n} > \gamma$; allora $|y|_v < |x|_v^{\frac{m}{n}}$, dunque $|y^n|_v \leq |x^m|_v$, cioè $\left|\frac{y^n}{x^m}\right|_v < 1$, da cui $\left|\frac{y^n}{x^m}\right|_w < 1$.
Analogamente, se $\mathbb{Q} \ni \frac{m}{n} < \alpha$, $\left|\frac{y^n}{x^m}\right|_w > 1$, quindi:

$$\begin{cases} |y|_w < |x|_w^{\frac{m}{n}} & \text{per } \frac{m}{n} > \alpha \\ |y|_w > |x|_w^{\frac{m}{n}} & \text{per } \frac{m}{n} < \alpha \end{cases}$$

e per continuità $|y|_w = |x|_w^\gamma$.
A questo punto, posto $|x|_v = |x|_w^\beta$ con $\beta > 0$:

$$|y|_v = |x|_v^\gamma = |x|_w^{\beta\gamma} = |y|_w^\beta.$$

Se invece $y \in A_v$, $y^{-1} \in B_v$ e dunque $|y^{-1}|_v = |y^{-1}|_w^\beta$, da cui $|y|_v = |y|_w^\beta$. □

Definizione 1.1.3. Un valore assoluto $|\cdot|$ su K si dice **non archimedeo** se $|x+y| \leq \max\{|x|, |y|\}$ $\forall x, y \in K$, cioè se $C = 1$.

Osservazione. Osserviamo che se $|x| \neq |y|$, allora $|x+y| = \max\{|x|, |y|\}$. Infatti, se ad esempio $|x| < |y|$, allora $y = x + y - x$ e dunque $|y| = |x+y-x| \leq \max\{|x+y|, |x|\}$, da cui $\max\{|x|, |y|\} = |y| \leq |x+y|$.

Esempio. Fissato $K = \mathbb{Q}$ e $p \in \mathbb{N}$ primo, definiamo **valore assoluto p-adico** la funzione $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ tale che, se $\mathbb{Q} \ni x = p^k \frac{m}{n}$, con $(mn, p) = 1$, $|x|_p = p^{-k}$ e ovviamente $|0|_p = 0$.
Tale funzione è evidentemente un valore assoluto ed è inoltre non archimedeo, in quanto, se $k \leq h$:

$$\left|p^k \frac{m}{n} + p^h \frac{m'}{n'}\right|_p = p^{-k} \left|\frac{m}{n} + p^{k-h} \frac{m'}{n'}\right| \leq p^{-k}.$$

Proposizione 1.1.4. *Sia K un campo con un valore assoluto $|\cdot|$. Sono equivalenti:*

1. *$|\cdot|$ è non archimedeo*
2. *Per ogni $n \in \mathbb{Z}$, $|n| \leq 1$.*

Dimostrazione. 1 ⇒ 2) Ovvio, perchè $|n| = |1 + \cdots + 1| \leq |1| = 1$.

2 ⇒ 1) Si ha:

$$|(x+y)^m| \leq \sum_{i=0}^m \left|\binom{m}{i}\right| |x^i||y^{m-i}| \leq \sum_{i=0}^m |x^i||y^{m-i}| \leq (m+1) \max_i \{|x^i||y^{m-i}|\},$$

quindi estraendo la radice m-esima e facendo tendere $m \to \infty$ si ha la tesi.

□

Corollario 1.1.5. *Se $\operatorname{char}(K) = p$, ogni valore assoluto su K è non archimedeo.*

Dimostrazione. Per ogni $n \in (\mathbb{Z}/p\mathbb{Z})^*$, $|n| = 1$ perchè n è radice di 1, quindi per la proposizione precedente $|\cdot|$ è non archimedeo. □

Osservazione. Se K è un campo con un valore assoluto archimedeo, presi comunque $x, y \in K \backslash \{0\}$, esiste $n \in \mathbb{N}$ tale che $|nx| > |y|$. Infatti, se $m \in \mathbb{Z}$ è tale che $|m| > 1$, $n = m^k$ (per un k opportuno) funziona.

Consideriamo ora un campo K a caratteristica 0 con un valore assoluto non archimedeo. Consideriamo $A = \{x \in K \mid |x| \leq 1\}$; questo è un sottoanello contenente $\mathbb{Z}$. Inoltre $M = \{x \in K \mid |x| < 1\}$ è il suo unico ideale massimale, in quanto evidentemente $M = A \backslash A^*$ e M è un ideale.

Definizione 1.1.4. Un dominio A è un **anello di valutazione** per $K = K(A)$ se per ogni $x \in K^*$ si ha $x \in A$ oppure $x^{-1} \in A$.

Osservazione. A è un anello di valutazione di K.

Proposizione 1.1.6. *Sia A un anello di valutazione per $K = K(A)$. Allora A è locale e integralmente chiuso.*

Dimostrazione. Per la località, basta far vedere che $M = A \backslash A^*$ è un ideale. Sia $a \in A$ e $m \in M$. Se $m = 0$, evidentemente $am \in M$; se $m \neq 0$, supponiamo per assurdo che $am \notin M$, cioè $am \in A^*$. Allora $(am)^{-1} \in A$ e $A \ni a(am)^{-1} = m^{-1}$, cioè $m \notin M$, assurdo.
Mostriamo ora la chiusura rispetto alla somma; siano $x, y \in M$. Per definizione, uno fra xy^{-1} e $x^{-1}y$ sta in A, dunque, senza perdita di generalità, possiamo supporre che $xy^{-1} \in A$. Allora:

$$x + y = \underbrace{y}_{\in M} \underbrace{(xy^{-1} + 1)}_{\in A} \in M.$$

Sia ora $x \in K$ intero su A. Per definizione, $x \in A$ oppure $x^{-1} \in A$. Se $x \in A$ si ha la tesi. Se invece $x^{-1} \in A$, dalla relazione di interezza $x^n + \sum_{i=0}^{n} a_i x^i = 0$ otteniamo:

$$x = -\left(a_1 + a_2 x^{-1} + \cdots + a_n x^{-n+1}\right) \in A.$$

□

Definizione 1.1.5. Sia K un campo. Una **valutazione** v su K è un omomorfismo $v \colon K^* \to \mathbb{R}$ tale che, $\forall x, y \in K^*$, $v(x + y) \geq \min\{v(x), v(y)\}$.

Osservazione. Se $|\cdot|$ è un valore assoluto non archimedeo su K, posso associargli la valutazione $v = \log_c |\cdot|$, dove $c \in \mathbb{R}$ è tale che $0 < c < 1$. Viceversa, se v è una valutazione, $|x| = c^{v(x)}$ definisce un valore assoluto non archimedeo.
É immediato notare che valori assoluti equivalenti definiscono valutazioni equivalenti (cioè con c diverso) e viceversa.

Esempio. Consideriamo il valore assoluto p-adico su $\mathbb{Q}$. Se prendiamo $c = \frac{1}{p}$, abbiamo che $v_p(p^a m/n) = a$.

Se v è una valutazione su K, possiamo considerare gli insiemi:

$$A_v = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\}, \qquad M_v = \{x \in K^* \mid v(x) > 0\} \cup \{0\},$$

che corrispondono a A e M precedentemente assegnati a un valore assoluto.

Definizione 1.1.6. Una valutazione $v : K^* \to \mathbb{R}$ si dice **discreta** se $v(K^*)$ è un sottogruppo discreto di $\mathbb{R}$.

Osservazione. Sia G un sottogruppo di $\mathbb{R}$. Sono equivalenti:

1. G è discreto (cioè 0 è isolato)

2. Ogni intervallo di lunghezza finita di $\mathbb{R}$ contiene un numero finito di punti di G.

Chiaramente $2 \Rightarrow 1$; viceversa, esiste $\varepsilon > 0$ tale che $|g| \geq \varepsilon$ per ogni $0 \neq g \in G$, quindi, $\forall g \neq h \in G$, $|g - h| \geq \varepsilon$, da cui, se un intervallo ha lunghezza l, in esso possono starci al massimo $\frac{l}{\varepsilon} < +\infty$ punti di G.

Corollario 1.1.7. *Sia G un sottogruppo discreto non banale di $\mathbb{R}$. Allora $G \cong \mathbb{Z}$.*

Dimostrazione. Sia $0 \neq g \in G$; $[0, g] \cap G$ è finito, quindi esiste $e_0 = \min\{(0, g] \cap G\}$. Mostriamo che $G = \langle e_0 \rangle$. Chiaramente l'inclusione $\subseteq$, in quanto G è un gruppo. Sia invece $x \in G$; sicuramente $x = \mu e_0$, con $\mu \in \mathbb{R}^*$. D'altra parte, $G \ni x - [\mu]e_0 = \{\mu\}e_0$ e $0 \leq \{\mu\}e_0 < e_0$, da cui $\{\mu\} = 0$ per minimalità di e_0 (cioè $\mu \in \mathbb{Z}$). $\square$

Di conseguenza, possiamo assumere a meno di normalizzazioni che $v(K^*) = \mathbb{Z}$.

Esempio. Per ogni $p \in \mathbb{N}$ primo, v_p è una valutazione discreta di $\mathbb{Q}$. In questo caso si ha:

$$A_{v_p} = \left\{ p^a \frac{m}{n} \in \mathbb{Q} \;\middle|\; a \geq 0 \right\} = \mathbb{Z}_{(p)}, \qquad M_{v_p} = \left\{ p^a \frac{m}{n} \in \mathbb{Q} \;\middle|\; a \geq 1 \right\} = p\mathbb{Z}_{(p)},$$

cioè A_{v_p} è il localizzato di $\mathbb{Z}$ rispetto al primo p.

Proposizione 1.1.8. *Sia v una valutazione di K. Allora v è discreta $\iff$ M_v è principale.*

Dimostrazione. Se v è una valutazione discreta, esiste $x \in K$ tale che $v(x) = 1$. Mostriamo che x genera M_v. Sia $y \in M_v$, cioè $v(y) \geq 1$. Allora $y = xx^{-1}y$, ma $x^{-1}y \in A_v$, in quanto $v(x^{-1}y) = v(y) - 1 \geq 0$, da cui $y \in (x)$.
Viceversa, se M_v è principale, sia x un suo generatore. Possiamo supporre che $v(x) = 1$ a meno di normalizzare. Dico che 0 è un punto isolato di $v(K^*)$. Infatti, se $y \in K$ e $v(x) > 0$, allora $y \in M_v$ e quindi $v(y) \geq 1$, e lavorando analogamente con y^{-1} si vede che $v(K^*) \cap (-1, 1) = \{0\}$. $\square$

Teorema 1.1.9 (Gelfand)**.** *Sia K un campo munito di un valore assoluto archimedeo. Allora K è isomorfo a un sottocampo di $(\mathbb{C}, \|\cdot\|)$.*

Teorema 1.1.10 (Ostrowski)**.** *Sia $|\cdot|$ un valore assoluto non banale su $\mathbb{Q}$. Allora $|\cdot|$ è equivalente al valore assoluto ordinario o a un valore assoluto p-adico.*

Dimostrazione. Supponiamo dapprima che $|\cdot|$ sia non archimedeo. Sappiamo allora che $|n| \leq 1$ $\forall n \in \mathbb{Z}$.
Consideriamo l'anello di valutazione A come definito prima; ovviamente $\mathbb{Z} \subseteq A$. Contraendo l'ideale M a $\mathbb{Z}$ si ottiene l'ideale primo $M^c = M \cap \mathbb{Z}$; questo può essere 0 o (p) per un certo primo $p \in \mathbb{Z}$.
Se questo è 0, allora $|n| = 1$ $\forall n \in \mathbb{Z}$ e questo genera il valore assoluto banale.
Se invece $M \cap \mathbb{Z} = (p)$, $|p| < 1$, quindi, a meno di normalizzazione, possiamo supporre che $|p| = 1/p$. Osserviamo che, per ogni $m \in \mathbb{Z}$ tale che $(m, p) = 1$, $m \notin (p)$ e dunque $m \notin M$, cioè $|m| = 1$. Da questo si deduce che, $\forall a \in \mathbb{Z}$, $\forall (b, p) = (c, p) = 1$:

$$\left| p^a \frac{b}{c} \right| = p^{-a},$$

cioè $|\cdot|$ è il valore assoluto p-adico.
Supponiamo ora che $|\cdot|$ sia archimedeo. Allora esiste $c \in \mathbb{Z}$ tale che $|c| > 1$. Sia $1 < b \in \mathbb{Z}$. Possiamo scrivere ogni intero n in base b:

$$n = a_k b^k + \cdots + a_1 b + a_0,$$

con $k \leq \frac{\log(n)}{\log(b)}$ e $a_i \leq b-1\ \forall i$. Allora:

$$|n| \leq \sum_{i=0}^{k} |a_i||b|^i \leq (k+1)\max|a_i b^i| \leq (k+1)(b-1)\max|b^i|,$$

da cui $|n| \leq (k+1)(b-1)\max\{1, |b|^k\}$ (a seconda che $|b|<1$ e $|b|>1$). Se $n = c^m$:

$$|c^m| \leq \left(\frac{m\log(c)}{\log(b)} + 1\right)(b-1)\max\{1, |b|^{\frac{m\log(c)}{\log(b)}}\},$$

quindi, passando alla radice m-esima e prendendo il limite $m \to \infty$, si ottiene:

$$1 < |c| \leq \max\{|1|, |b|^{\frac{\log(c)}{\log(b)}}\}$$

e dunque $|b| > 1$, cioè ogni intero ha valutazione > 1. Inoltre $|c| \leq |b|^{\frac{\log(c)}{\log(b)}}$, quindi $|c|^{\frac{1}{\log(c)}} \leq |b|^{\frac{1}{\log(b)}}$, ma per simmetria si ha che $|c|^{\frac{1}{\log(c)}} = |b|^{\frac{1}{\log(b)}} = \lambda\ \forall b, c \in \mathbb{Z},\ b, c > 1$.
Denotando infine $\gamma = \log(\lambda) = \frac{\log|c|}{\log(c)} = \frac{\log|b|}{\log(b)}$, evidentemente $|c| = c^\gamma$ per ogni $c \in \mathbb{Z}$ e perciò $|\cdot|$ è equivalente al valore assoluto ordinario. □

Corollario 1.1.11 (Formula del prodotto per valori assoluti di $\mathbb{Q}$)**.** *Sia $M_\mathbb{Q}$ l'insieme dei valori assoluti non banali di $\mathbb{Q}$ opportunamente normalizzati (ossia i valori assoluti p-adici e quello ordinario). Allora, $\forall x \in \mathbb{Q}^*$:*

$$\prod_{|\cdot| \in M_\mathbb{Q}} |x| = 1$$

Dimostrazione. Se $n \in \mathbb{N}$, allora $n = \prod_{i=0}^r p_i^{e_i}$ e dunque:

$$\prod |n| = p_1^{e_1} \dots p_r^{e_r} \prod_p |n|_p = 1.$$

□

Osservazione. Abbiamo definito l'insieme dei valori assoluti discreti come sottoinsieme dei valori assoluti non archimedei; tale definizione non è restrittiva, in quanto, anche definendo un valore assoluto **discreto** se l'immagine di $\log_c|\cdot|$ è un sottogruppo discreto di $\mathbb{R}$, ogni valore assoluto discreto risulta essere non archimedeo.

Dimostrazione. Se $\mathrm{char}(K) = p \neq 0$, necessariamente il valore assoluto è non archimedeo.
Se invece $\mathrm{char}(K) = 0$, basta studiare il valore assoluto su $\mathbb{Q}$. Ma per il teorema di Ostrowski sappiamo che l'unico valore assoluto archimedeo è non discreto, da cui la tesi. □

Esempio (Valore assoluto non discreto e non archimedeo). Consideriamo il campo $K(x,y)$ e la valutazione:

$$\begin{array}{cccc} v: & K(x,y)^* & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & 1 \\ & y & \longrightarrow & \sqrt{2} \\ & \sum_{i,j} a_{ij}x^i y^j & \longrightarrow & \min\{v(x^i y^j)\} \end{array}$$

Con una semplice verifica si vede che è un omomorfismo, ed evidentemente $v(K(x,y)^*) = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$, che non è un sottogruppo discreto di $\mathbb{R}$.

Lo stesso studio dei valori assoluti può essere generalizzato al campo $K(t)$. Vediamo ora quali possono essere i valori assoluti che sono banali su K. Consideriamo un polinomio irriducibile $p(t) \in K[t]$ e assegniamogli un valore $|p| = c$ con $0 < c < 1$; possiamo allora considerare il valore assoluto tale che, se $f = p^k q_1^{e_1} \dots q_k^{e_k}$, con $(q_i, p) = 1 \ \forall i$, $|f| = c^k$. Questo è effettivamente un valore assoluto non archimedeo. Un altro valore assoluto su $K(t)$ banale su K può essere quello tale che $\left|\frac{f(t)}{g(t)}\right| = c^{\deg(g)-\deg(f)}$ per un certo $0 < c < 1$; anche questo è non archimedeo:

$$\left|\frac{f}{g} + \frac{h}{l}\right| = \left|\frac{fl+hg}{gl}\right| = c^{\deg(gl)-\deg(fl+hg)} \leq \max\left\{\left|\frac{f}{g}\right|, \left|\frac{h}{l}\right|\right\}.$$

Teorema 1.1.12. *Questi sono tutti e soli i valori assoluti su $K(t)$ banali su K (a meno di equivalenza).*

Dimostrazione. Per la banalità su K, un valore assoluto è necessariamente non archimedeo, perchè per ogni $k \in K$, $|k| = 1$.
Denotiamo A, M rispettivamente l'anello di valutazione e l'ideale massimale corrispondente. Dividiamo due casi:

- Se $|t| \leq 1$, t appartiene all'anello di valutazione e dunque $K[t] \subseteq A$. La contrazione di M a $K[t]$ è primo, quindi può essere 0 o $p(t)$, con p irriducibile. Il primo caso fornisce il valore assoluto banale. Nel secondo caso, se $q(t) \in K[t]$ è un polinomio coprimo con p, necessariamente $|q(t)| = 1$, in quanto non appartiene all'ideale massimale, dunque, dato $f(t) = p(t)^k g(t)$ un polinomio qualsiasi, $|f(t)| = |p(t)|^k$, da cui il primo caso.
- Se $|t| > 1$, allora $\frac{1}{t} \in M$ e $K\left[\frac{1}{t}\right] \subseteq A$. La contrazione di M a $K\left[\frac{1}{t}\right]$ contiene l'ideale $\left(\frac{1}{t}\right)$, che è massimale, da cui $K\left[\frac{1}{t}\right] = \left(\frac{1}{t}\right)$. A questo punto, se:
$$\frac{f(t)}{g(t)} = \frac{t^m(a_m + a_{m-1}1/t + \dots + a_0 t^{-m})}{t^n(b_n + b_{n-1}t^{-1} + \dots + b_0 t^{-n})},$$
con $m = \deg(f)$, $n = \deg(g)$ e $a_m, b_n \neq 0$, i polinomi fra parentesi stanno in $K\left[\frac{1}{t}\right]$ ma non in M, dunque hanno valore assoluto 1, perciò $\left|\frac{f}{g}\right| = \left|\frac{1}{t}\right|^{n-m}$.

□

Teorema 1.1.13 (Approssimazione debole). *Siano $|\cdot|_1, \dots, |\cdot|_n$ valori assoluti non banali e non equivalenti su un campo K. Allora, per ogni $\alpha_1, \dots, \alpha_n \in K$ e per ogni $\varepsilon > 0$, esiste $\beta \in K$ tale che $|\alpha_i - \beta|_i < \varepsilon \ \forall i = 1, \dots, n$. Equivalentemente, in $K^n = (K, |\cdot|_1) \times \dots \times (K, |\cdot|_n)$ la diagonale è densa.*

Dimostrazione. Basta trovare $\xi_1, \dots, \xi_n \in K$ tali che $|\xi_i|_i > 1$ e $|\xi_i|_j < 1$ per ogni $j \neq i$. In tal caso, infatti, notando che:

$$\frac{\xi_i^m}{1+\xi_i^m} \longmapsto \begin{cases} 1 & \text{rispetto a } |\cdot|_i \\ 0 & \text{rispetto a } |\cdot|_j \end{cases}$$

basta considerare $\beta = \sum_{i=1}^n \frac{\xi_i^m}{1+\xi_i^m}\alpha_i$ con $m = m(\varepsilon)$ opportuno.
Mostriamo dunque che possiamo trovare ξ tale che $|\xi|_1 > 1$ e $|\xi|_i < 1$ per $i \neq 1$ (poi per gli altri è analogo); vediamolo per induzione su n.
Se $n = 2$, dato che i valori assoluti non sono equivalenti, tra le palle di centro 0 e raggio 1 non esiste un contenimento, dunque, se α sta nella palla rispetto a $|\cdot|_1$ e non in quella rispetto a $|\cdot|_2$ e β sta nella palla rispetto a $|\cdot|_2$ e non in quella rispetto a $|\cdot|_1$, scegliamo $\xi = \alpha^{-1}\beta$.
Per il passo induttivo, sia ξ tale che $|\xi|_1 > 1$ e $|\xi|_i < 1 \ \forall 2 \leq i \leq n-1$. Se $|\xi|_n < 1$, abbiamo finito. Se $|\xi|_n = 1$, per il caso $n = 2$ esiste $\lambda \in K^*$ tale che $|\lambda|_1 > 1$ e $|\lambda|_n < 1$, quindi $\xi^m\lambda$ funziona come nuovo ξ per un certo m abbastanza grande
. Se infine $|\xi|_n > 1$, ragionando analogamente con $\frac{\xi^m}{1+\xi^m}\lambda$ si ha la tesi. □

1.2 Completamenti

Sia K un campo e $|\cdot|$ un valore assoluto su K. Su K può essere costruita una distanza nel modo ovvio: $d(x,y) = |x-y|$ per ogni $x, y \in K$; con tale distanza, lo spazio (K,d) risulta essere metrico, dunque può essere completato aggiungendo a K tutti i limiti delle successioni di Cauchy di (K,d). Tale completamento $\overline{K}$ è unico a meno di isomorfismo e omeomorfismo e anch'esso risulta essere metrico con la distanza $\overline{d}$ indotta dal valore assoluto $|\cdot|'$ tale che $|\lim_{n\to\infty} a_n|' := \lim_{n\to\infty} |a_n|$, con $(a_1, a_2, \dots)$ successione di Cauchy in (K,d). Inoltre il completamento $(\overline{K}, \overline{d})$ è evidentemente uno spazio completo.
In tale situazione, l'immersione:

$$\begin{array}{ccc} K & \longrightarrow & \overline{K} \\ a & \longmapsto & (a,a,a,\dots) \end{array}$$

ha per definizione immagine densa.

Esempi. Il completamento di $\mathbb{Q}$ rispetto al valore assoluto ordinario è $\mathbb{R}$.
Il completamento di $\mathbb{Q}$ rispetto al valore assoluto p-adico sono i **numeri p-adici** $\mathbb{Q}_p$.

I numeri p-adici sono un'estensione dei numeri razionali $\mathbb{Q}$, da cui ereditano naturalmente un'aritmetica. Per caratterizzarli, dobbiamo caratterizzare le successioni di Cauchy in $(\mathbb{Q}, |\cdot|_p)$; sia $\{a_k \mid k \in \mathbb{N}\}$ una di esse. Supponiamo in prima ipotesi che i numeri a_k siano interi di $\mathbb{Z}$ e siano $a_k = b_{0k} + b_{1k}p + \ldots + b_{l_k k}p^{l_k}$ i loro sviluppi p-adici. Per definizione di successione di Cauchy, si ha che per ogni $\varepsilon > 0$ esiste $N = N(\varepsilon)$ tale che $\forall m, n > N$:

$$\varepsilon > |a_m - a_n|_p = p^{-s},$$

dove s è il numero di cifre p-adiche iniziali che a_m e a_n hanno in comune; di conseguenza, le cifre iniziali dello sviluppo p-adico degli a_k sono definitivamente costanti. Se le denotiamo con c_i, per $i \in \mathbb{N}$, riusciamo ad associare alla successione di Cauchy $\{a_k \mid k \in \mathbb{N}\}$ il suo limite:

$$\{a_k \mid k \in \mathbb{N}\} \longmapsto \sum_{i=0}^{\infty} c_i p^i \in \mathbb{Q}_p.$$

Con il ragionamento appena fatto, siamo riusciti ad individuare dentro $\mathbb{Q}_p$ il sottoinsieme degli **interi p-adici**, che denotiamo con $\mathbb{Z}_p$ e che coincidono con il limite proiettivo $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$; in quanto limite proiettivo, $\mathbb{Z}_p$ risulta essere un gruppo profinito, dunque $T2$ e compatto (nella topologia indotta dal limite proiettivo).
D'altra parte, è evidente che gli interi p-adici non coprono tutti i numeri p-adici, in quanto le successioni di Cauchy che dobbiamo considerare hanno gli elementi in $\mathbb{Q} \supsetneq \mathbb{Z}$; la seguente proposizione caratterizza completamente gli elementi di $\mathbb{Q}_p$.

Proposizione 1.2.1. *$\mathbb{Q}_p$ è il campo dei quozienti di $\mathbb{Z}_p$, cioè:*

$$\mathbb{Q}_p = \bigcup_{n\in\mathbb{N}} \frac{1}{p^n}\mathbb{Z}_p.$$

I numeri p-adici sono scrivibili tramite una serie di Laurent, in quanto le potenze di p variano fra m e ∞, con $-\infty < m < +\infty$ possibilmente negativo.

Dimostrazione. Sia $a \in \mathbb{Q}_p$. A meno di moltiplicare per p^M, con M sufficientemente grande, possiamo supporre che $|a|_p \leq 1$. Vogliamo provare per induzione su N che esistono dei coefficienti $a_0, \dots, a_N \in \{0, \dots, p-1\}$ tali che:

$$\left| a - \sum_{i=0}^{N} a_i p^i \right|_p < p^{-N}.$$

Vediamo il passo base $N = 0$; preso un razionale $c = \frac{d}{e}$ (ridotto ai minimi termini) tale che $|a - c|_p < 1$, necessariamente si deve avere che $(e, p) = 1$ per la limitazione sul valore assoluto, dunque esistono interi x, y che soddisfano l'identità di Bezout $xe + yp = 1$. Ma allora:

$$|a - xd|_p = |a - (1 - yp)c|_p \leq \max\{|a - c|_p, |ypc|_p\} < 1,$$

in quanto $|ypc|_p = |y|_p|p|_p|c|_p \leq \frac{1}{p}$, dunque sottraendo a xd un opportuno multiplo r di p in modo che $b = xd - pr \in \{0, \dots, p-1\}$ si ottiene il b voluto.
In modo analogo al passo base si vede anche il passo induttivo e la dimostrazione è completa. □

Osservazione. $\mathbb{Q}_p$ è localmente compatto, perchè $\mathbb{Z}_p$ è compatto e aperto e dunque, per ogni $x \in \mathbb{Q}_p$, esiste l'intorno $x + \mathbb{Z}_p$ ($\mathbb{Z}_p$ è aperto e compatto perchè $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x| \leq 1\} = \{x \in \mathbb{Q}_p \mid |x| < p\}$.

Osservazione. Sia K un campo con una valutazione discreta v. Allora $v(\overline{K}^*) = v(K^*)$, cioè i valori assoluti del completamento di K sono gli stessi di quelli di K. Infatti, data una successione di Cauchy $\{x_n\}$, abbiamo che $|x_n|$ è definitivamente costante, in quanto a valori in un insieme discreto e la distanza tra due termini successivi tende a 0.

Osservazione. $\mathbb{Q}_p \supseteq \mathbb{Q}$, dunque $\mathrm{char}(\mathbb{Q}_p) = 0$.

Ci spostiamo adesso verso lo studio degli elementi invertibili dell'anello $\mathbb{Z}_p$; sicuramente essi formano un gruppo abeliano, quindi è conveniente trovare subito gli invertibili di $\mathbb{Z}_p$ di ordine finito. Se $x \in \mathbb{Z}_p^*$ è tale che $x^n = 1$, allora $x^n \equiv 1 \pmod p$, dunque $n \mid p - 1$.

Lemma 1.2.2 (Lemma di Hensel)**.** *Sia $f \in \mathbb{Z}[x]$ e sia $a \in \mathbb{Z}$ tale che $f(a) \equiv 0 \pmod p$. Supponiamo inoltre che $f'(a) \not\equiv 0 \pmod p$. Allora esiste un unico $\alpha \in \mathbb{Z}_p$ tale che $f(\alpha) = 0$ e $\alpha \equiv a \pmod p$.*

Dimostrazione. Utilizzando la formula di Taylor, abbiamo:

$$f(x) = f(a) + f'(a)(x - a) + \frac{f''(a)}{2}(x - a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(x - a)^n + \ldots$$

Sappiamo che $f(a) = bp$; cerchiamo di sollevare questo a un $a' = a + tp$ tale che $f(a') \equiv 0 \pmod{p^2}$. $f(a') \equiv f(a) + f'(a)tp \pmod{p^2}$, quindi otteniamo l'equazione:

$$f(a) + f'(a)tp \equiv 0 \pmod p^2$$

che ammette una e una sola soluzione grazie all'ipotesi $f'(a) \not\equiv 0 \pmod p$.
In generale, supponiamo di avere una soluzione di $f(a) \equiv 0 \pmod{p^n}$. Posto $f(a) = bp^n$, cerchiamo $a' = a + tp^n$ tale che $f(a') \equiv 0 \pmod{p^{n+1}}$. Sostituendo nello sviluppo di Taylor, otteniamo come prima l'equazione:

$$f(a') = f(a) + f'(a)tp^n \pmod{p^{n+1}}$$

Sollevando ricorsivamente le soluzioni in questo modo, si arriva all'elemento $\alpha \in \mathbb{Z}_p$, che risulta essere unico perchè ad ogni passaggio la scelta del sollevamento è unica. □

Grazie al lemma di Hensel, abbiamo allora un'unica radice $p - 1$-esima dell'unità x tale che $x \equiv a \pmod p$ per ogni $a \in (\mathbb{Z}/p\mathbb{Z})^*$ (l'ordine è proprio $p - 1$ perchè a ha tale ordine in $(\mathbb{Z}/p\mathbb{Z})^*$). Siamo adesso pronti per dimostrare la struttura di $\mathbb{Z}_p^*$:

Teorema 1.2.3. *Se $p \neq 2$, abbiamo che $\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p$.*

Dimostrazione. Dato che abbiamo già individuato il fattore $(\mathbb{Z}/p\mathbb{Z})^*$, basta individuare il secondo. Se poniamo $U_1 = 1 + p\mathbb{Z}_p$, ovviamente l'intersezione tra questi sottogruppi è banale; d'altra parte generano tutto $\mathbb{Z}_p^*$, in quanto, se $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^*$, abbiamo che $a_i \in (\mathbb{Z}/p\mathbb{Z})^*$ $\forall i$ e dunque:

$$\sum_{i=0}^{\infty} a_i p^i = a_0 \left(\sum_{i=0}^{\infty} \frac{a_i}{a_0} p^i \right) = \widetilde{a_0} \underbrace{\left(\sum_{i=0}^{\infty} \frac{a_i}{\widetilde{a_0}} p^i \right)}_{\in U_1},$$

dove $\widetilde{a_0}$ è una radice dell'unità tale che $\widetilde{a_0} \equiv a_0 \pmod p$.
Rimane da vedere che $U_1 \cong \mathbb{Z}_p$; osserviamo che esiste una catena discendente di sottogruppi:

$$U_1 = 1 + p\mathbb{Z}_p \supseteq U_2 = 1 + p^2\mathbb{Z}_p \supseteq \ldots \supseteq U_n = 1 + p^n\mathbb{Z}_p \supseteq \ldots$$

tale che i quozienti $\frac{U_1}{U_n}$ sono ciclici, generati da $1+p$ (in quanto, per l'ipotesi $p \neq 2$, $(1+p)^{p^i} \equiv 1 + p^{i+1} \pmod{p^{i+2}}$, dunque $\mathrm{ord}_{U_1/U_n}(1+p) = p^{n-1} = \left|\frac{U_1}{U_n}\right|$). Ma allora, visto che i diagrammi:

$$\begin{array}{ccc} \frac{U_1}{U_n} & \xrightarrow{\sim} & \mathbb{Z}/p^{n-1}\mathbb{Z} \\ {\scriptstyle f_{mn}}\downarrow & & \downarrow{\scriptstyle \pi_{mn}} \\ \frac{U_1}{U_m} & \xrightarrow{\sim} & \mathbb{Z}/p^{m-1}\mathbb{Z} \end{array}$$

commutano per ogni $n \geq m$, allora $U_1 = \varprojlim \frac{U_1}{U_n} \cong \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \cong \mathbb{Z}_p$. □

Come si può immaginare, il primo $p = 2$ si comporta in modo leggermente diverso; procedendo come nella dimostrazione precedente e sfruttando il fatto che $\frac{U_1}{U_n} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-3}\mathbb{Z}$, si può mostrare:

Teorema 1.2.4. $\mathbb{Z}_2^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \cong \{\pm 1\} \times \mathbb{Z}_2$.

Sia K un campo completo con valore assoluto $|\cdot|$ e sia L un'estensione algebrica finita di K; poniamo $[L : K] = n$. Allora $L \cong K^n$ e dunque possiamo munirlo del valore assoluto di K su ogni componente; in questo modo viene indotta naturalmente una norma in L:

$$\|x\|_\infty = \sup_i |x_i|.$$

Proposizione 1.2.5. *Sia K un campo completo localmente compatto e sia L un'estensione algebrica finita di k. Allora tutte le norme di L come K-spazio vettoriale sono equivalenti.*

Dimostrazione. Basta confrontare una qualsiasi norma con la norma $\|\cdot\|_\infty$ introdotta sopra; sia $\|\cdot\|$ una norma qualsiasi. Dato che K è localmente compatto, lo stesso vale per L, e formando le palle una base di intorni di 0, esse sono compatte e sulla palla unitaria secondo $\|\cdot\|_\infty$, $\|\cdot\|$ assume massimo Δ e minimo $\delta > 0$.
A questo punto, preso $x \in L$ e $y \in L$ tale che $\|y\| = 1$, si ha che $x = \lambda y$ e dunque $\lambda\delta \leq \|\lambda y\| \leq \lambda\Delta$, da cui la norma $\|\cdot\|$ ha intorni di 0 compresi fra intorni di 0 secondo $\|\cdot\|_\infty$. □

Corollario 1.2.6. *Nella ipotesi della proposizione precedente, dato v_0 un valore assoluto su K, esiste un unico valore assoluto L su K che estende v_0.*

Dimostrazione. L'unicità segue dal fatto che un valore assoluto, a meno di equivalenza, è una norma. Per l'esistenza, esibiamo un tale valore assoluto. Consideriamo:

$$|x|_e = |\,\mathrm{N}_{L/K}(x)|^{\frac{1}{n}}.$$

□

<u>*Osservazione*</u>. Consideriamo $\mathbb{Q}_p$ e una sua estensione finita L. Allora su L abbiamo un solo valore assoluto che estende il valore assoluto di $\mathbb{Q}_p$.

1.3 Valori assoluti su un campo di numeri

Sia K un campo di numeri. Allora, dato $v : K \to \mathbb{R}$ un valore assoluto su K, $v_{|\mathbb{Q}}$ è un valore assoluto su $\mathbb{Q}$ e dunque per il teorema di Ostrowski deve coincidere con il valore assoluto ordinario o un valore assoluto p-adico. Possiamo scrivere $[K : \mathbb{Q}] = n = r + 2s$, dove r è il numero delle immersioni reali e $2s$ quello delle immersioni complesse.

Osservazione. Se $v_{|\mathbb{Q}}$ è (non) archimedeo, anche v lo è, in quanto l'essere (o meno) archimedeo dipende solo dalla limitatezza dei valori $v(n)$ per $n \in \mathbb{Z}$.

Se $v_{|\mathbb{Q}}$ (e dunque v) è archimedeo, allora ho $r + s$ valori assoluti su K, uno per ciascuna immersione $\sigma : K \hookrightarrow \mathbb{C}$ (quelle coniugate si contano una volta sola).
Se invece $v_{|\mathbb{Q}}$ è non archimedeo, corrisponde a una valutazione e gli associamo come al solito l'anello A e l'ideale massimale M.

Osservazione. Data una valutazione non archimedea su un campo di numeri, l'anello di valutazione A contiene $\mathscr{O}_K$. Infatti, dato $x \in \mathscr{O}_K$, $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ e dunque:

$$|x^n| \leq \max_i |a_i x^i| = \max |a_i||x|^i \leq \max |x|^i$$

da cui $|x^{n-i}| \leq 1$, cioè $|x| \leq 1$.

Consideriamo l'immersione $\mathscr{O}_K \to A$ e la contrazione del suo massimale M. Questa contrazione non può essere banale, in quanto stiamo considerando valori assoluti non banali. Allora $M \cap \mathscr{O}_K$ è un ideale primo non nullo di $\mathscr{O}_K$, che è un dominio di Dedekind, dunque $M \cap \mathscr{O}_K$ è massimale; inoltre $M \cap \mathbb{Z}$ è un primo di $\mathbb{Z}$. Evidentemente $M \cap \mathscr{O}_K$ è un primo sopra p. Denotiamo $P = M \cap \mathscr{O}_K$ e consideriamo $S^{-1}\mathscr{O}_K$, dove $S = \mathscr{O}_K \backslash P$; è immediato osservare che $S^{-1}\mathscr{O}_K$ è un anello di valutazione di K. Dico che $A = S^{-1}\mathscr{O}_K$.
Sia $x \in A$. $S^{-1}\mathscr{O}_K$ è di valutazione per K, dunque, se per assurdo $x \notin S^{-1}\mathscr{O}_K$, allora $x^{-1} \in S^{-1}\mathscr{O}_K$. Ma x^{-1} non è invertibile in $S^{-1}\mathscr{O}_K$, quindi $x^{-1} \in P = M \cap \mathscr{O}_K$ e perciò $|x^{-1}| < 1$, da cui $|x| > 1$, assurdo in quanto gli elementi di $S^{-1}\mathscr{O}_K$ hanno valore assoluto ≤ 1.
Viceversa, preso $x \in S^{-1}\mathscr{O}_K$, se per assurdo $x \notin A$ allora $x^{-1} \in A$ non è invertibile, quindi $|x^{-1}| < 1$, da cui $|x| > 1$.
Inoltre A, essendo il localizzato di un dominio di Dedekind, è un **anello a valutazione discreta** (**DVR**), e perciò è PID (questo è vero perchè il localizzato di un dominio di Dedekind è ancora un dominio di Dedekind e perchè un dominio di Dedekind con un numero finito di ideali primi è un PID); da questo si ricava che l'unico ideale primo di A, cioè M, è generato da un certo elemento π.
Di conseguenza, ogni elemento $x \in A$ si scrive come $x = \pi^r u$, con $u \in A^*$, quindi il valore assoluto v su K è completamente determinato dalla scelta di $|\pi| \in (0, 1)$. Per normalizzare, scegliamo c in modo tale che $|p| = 1/p$; questo si può fare perchè $(p) = (\pi)^e$ per un certo e indice di ramificazione.

Cerchiamo di trasportare in questo ambito la formula del prodotto dei valori assoluti. Consideriamo $p \in \mathbb{Z}$ e la sua estensione $p\mathscr{O}_K = P_1^{e_1} \dots P_r^{e_r}$; detto π_i il generatore del massimale di $S_i^{-1}\mathscr{O}_K$, con $S_i = \mathscr{O}_K \backslash P_i$, allora possiamo normalizzare il valore assoluto come:

$$|\pi_i|_{P_i} = \frac{1}{p^{e_i f_i}}.$$

In questo modo otteniamo la relazione:

$$\prod_i |\pi_i|_{P_i} = \frac{1}{p^{\sum_{i=1}^r e_i f_i}} = \frac{1}{p^n}.$$

Proposizione 1.3.1. *Sia K un campo di numeri e sia v un valore assoluto di K. Sia E/K un'estensione finita e sia K_v il completamento di K rispetto al valore assoluto v. Due immersioni $\sigma, \tau \colon E \to \overline{K_v}$ danno luogo allo stesso valore assoluto su E se e solo se sono coniugate su K_v, cioè il diagramma:*

$$\begin{tikzcd} E \arrow[r, "\sigma"] \arrow[dr, "\tau"'] & \overline{K_v} \arrow[d, "\varphi"] \\ & \overline{K_v} \end{tikzcd}$$

dove $\varphi \in \mathrm{Aut}_{K_v}(\overline{K_v})$, commuta.

Dimostrazione. Supponiamo che σ, τ siano coniugate su K_v. Per l'unicità del valore assoluto, i valori assoluti indotti da σ e $\tau = \varphi \circ \sigma$ devono coincidere.
Viceversa, supponiamo che σ e τ inducano lo stesso valore assoluto su E. Sappiamo che $\sigma(E) \cong \tau(E) \cong E$, dunque costruiamo $\lambda \colon \sigma(E) \to \tau(E)$ isomorfismo su K. Vogliamo estendere questo isomorfismo a $\widetilde{\lambda} \colon \sigma(E)K_v \to \tau(E)K_v$; dato che i valori assoluti coincidono, la successione $\{\sigma(x_n)\}$ è di Cauchy $\iff$ $\{\tau(x_n)\}$ lo è, dunque, dato $x \in \sigma(E)K_v$ e data $x_n \in E$ una successione di Cauchy tale che $\lim_{n\to\infty} \sigma(x_n) = x$, basta porre:

$$\widetilde{\lambda}(x) = \lim_{n\to\infty} \lambda(\sigma(x_n)).$$

Tale mappa è ben definita, è un isomorfismo e fissa effettivamente K_v, perchè questo è definito come limite di successioni in K, che viene fissato da λ. $\square$

Questa proposizione ha alcune conseguenze importanti:

Corollario 1.3.2. *Sia E/K un'estensione finita, $[E : K] = n$, con K campo di numeri. Sia $v \in M_K$ un valore assoluto su K a meno di equivalenza. Per ogni $w \in M_E$ che estende v (cioè $w|_K = v$), poniamo $n_w = [E_w : K_v]$ il* ***grado locale****. Allora:*

$$n = \sum_{w|v} n_w,$$

dove con $w \mid v$ abbiamo indicato che w estende v.

Dimostrazione. Ovvio, perchè n_w indica il numero di campi coniugati con E_w su K_v, dunque basta dividere le immersioni di E/K per classi di equivalenza rispetto al valore assoluto indotto. $\square$

Corollario 1.3.3. *Nelle ipotesi precedenti, supponiamo $K = \mathbb{Q}$ ed E campo di numeri. Sia $v_0 \in M_{\mathbb{Q}}$ e sia $\alpha \in E$. Allora:*

$$\prod_{v|v_0} |\alpha|_v^{n_v} = |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|_{v_0}$$

Dimostrazione. Suddividendo le valutazioni che inducono lo stesso valore assoluto, abbiamo:

$$|N_{K/\mathbb{Q}}(\alpha)|_{v_0} = \left| \prod_i \sigma_i(\alpha) \right|_{v_0} = \prod_{v|v_0} |\alpha|_v^{n_v}.$$

$\square$

In modo del tutto analogo si prova:

Corollario 1.3.4. *Supponiamo E/K finita e supponiamo che $w \mid v$. Consideriamo la norma e traccia locale:*

$$\begin{array}{rccc} \mathrm{N}_w : & E_w & \longrightarrow & K_v \\ & \alpha & \longmapsto & \prod_i \widetilde{\sigma}_i(\alpha) \end{array} \qquad \begin{array}{rccc} \mathrm{Tr}_w : & E_w & \longrightarrow & K_v \\ & \alpha & \longmapsto & \sum_i \widetilde{\sigma}_i(\alpha) \end{array}$$

Allora:

$$\mathrm{N}_{E/K}(\alpha) = \prod_{w|v} \mathrm{N}_w(\alpha) \qquad\qquad \mathrm{Tr}_{E/K}(\alpha) = \sum_{w|v} \mathrm{Tr}_w(\alpha).$$

Osservazione. Sia $K = \mathbb{Q}_p$ e supponiamo che E/K sia finita. Allora $\mathscr{O}_K = \mathbb{Z}_p$ è un anello locale a ideali principali, con ideali i (p^n). Allora $\mathscr{O}_E$ è un anello a ideali principali, in quanto sappiamo che esiste un unico valore assoluto che estende il valore assoluto p-adico.
Dato $\alpha \in \mathscr{O}_K$, α soddisfa un'equazione $\alpha^n + \sum c_i\alpha^i = 0$ e dunque, dato che stiamo trattando un valore assoluto non archimedeo, esiste un'uguaglianza di valore assoluti tra due addendi, altrimenti, usando che $|x| < |y| \Rightarrow |x+y| = |y|$, varrebbe che $|\alpha^n + \sum c_i\alpha^i| = \max_i |c_i\alpha^i| \neq 0$. Perciò esistono $i < j$ tali che $|c_i\alpha^i| = |c_j\alpha^j|$, da cui $|\alpha^{j-i}| = |c_i/c_j|$. Dato che i valori assoluti sono discreti, $v(\alpha) \in \frac{1}{n}\mathbb{Z}$ per un certo $n \in \mathbb{N}$. Se α è un generatore di $\mathscr{O}_K$, $v(K)$ è discreta; di conseguenza, se K è un campo con una valutazione discreta, l'anello di valutazione $\mathscr{O}_K$ è un dominio locale a ideali principali, ossia un DVR, i cui ideali principali sono della forma (π^n), con π di valutazione minima (o valore assoluto massimo).

Teorema 1.3.5 (Ore)**.** *Sia $K = \mathbb{Q}(\alpha)$ un'estensione di $\mathbb{Q}$ di grado n e supponiamo che $\mathscr{O}_K = \mathbb{Z}[\alpha]$. Sia μ il polinomio minimo di α su $\mathbb{Q}$. Supponiamo che in $\mathbb{Q}_p[x]$ μ ammetta una fattorizzazione $\mu(x) = \prod_{i=1}^r \mu_i(x)$. Allora $p\mathscr{O}_K = \prod_{i=1}^r P_i^{e_i}$, con $f(P_i|p) = f_i$ e $e_if_i = \deg \mu_i$.*

Dimostrazione. Le valutazioni che estendono quella p-adica sono r, corrispondenti ai primi $P_1, \dots, P_r$. Consideriamo le classi di equivalenza delle immersioni $\sigma_i \colon K \hookrightarrow \overline{\mathbb{Q}_p}$ secondo il valore assoluto indotto; queste corrispondono ai primi $P_1, \dots, P_r$. Se $[K : \mathbb{Q}] = n = \sum_{v|v_p} n_v$, con $[K_v : \mathbb{Q}_p] = n_v$, abbiamo che $p\mathscr{O}_{K_{v_i}} = P_i^{e_i}$ $\forall i$ e $e_if_i = n_{v_i}$, da cui la tesi. □

Proposizione 1.3.6. *Sia A un anello a valutazione discreta con ideale massimale P con $E = K(A)$ (cioè $A = \mathscr{O}_E$) e sia L/E finita e separabile. Supponiamo che esista un solo primo Q sopra P in $\mathscr{O}_L$ e sia $\beta \in \mathscr{O}_L$ tale che $\overline{\beta}$ generi il campo residuo, cioè $\frac{\mathscr{O}_L}{Q} = \frac{\mathscr{O}_E}{P}[\overline{\beta}]$. Sia $\pi \in Q$ un elemento di valutazione minima (dunque $Q = (\pi)$ e, a meno di normalizzare, $v(\pi) = 1$); allora $\mathscr{O}_L = \mathscr{O}_E[\pi, \beta]$.*

Dimostrazione. Dobbiamo mostrare che $C = A[\pi, \beta] = \mathscr{O}_L$. Chiaramente $C \subseteq \mathscr{O}_L$. Per Nakayama, basta mostrare che $P\mathscr{O}_L + C = \mathscr{O}_L$, in quanto avremmo che $P\frac{\mathscr{O}_L}{C} = \frac{\mathscr{O}_L}{C}$ e perciò $\frac{\mathscr{O}_L}{C} = 0$. Sappiamo che $P\mathscr{O}_L = Q^e$ e $\frac{\mathscr{O}_L}{Q^e}$ è generato dalle classi dei prodotti $\beta^i\pi^j$ sul campo $\frac{\mathscr{O}_E}{P}$, con $0 \leq j < e$ e $0 \leq i < \left[\frac{\mathscr{O}_L}{Q} : \frac{\mathscr{O}_E}{P}\right]$, da cui appunto $Q^e + C = \mathscr{O}_L$. □

La precedente proposizione può essere migliorata in un caso particolare:

Proposizione 1.3.7. *Sia A un dominio a valutazione discreta con campo dei quozienti K. Sia L/K un'estensione di campi finita e separabile, sia B l'anello di valutazione di L e siano P, Q gli ideali massimali rispettivamente di A e B. Supponiamo che $\frac{B}{Q}$ sia un'estensione separabile di $\frac{A}{P}$. Allora esiste $\alpha \in B$ tali che $B = A[\alpha]$.*

Dimostrazione. Sia $\beta \in B$ tale che $\frac{B}{Q} = \frac{A}{P}[\overline{\beta}]$ (che esiste per il teorema dell'elemento primitivo) e π un generatore di Q. Mostriamo che possiamo prendere $\alpha = \beta$ oppure $\alpha = \beta + \pi$. Evidentemente $\overline{\beta} = \overline{\beta + \pi}$. Sia $\mu_{\overline{\beta}}$ il polinomio minimo di $\overline{\beta}$ e sia $f \in A[x]$ un suo sollevamento monico. Notiamo che:

$$f(\beta + \pi) \equiv f(\beta) + f'(\beta)\pi \pmod{\pi^2}$$

e $f'(\beta) \not\equiv 0 \pmod{\pi}$ per separabilità dell'estensione. $f(\beta) \equiv 0 \pmod{\pi}$, perciò la valutazione di $f(\beta)$ è almeno 1; dunque deve valere una delle seguenti:

- Se $f(\beta)$ ha valutazione minima, prendiamo $\alpha = f(\beta)$ e dunque abbiamo aggiunto un elemento che genera il massimale
- Se $f(\beta)$ non ha valutazione minima, allora prendiamo $\alpha = f(\beta + \pi)$ che ha valutazione 1 e abbiamo la tesi.

□

Lemma 1.3.8 (Lemma di Hensel generalizzato)**.** *Sia A un anello di valutazione discreta completo con ideale massimale P e sia $\pi\colon A \to \frac{A}{P}$ la proiezione. Sia $h(x) \in A[x]$ un polinomio monico tale che $\overline{h} = \overline{f} \cdot \overline{g}$ e $(\overline{f}, \overline{g}) = 1$. Allora esistono $f, g \in A[x]$ tali che $h = f \cdot g$ con $\deg(f) = \deg(\overline{f})$ e $\deg(g) = \deg(\overline{g})$ e $\pi(g) = \overline{g}$, $\pi(f) = \overline{f}$.*

Dimostrazione. Chiamiamo $m = \deg(\overline{f})$, $n = \deg \overline{g}$. Definiamo induttivamente una successione $f_k, g_k \in A[x]$ tali che:

- $\deg(f_k) = m$, $\deg(g_k) = n$
- $h - f_k g_k$ abbia coefficienti in P^{k+1}
- $f_k \equiv f_{k-1} \pmod{p^k}$ e $g_k \equiv g_{k-1} \pmod{p^k}$
- $\overline{f}_0 = \overline{f}$ e $\overline{g}_0 = \overline{g}$.

Tali successioni sono sufficienti per la tesi, in quanto f_k, g_k sono di Cauchy per la terza ipotesi e dunque convergenti agli F, G voluti. Costruiamo dunque tali successioni. Come primo passo, scegliamo F_0, G_0 sollevamenti qualsiasi di $\overline{F}$ e $\overline{G}$. Adesso supponiamo di avere f_k, g_k coprimi e mostriamo come costruire f_{k+1}, g_{k+1}. Per ipotesi, $h - f_k g_k \in P^{k+1} = (\pi^{k+1})$, dunque $h(x) - f_k(x) g_k(x) = \pi^{k+1} c_k(x)$ per un certo $c_k(x) \in A[x]$. Dato che $(\overline{f}_k, \overline{g}_k) = 1$, per Bezout possiamo trovare $r_k, s_k \in A[x]$ tali che $r_k f_k + s_k g_k \equiv c_k \pmod{\pi}$ e possiamo supporre senza perdita di generalità che $\deg(r_k) < n$ e $\deg(s_k) < m$. Poniamo allora:

$$f_{k+1} := f_k + s_k \pi^{k+1} \qquad\qquad g_{k+1} := g_k + r_k \pi^{k+1}.$$

Con questa definizione:

$$h - f_{k+1} g_{k+1} \equiv h - f_k g_k - \pi^{k+1}(r_k f_k + s_k g_k) \equiv 0 \pmod{\pi^{k+2}},$$

da cui la tesi. □

Consideriamo ora un campo di numeri E; sia $p \in \mathbb{Z}$ e $v_P \mid v_p$ estensione della valutazione p-adica, con $P \mid (p)$. Sappiamo che $p\mathscr{O}_E = P^e \prod_{i=1}^n P_i^{e_i}$, dunque, se completiamo E rispetto alla valutazione P-adica, otteniamo un'estensione E_P di $\mathbb{Q}_p$. In questo campo, abbiamo che $p\mathscr{O}_{E_p} = Q^e$, con e e P coincidenti con il caso globale, e lo stesso vale per il grado di inerzia f. Infatti, se e' e f' sono rispettivamente indice di ramificazione e grado di inerzia di Q in $\mathscr{O}_{E_P}$, sicuramente $e \leq e'$ e $f \leq f'$, in quanto c'è un'immersione $\frac{\mathscr{O}_E}{P} \hookrightarrow \frac{\mathscr{O}_{E_P}}{Q}$; ma per la formula delle dimensioni, considerando anche le altre valutazioni P_i-adiche, abbiamo necessariamente:

$$\sum_{i=1}^n e_i f_i + ef = \sum_{i=1}^n e_i' f_i' + e' f',$$

da cui l'uguaglianza.

Proposizione 1.3.9 (Lemma di Krasner)**.** *Sia K un campo completo rispetto a una valutazione v non archimedea e siano α, β algebrici su K. Supponiamo che α sia separabile su $K(\beta)$ e che per ogni $\sigma\colon K(\alpha) \hookrightarrow \overline{K}$ non identica con $\sigma_{|K} = \mathrm{id}$ valga $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$.*
Allora $K(\alpha) \subseteq K(\beta)$.

Dimostrazione. Basta mostrare che per ogni immersione $K(\alpha, \beta) \hookrightarrow \overline{K}$ su $K(\beta)$, α rimane fisso. Sia τ una di queste immersioni. Allora $|\tau(\alpha) - \beta| = |\tau(\alpha - \beta)| = |\alpha - \beta|$.
D'altra parte, per ogni $\sigma \neq \mathrm{id}$:

$$|\tau(\alpha) - \alpha| = |\tau(\alpha) - \beta + \beta - \alpha| \leq \max\{|\tau(\alpha) - \beta|, |\beta - \alpha|\} = |\beta - \alpha| < |\sigma(\alpha) - \alpha|,$$

ma $\tau(\alpha) = \sigma_0(\alpha)$ per $\sigma_0 = \tau_{|K(\alpha)}$, dunque $\tau = \mathrm{id}$. □

Corollario 1.3.10. *K campo completo, $\mathscr{O}_K$ il suo anello di valutazione e $P \subsetneq \mathscr{O}_K$ l'unico ideale massimale di $\mathscr{O}_K$. Sia $f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \mathscr{O}_K[x]$ un polinomio irriducibile, $\alpha_1, \ldots, \alpha_n \in \overline{K}$ le radici di f e poniamo $M = \min_{i \neq j} |\alpha_i - \alpha_j|$; scelta inoltre una radice α di f, poniamo $B = \max\{1, |\alpha|^n\}$. Se $g(x) = x^n + b_1x^{n-1} + b_n \in \mathscr{O}_K$ è un polinomio tale che $\max|a_i - b_i| < \frac{M^n}{B}$, allora G è irriducibile ed esiste una radice $\beta \in \overline{K}$ di g tale che $K(\alpha) = K(\beta)$.*

Dimostrazione. Per ipotesi $[K(\alpha) : K] = n$ e $[K(\beta) : K] \leq n$, quindi per il lemma di Krasner basta vedere che esiste una radice β di g tale che $|\alpha - \beta| < M$, in quanto in questo modo avremmo $K(\alpha) \subseteq K(\beta)$ e dunque l'uguaglianza per dimensione.
Se $g(x) = \prod_{i=1}^n x - \beta_i$, allora:

$$|g(\alpha)| = \prod_{i=1}^n |\alpha - \beta_i| \geq |\alpha - \beta|^n,$$

dove β è la radice di g più vicina a α, ma d'altra parte:

$$|g(\alpha)| = |f(\alpha) - g(\alpha)| = \left| \sum_{i=1}^n (a_i - b_i)a^{n-1} \right| \leq \max_i |a_i - b_i| \cdot \max_i \{1, |\alpha^{n-i}|\},$$

da cui, se $|a_i - b_i| < \frac{M^n}{B}$, $|\alpha - \beta|^n < M^n$, cioè la tesi. □

<u>*Osservazione*</u>. L'insieme dei polinomi monici di grado n di $\mathbb{Z}_p[x]$ è un insieme compatto, perchè omeomorfo a $\mathbb{Z}_p^n$, dunque si può prendere un ricoprimento aperto di esso ed estrarre un sottoricoprimento finito in cui ciascun aperto contiene polinomi sufficientemente vicini da generare lo stesso campo; in questo modo abbiamo dimostrato che le estensioni di $\mathbb{Q}_p$ di grado n sono in numero finito.

2 Campi locali

2.1 Struttura di $\mathscr{O}_K^*$

Sia K un campo p-adico completo, $[K : \mathbb{Q}_p] = n = e \cdot f$, e sia P l'unico ideale massimale di $\mathscr{O}_K$. Ovviamente si ha che $p\mathscr{O}_K = P^e$. In questa sezione vogliamo studiare la struttura del gruppo degli invertibili $U = \mathscr{O}_K^*$ ed estendere il risultato già ottenuto nel caso $K = \mathbb{Q}_p$.

Cominciamo con qualche notazione: se $\alpha \in \mathscr{O}_K$, α è della forma $\alpha = \sum_{i\geq 0} a_i\pi^i$, dove $(\pi) = P$; sicuramente $P = \{\alpha \mid a_0 = 0\}$.
Osserviamo subito che, una volta trovata la struttura di U, segue immediatamente anche quella di K^*, in quanto, se $\gamma = \sum_{i\geq i_0} a_i\pi^i \in K^*$, $\gamma = \pi^{i_0}\beta$, con $\beta \in U$, dunque:

$$K^* \cong \langle\pi\rangle \times U \cong \mathbb{Z} \times U.$$

Definiamo $U_m = \{\alpha \in U \mid \alpha \equiv 1 \pmod{P^m}\}$ per ogni $m \in \mathbb{N}$; se $k_K = \frac{\mathscr{O}_K}{P} = \mathbb{F}_{p^f}$ è il campo residuo, con un ragionamento analogo a quello fatto per $\mathbb{Q}_p^*$, si ottiene che le radici di $x^{p^f} - 1$ stanno in U: infatti le $p^f - 1$ radici semplici modulo P del polinomio si sollevano per Hensel a unità di U, cioè $E_1 = \langle\zeta_{p^f-1}\rangle \subseteq U$. Gli elementi di E_1 si chiamano **rappresentanti di Teichmuller** e sono tali che ogni elemento $\alpha \in U$ può essere scritto come $\alpha = a_0\beta$, con $a_0 \in E_1$ e $\beta \in U_1$, cioè $U = E_1 \times U_1$.

Proposizione 2.1.1. *1. Gli U_m sono una base di intorni aperti e compatti di* 1.

2. Per ogni $m \geq 1$, $\frac{U_m}{U_{m+1}} \cong \mathbb{Z}/p^f\mathbb{Z}$.

3. Per ogni $m \geq 1$, $\frac{U}{U_m} \cong \left(\frac{\mathscr{O}_K}{P^m}\right)^*$.

Dimostrazione. 1. Che gli U_m siano intorni aperti è ovvio. Per vedere che sono compatti, basta osservare che $U = \mathscr{O}_K \setminus P$ è chiuso nel compatto $\mathscr{O}_K$, dunque U è compatto, ma U_m è un sottogruppo aperto (e perciò chiuso) di U, per cui è compatto.

2. Definiamo:

$$\begin{array}{rccc} \varphi: & P^m & \longrightarrow & \frac{U_m}{U_{m+1}} \\ & x & \longmapsto & \overline{1+x} \end{array}$$

φ è un omomorfismo, in quanto:

$$\varphi(x+y) = \overline{1+x+y} = \overline{1+x+y} \cdot \overline{1+xy} = \overline{1+x} \cdot \overline{1+y}.$$

φ è evidentemente surgettivo; inoltre $\mathrm{Ker}(\varphi) = \{x \mid 1+x \in U_{m+1}\} = P^{m+1}$, da cui $\frac{\mathscr{O}_K}{P} \cong \frac{P^m}{P^{m+1}} \cong \frac{U_m}{U_{m+1}}$.

3. Consideriamo l'omomorfismo:

$$\begin{array}{rccc} \psi: & U & \longrightarrow & \left(\frac{\mathscr{O}_K}{P^m}\right)^* \\ & u & \longmapsto & u + P^m \end{array}$$

ψ è surgettivo, in quanto, dato un qualunque a_0, esiste un'unità di U con a_0 come termine noto; inoltre $\mathrm{Ker}(\psi) = \{u \mid u + P^m = 1 + P^m\} = 1 + P^m = U_m$, da cui la tesi.

□

A questo punto vogliamo definire su U una struttura di $\mathbb{Z}_p$-modulo; per farlo, dato $\varepsilon \in U$ e $\sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p$, consideriamo la successione $\{\varepsilon_n\} \subseteq U$ tale che $\varepsilon_n = \varepsilon^{\sum_{i=0}^{n} a_i p^i}$. Essa è di Cauchy in U (o in U_m se $\varepsilon \in U_m$), perciò possiamo definire:

$$\varepsilon^{\sum_{i\geq 0} a_i p^i} := \lim_{n\to\infty} \varepsilon_n.$$

Con tale azione, anche gli U_m risultano $\mathbb{Z}_p$-moduli.

<u>*Osservazione*</u>. Se $(k,p) = 1$ e $\varepsilon \in U_m$, allora $\varepsilon^{\frac{1}{k}} \in U_m$, in quanto $\frac{1}{k} \in \mathbb{Z}_p$.

Sia adesso $u \in U_m \backslash U_{m+1}$, cioè $u = 1 + \alpha\pi^m$, con $\alpha \in \mathscr{O}_K \backslash P = U$; un tale elemento può essere individuato calcolando la valutazione di $1-u$, in quanto $v(1-u) = m \iff u \in U_m \backslash U_{m+1}$.
Per la formula del binomio di Newton abbiamo:

$$u^p = (1+\alpha\pi^m)^p = 1 + p\alpha\pi^m + \binom{p}{2}\alpha^2\pi^{2m} + \ldots + \alpha^p\pi^{mp},$$

ma usando che $v(p) = e$, $v(\alpha) = 0$ e $v(\pi) = m$, si deduce facilmente che:

- se $mp < e + m$, cioè $m < \frac{e}{p-1}$, $v(u^p) = mp$ e dunque $u^p \in U_{mp} \backslash U_{mp+1}$;
- se $e + m < mp$, cioè $m > \frac{e}{p-1}$, $v(u^p) = e + m$ e dunque $u^p \in U_{e+m} \backslash U_{e+m+1}$;
- se $m = \frac{e}{p-1}$, $u^p \in U_{mp} = U_{m+e}$, ma potrebbe essere che $u^p \in U_{mp+1}$.

In realtà vale qualcosa di più forte:

Proposizione 2.1.2. *Se $m > \frac{e}{p-1}$, la mappa:*

$$\begin{array}{rccc} g: & U_m & \longrightarrow & U_{m+e} \\ & u & \longmapsto & u^p \end{array}$$

è un isomorfismo, cioè $U_m^p = U_{m+e}$.
Se invece $m < \frac{e}{p-1}$, la mappa:

$$\begin{array}{rccc} h: & U_m & \longrightarrow & U_{mp} \\ & u & \longmapsto & u^p \end{array}$$

è un isomorfismo, cioè $U_m^p = U_{mp}$.

Dimostrazione. Vediamo solo il primo enunciato, l'altro è analogo.
Sicuramente g è un omomorfismo, ed è iniettivo, poichè se $u \in U_l \backslash U_{l+1}$, $l \geq m$, è tale che $u^p = 1$, allora $u^p \in U_{l+e} \backslash U_{l+e+1}$, mentre $1 \in U_{l+e+1}$.
Vediamo adesso che g è surgettivo: sia $1 + a\pi^{m+e} \in U_{m+e}$ e cerchiamo $1 + y\pi^m \in U_m$ tale che $(1+y\pi^m)^p = 1 + a\pi^{m+e}$. Equivalentemente, posto $f(y) = (1+y\pi^m)^p - (1+a\pi^{m+e})$, cerco una radice $y \in \mathscr{O}_K$ di f.
Detto $p = v\pi^e$, con $v \in U$, sviluppando la potenza abbiamo:

$$f(y) = 1 + py\pi^m + p\pi^{2m}A + y^p\pi^{mp} - 1 - a\pi^{m+e} = \pi^{m+e}(vy + v\pi^m A + y^p\pi^{mp-m-e} - a),$$

dunque, detto $g(y) = \frac{1}{\pi^{m+e}} f(y)$, $g(y) \equiv vy - a \pmod{P}$, quindi g ha una radice semplice modulo P, che per Hensel si solleva a una radice di g (e di f). □

Lemma 2.1.3. *Dato $m \in \mathbb{N}$, allora:*

$$U_m \cong \varprojlim \frac{U_m}{U_{m+ke}}.$$

Dimostrazione. Consideriamo l'omomorfismo:

$$\begin{array}{rccc} \varphi: & U_m & \longrightarrow & \varprojlim \frac{U_m}{U_{m+ke}} \\ & u & \longmapsto & \left([u]_{U_{m+ke}}\right)_k \end{array}$$

Sicuramente φ è surgettivo, in quanto basta vedere la successione coerente come il suo elemento limite; per vedere che è iniettivo, osserviamo che $\mathrm{Ker}(\varphi) = \bigcap_k U_{m+ke} = \{1\}$, in quanto se $u \neq 1$ e $v(1-u) = j$, allora $u \in U_j \backslash U_{j-1}$. □

Lemma 2.1.4. *Se $m > \frac{e}{p-1}$, allora:*

$$\frac{U_m}{U_{m+ke}} \cong \left(\mathbb{Z}/p^k\mathbb{Z}\right)^n$$

e il sistema proiettivo degli $\frac{U_m}{U_{m+ke}}$ coincide con quello degli $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^n$.

Dimostrazione. $X_k = \frac{U_m}{U_{m+ke}}$ è uno $\mathbb{Z}/p^k\mathbb{Z}$-modulo, perchè è uno $\mathbb{Z}_p$-modulo con annullatore $p^k\mathbb{Z}_p$; detto $A = \mathbb{Z}/p^k\mathbb{Z}$ e $\mathfrak{m} = \langle \overline{p} \rangle$ l'unico ideale massimale di A, abbiamo:

$$\frac{U_m}{U_{m+e}} \cong \frac{X_k}{\frac{U_{m+e}}{U_{m+ke}}} = \frac{X_k}{\mathfrak{m}X_k},$$

in quanto moltiplicare per $\mathfrak{m}$ non è altro che elevare alla potenza p. Da questo $\frac{U_m}{U_{m+e}}$ è uno $\mathbb{Z}/p\mathbb{Z}$-modulo, e se $\{\overline{x_1}, \dots, \overline{x_n}\}$ è una base di $\frac{U_m}{U_{m+e}}$ come $\mathbb{Z}/p\mathbb{Z}$-modulo, $\mathrm{ord}(\overline{x_i}) = p$; per il lemma di Nakayama, $X_k = \langle x_1, \dots, x_n \rangle_A$, dove x_i è un sollevamento di $\overline{x_i}$, e $\mathrm{ord}(x_i) = p^k$, in quanto $x_1, \dots, x_n \notin U_{m+e}$.
Ma allora ogni $x \in X_k$ si scrive nella forma $x = \prod_i x_i^{\alpha_i}$, e tale scrittura è unica $\iff$ $|X_k| = p^{kn}$; ma questo è vero, in quanto:

$$\left|\frac{U_m}{U_{m+ke}}\right| = \prod_{i=0}^{ke-1} \left|\frac{U_{m+i}}{U_{m+i+1}}\right| = p^{f\cdot ke} = p^{kn}.$$

Ne deduciamo che gli x_i sono indipendenti e dunque $X_k \cong \langle x_1 \rangle \times \langle x_n \rangle \cong (\mathbb{Z}/p^k\mathbb{Z})^n$. □

Teorema 2.1.5 (di struttura di $\mathscr{O}_K^*$)**.** *Esiste $s > 0$ tale che:*

$$U_1 \cong \langle \zeta_{p^s} \rangle \times \mathbb{Z}_p^n.$$

Dimostrazione. Se m è abbastanza grande, cioè $m > \frac{e}{p-1}$, allora dai due lemmi si ricava che:

$$U_m \cong \varprojlim (\mathbb{Z}/p^k\mathbb{Z})^n \cong \mathbb{Z}_p^n.$$

Ora $\frac{U_1}{U_m}$ è finito, in quanto contiene le somme finite $\sum_{i=0}^{m-1} a_i\pi^i$, dunque U_1 è finitamente generato come $\mathbb{Z}_p$-modulo e $\mathrm{rk}(U_1) = n$.
Da questo segue che $U_1 = T \times \mathbb{Z}_p^n$, con T prodotto di $\mathbb{Z}_p$-moduli ciclici finiti; visto che un tale $\mathbb{Z}_p$-modulo ciclico finito è della forma $\langle x \rangle \cong \frac{\mathbb{Z}_p}{\mathrm{Ann}(x)}$, con $0 \neq \mathrm{Ann}(x) = p^r\mathbb{Z}_p$, allora $\langle x \rangle \cong \mathbb{Z}/p^r\mathbb{Z}$, quindi T è un p-gruppo finito. Visto che $T < K^*$ è un sottogruppo moltiplicativo finito di un campo, è ciclico, quindi $T \cong \mathbb{F}_{p^s}$, cioè gli elementi di T sono radici p^s-esime di 1. □

2.2 Estensioni non ramificate

Sia L/K un'estensione finita di campi p-adici. Sappiamo che $[L:K] = e_{L/K} f_{L/K}$, dove $e_{L/K}$ è l'indice di ramificazione dell'estensione e $f_{L/K}$ è il grado d'inerzia.

Definizione 2.2.1. L/K si dice **non ramificata** se $e_{L/K} = 1$, mentre si dice **totalmente ramificata** se $f_{L/K} = 1$.
In generale, L/K (anche infinita) è non ramificata se L è unione di sottoestensioni finite non ramificate su K.

Osservazione. Se L/K è non ramificata e $K \subseteq E \subseteq L$, allora E/K è non ramificata. Questo è ovvio nel caso di estensioni finite, in quanto vale la moltiplicatività del grado nelle torri dei campi residui. Nel caso di estensioni infinite, sia E_0 un campo intermedio tra E e K tale che E_0/K è finita. Allora $E_0 = K(\alpha)$ e, se $L = \bigcup_i L_i$ è tale che L_i/K è finita e non ramificata su K per ogni i, esiste i tale che $\alpha \in L_i$, da cui la tesi in quanto $K \subseteq E_0 \subseteq L_i$.

Osservazione. Sia $L = K(\alpha)$, sia $\alpha \in \mathscr{O}_L$ e sia $\mu_\alpha \in \mathscr{O}_K[x]$. Allora $\mu_\alpha(x) = g(x)^e \pmod{P_K}$ per Hensel, poichè se $\mu_\alpha(x) = p_1(x)p_2(x) \pmod{P}$ con $(p_1, p_2) = 1$, potrei sollevare questi polinomi e scomporre μ_α in $\mathscr{O}_K[x]$.
Supponiamo che $\mathscr{O}_L = \mathscr{O}_K[\alpha]$. Allora, se L/K è non ramificata, μ_α è irriducibile modulo P_K, in quanto l'estensione di campi residui $k_L = \frac{\mathscr{O}_K[\alpha]}{P_L} = \frac{\mathscr{O}_K}{P_K}[\overline{\alpha}]/k_K$ ha esattamente grado $n = f$.

Proposizione 2.2.1. *Sia L/K un'estensione finita di campi p-adici. Sono equivalenti:*

1. *L/K è non ramificata.*
2. *Esiste $\alpha \in \mathscr{O}_L$ tale che $L = K(\alpha)$ e $\overline{\alpha} \in k_L$ è radice semplice di $\overline{\mu_\alpha} \in k_L[x]$.*

Dimostrazione. $1 \Rightarrow 2)$ Per ipotesi, $[L:K] = [k_L : k_K]$; sia $\overline{\alpha}$ un generatore dell'estensione dei campi residui. Detto φ il polinomio minimo di $\overline{\alpha}$ e preso f un sollevamento monico di φ a $\mathscr{O}_K[x]$, si ha $\overline{f} = \varphi$ ed esiste una radice (semplice) di f che si proietta su $\overline{\alpha}$, da cui la tesi.

$2 \Rightarrow 1)$ Sappiamo che $\overline{\mu}_\alpha$ è potenza di un polinomio irriducibile; d'altronde $\overline{\alpha}$ è una radice semplice e dunque $e_{L/K} = 1$.

□

Proprietà (Estensioni non ramificate). Supponiamo dapprima che le estensioni che consideriamo siano finite.

1. La proprietà delle torri è verificata, cioè, se $K \subseteq L \subseteq E$, E/K è non ramificata $\iff$ E/L e L/K sono non ramificate. Segue infatti dalla proprietà di moltiplicatività del grado nelle torri, in quanto:
$$[E:K] = [E:L][L:K] \qquad\qquad [k_E : k_K] = [k_E : k_L][k_L : k_K]$$
e $[E:K] = [k_E : k_K] \iff [E:L] = [k_E : k_L]$ e $[L:K] = [k_L : k_K]$.

2. Anche la proprietà del traslato è verificata; consideriamo un diagramma:
$$\begin{tikzcd} & ML \arrow[dl, dash] \arrow[dr, dash] & \\ M \arrow[dr, dash] & & L \arrow[dl, dash, "\text{non ram.}"] \\ & K & \end{tikzcd}$$

Se $L = K(\alpha)$, allora $ML = M(\alpha)$ e $\overline{\alpha}$ è radice semplice di $\overline{\mu}_\alpha$. Detto μ_M il polinomio minimo di α su M, $\mu_M \mid \mu_\alpha$ e dunque $\overline{\alpha}$ è radice semplice di $\overline{\mu}_M$, da cui la tesi.

3. Dalle proprietà delle torri e del traslato, segue la proprietà del composto.

Queste proprietà si generalizzano al caso di estensioni infinite.

1. Supponiamo di avere una torre $K \subseteq L \subseteq E$. Se E è non ramificata su K, allora $E = \bigcup_i E_i = \bigcup_i E_i L$ e queste ultime sono non ramificate su L per il caso finito.
   Viceversa, supponiamo che E/L e L/K siano non ramificate. Sia E_0 una sottoestensione finita di E/K. Possiamo considerare il traslato E_0L su L; dato che E_0L/L è finita, è non ramificata su L, quindi possiamo scegliere α tale che $E_0L = L(\alpha)$ con $\mu_\alpha \in \mathscr{O}_L[x]$ e $\overline{\alpha}$ radice semplice di $\overline{\mu}_\alpha$. Consideriamo allora L_0 la sottoestensione di L generata dai coefficienti di μ_α. Valgono allora i contenimenti $L_0(\alpha) \supseteq L_0 \supseteq K$, con entrambe le estensioni non ramificate e finite, da cui $L_0(\alpha)$ è non ramificata su K e quindi anche $K(\alpha) = E_0 \subseteq L_0(\alpha)$ lo è.

2. Scrivendo i campi interessati come unione delle loro sottoestensioni finite e non ramificate, si ha facilmente che la proprietà di essere non ramificato passa al traslato.

Teorema 2.2.2. *Sia K un campo p-adico. Esiste una corrispondenza biunivoca tra le estensioni non ramificate di K contenute in una fissata chiusura algebrica e le estensioni algebriche di k_K:*

$$\begin{array}{rccc} \varphi: & \{L \subseteq \overline{\mathbb{Q}_p} \mid L/K \text{ non ramificata}\} & \longleftrightarrow & \{k \subseteq \overline{\mathbb{F}_p} \mid k \supseteq k_K\} \\ & L & \longrightarrow & k_L \end{array}$$

Inoltre, se L/K è non ramificata, è di Galois e il gruppo di Galois è isomorfo al gruppo di Galois dei campi residui.

Dimostrazione. Vediamo la dimostrazione nel caso in cui le estensioni L/K e k_L/k_K siano finite. φ è evidentemente surgettiva, poichè, se $k \supseteq k_K$ è un'estensione finita, $k = k_K(\overline{\alpha})$ e un sollevamento monico del polinomio minimo g di α a $\mathscr{O}_K[x]$ ha una radice α con $\pi(\alpha) = \overline{\alpha}$ che genera un'estensione di K non ramificata.
Mostriamo ora l'iniettività. Siano L, L' due campi non ramificati su K e supponiamo che $k_L = k_{L'}$. Allora $L = K(\alpha)$ e $k_L = k_K(\overline{\alpha})$. $\overline{\alpha} \in k_{L'}$, quindi, per Hensel, L' deve contenere un sollevamento di $\overline{\alpha}$; ma in LL', ho sia α che il sollevamento precedente di $\overline{\alpha}$, che per unicità del sollevamento devono coincidere, cioè $\alpha \in L'$ e $L \subseteq L'$. L'uguaglianza $L = L'$ segue dall'uguaglianza dei campi residui e dal fatto che $[L : K] = [k_L : k_K]$ e $[L' : K] = [k_{L'} : k_K]$.
La normalità segue da Hensel, in quanto L è campo di spezzamento del polinomio minimo G di un sollevamento in $\mathscr{O}_K[x]$ del polinomio minimo g di un generatore dell'estensione dei campi residui (che è di Galois e dunque k_L è campo di spezzamento di $\overline{g}$ su k_K).
Per l'isomorfismo tra i gruppi di Galois, notiamo che, essendoci un solo primo, il gruppo di Galois coincide con il gruppo di decomposizione $D(P_L : P_K)$, e dato che l'estensione è non ramificata, si ha $D(P_L|P_K) \cong \mathrm{Gal}(k_L : k_K)$.
Diamo solo un'idea della dimostrazione nel caso infinito. Sia $k \supseteq k_K$. Allora $k = \bigcup_i k_i$ con k_i/k_K finita per ogni i e, dette $L_i = \varphi^{-1}(k_i)$, basta considerare $L = \cup L_i$ per avere la surgettività, in quanto si verifica che il campo residuo k_L è proprio k.
Per quanto riguarda l'iniettività, se L, L', $L = \bigcup_i L_i$, $L' = \bigcup_i L'_i$ sono tali che $k_L = k_{L'}$, il contenimento $k_{L'} \supseteq k_{L_i}$ per ogni i implica che $L' \supseteq L_i$ per ogni i, cioè $L' \supseteq L$. Se invece $\beta \in L'$, $k_K(\overline{\beta}) \subseteq k_{L'} = k_L$ e $\overline{\beta}$ si solleva a un elemento di L, che per unicità del sollevamento è proprio β. □

Corollario 2.2.3. *Sia K un campo p-adico. Le estensioni non ramificate di K sono in corrispondenza biunivoca con i sottogruppi chiusi di $\hat{\mathbb{Z}}$. In particolare, per ogni $n \in \mathbb{N}$, esiste un'unica estensione di K non ramificata di grado n, che è ciclica.*

Esempio. L'unica estensione non ramificata di $\mathbb{Q}_p$ di grado 5 è generata da un elemento a la cui proiezione $\overline{a}$ sul campo residuo genera l'estensione $\mathbb{F}_{p^5}/\mathbb{F}_p$. Visto che $\mathbb{F}_{p^5}^* = \langle \overline{\zeta_{p^5-1}} \rangle$, abbiamo che $\mathbb{Q}_p(\zeta_{p^5-1})$ è l'estensione cercata.

Corollario 2.2.4. *Se L/K è un'estensione di campi p-adici, L/K è non ramificata se e solo se esiste $m \in \mathbb{N}$, $p \nmid m$, tale che $L = K(\zeta_m)$.*

Dimostrazione. $\Rightarrow$) Se L/K è non ramificata, $[L : K] = [k_L : k_K] = f$ e $|k_L^*| = p^f - 1$, dunque $k_L = k_K(\overline{\zeta_{p^f-1}})$. Per Hensel, le radici del polinomio minimo di ζ_{p^f-1} sono in L, dunque $K \subseteq K(\zeta_{p^f-1}) \subseteq L$. Visto che L e $K(\zeta_{p^f-1})$ sono non ramificate con lo stesso campo residuo, per il teorema $L = K(\zeta_{p^f-1})$.

$\Leftarrow$) Se $L = K(\zeta_m)$, con $p \nmid m$, il polinomio minimo $\mu_{\zeta_m} \mid x^m - 1$ ha radici semplici modulo p, quindi L/K è non ramificata.

□

Corollario 2.2.5. *Sia $L = K(\zeta_m)$ con $p \nmid m$. Allora ogni sottoestensione di L/K è della forma $E = K(\zeta_r)$, con $p \nmid r$.*

Proposizione 2.2.6. *Sia K un campo p-adico e supponiamo che L/K sia non ramificata. Allora ogni unità di K è norma di una unità di L.*

Dimostrazione. Vogliamo mostrare che $\mathrm{N}_{L/K} : U(L) \to U(K)$ è surgettiva. Per i campi finiti, sappiamo che norma e traccia sono surgettive; infatti per la traccia è evidente, mentre se $G = \langle \phi \rangle$ è il gruppo di Galois di $\mathbb{F}_{q^a}/\mathbb{F}_q$, $\mathrm{N}_{\mathbb{F}_{q^a}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{a-1}} = \alpha^{\frac{q^a-1}{q-1}}$, dunque, se $\mathbb{F}_{q^a}^* = \langle \alpha \rangle$, evidentemente $\mathbb{F}_q^* = \langle \alpha^{\frac{q^a-1}{q-1}} \rangle$, cioè la norma è surgettiva.
Sia adesso $u \in U_K$. Per quanto detto sui campi finiti, sappiamo che esiste $\alpha_0 \in L$ tale che $N_{L/K}(\alpha_0) \equiv u \pmod{P_K}$. $u\,\mathrm{N}_{L/K}(\alpha_0^{-1}) \equiv 1 \pmod{P_K}$, quindi $u\,\mathrm{N}(\alpha_0^{-1}) \equiv 1 + c_1\pi \pmod{\pi^2}$, dove $P_K = (\pi)$. Sia $\alpha_1 \in L$ tale che $\alpha_1 \equiv 1 + x_1\pi$ con $x_1 \in \mathscr{O}_L$; allora $\mathrm{N}_{L/K}(\alpha_1) \equiv 1 + \mathrm{Tr}_{L/K}(x_1)\pi \pmod{p^2}$. Ma sicuramente esiste x_1 tale che $\mathrm{Tr}_{L/K}(x_1) \equiv c_1 \pmod{\pi}$, perciò abbiamo trovato α_1 tale che $\mathrm{N}_{L/K}(\alpha_1) \equiv 1 + c_1\pi \equiv u\,\mathrm{N}_{L/K}(\alpha_0^{-1}) \pmod{\pi^2}$, cioè $u\,\mathrm{N}_{L/K}(\alpha_0^{-1}\alpha_1^{-1}) \equiv 1 \pmod{\pi^2}$. Induttivamente si può costruire un'unità α_n tale che $u\,\mathrm{N}_{L/K}(\alpha_0^{-1} \ldots \alpha_n)^{-1} \equiv 1 \pmod{\pi^{n+1}}$; detto $\alpha = \prod_i \alpha_i$, che converge, allora $\alpha \in U_L$ e $\mathrm{N}_{L/K}(\alpha) = u$. □

Teorema 2.2.7. *L/K estensione algebrica di campi p-adici. Allora esiste un'estensione intermedia U tale che U/K è non ramificata e L/U è totalmente ramificata.*

Dimostrazione. Supponiamo innanzitutto che l'estensione L/K sia finita. $U = \prod_{\substack{K \subseteq M \subseteq L \\ M/K \text{ non ram.}}} M$ è non ramificata su K per la proprietà del composto finito; vediamo inoltre che L/U è totalmente ramificata.
Se per assurdo $k_U \subsetneqq k_L$, per il teorema di corrispondenza a k_L corrisponde un'estensione propria F di U non ramificata, che per Hensel è contenuta in L; l'assurdo segue dunque dalla definizione di U.
Per il caso infinito, definiamo $K_u = \prod_{M \in \mathcal{F}_{L/K}} M$, dove $\mathcal{F}_{L/K} = \{M \mid K \subseteq M \subseteq L \text{ e } M/K \text{ non ram.}\}$. Sicuramente $L \supseteq K_u \supseteq K$; per vedere che K_u è il campo cercato basta mostrare che K_u è la massima sottoestensione di L/K non ramificata su K.
Osserviamo che $K_u = \bigcup_{M \in \mathcal{F}_{L/K}} M$, dunque K_u/K è non ramificata in quanto unione di estensioni non ramificate; la massimalità di K_u è invece del tutto ovvia. □

Osservazione. La massima sottoestensione di $\mathbb{Q}_p \subseteq \overline{\mathbb{Q}_p}$ non ramificata su $\mathbb{Q}_p$ è $\widetilde{\mathbb{Q}_p} = \mathbb{Q}_p(\{\zeta_n \mid (n,p) = 1\})$.

Osservazione. $\widetilde{\mathbb{Q}_p}$ non è un campo completo. In particolare neanche $\overline{\mathbb{Q}_p}$ lo è.

Dimostrazione. Sia $\alpha_k = \sum_{n=1}^{k} \zeta_{n(p)} p^n$, dove $n(p) = n$ se $(n,p) = 1$ e $n(p) = 1$ altrimenti; α_k è di Cauchy in $\widetilde{\mathbb{Q}_p}$, quindi dico che $\alpha = \lim_{k\to\infty} \alpha_k \notin \widetilde{\mathbb{Q}_p}$.
Se per assurdo $\alpha \in \overline{\mathbb{Q}_p}$, considero $K = \mathbb{Q}_p(\alpha)$, che è un'estensione finita di $\mathbb{Q}_p$, di grado d. Diciamo che $\zeta_{n(p)} \in K$ per $n < n_0$, ma $\zeta_{n_0(p)} \in K$, in quanto non possono starci tutte; sicuramente $(n_0, p) = 1$.
$\beta = \frac{1}{p^{n_0}}(\alpha - \alpha_{n_0 - 1}) = \sum_{n \geq n_0} \zeta_{n(p)} p^{n-n_0} \in K$, e $\beta \equiv \zeta_{n_0(p)} = \zeta_{n_0} \pmod p$. Ma il polinomio $x^{n_0} - 1$ ha radici semplici modulo p in quanto $(n_0, p) = 1$, dunque per Hensel una di queste radici si solleva a un elemento di K, che per unicità del sollevamento è ζ_{n_0}, da cui l'assurdo. □

2.3 Estensioni totalmente ramificate

Osservazione. Sia K un campo p-adico. Allora sono equivalenti:

1. L/K è totalmente ramificata;
2. $k_L = k_K$;
3. Ogni sottoestensione finita F di L/K è totalmente ramificata su K;
4. La massima sottoestensione non ramificata di L/K è K.

Teorema 2.3.1. *Sia L/K finita, $[L : K] = n$, e totalmente ramificata. Allora ogni $\pi \in \mathscr{O}_L$ di valutazione 1 è tale che $\mathscr{O}_L = \mathscr{O}_K[\pi]$ e μ_π è di Eisenstein.*
Viceversa, ogni estensione generata da una radice di un polinomio di Eisenstein è totalmente ramificata.

Dimostrazione. Sia π di valutazione 1. Allora sicuramente $\mathscr{O}_L = \mathscr{O}_K[\pi]$, in quanto l'estensione dei campi residui è banale; inoltre, se $\mu_\pi(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_0 \in \prod_\sigma \sigma(\pi)$, dunque $|a_0| = |\pi|^n = |\underbrace{P_K}_{=(\pi_K)}|$, in quanto $P_K\mathscr{O}_L = P_L^n$. Ma allora $a_0 \in P_K \backslash P_K^2$. Inoltre gli a_i per $i > 0$ hanno tutti valutazione ≥ 1, in quanto sono somme e prodotti di coniugati di π, perciò $a_i \in P_K$ per ogni $i > 0$.
Per il viceversa, sia $\mu(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathscr{O}_K[x]$ di Eisenstein e sia $\alpha \in \overline{K}$ una radice di μ. μ è irriducibile, quindi $[K(\alpha) : K] = n$.
Se $L = K(\alpha)$, come prima $v(\alpha_0) = v(\pi_K) = 1$; inoltre, visto che $v(a_{n-i}\alpha^{n-i}) > 1$ per ogni $0 < i < n$, necessariamente $v(\alpha^n) = v(a_0) = 1$, in quanto altrimenti si avrebbe $v(\alpha^n + \ldots + a_0) = 1$. Ma allora $v_K(\alpha) = \frac{1}{n}$, cioè $n \leq e_{L/K}$, da cui $n = e_{L/K}$. □

Corollario 2.3.2. *Sia K un campo p-adico. Per ogni $n \in \mathbb{N}$ esiste un'estensione L_n di K di grado n totalmente ramificata.*

Dimostrazione. Basta considerare i polinomi di Eisenstein del tipo $x^n - \pi_K$, dove $(\pi_K) = P_K$. □

Proposizione 2.3.3. *Ogni campo p-adico K ha solo un numero finito di estensioni di grado n fissato.*

Dimostrazione. Visto che di estensioni non ramificate ce n'è una sola, spezzando in parte non ramificata e parte totalmente ramificata basta dimostrare la proposizione solo nel caso delle estensioni totalmente ramificate. Tali estensioni si ottengono tutte con polinomi di Eisenstein, che identifico come n-uple in $X = P \times \ldots \times (P\backslash P^2)$, $P = P_K$; visto che ogni polinomio ha un numero finito di radici, basta vedere che esistono finiti polinomi di Eisenstein con radici che generano campi distinti.
X è compatto perchè prodotto di compatti, in quanto P e P^2 sono aperti e dunque chiusi; per

Krasner ogni polinomio f in X ha un intorno aperto fatto da polinomi le cui radici generano gli stessi campi delle radici di f, quindi possiamo prendere un tale ricoprimento aperto e trovarne un sottoricoprimento finito per compattezza. $\square$

2.4 Estensioni tame

Definizione 2.4.1. L/K finita si dice **tame** se $p \nmid e_{L/K}$, **wild** altrimenti. Se L/K è infinita, si dice **tame** se lo sono tutte le sue sottoestensioni finite.

Osservazione. K campo p-adico, $(e,p)=1$. Il polinomio $x^e - \pi_K$è di Eisenstein, dunque genera un'estensione totalmente ramificata, che per l'ipotesi è tame.

Proposizione 2.4.1. *Sia $\alpha \in \mathscr{O}_K$, $(e,p)=1$. Ogni radice del polinomio $x^e - a$ genera un'estensione tame di K.*
Se inoltre $(v_p(a), e) = 1$, allora l'estensione generata, di grado e, è totalmente ramificata.

Dimostrazione. Sappiamo che $K^* = \langle \pi \rangle \times U = \langle \pi \rangle \times k_K^* \times U_1$, dove $k_K^* = \langle \zeta_{p^f-1} \rangle$, $f = f_{K/\mathbb{Q}_p}$. $a \in K^*$, dunque $a = \pi^r \zeta_m v$, con $(m,p)=1$ e $v \in U_1$.
Se α è radice di $x^e - a$, $\alpha^e = a$, dunque $\alpha \in K\left(\zeta_e, \pi^{\frac{1}{e}}, \zeta_m^{\frac{1}{e}}, v^{\frac{1}{e}}\right)$. Possiamo però attuare le seguenti semplificazioni: $\zeta_m^{\frac{1}{e}} = \zeta_{me}$, $v \in U_1$ e $\frac{1}{e} \in \mathbb{Z}_p$, quindi $v^{\frac{1}{e}} \in U_1$, perciò $\alpha \in K\left(\zeta_{me}, \pi^{\frac{1}{e}}\right)$.
$U = K(\zeta_{me})$ è non ramificata su K, perchè $(m,p) = (e,p) = 1$, dunque $K \subseteq U \subseteq U\left(\pi^{\frac{1}{e}}\right) \ni \alpha$, con $U\left(\pi^{\frac{1}{e}}\right)/U$ tame, in quanto generata da una radice del polinomio $x^e - \pi$, $(e,p)=1$. Ma allora α genera un'estensione tame, in quanto sottoestensione di un'estensione tame.
Sia adesso $v_K(a) = r$; $(r,e) = 1$, quindi esistono h, l tali che $hr + le = 1$. $a = \pi^r u$, con $u \in U$; definisco $\beta = \alpha^h \pi_K^e \in K(\alpha)$. Abbiamo:

$$\beta^e = \alpha^{he}\pi_K^{el} = a^h \pi_K^{el} = \pi_K^{rh} u^h \pi_K^{rl} = \pi_K u^h,$$

quindi β è radice di $x^e - \pi_K u^h$. Essendo l'elemento $\pi_K u^h$ un generatore di P_K, segue che $K(\beta)/K$ è totalmente ramificata di grado e.
Per concludere basta osservare che $K(\beta) \subseteq K(\alpha)$ ed hanno lo stesso grado su K. $\square$

Esempio. Se $(v_p(a), e) = d > 1$ e α è una radice di $x^e - a$, $K(\alpha)/K$ è tame ma non necessariamente totalmente ramificata.
Consideriamo infatti $\mathbb{Q}_7(\alpha)$, dove α è radice di $x^6 - 7^2\zeta_6$. $\alpha = \zeta_6^i \cdot \sqrt[6]{7^2\zeta_6} = \sqrt[3]{7}\zeta_{36}^j$ per certi i, j, dunque ha valutazione $\frac{1}{3}$, da cui $e = 3$ o $e = 6$.
Ma se $\alpha = \sqrt[3]{7}\zeta_{36}$, $\alpha^3 = 7\zeta_{12}$, quindi $\zeta_{12} \in \mathbb{Q}_7(\alpha)$; visto che $[\mathbb{F}_7(\overline{\zeta_{12}}) : \mathbb{F}_7] = 2$, necessariamente si ha $e = 3$.

Lemma 2.4.2. *Sia K un campo p-adico, $e \in \mathbb{N}$ coprimo con p e E/K totalmente ramificata e finita, $P_K = (\pi_0)$. Sia $\beta \in E$ tale che $|\beta^e| = |\pi_0|$. Allora esiste $\pi \in \mathscr{O}_K$, $|\pi| = |\pi_0|$ tale che una radice di $x^e - \pi$ è contenuta in $K(\beta)$ (e dunque le due estensioni coincidono per grado).*

Dimostrazione. Sia $\beta^e = \pi_0 u$, $u \in \mathscr{O}_E^*$. $u = \sum_{i \geq 0} u_i \pi_E^i$, con $u_i \in \mathscr{O}_K^*$, in quanto $k_K = k_E$, perciò $\beta^e \equiv \pi_0 u_0 \pmod{\pi_E}$. Poniamo $\pi = \pi_0 u_0$; sicuramente a meno di normalizzare $v(\pi) = 1$ e $|\beta^e - \pi| < |\pi|$.
Posto $f(x) = x^e - \pi$, $f(\beta) = \beta^e - \pi = \prod_{i=1}^e (\beta - \alpha_i)$, dove $\alpha_1, \ldots, \alpha_e$ sono le radici di f; visto che $|f(\beta)| < |\pi|$, esiste un indice i tale che $|\beta - \alpha_i| < |\pi|^{\frac{1}{e}} = |\alpha_j|$ per ogni j. Valendo l'uguaglianza:

$$f'(\alpha_i) = |e\alpha_i^{e-1}| = |\alpha_i|^{e-1} = \prod_{j \neq i} |\alpha_i - \alpha_j|,$$

abbiamo che $|\alpha_i - \alpha_j| = |\alpha_j|$ per ogni $j \neq i$, in quanto evidentemente vale la disuguaglianza $\leq$. Mettendo insieme tutti i risultati otteniamo che $|\beta - \alpha_i| < |\alpha - \alpha_j|$ per ogni $j \neq i$, da cui per Krasner $K(\alpha_i) \subseteq K(\beta)$. $\square$

Proposizione 2.4.3. *L/K totalmente ramificata tame di grado e, $(e,p) = 1$. Se $\mu_{\pi_L}(x) = x^e - a_{n-1}x^{n-1} + \ldots + a_0 \in \mathscr{O}_K[x]$ (di Eisenstein in quanto $v(\pi_L) = 1$), allora L/K è generata da una radice di $x^e - a_0$.*

Dimostrazione. Dalle ipotesi $\mathscr{O}_L = \mathscr{O}_K[\pi_L]$, $L = K(\pi_L)$. Se $f(x) = x^e - a_0$, con $a_0 = \pi_K$, allora, presa α_1 radice di $f(x)$, $v(\alpha_1) = 1$ in L (in quanto $v_L(a_0) = e$). Dico che $K(\alpha_1) = K(\pi_L)$. Applicando il lemma a μ_{π_L} e a $x^e - a_0$, osserviamo che può essere scelto un π generatore di P_K tale che $K(\pi_L) = K(\beta)$ e $K(\alpha_1) = K(\gamma)$, dove β e γ sono due radici del polinomio $x^e - \pi$. A meno di cambiare α_1, abbiamo perciò $K(\pi_L) = K(\alpha_1)$. $\square$

Vediamo ora quali delle solite proprietà soddisfano le estensioni tame. Consideriamo solo estensioni finite, ma tali proprietà valgono anche per estensioni infinite.

Proprietà (Estensioni tame).

1. Evidentemente l'essere tame si conserva nelle torri, in quanto se $K \subseteq E \subseteq L$, $(e_{L/K}, p) = 1 \iff (e_{L/E}, p) = (e_{E/K}, p) = 1$.

2. Se consideriamo un diagramma:

$$\begin{tikzcd} & ML \arrow[dl, dash] \arrow[dr, dash] & \\ M \arrow[dr, dash] & & L \arrow[dl, dash, "\text{tame}"] \\ & K & \end{tikzcd}$$

   prendiamo la massima sottoestensione U di L/K non ramificata su K; L/U è totalmente ramificata, quindi è generata da un certo $x^e - \pi$. Se α è una radice di $x^e - \pi$ tale che $L = U(\alpha)$, allora $ML = MU(\alpha)$, quindi ML/MU è tame, da cui la tesi in quanto MU/M è tame perchè non ramificata.

3. La conservazione nel composto deriva dalle due precedenti proprietà.

Proposizione 2.4.4. *L/K estensione finita, $e_{L/K} = p^s e_0$, con $(e_0, p) = 1$, $s \geq 0$. Esiste un'estensione E/K tame massimale fra quelle contenute in L tale che L/E è totalmente ramificata, $e_{L/E} = p^s$.*

Dimostrazione. Sia U la sottoestensione di L/K tale che L/U è totalmente ramificata e U/K è non ramificata e poniamo $\beta = \pi_L^{p^s}$. Visto che $|\beta^{e_0}| = |\pi_L^{p^s e_0}| = |\pi_K| = |\pi_U|$, per il lemma precedente esiste β' tale che $U(\beta') = U(\beta)$ e $\beta'^{e_0} = \pi_K u$, $u \in \mathscr{O}_U^*$.
Consideriamo $E = K(\beta')$. E/K è tame perchè $\mu_{\beta'}(x) = x^{e_0} - \pi_K u_0$ e per ragioni di grado $e_{L/E} = p^s$. $\square$

Lemma 2.4.5 (Abhyankar)**.** *Sia L/K un'estensione tame e M/K un'estensione finita tali che $e_{L/K} \mid e_{M/K}$. Allora ML/M è non ramificata.*

Dimostrazione. Se U è come al solito l'estensione intermedia di L/K che spezza la parte totalmente ramificata da quella non ramificata, abbiamo un diagramma:

$$\begin{tikzcd}
 & & ML \arrow[dl, dash, "\text{tot. ram.}"'] \arrow[dr, dash] & \\
 & MU \arrow[dl, dash, "\text{non ram.}"'] \arrow[dr, dash] & & L \arrow[dl, dash, "\text{tot. ram.}"] \\
M \arrow[dr, dash] & & U \arrow[dl, dash, "\text{non ram.}"] & \\
 & K & &
\end{tikzcd}$$

Visto che $e_{L/K} = e_{L/U}$ e $e_{M/K} = e_{MU/U}$, posso ridurmi a considerare solamente il caso in cui L/K è totalmente ramificata.
$L = K(\pi_L)$, dove π_L è radice del polinomio $x^e - \pi_K$, $e = e_{L/K}$; scelgo $\pi_M \in M$ in modo che $(\pi_K)\mathscr{O}_M = (\pi_M)^{e_{M/K}}$, cioè $\pi_K = \pi_M^{e_{M/K}} u$, dove $u \in \mathscr{O}_M^* = E(M) \times U_1(M)$. In particolare scrivo $u = \zeta_m v$, dove $(m, p) = 1$ e $v \in U_1(M)$.
Sicuramente $ML = M(\pi_L)$ e $\pi_L^e = \pi_K = \pi_M^{e_{M/K}}$; se $e' = \frac{e_{M/K}}{e}$, allora:

$$\left(\pi_L \pi_M^{-e'}\right)^e = \zeta_m v.$$

Visto che $\frac{1}{e} \in \mathbb{Z}_p$, allora $v^{\frac{1}{e}}$, quindi $M(\pi_L) = M\left((\zeta_m v)^{\frac{1}{e}}\right) = M(\zeta_{me})$, da cui la tesi in quanto $(me, p) = 1$. $\square$

<u>*Osservazione*</u> (Numero di estensioni tame totalmente ramificate di K). Fissiamo un numero $e \in \mathbb{N}$ coprimo con p e contiamo le estensioni di K tame totalmente ramificate di grado e. Consideriamo il polinomio $x^e - \pi u$, $(\pi) = P_K$, $u \in U(K)$, $q = |k_K|$.
Scriviamo $u = \zeta_{q-1}^a u_1$; visto che $U_1^e = U_1$, u_1 è potenza e-esima in K, quindi possiamo considerare $u = \zeta_{q-1}^a$, in quanto i campi generati dalle radici di $x^e - t$ rimangono invariati se moltiplichiamo t per una potenza e-esima. Quindi mi limito ai polinomi del tipo $x^e - \pi\zeta^a$, dove $\zeta = \zeta_{q-1}$.
Osserviamo che $x^e - \pi\zeta^a$ e $x^e - \pi\zeta^b$ generano lo stesso campo se ζ^{a-b} è potenza e-esima, quindi possiamo scegliere $a \in \mathbb{Z}/e\mathbb{Z}$. Ma allora:

$$\zeta^a \in \frac{\langle\zeta\rangle}{\langle\zeta^e\rangle} \cong \frac{\mathbb{Z}/(q-1)\mathbb{Z}}{e\mathbb{Z}/(q-1)\mathbb{Z}} \cong \mathbb{Z}/(e, q-1)\mathbb{Z},$$

cioè $0 \leq a < (e, q-1)$.
Siano perciò $0 \leq a, b < (e, q-1)$. $\alpha^e = \pi\zeta^a$ e $\beta^e = \pi\zeta^b$, quindi:

$$K(\alpha) = K(\beta) \iff \frac{\alpha}{\beta} = \zeta^{\frac{a-b}{e}} = \zeta_{(q-1)e}^{a-b} \in K(\alpha) \iff \zeta^{\frac{a-b}{e}} \in \langle\zeta\rangle,$$

in quanto $k_{K(\alpha)} = k_K$. Otteniamo dunque che $K(\alpha) = K(\beta) \iff a \equiv b \pmod{e}$, condizione equivalente a $a \neq b$ per $0 \leq a, b < (e, q-1)$.
Fissiamo allora un a e contiamo il numero di estensioni diverse che generano le radici di $x^e - \pi\zeta^a$.
Date due radici α, $\alpha\zeta_e^i$, si ha che:

$$K(\alpha) = K(\alpha\zeta_e^i) \iff (\mathrm{ord}_{K^*}(\zeta_e^i), p) = 1 \iff \zeta_e^i \in \langle\zeta\rangle \iff \zeta_e^{i(q-1)} = 1 \iff$$
$$\iff i(q-1) \equiv 0 \pmod{e} \iff i \equiv 0 \pmod{\left(\frac{e}{(e, q-1)}\right)}.$$

Quindi i campi coincidono a $(e, q-1)$ a $(e, q-1)$, cioè abbiamo $(e, q-1)$ estensioni diverse generate dalle radici di $x^e - \pi\zeta^a$ per ogni $0 \leq a < (e, q-1)$, per un totale di e estensioni diversi di K tame totalmente ramificate di grado e.

<u>*Esempio*</u> (Estensioni quadratiche di K). Sappiamo che le estensioni quadratiche di K corrispondono ai sottogruppi di $\frac{K^*}{(K^*)^2}$.

$p \neq 2$) $K^* = \langle \pi \rangle \times \mathbb{F}_q^* \times \langle \zeta_{p^s} \rangle \times \mathbb{Z}_p^n$, dunque $\frac{K^*}{(K^*)^2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
I sottogruppi di ordine 2 sono 3 e le estensioni corrispondenti sono $K(\sqrt{\pi_K})$, $K(\sqrt{\zeta_{q-1}\pi_K})$ (totalmente ramificate) e $K(\sqrt{\zeta_{q-1}})$ (non ramificata).

$p = 2$) Procedendo come sopra abbiamo $\frac{K^*}{(K^*)^2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, che contiene 7 sottogruppi di ordine 2.

2.5 Differente

Sia K un campo, $R \subseteq K$ un dominio di Dedekind, E/K un'estensione finita e separabile, e S la chiusura integrale di R in E.

Definizione 2.5.1. Se M è un sottogruppo additivo di E, si definisce il **sottogruppo complementare** di M (rispetto alla traccia) $M' = \{x \in E \mid \mathrm{Tr}_{E/K}(xM) \subseteq R\}$.

Se M è un R-modulo, anche M' lo è, e se M è un ideale frazionario di E, anche M' lo è.

Definizione 2.5.2. Si definisce **differente** dell'estensione L/K l'ideale frazionario $\mathfrak{D}_{E/K} = \mathfrak{D}_{S/R} = (S')^{-1} \subseteq S$.

Richiamiamo una proposizione ben nota che permette di calcolare esplicitamente il differente di estensioni di campi p-adici.

Proposizione 2.5.1. *Se $E = K(\alpha)$, con $[E : K] = n$ separabile. Allora la base duale di $\{1, \dots, \alpha^{n-1}\}$ è $\left\{\frac{b_0}{f'(\alpha)}, \dots, \frac{b_{n-1}}{f'(\alpha)}\right\}$, dove $f(x) = (x-\alpha)(b_{n-1}x^{n-1} + \dots + b_0)$ è il polinomio minimo di α.*

Corollario 2.5.2. *Supponiamo che, oltre alle ipotesi precedenti, valga $S = R[\alpha]$ (cosa che vale sempre in estensioni di campi p-adici). Allora $S' = \frac{S}{(f'(\alpha))}$, cioè $\mathfrak{D}_{E/K} = (f'(\alpha))\mathscr{O}_E$ nei campi p-adici.*

Dimostrazione. Basta dimostrare che $\langle b_0, \dots, b_{n-1} \rangle_R = \langle 1, \dots, \alpha^{n-1} \rangle_R$. Usando la decomposizione $f(x) = (b_0 + \dots + b_{n-1}x^{n-1})(x - \alpha)$ ed uguagliando i coefficienti corrispondenti, si ottiene che la matrice di cambio di base da $\{b_0, \dots, b_{n-1}\}$ a $\{1, \dots, \alpha^{n-1}\}$ è triangolare, cioè invertibile. $\square$

Ricordiamo inoltre che il differente è moltiplicativo nelle torri, cioè, se $K \subseteq F \subseteq E$ sono estensioni di campi e S, T sono rispettivamente le chiusure integrali di R in F e E, allora $\mathfrak{D}_{E/K} = \mathfrak{D}_{E/F}\mathfrak{D}_{F/K}$.

Proposizione 2.5.3. *Sia $U \subseteq R$ moltiplicativamente chiuso. Allora $\mathfrak{D}_{U^{-1}S/U^{-1}R} = U^{-1}\mathfrak{D}_{S/R}$.*

Dimostrazione. La tesi è equivalente a dimostrare che $(U^{-1}S)' = U^{-1}S'$. Visto che:

$$(U^{-1}S)' = \{x \in E \mid \mathrm{Tr}_{E/K}(xU^{-1}S) \subseteq U^{-1}R\} = \{x \in E \mid U^{-1}\,\mathrm{Tr}_{E/K}(xS) \subseteq U^{-1}R\},$$

evidentemente vale l'inclusione $(U^{-1}S)' \supseteq U^{-1}S'$.
Viceversa, se $x \in (U^{-1}S)'$, $U^{-1}\,\mathrm{Tr}_{E/K}(xS) \subseteq U^{-1}R$, allora $\mathrm{Tr}_{E/K}(xS) \subseteq U^{-1}R$ a meno di moltiplicare per un u opportuno, cioè $\mathrm{Tr}_{E/K}(xuS) \subseteq R$, da cui $xu \in S'$ e $x \in U^{-1}S'$. $\square$

Proposizione 2.5.4. *Sia $R \subseteq K$ un anello a valutazione discreta, P il suo ideale massimale e Q un ideale primo di S sopra P. Sia $v = v_P$ la valutazione P-adica in K e w_Q la sua estensione a E. Se R_v e S_{w_Q} sono i completati di R e S rispetto alle precedenti valutazioni, allora $\mathfrak{D}_{S_{w_Q}/R_v} = \mathfrak{D}_{S/R}S_{w_Q}$.*

Dimostrazione. Prendendo gli inversi, la tesi è equivalente all'uguaglianza $S'_{w_Q} = S'$. Sia dunque $x \in S'_{w_Q}$; denotando Tr_Q la traccia da S_{w_Q} a R_v, abbiamo $\mathrm{Tr}_Q(xS_{w_Q}) \subseteq R_v$.
Sia $\xi \in E$ tale che $|\xi - x|_{w_Q} < \varepsilon$ e $|\xi|_{w_{Q'}} < \varepsilon$ per ogni $Q' \neq Q$, dove $\varepsilon > 0$ è un numero sufficientemente piccolo. Se $y \in S$, per la seconda ipotesi su ξ otteniamo che $\mathrm{Tr}_{Q'}(\xi y) < \varepsilon'$, mentre per continuità e per la prima ipotesi abbiamo che $\mathrm{Tr}_Q(\xi y) \in R_v \cap K = R$, cioè $\xi \in S'$. Ma allora, prendendo una successione ξ_n che converge a x con le proprietà precedenti, si ha che $x \in S'$.
Sia invece $x \in S'$. Sia $y \in S_{w_Q}$ e scegliamo un $\eta \in S$ tale che $|\eta - y|_{w_Q} < \varepsilon$ e $|\eta|_{w_{Q'}} < \varepsilon$ per ogni $Q' \neq Q$. Visto che vale l'identità:

$$\underbrace{Tr_{E/K}(x\eta)}_{\in R} = \mathrm{Tr}_Q(x\eta) + \sum_{Q' \neq Q} \mathrm{Tr}_{Q'}(x\eta)$$

e il secondo addendo sta in R_v perchè sufficientemente vicino a 0, allora per differenza anche $\mathrm{Tr}_Q(x\eta) \in R_v$, da cui per continuità $\mathrm{Tr}_Q(xy) \in R_v$, cioè $x \in S'_{w_Q}$. □

Corollario 2.5.5. *Sia $R \subseteq K$ un dominio di Dedekind e P il suo unico ideale massimale. Vale la seguente identità locale-globale:*

$$\mathfrak{D}_{S/R} = \prod_{Q|P} \mathfrak{D}_{S_{w_Q}/R_v}.$$

Dimostrazione. Per la conservazione del differente nel localizzato, possiamo ridurci al caso in cui R è un DVR; ma allora per la proposizione precedente la potenza di Q in $\mathfrak{D}_{S/R}$ è la stessa della potenza di Q in $\mathfrak{D}_{S_{w_Q}/R_v}$. □

Proposizione 2.5.6. *$R \subseteq K$ dominio di Dedekind, P primo di R e $Q|P$. Se $PS = Q^eQ'$, con $(Q, Q') = 1$, allora:*

1. *Se Q è non ramificato, $Q \nmid \mathfrak{D}_{S/R}$.*

2. *$Q^{e-1} \mid \mathfrak{D}_{S/R}$ e lo divide esattamente $\iff$ l'estensione è tame.*

3. *$\mathfrak{D}_{S/R}$ è l'ideale generato da tutti gli elementi $f'(\alpha)$, dove $\alpha \in S$ e f è il polinomio minimo di α.*

Dimostrazione. Osserviamo subito che, per la proposizione precedente, nei primi due punti possiamo ricondurci al caso locale.

1. Se E/K di campi p-adici è non ramificata, $S = R[\zeta_m]$, con $p \nmid m$, quindi, detto f il polinomio minimo di ζ_m, $x^m - 1 = f(x)g(x)$, allora $m\zeta_m^{m-1} = f'(\zeta_m)g(\zeta_m)$, da cui $f'(\zeta_m) \notin P$ (in quanto altrimenti $m\zeta_m^{m-1} \in (p)R$), cioè $Q \nmid (f'(\zeta_m))S$.

2. Innanzitutto possiamo considerare l'estensione totalmente ramificata per il punto precedente. Posto $S = R[\pi]$, π radice di un polinomio di Eisenstein $f(x) = x^e - a_{e-1}x^{e-1} + \ldots + a_0$, $a_i \in P\ \forall i > 0$, $a_0 \in P \backslash P^2$, abbiamo $f'(\pi) \equiv e\pi^{e-1} \pmod{P}$, dunque $f'(\pi) \equiv e\pi^{e-1}$ $\pmod{Q}$, da cui la tesi.

3. Sia α un generatore intero dell'estensione E/K, $S \supseteq R[\alpha]$. Allora $\mathfrak{D}_{S/R} \supseteq \mathfrak{D}_{R[\alpha]/R} = (f'(\alpha))$. Segue dunque facilmente l'inclusione $\mathfrak{D}_{S/R} \supseteq \{f'(\alpha) \mid \alpha \in R\}$.
Sia Q uno dei (finiti) primi che divide $\mathfrak{D}_{S/R}$; bisogna verificare che $\exp_Q(\mathfrak{D}_{S/R}) = \exp_Q(f'(\alpha))$ per un certo α generatore intero dell'estensione. Denotiamo $v = v_P$ e consideriamo $w_Q \mid v$; sia inoltre $f(x)$ il polinomio minimo di α.
Se $\sigma_1 : E \to \overline{K_v}$ è un'immersione che genera il valore assoluto w_Q, si ha facilmente:
$$\sigma_1(f'(\alpha)) = f'(\sigma_1(\alpha)) = \prod_{\sigma \neq \sigma_1} (\sigma_1(\alpha) - \sigma(\alpha)).$$
Indicheremo come al solito $\sigma \sim \tau$ se σ e τ sono coniugate su K_v, cioè se esiste un automorfismo λ di $\overline{K_v}$ su K_v tale che $\tau = \lambda \circ \sigma$ su E.
L'estensione S_{w_Q}/R_v è monogenica, cioè $S_{w_Q} = R_v[\beta]$ per un certo $\beta \in S_{w_Q}$; dico che, se β' è sufficientemente vicino a β, allora $S_{w_Q} = R_v[\beta']$. Infatti, se $|\beta - \beta'| < 1$, allora $\beta' \equiv \beta \pmod{\hat{Q}}$, dove $\hat{Q}$ è l'ideale massimale di S_{w_Q}, cioè β e β' generano lo stesso campo residuo; inoltre, se $|\beta - \beta'| < \varepsilon$, allora $|f(\beta') - f(\beta)|$ è abbastanza piccolo e dunque $|f(\beta)| = |f(\beta')|$, cioè β' genera anche l'ideale massimale.
Vediamo adesso che esiste $a \in R_v$ tale che $|\lambda(\beta) - a| = 1$ per ogni $\lambda : \overline{K_v} \to \overline{K_v}$ estensione dell'identità su K_v. Basta mostrare che $\overline{\lambda(\beta)} \neq \overline{a}$ nel campo residuo, quindi scelgo $a = 1$ se le classi dei $\lambda(\beta)$ nel campo residuo (coniugate sul campo residuo) sono 0 e $a = 0$ altrimenti.
Siano $\sigma_1, \ldots, \sigma_r$ dei rappresentanti delle classi di equivalenza delle immersioni $E \to \overline{K_v}$ rispetto a $\sim$. Per il teorema di approssimazione, possiamo trovare un elemento $\alpha \in E$ tale che $|\sigma_1(\alpha) - \beta|$ è piccolo e $|\sigma_i(\alpha) - a|$ è piccolo per $i \neq 1$. Senza perdita di generalità, possiamo supporre che tale α sia intero e generi l'estensione E/K: infatti se α non fosse intero, basterebbe moltiplicarlo per un elemento di R congruo a 1 modulo P_K e divisibile per potenze elevate di certi altri primi; se non generasse, potremmo cambiare α con $\alpha + \pi^N \gamma$, dove γ è un generatore di E/K, e per il teorema dell'elemento primitivo avremmo che $E = K(\alpha, \gamma) = K(\alpha + \pi^N \gamma)$ per un certo N abbastanza grande.
Per quanto detto prima, $S_{w_Q} = R_v[\sigma_1(\alpha)]$, dunque:
$$\exp_Q(\mathfrak{D}_{S_{w_Q}/R_v}) = \exp_Q\left(\prod_{\substack{\sigma \sim \sigma_1 \\ \sigma \neq \sigma_1}} (\sigma_1(\alpha) - \sigma(\alpha))\right).$$
Ci resta quindi da vedere che gli altri fattori non danno alcun contributo in termini di potenze di Q. Sia perciò $\sigma \not\sim \sigma_1$; scriviamo $\sigma = \lambda \circ \sigma_i$, con $i \neq 1$. Allora:
$$|\sigma_1(\alpha) - \sigma(\alpha)| = |\sigma_1(\alpha) - \lambda \circ \sigma_i(\alpha)| = |\lambda^{-1} \circ \sigma_1(\alpha) - \sigma_i(\alpha)| = |\lambda^{-1} \circ \sigma_1(\alpha) - a + a - \sigma_i(\alpha)|.$$
Ma $|\sigma_i(\alpha) - a|$ è piccolo, e $\lambda^{-1} \circ \sigma_1(\alpha)$ è vicino a $\lambda^{-1}(\beta)$. Visto che $|\lambda^{-1}(\beta) - a| = 1$, segue che $\lambda^{-1} \circ \sigma_1(\alpha) - a| = 1$ e dunque anche $|\sigma_1(\alpha) - \sigma(\alpha)| = 1$, cioè la tesi.

□

2.6 Gruppi di ramificazione

Sia K un campo completo rispetto a una valutazione discreta v, e indichiamo come al solito con $\mathcal{O}_K$ il suo anello di valutazione, con P_K l'unico ideale massimale di $\mathcal{O}_K$, con $U(K)$ il gruppo delle unità e con k_K il campo residuo. Consideriamo inoltre L/K un'estensione di Galois con gruppo di Galois $G = \mathrm{Gal}(L/K)$ tale che l'estensione dei campi residui k_L/k_K sia separabile. Sappiamo che $\mathcal{O}_L$ è un $\mathcal{O}_K[G]$-modulo e esiste un generatore intero α tale che $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Lemma 2.6.1. *$\sigma \in G$, $i \in \mathbb{Z}_{\geq 0}$. Sono fatti equivalenti:*

1. *σ agisce banalmente su $\frac{\mathscr{O}_L}{P_L^{i+1}}$.*
2. *$v_L(\sigma(\gamma) - \gamma) \geq i + 1$ per ogni $\gamma \in \mathscr{O}_L$.*
3. *$v_L(\sigma(\alpha) - \alpha) \geq i + 1$.*

Dimostrazione. L'implicazione $1 \Rightarrow 2$ segue dall'osservazione che $\sigma(\gamma) + P_L^{i+1} = \gamma + P_L^{i+1}$, mentre l'implicazione $3 \Rightarrow 1$ segue dall'osservazione che σ agisce banalmente su $\overline{\alpha} = \alpha + P_L^{i+1}$, che genera $\frac{\mathscr{O}_L}{P_L^{i+1}}$ su $\mathscr{O}_K$. □

Definizione 2.6.1. Per ogni $i \geq -1$, si definisce $G_i = \{\sigma \in G \mid v_L(\sigma(\alpha) - \alpha) \geq i+1\}$ ***i*-esimo gruppo di ramificazione**.

Si ha evidentemente che $G = G_{-1} \supseteq G_0 \supseteq \ldots \supseteq G_n = \{\mathrm{id}\}$ e $G_i \triangleleft G$, in quanto la catena si fermerà dopo $\max_\sigma \{v_L(\sigma(\alpha) - \alpha)\} + 1$ passi. Inoltre si osserva che $G_0 = E$ gruppo di inerzia.

Definizione 2.6.2. I numeri i tali che $G_i \neq G_{i+1}$ si dicono **salti della ramificazione**.

Definizione 2.6.3. Definiamo la funzione i_G tale che:

$$\begin{array}{rccc} i_G : & G & \longrightarrow & \mathbb{N} \cup \{+\infty\} \\ & \sigma & \longmapsto & v_L(\sigma(\alpha) - \alpha) \end{array}$$

con la convenzione che $i_G(\mathrm{id}) = +\infty$.

<u>Osservazioni</u>. 1. $i_G(\sigma) = i + 1 \iff \sigma \in G_i \backslash G_{i+1}$.

2. $i_G(\tau\sigma\tau^{-1}) = i_G(\sigma)$ per ogni $\tau \in G$.
3. $i_G(\sigma\tau) \geq \min\{i_G(\sigma), i_G(\tau)\}$.

Proposizione 2.6.2. *Sia $H < G$ e $K' = L^H$. Allora $H_i = G_i \cap H$.*

Dimostrazione. $\sigma \in H$ agisce banalmente su $\frac{\mathscr{O}_L}{P_L^{i+1}} \iff$ agisce banalmente su $\frac{\mathscr{O}_{K'}}{P_{K'}^{i+1}}$. □

Corollario 2.6.3. *Sia K_r la massima sottoestensione non ramificata di L/K. Allora $K_r = L^E = L^{G_0}$ e i gruppi di ramificazione di L/K di indice ≥ 0 coincidono con quelli di L/K_r, che è totalmente ramificata.*

Proposizione 2.6.4. *Sia $H \triangleleft G$ e $K' = L^H$. Allora:*

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{s \to \sigma} i_G(s),$$

dove $s \to \sigma$ significa che $\overline{s} = \sigma$ in G/H.

Dimostrazione. Sia β un generatore di $\mathscr{O}_{K'}$ su $\mathscr{O}_K$. Per l'unicità dell'estensione di una valutazione, abbiamo che:

$$i_{G/H}(\sigma) = v_{K'}(\sigma(\beta) - \beta) = \frac{1}{e_{L/K'}} v_L(\sigma(\beta) - \beta).$$

Osserviamo che:

$$\sum_{s \to \sigma} v_L(s(\alpha) - \alpha) = \sum_{\tau \in H} v_L(s\tau(\alpha) - \alpha),$$

dove s è un qualunque elemento tale che $s \to \sigma$, e $v_L(\sigma(\beta) - \beta) = v_L(s(\beta) - \beta)$.
Se poniamo $b = s(\beta) - \beta$ e $a = \prod_{\tau \in H} (s\tau(\alpha) - \alpha)$, la tesi equivale a dimostrare che a e b hanno la stessa valutazione, cioè $(a) = (b)$.
Sia $\mu_\alpha(x) = \prod_{\tau \in H} (x - \tau(\alpha))$ il polinomio minimo di α su K'; sicuramente $(s\mu_\alpha)(x) = \prod_{\tau \in H} (x - s\tau(\alpha))$.
I coefficienti del polinomio $(s\mu_\alpha)(x) - \mu_\alpha(x)$ sono tutti divisibili per b, in quanto $\mu_\alpha(x) \in \mathscr{O}_{K'} = \mathscr{O}_K[\beta]$, quindi:

$$b \mid (s\mu_\alpha)(\alpha) - \mu_\alpha(\alpha) = (s\mu_\alpha)(\alpha) = \prod_{\tau \in H} (\alpha - s\tau(\alpha)) = \pm a.$$

Ci rimane da mostrare l'altra divisibilità. $\beta \in \mathscr{O}_K[\alpha]$, quindi possiamo trovare un polinomio $g(x) \in \mathscr{O}_K[x]$ tale che $g(\alpha) = \beta$. $g(x) - \beta \in \mathscr{O}_{K'}[x]$ ha α come radice, quindi $\mu_\alpha(x) \mid g(x) - \beta$ in $\mathscr{O}_{K'}[x]$. Poniamo $g(x) - \beta = \mu_\alpha(x)p(x)$. Applicando s e poi valutando in a si ottiene:

$$\pm a = (s\mu_\alpha)(\alpha) \mid \underbrace{(sg)}_{=g}(\alpha) - s(\beta) = \beta - s(\beta) = b.$$

□

Corollario 2.6.5. *Se $H = G_j$, con $j \geq 0$, allora $\left(\frac{G}{H}\right)_i = \frac{G_i}{G_j}$ per $i \leq j$, ed è banale altrimenti.*

Dimostrazione. $\frac{G}{G_j} \supseteq \frac{G_0}{G_j} \supseteq \ldots \supseteq \frac{G_j}{G_j} = \{\mathrm{id}\}$ e $\frac{G}{G_j} \supseteq \left(\frac{G}{G_j}\right)_0 \supseteq \ldots \supseteq \left(\frac{G}{G_j}\right)_k = \{\mathrm{id}\}$ sono due catene per $\frac{G}{G_j}$. Dico che coincidono.
Preso $\sigma \in \frac{G}{G_j}$ diverso dall'identità, esiste un unico indice i tale che $\sigma \in \frac{G_i}{G_j} \backslash \frac{G_{i+1}}{G_j}$. Sia $s \in G$ tale che $s \to \sigma$; allora $s \in G_i \backslash G_{i+1}$, cioè $i_G(s) = i + 1$. Se $K' = L^{G_j}$, L/K' è totalmente ramificata, in quanto $G_0 \supseteq G_j$, dunque $e_{L/K'} = [L : K'] = |G_j|$.
Per la proposizione precedente, $i_{\frac{G}{G_j}}(\sigma) = \frac{1}{|G_j|}|G_j|(i+1) = i + 1$, cioè $\sigma \in \left(\frac{G}{G_j}\right)_i \backslash \left(\frac{G}{G_j}\right)_{i+1}$, da cui la tesi. □

Proposizione 2.6.6. $v_L(\mathfrak{D}_{L/K}) = \sum_{s \neq \mathrm{id}} i_G(s) = \sum_{i \geq 0} (|G_i| - 1)$.

Dimostrazione. Sappiamo che $\mathfrak{D}_{L/K} = (f'(\alpha)) = \left(\prod_{s \neq \mathrm{id}} (\alpha - s(\alpha))\right)$, quindi $v_L(\mathfrak{D}_{L/K}) = \sum_{s \neq \mathrm{id}} v_L(s(\alpha) - \alpha) = \sum_{s \neq \mathrm{id}} i_G(s)$.
Poniamo $g_i = |G_i| - 1$; allora $|\{s \mid i_G(s) = i + 1\}| = |G_i| - |G_{i+1}| = g_i - g_{i+1}$, da cui:

$$v_L(\mathfrak{D}_{L/K}) = \sum_{i \geq 0} (i+1)(g_i - g_{i+1}) = g_1 - g_2 + 2(g_2 - g_3) + \ldots = \sum_{i \geq 0} g_i.$$

□

Corollario 2.6.7. *$H < G$, $K' = L^H$. Allora $v_{K'}(\mathfrak{D}_{K'/K}) = \frac{1}{e_{L/K'}} \sum_{s \notin H} i_G(s)$.*

Dimostrazione. Visto che $\mathfrak{D}_{L/K} = \mathfrak{D}_{L/K'}\mathfrak{D}_{K'/K}$, la tesi segue passando alle valutazioni. □

Vediamo adesso come si possono studiare i gruppi di ramificazione nel caso globale avendo informazioni solo a livello locale.

Sia R un dominio di Dedekind con campo delle frazioni K, sia L/K finita di Galois con gruppo di Galois G e sia S la chiusura integrale di R in L. Sia P un primo di R e scegliamo un primo Q di S sopra P. Come è usuale, indichiamo con $D = D(Q|P)$ ed $E = E(Q|P)$ i gruppi di decomposizione e di inerzia di $Q|P$. Se L_Q e K_P sono i completati di L e K rispetto alle valutazioni v_Q e v_P, allora l'estensione L_Q/K_P risulta di Galois, in quanto $L_Q = LK_P$ e normalità e separabilità si conservano nel traslato. Inoltre, se $\hat{Q}$ e $\hat{P}$ sono i completati di Q e P, abbiamo un omomorfismo:

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(L_Q/K_P) & \longrightarrow & D(Q|P) \\ & \sigma & \longmapsto & \sigma_{|L} \end{array}$$

in quanto $\sigma(\hat{Q}) = \hat{Q}$ implica che $\sigma_{|L}(Q) = \sigma_{|L}(\hat{Q} \cap L) = \hat{Q} \cap L = Q$. Tale omomorfismo è però un isomorfismo: le cardinalità coincidono, e l'iniettività segue dalla continuità degli elementi del gruppo di Galois rispetto alla topologia Q-adica, in quanto $v_Q(\sigma(\alpha)) = v_Q(\alpha)$ per ogni $\sigma : L_Q \to L_Q$ automorfismo, da cui $\sigma_{|L} = \mathrm{id}$ implica $\sigma = \mathrm{id}$.
Definiamo $G_i(Q) = \{\sigma \in G \mid \sigma(\gamma) \equiv \gamma \pmod{Q^{i+1}}\ \forall \gamma \in S\}$; se i G_i denotano i gruppi di ramificazione dei campi locali, dico che $\varphi(G_i) = G_i(Q)$.
Sicuramente $\varphi(G_i) \subseteq G_i(Q)$, in quanto, se $\sigma(\gamma) \equiv \gamma \pmod{\hat{Q}^{i+1}}$ per ogni $\gamma \in \mathscr{O}_{L_Q}$, allora $\sigma_{|L}(\gamma) \equiv \gamma \pmod{\underbrace{Q^{i+1}}_{=\hat{Q}^{i+1} \cap S}}$ per ogni $\gamma \in S$. Vediamo quindi che $\varphi : G_i \to G_i(Q)$ è surgettiva: sia $\tau \in G_i(Q)$ e cerchiamo $\hat{\tau}$ tale che $\hat{\tau}_{|L} = \tau$.
$\hat{\tau} \in G_i \iff v_Q(\hat{\tau}(\alpha) - \alpha) \geq i + 1 \iff \hat{\tau}(\alpha) - \alpha \in \hat{Q}^{i+1}$ per ogni $\alpha \in \mathscr{O}_{L_Q}$. Ma se $\alpha = \lim_{n\to\infty} \alpha_n$, definitivamente $\alpha_n \in \alpha \in \hat{Q}^{i+1}$. Per questo $\tau(\alpha_n) - \alpha_n \in Q^{i+1} \subseteq \hat{Q}^{i+1}$, dunque $\tau(\alpha_n) \in \alpha + \hat{Q}^{i+1}$. Ma allora basta definire $\hat{\tau}(\alpha) = \lim_{n\to\infty} \tau(\alpha_n)$ e si ha che $\hat{\tau}(\alpha) \in \alpha + \hat{Q}^{i+1}$, cioè $\hat{\tau} \in G_i$.
Consideriamo adesso un'estensione L/K di campo locali come sopra e totalmente ramificata (se non lo fosse basterebbe considerare L/K_r, dove $K_r = L^E$ è la massima sottoestensione non ramificata). Denotiamo con π un generatore del massimale P_L di $\mathscr{O}_L$.

Proposizione 2.6.8. *Sia $i \geq 0$ e $s \in G$. $s \in G_i \backslash G_{i+1} \iff \frac{s(\pi)}{\pi} \equiv 1 \pmod{P_L^{i+1}} \iff \frac{s(\pi)}{\pi} \in U_i(L)$.*

Dimostrazione. $s \in G_i \backslash G_{i+1} \iff i_G(s) = i + 1 = v_L(s(\pi) - \pi)$, in quanto $\mathscr{O}_L = \mathscr{O}_K[\pi]$. Ma $v_L(s(\pi) - \pi) = 1 + v_L\left(\frac{s(\pi)}{\pi} - 1\right) = i + 1 \iff v_L\left(\frac{s(\pi)}{\pi} - 1\right) = i \iff \frac{s(\pi)}{\pi} \equiv 1 \pmod{P_L^{i+1}}$. □

Indicato $U_i(L)$ con U_i, ricordiamo che $\frac{U}{U_1} \cong k_L^*$ e $\frac{U_i}{U_{i+1}} \cong \frac{P_L^i}{P_L^{i+1}} \cong k_L$.

Proposizione 2.6.9. *La mappa*

$$\begin{array}{rccc} \theta_i: & \frac{G_i}{G_{i+1}} & \longrightarrow & \frac{U_i}{U_{i+1}} \\ & [s] & \longmapsto & \left[\frac{s(\pi)}{\pi}\right] \end{array}$$

è un omomorfismo iniettivo e non dipende da π.

Dimostrazione. Vediamo prima l'indipendenza dal generatore di P_L. Se $(\pi) = (\pi')$, allora $\pi' = u\pi$, con $u \in U$, dunque $\frac{s(\pi')}{\pi'} = \frac{s(u)}{u}\frac{s(\pi)}{\pi}$, ma $s(u) \equiv u \pmod{P_L^{i+1}}$, quindi $\frac{s(u)}{u} \in U_{i+1}$.
Con abuso di notazione, consideriamo θ_i definita su G_i. Se $u = \frac{\tau(\pi)}{\pi}$, θ_i è un omomorfismo se e solo se $\frac{\theta_i(s\tau)}{\theta_i(s)\theta_i(\tau)} = \frac{s(u)}{u} \equiv 1 \pmod{P_L^{i+1}}$, ma questo è vero perchè $\frac{s(u)}{u}$ è un'unità (in quanto quoziente di elementi della stessa valutazione) e perchè $s \in G_i$.
Infine, $\mathrm{Ker}(\theta_i) = \left\{s \in G_i \,\middle|\, \frac{s(\pi)}{\pi} \in U_{i+1}\right\} = \{s \in G_i \mid s(\pi) \equiv \pi \pmod{P_L^{i+2}}\} = G_{i+1}$. □

Corollario 2.6.10. *Il gruppo $\frac{G}{G_1} = \frac{G_0}{G_1}$ è ciclico e $\theta_0\left(\frac{G_0}{G_1}\right) < k_L^*$, quindi, se $\mathrm{char}(k_L) = p \neq 0$, p è coprimo con $\left|\frac{G_0}{G_1}\right|$.*

Corollario 2.6.11. *Se $\mathrm{char}(k_L) = 0$, allora $G_1 = \{\mathrm{id}\}$ e G_0 è ciclico.*

Dimostrazione. I quozienti $\frac{G_i}{G_{i+1}}$ sono sottogruppi finiti di $\frac{U_i}{U_{i+1}} \cong k_L$, che è un campo a caratteristica 0, dunque i quozienti $\frac{G_i}{G_{i+1}}$ sono banali per ogni $i \geq 1$, da cui $G_1 = \{\mathrm{id}\}$ (altrimenti la successione dei G_i non arriverebbe mai a $\{\mathrm{id}\}$). □

Corollario 2.6.12. *Se* $\mathrm{char}(k_L) = p \neq 0$*, allora i quozienti* $\frac{G_i}{G_{i+1}}$ *sono p-gruppi abeliani elementari (cioè prodotto di copie di* $\mathbb{Z}/p\mathbb{Z}$*) e* G_1 *è il p-Sylow di* G_0*.*

Dimostrazione. Il primo fatto segue dal fatto che $\frac{G_i}{G_{i+1}}$ si immerge nel gruppo additivo k_L, mentre il secondo è un'immediata conseguenza del primo corollario. □

Corollario 2.6.13. L/K *estensione di campi p-adici,* $e = e_0 p^n$ *con* $(e_0, p) = 1$*,* $L_i = L^{G_i}$*. Allora* $L_0 = K_r$ *e* L_1 *è la massima sottoestensione tame di* L/K*.*

Dimostrazione. Sappiamo che $L_0 = K_r$ e $[L_0 : K] = f$; inoltre $G_1 = \mathrm{Gal}(L/L_1)$ è un p-gruppo e $\frac{G_0}{G_1} = \mathrm{Gal}(L_1/L_0)$ ha cardinalità coprima con p, dunque $|G_1| = p^n$ e $\left|\frac{G_0}{G_1}\right| = e_0$. □

Corollario 2.6.14. *Se* $\mathrm{char}(k_L) = p \neq 0$*,* $G_0 \cong G_1 \rtimes H$*, dove* $H \cong \frac{G_0}{G_1}$ *è ciclico.*

Dimostrazione. Consideriamo la successione:

$$1 \hookrightarrow G_1 \longrightarrow G_0 \longrightarrow \frac{G_0}{G_1} \longrightarrow 1.$$

Sia $\overline{s}$ un generatore di $\frac{G_0}{G_1}$; visto che $(e_0, p) = 1$, posso trovare un $N \geq n$ tale che $p^N \equiv 1 \pmod{e_0}$. Se $t = s^{p^N}$, $t^{e_0} = s^{p^N e_0} = 1$, in quanto $|G_0| = e_0 p^n \mid e_0 p^N$, e $\overline{t} = \overline{s}^{p^N} = \overline{s}$, dunque $H = \langle t \rangle$ ha ordine e_0 ed ha intersezione banale con G_1. □

Corollario 2.6.15. G_0 *è risolubile. Inoltre, se* k_L *è finito, anche* G *è risolubile.*

Esempio. Sia k un campo algebricamente chiuso di caratteristica 0 e consideriamo $K = k((t))$. Denotiamo con $\overline{K}$ la chiusura algebrica di K; dico che $\overline{K} = \bigcup_{n \geq 1} k\left(\left(t^{\frac{1}{n}}\right)\right)$.
L'inclusione $\supseteq$ è ovvia; per vedere l'altra sia $K \subseteq L \subseteq \overline{K}$ tale che L/K è finita e di Galois. k è algebricamente chiuso, quindi $k_K = k_{\overline{K}} = k$, dunque L/K è totalmente ramificata e $G = G_0$ è ciclica. Da questo si deduce che ogni estensione finita è di Galois ciclica, e per ogni n esiste un'unica estensione di K di grado n, poichè altrimenti il gruppo di Galois del composto non sarebbe ciclico. Visto che $k\left(\left(t^{\frac{1}{n}}\right)\right)$ è un'estensione di grado n di K, essa deve essere l'unica e segue quindi l'altra inclusione.
Di conseguenza, $\mathrm{Gal}(\overline{K}/K) \cong \varprojlim \mathrm{Gal}\left(k\left(\left(t^{\frac{1}{n}}\right)\right)/K\right) \cong \hat{\mathbb{Z}}$.

Proposizione 2.6.16. $s \in G_0$*,* $\tau \in \frac{G_i}{G_{i+1}}$*, con* $i \geq 1$*. Allora* $\theta_i(s\tau s^{-1}) = \theta_0(s)^i \theta_i(\tau)$*, dove si intende che* $\theta_0(s) \in k_L'$ *e* $\theta_i(\tau) \in \frac{P_L^i}{P_L^{i+1}}$*.*

Dimostrazione. Scegliamo $t \in G_i$ tale che $\overline{t} = \tau$. Posto $\pi' = s^{-1}(\pi)$, abbiamo che $t(\pi') = \pi'(1 + a)$, con a$a = b\pi^i \in P^i$. $\theta_i(t) = \overline{a} \in \frac{P_L^i}{P_L^{i+1}}$, da cui $sts^{-1} = s(\pi'(1 + a)) = \pi(1 + s(a))$ e perciò $\theta_i(sts^{-1}) = \overline{s(a)}$. Se $s(\pi) = u\pi$, con $u \in U$, allora $s(a) = s(b)u^i\pi^i$, ma $s(b) \equiv b \pmod{P_L}$, quindi $s(a) \equiv bu^i\pi^i = au^i \pmod{\pi^{i+1}}$; si giunge alla tesi osservando che $\theta_0(s) = \left[\frac{s(\pi)}{\pi}\right] = [u]$. □

Corollario 2.6.17. $s \in G_0$*,* $t \in G_i$*,* $i \geq 1$*.* $sts^{-1}t^{-1} \in G_{i+1} \iff s^i \in G_1 \ \vee \ t \in G_{i+1}$*.*

Dimostrazione. $sts^{-1}t^{-1} \in G_{i+1} \iff sts^{-1} \in tG_{i+1} \iff \theta_i(sts^{-1}) = \theta_i(t) \iff \theta_0(s)^i\theta_i(t) = \theta_i(t) \iff \theta_0(s)^i = 1 \ \vee \ \theta_i(t) = 0 \iff s^i \in G_i \ \vee \ t \in G_{i+1}$. □

Corollario 2.6.18. *Se G è abeliano, $e_0 = \left|\frac{G_0}{G_1}\right|$. Se $i \geq 0$ e $e_0 \nmid i$, allora $G_i = G_{i+1}$.*

Dimostrazione. Sia $t \in G_i$ e scegliamo $s \in G_0$ tale che $\langle \overline{s} \rangle = \frac{G_0}{G_1}$. Se $e_0 \nmid i$, allora $s^i \notin G_i$; ma visto cge $\mathrm{id} = sts^{-1}t^{-1} \in G_{i+1}$, allora $t \in G_{i+1}$. □

Vogliamo adesso dimostrare una dei più importanti teoremi sui salti della ramificazione; per farlo, abbiamo bisogno di due risultati, di cui tralasciamo la dimostrazione, che può essere trovata nel libro *Local Fields* di Serre.

Lemma 2.6.19. *$s \in G_i$, $t \in G_j$, $i, j \geq 1$. Allora $sts^{-1}t^{-1} \in G_{i+1}$ e $\theta_{i+j}(sts^{-1}t^{-1}) = (j - i)\theta_i(s)\theta_j(t)$.*

Proposizione 2.6.20. *$s \in G_i$, $t \in G_j$, $i, j \geq 1$. Allora $sts^{-1}t^{-1} \in G_{i+j+1}$.*

Teorema 2.6.21. *I salti della ramificazione sono congrui fra loro modulo $p = \mathrm{char}(k_L)$.*

Dimostrazione. Sia $j = \max\{i \mid |G_i| \neq 1\}$. Ovviamente j è un salto. Sia inoltre i un altro salto e scegliamo $s \in G_i \backslash G_{i+1}$ e $t \in G_j \backslash G_{j+1}$.
$sts^{-1}t^{-1} \in G_{i+1} = \{\mathrm{id}\}$, quindi $0 = \theta_{i+j}(sts^{-1}t^{-1}) = (j - i)\theta_i(s)\theta_j(t)$ in $\frac{P_L^{i+j}}{P_L^{i+j+1}}$, cioè $j - i \equiv 0 \pmod{p}$. □

<u>*Esempio*</u>. Consideriamo $K = \mathbb{Q}_p(\zeta_p)$ e $L = K(\sqrt[p]{\pi_K})$. $\mathrm{Gal}(L/K) = \langle s \rangle \cong \mathbb{Z}/p\mathbb{Z}$. L'estensione è totalmente ramificata, quindi $G = G_0$ ed esiste un unico salto della ramificazione, sia esso t. Sappiamo che $\mathfrak{D}_{L/K} = (f'(\pi)) = (p\pi^{p-1})$, quindi $v_L(\mathfrak{D}_{L/K}) = v_L(p) + p - 1 = e + p - 1$; ricordando che:

$$v_L(\mathfrak{D}_{L/K}) = \sum_{i \geq 0} (|G_i| - 1) = (t + 1)(p - 1) = t(p - 1) + p - 1,$$

si ottiene che $e = t(p - 1)$, cioè $t = \frac{e}{p-1}$.
Adesso vogliamo rinumerare i gruppi di ramificazione G_i in modo da dedurne altre proprietà; innanzitutto poniamo $G_u = G_{\lceil u \rceil}$ per ogni $u \in \mathbb{R}_{\geq -1}$ e definiamo la funzione $\varphi = \varphi_{L/K}$ tale che:

$$\varphi_{L/K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]} = \int_0^u \frac{|G_t|}{|G_0|} dt.$$

Si osserva subito che $\varphi_{L/K}$ è l'identità su $[-1, 0]$, mentre, se $m < u \leq m + 1$, vale l'identità:

$$\varphi_{L/K}(u) = \frac{1}{g_0} \left(\sum_{i=1}^{m} g_i + (u - m) g_{m+1} \right),$$

dove $g_i = |G_i|$.

Proposizione 2.6.22. *1. φ è continua, lineare a tratti, crescente e concava.*

2. $\varphi(0) = 0$.

3. Se φ'_+ e φ'_- sono le derivata destra e sinistra di φ, allora $\varphi'_+(u) = \varphi'_-(u) = \frac{1}{[G_0:G_u]}$ se $u \notin \mathbb{Z}$, mentre $\varphi'_-(m) = \frac{1}{[G_0:G_m]}$ e $\varphi'_+(m) = \frac{1}{[G_0:G_{m+1}]}$ se $m \in \mathbb{Z}$.

4. Tali proprietà identificano univocamente φ.

φ è una funzione invertibile, quindi denotiamo con $\psi = \psi_{L/K}$ la sua inversa.

Proposizione 2.6.23. *1. ψ è continua, lineare a tratti, crescente e convessa.*

2. $\psi(0) = 0$.

3. $\psi'_\pm(v) = \frac{1}{\varphi'_\pm(u)} \in \mathbb{Z}$, *dove* $u = \psi(v)$.

4. *Se* $v \in \mathbb{Z}$, *allora* $u = \psi(v) \in \mathbb{Z}$.

Dimostrazione. I primi tre punti sono evidenti. Per l'ultimo, visto che $\varphi(u) = v$, abbiamo:

$$g_0\varphi(u) = \sum_{i=1}^{m} g_i + (u - m)g_{m+1},$$

da cui $u - m \in \mathbb{Z}$ e quindi $u \in \mathbb{Z}$. □

Definizione 2.6.4. Definiamo **gruppi di ramificazione con indice in alto** i gruppi $G^v := G_{\psi(v)}$. Analogamente agli usuali gruppi di ramificazione, si dice che v è un salto in alto della ramificazione se $G^v \supsetneq G^{v'}$ per ogni $v' > v$.

É immediato osservare che $G^0 = G_0$; inoltre, ψ può essere scritta:

$$\psi(v) = \int_0^v [G^0 : G^w]dw.$$

Lemma 2.6.24. $\varphi(u) = \frac{1}{g_0}\sum_{s\in G}\min\{i_G(s), u+1\} - 1$.

Dimostrazione. Sia m intero tale che $m - 1 < u \leq m$. Allora, spezzando $G = (G\backslash G_0) \sqcup (G_0\backslash G_1) \sqcup (G_1\backslash G_2) \sqcup \ldots$, si ha:

$$\frac{1}{g_0}\sum_{s\in G}\min\{i_G(s), u+1\} = \frac{1}{g_0}(1(g_0 - g_1) + 2(g_1 - g_2) + \ldots + m(g_{m-1} - g_m) + g_m(u+1)) =$$
$$= \frac{1}{g_0}\sum_{i=0}^{m-1} g_i + g_m(u - (m-1)) = \varphi(u) + 1.$$

□

Lemma 2.6.25. *Sia* $H \lhd G$, $\sigma \in \frac{G}{H}$ *e poniamo* $j(\sigma) = \max\{i_G(s) \mid s \in \sigma H\}$. *Allora, se* $K' = L^H$, *vale la relazione:*

$$i_{\frac{G}{H}}(\sigma) - 1 = \varphi_{L/K'}(j(\sigma) - 1).$$

Dimostrazione. Sappiamo che $i_{\frac{G}{H}}(\sigma) = \frac{1}{e_{L/K'}}\sum_{s\to\sigma} i_G(s) = \frac{1}{e_{L/K'}}\sum_{t\in H} i_G(st)$, dove $\sigma = sH$. Sia $\overline{s} \in sH$ tale che $i_G(\overline{s}) = \max\{i_G(st) \mid t \in H\} = j(\sigma) = m$, cioè $\overline{s} \in G_{m-1}\backslash G_m$; allora $i_{\frac{G}{H}}(\sigma) = \frac{1}{e_{L/K'}}\sum_{t\in H} i_G(\overline{s}t)$.
Come al solito, supponiamo che l'estensione L/K sia totalmente ramificata; se poniamo $i_G(t) = k$, allora:

$$\overline{s}t(\pi) - \pi = \overline{s}(\pi + \pi^k u) - \pi = \overline{s}(\pi) + \overline{s}(\pi)^k\overline{s}(u) - \pi = \pi + \pi^m u' + \pi^k u'' - \pi.$$

Da tale conto, si deduce immediatamente che $i_G(\overline{s}t) = \min\{i_G(\overline{s}), i_G(t)\}$ se $k \neq m$; se invece $k = m$, allora $m \geq i_G(\overline{s}t) \geq m$ e quindi anche in questo caso $i_G(\overline{s}t) = \min\{i_G(\overline{s}), i_G(t)\}$.
In conclusione, per il lemma precedente:

$$i_{\frac{G}{H}}(\sigma) = \frac{1}{e_{L/K'}}\sum_{t\in H}\min\{m, i_G(t)\} = \varphi_{L/K'}(m-1) + 1.$$

□

Il prossimo teorema mostra finalmente l'utilità dei gruppi di ramificazione con indice in alto.

Teorema 2.6.26 (Herbrandt)**.** $\frac{G_u H}{H} = \left(\frac{G}{H}\right)_v$*, dove* $v = \varphi_{L/K'}(u)$*.*

Dimostrazione. $\sigma \in \frac{G_u H}{H} \iff$ esiste $s \in G_u \cap \sigma H$ tale che $\sigma H = sH$. Ma $sH = \sigma H \iff i_G(s) \geq u+1 \iff j(\sigma) \geq u+1 \iff j(\sigma)-1 \geq u \iff \varphi_{L/K'}(j(\sigma)-1) \geq \varphi_{L/K'}(u) \iff i_{\frac{G}{H}}(\sigma) \geq \varphi_{L/K'}(u)+1 \iff \sigma \in \left(\frac{G}{H}\right)_{\varphi_{L/K'}(u)}$. □

Proposizione 2.6.27. *φ e ψ verificano le formule di transitività: se $K \subseteq F \subseteq L$ sono estensioni di Galois, allora $\varphi_{L/K} = \varphi_{F/K} \circ \varphi_{L/F}$ e $\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}$.*

Dimostrazione. Verifichiamo la relazione sono per φ, in quanto quella per ψ seguirà prendendo gli inversi. Basta verificare che $\varphi_{F/K} \circ \varphi_{L/F}$ soddisfa le proprietà caratterizzanti $\varphi_{L/K}$; le uniche verifiche non banali sono quelle sulle derivate.
Se $v = \varphi_{L/F}(u)$, ovviamente vale che $(\varphi_{F/K} \circ \varphi_{L/F})'(u) = \varphi'_{F/K}(v)\varphi'_{L/F}(u)$; detto $G = \mathrm{Gal}(L/K)$ e $H = \mathrm{Gal}(L/F)$, si ha:

$$\varphi'_{F/K}(v) = \frac{|(G/H)_v|}{|(G/H)_0|} \qquad \text{e} \qquad \varphi'_{L/F}(u) = \frac{|H_u|}{|H_0|}.$$

Visto che $\left|\left(\frac{G}{H}\right)_v\right| = \left|\frac{G_u H}{H}\right| = \frac{|G_u||H|}{|G_u \cap H|} \cdot \frac{1}{|H|} = \frac{|G_u|}{|H_u|}$, segue facilmente:

$$\varphi'_{F/K}(v)\varphi'_{L/F}(u) = \frac{|G_u||H_u|}{|H_u|e_{L/F}} \cdot \frac{1}{e_{F/K}} = \frac{1}{e_{L/K}}|G_u| = \frac{|G_u|}{|G_0|} = \varphi'_{L/K}(u).$$

□

Proposizione 2.6.28. *$H \lhd G$. Allora $\left(\frac{G}{H}\right)^v = \frac{G^v H}{H}$.*

Dimostrazione. Sappiamo che $\left(\frac{G}{H}\right)^v = \left(\frac{G}{H}\right)_x = \frac{G_u H}{H}$, dove $x = \psi_{K'/K}(v)$, $K' = L^H$, e $u = \psi_{L/K'}(x) = \psi_{L/K'}(\psi_{K'/K}(v)) = \psi_{L/K}(v)$. Si conclude facilmente osservando che da questa uguaglianza segue $G_u = G^v$. □

Enunciamo adesso un importantissimo teorema, che dimostreremo più avanti:

Teorema 2.6.29 (Hasse-Arf)**.** *Se L/K è abeliana, i salti in alto sono interi.*

Esempio (Salti in alto non interi). Preso $\pi = \zeta_p - 1$, consideriamo le estensioni di $\mathbb{Q}_p$ $K = \mathbb{Q}_p(\zeta_p)$ e $L = K(\sqrt[p]{\pi})$; si ha che $[K : \mathbb{Q}_p] = p-1$ e $[L : K] = p$ e l'estensione $L/\mathbb{Q}_p$ è totalmente ramificata. É facile vedere che $\mathrm{Gal}(L/\mathbb{Q}_p) = \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^*$; sia $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$ un generatore dello $\mathbb{Z}/p\mathbb{Z}$.
$G = G_0$ e $G_1 = \langle\sigma\rangle \cong \mathbb{Z}/p\mathbb{Z}$; 0 è quindi un salto della ramificazione, e ne esiste solo un altro, che chiamiamo t. Visto che $\zeta_p - 1$ genera l'ideale massimale di $\mathscr{O}_K$, abbiamo:

$$i_G(\sigma) = v_L(\sigma(\sqrt[p]{\pi}) - \sqrt[p]{\pi}) = v_L(\zeta_p\sqrt[p]{\pi} - \sqrt[p]{\pi}) = v_L(\sqrt[p]{\pi}) + v_L(\zeta_p - 1) = 1 + p,$$

da cui $t = p$. Se calcoliamo i salti in alto, il primo sarà ovviamente $\varphi(0) = 0$; il secondo è invece:

$$\varphi(p) = \frac{1}{g_0}\sum_{i=1}^{p} g_i = \frac{1}{p(p-1)}p^2 = \frac{p}{p-1},$$

che non è intero se $p \neq 2$.

Esempio. Sia L/K ciclica totalmente ramificata di grado p^n, dove p è la caratteristica del campo residuo k_K. Allora $G = G_0 = G_1 = \mathbb{Z}/p^n\mathbb{Z}$. Sappiamo inoltre che i quozienti $\frac{G_i}{G_{i+1}}$ sono isomorfi a $\mathbb{Z}/p\mathbb{Z}$, dunque ci sono esattamente n salti della ramificazione. Denotiamo con $e_0, e_0 + e_1, \dots, e_0 + \dots + e_{n-1}$ i salti in basso e con $i_0, i_0 + i_1, \dots, i_0 + \dots + i_{n-1}$ i salti in alto. Si hanno le relazioni:

$$i_0 = \varphi(e_0) = \frac{1}{g_0}(g_1 + \dots + g_{e_0}) = e_0$$
$$i_0 + i_1 = \varphi(e_0 + e_1) = \frac{1}{g_0}(g_1 + \dots + g_{e_0}) + \frac{1}{g_0}(g_{e_0+1} + \dots + g_{e_0+e_1}) = i_0 + \frac{1}{p}e_1$$

e continuando ricorsivamente si può vedere che $e_j = p^j i_j$ per ogni $0 \leq j \leq n-1$.

Esempio (Estensioni ciclotomiche di $\mathbb{Q}_p$). Denotiamo $K_n = \mathbb{Q}_p(\zeta_{p^n})$. Allora $K_n/\mathbb{Q}_p$ è totalmente ramificata, ha grado $\phi(p^n)$ ed il suo gruppo di Galois G è isomorfo a $(\mathbb{Z}/p^n\mathbb{Z})^*$; inoltre $G = G_0$ e G_1 è ciclico di ordine p^{n-1}. Denotiamo s_a l'elemento di G tale che $s_a(\zeta_{p^n}) = \zeta_{p^n}^a$ e consideriamo i sottogruppi di G:

$$G(p^n)^\nu = \{a \in (\mathbb{Z}/p^n)^* \mid a \equiv 1 \pmod{p^\nu}\} = \{s_a \in G \mid a \equiv 1 \pmod{p^\nu}\}.$$

Evidentemente $|G(p^n)^\nu| = p^{n-\nu}$ e $K^{G(p^n)^\nu} = K_\nu$. La prossima proposizione caratterizza completamente i gruppi di ramificazione di K_n.

Proposizione 2.6.30. *I gruppi di ramificazione di G sono $G = G_0$ e $G_u = G(p^n)^\nu$ per un certo ν. In particolare:*

$$G_u = \begin{cases} G(p^n)^1 & \text{per } 1 \leq u \leq p-1 \\ G(p^n)^2 & \text{per } p \leq u \leq p^2-1 \\ \vdots & \\ G(p^n)^n = \{\mathrm{id}\} & \text{per } u \geq p^{n-1}-1 \end{cases}$$

I salti sono dunque $0, p-1, p^2-1, \dots, p^{n-1}-1$.

Dimostrazione. La tesi equivale a dimostrare che, per ogni $u \leq p^\nu - 1$, $a \in G(p^n)^\nu \iff s_a \in G_u$. Sia $a \equiv 1 \pmod{p^\nu}$, $a \not\equiv 1 \pmod{p^{\nu+1}}$; allora:

$$v_{K_n}(s_a(\zeta_{p^n}) - \zeta_{p^n}) = v_{K_n}(\zeta^{a-1} - 1) = v_{K_n}(\zeta_{p^{n-\nu}} - 1) = \frac{\phi(p^n)}{\phi(p^{n-\nu})} = p^\nu.$$

□

Corollario 2.6.31. *I salti in alto dell'estensione $K_n/\mathbb{Q}_p$ sono* $0, p-1, p^2-1, \dots, p^{n-1}-1$.

Dimostrazione. Basta osservare che:

$$\begin{aligned}\varphi_{K_n/\mathbb{Q}_p}(p^{k-1}) &= \frac{1}{g_0}\left((g_1 + \dots + g_{p-1}) + (g_p + \dots + g_{p^2-1}) + \dots + (g_{p^{n-1}} + \dots + g_{p^n-1})\right) = \\ &= \frac{1}{(p-1)p^{n-1}}\left((p-1)p^{n-1} + (p^2-p)p^{n-2} + \dots + (p^k - p^{k-1})p^{n-k}\right) = \\ &= 1 + \dots + 1 = k.\end{aligned}$$

□

Vogliamo concludere questa sezione con qualche accenno riguardo a cosa si può dire in generale su estensioni cicliche di grado p e p^n di un campo locale K.

Innanzitutto, se $\zeta_p \in K$ e L/K è un'estensione di Galois di grado p con gruppo di Galois $G = \langle\sigma\rangle$, allora il teorema di Kummer assicura che $L = K(\sqrt[p]{x})$ per un certo $x \in K^*$; scriviamo come al solito $x = \pi^a u$, dove π è il generatore dell'ideale massimale di $\mathscr{O}_K$ e $0 \leq a < p$. Distinguiamo due casi:

$v(x) > 0)$ In questo caso possiamo supporre che $v(x) = 1$, in quanto esiste un h tale che $ah \equiv 1 \pmod p$, da cui $x^h = \pi^{ah}u^h$ è uguale a meno di potenze p-esime a $\pi u'$, che ha norma 1. Supponiamo quindi $x = \pi$. Allora:

$$v_L(\sigma(\sqrt[p]{x}) - \sqrt[p]{x}) = 1 + \frac{pe_k}{p-1} = t + 1,$$

da cui il salto della ramificazione è $t = \frac{pe_k}{p-1}$.

$v(x) = 0)$ In questo caso $x \in \frac{U_1}{U_1^p}$. Se $m > \frac{pe_k}{p-1}$, $U_m \subseteq U_1^p$, dunque, se $x \in U_l \backslash U_{l+1}$, consideriamo $l \leq \frac{pe_k}{p-1}$.
Visto che se $m < \frac{e_k}{p-1}$, $U_m^p \cong U_{mp}$, se $m > \frac{e_k}{p-1}$, $U_m^p \cong U_{m+e_k}$ e se $m = \frac{e_k}{p-1}$, $U_m^p \subseteq U_{pm}$, allora se $1 \leq l < \frac{pe_k}{p-1}$ e $p \mid l$ oppure se $l > \frac{pe_k}{p-1}$, tutti gli elementi di $U_l \backslash U_{l+1}$ sono potenze p-esime.
Quindi consideriamo solo gli l tali che $1 \leq l < \frac{pe_k}{p-1}$ e $p \nmid l$ e $l = \frac{pe_k}{p-1}$.
Se può mostrare che l'unica fra le estensioni $K(\sqrt[p]{u_l})/K$, $u_l \in U_l \backslash U_{l+1}$ a essere non ramificata è quella tale che $l = \frac{pe_k}{p-1}$; da questo si ricava inoltre che le altre estensioni di questo tipo con $1 \leq l < \frac{pe_k}{p-1}$ e $p \nmid l$ sono tutte totalmente ramificate.
Infine si può calcolare che in $K(\sqrt[p]{u_l})/K$, con $1 \leq l < \frac{pe_k}{p-1}$ e $p \nmid l$, il salto della ramificazione è $t = \frac{pe_k}{p-1} - l$.

Concludiamo con il seguente teorema, che ovviamente non dimostriamo, che stabilisce condizioni necessarie e sufficienti affinchè una n-upla $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ sia l'elenco dei salti in alto di un'estensione L/K ciclica di grado p^n:

Teorema 2.6.32. *Se $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ con $t_1 < \ldots < t_n$, allora esiste un'estensione L/K ciclica di grado p^n con salti in alto esattamente $t_1, \ldots, t_n$ se e solo se valgono le seguenti condizioni:*

- $1 \leq t_i < \frac{pe_k}{p-1}$ *e* $(t_i, p) = 1$*;*
- *se* $t_i z \frac{e_k}{p-1}$*, allora* $t_{i+1} = pt_i$ *oppure* $pt_i < t_{i+1} < \frac{pe_k}{p-1}$*;*
- *se* $t_i \geq \frac{e_k}{p-1}$*, allora* $t_{i+1} = t_i + e_k$*.*

3 Appendice

3.1 Adeli e ideli

Sia K un campo di numeri, v una valutazione su K e $\alpha \in K$. Consideriamo l'immersione:

$$\begin{array}{ccc} K & \hookrightarrow & \prod_{v \in M_K} K_v \\ \alpha & \longmapsto & \{\alpha_v\}_{v \in M_K} \end{array}$$

dove M_K indica l'insieme delle valutazioni normalizzate su K. Se $(\alpha) = \frac{P_1^{a_1} \cdot \ldots \cdot P_r^{a_r}}{Q_1^{b_1} \cdot \ldots \cdot Q_s^{b_s}}$, è facile vedere che gli α_v sono quasi tutti interi (in particolare $\alpha_v \in \mathscr{O}_{K_v} \iff v \neq v_{Q_i}$ per ogni $i = 1, \ldots, s$). Per questo motivo, lo spazio $\prod_{v \in M_K} K_v$ è "troppo grande".

Definizione 3.1.1. Sia $\{\Omega_\lambda\}_{\lambda \in \Lambda}$ una famiglia di spazi topologici. Per ogni λ, sia $A_\lambda \subseteq \Omega_\lambda$ un aperto. Si definisce prodotto topologico ristretto relativo agli A_λ lo spazio $\Omega \subseteq \prod_\lambda \Omega_\lambda$ tale che $\{\alpha_\lambda\} \in \Omega \iff \alpha_\lambda \in A_\lambda$ per quasi tutti i λ.

La topologia su Ω è definita dalla base di aperti $\Gamma = \prod_\lambda \Gamma_\lambda$, dove $\Gamma_\lambda \subseteq \Omega_\lambda$ è aperto e $\Gamma_\lambda = A_\lambda$ per quasi tutti i λ.

Proposizione 3.1.1. *Sia $S \subseteq \Lambda$ un sottoinsieme finito e definiamo $\Omega_S = \prod_{\lambda \in S} \Omega_\lambda \prod_{\lambda \notin S} A_\lambda$. Allora Ω_S è aperto in Ω e la topologia indotta su Ω_S è la topologia prodotto.*

Dimostrazione. Basta osseervare che $\Gamma_\lambda \cap \Omega_S$ è del tipo $\prod_{\lambda \in S \cup S'} B_\lambda \prod_{\lambda \notin S \cup S'} A_\lambda$, dove S' è finito e $B_\lambda \subseteq \Omega_\lambda$ è aperto, e tali sottoinsiemi formano una base di aperti per la topologia prodotto di Ω_S. $\square$

Osservazione. È immediato osservare che se $\{A'_\lambda\}$ è un'altra famiglia di aperti tale che $A'_\lambda = A_\lambda$ per quasi tutti i λ, allora i prodotti topologici ristretti relativi alle due famiglie coincidono.

Proposizione 3.1.2. *Se gli Ω_λ sono localmente compatti e gli A_λ sono compatti, allora Ω è localmente compatto.*

Dimostrazione. Dalla definizione è chiaro che gli Ω_S sono localmente compatti. Ma allora l'osservazione che $\Omega = \bigcup_S \Omega_S$ conclude la dimostrazione. $\square$

Supponiamo ora che gli spazi Ω_λ abbiano una misura μ_λ tale che $\mu_\lambda(A_\lambda) = 1$. Allora si può definire una misura μ su Ω tale che una base di insiemi misurabili sia $C = \prod_\lambda C_\lambda$, dove C_λ ha misura finita e $C_\lambda = A_\lambda$ per quasi ogni λ.
In questo modo inoltre μ non è altro che la misura prodotto su Ω_S.

Definizione 3.1.2. L'**anello degli adeli** V_K è il prodotto topologico ristretto dei K_v relativo agli aperti $\mathscr{O}_{K_v} \subseteq K_v$ se v è non archimedeo e agli aperti K_v se v è archimedeo.

Osservazioni.

1. V_K è un anello topologico, dove somma e moltiplicazioni sono applicazioni continue (infatti basta vederlo sugli Ω_S, su cui c'è la topologia prodotto, quindi possiamo verificarlo componente per componente).
2. V_K è localmente compatto.
3. K si immerge in modo naturale in V_K. Inoltre le immagini $\{\alpha_v\}_{v \in M_K}$ di K tramite questa immersione prendono il nome di **adeli principali**.

Proposizione 3.1.3. *Sia L/K un'estensione finita e separabile di campi di numeri. Allora $V_K \otimes_K L \cong V_L$ algebricamente e topologicamente.*

Dimostrazione. Detto $L = K(\alpha)$, $\{1, \alpha, \dots, \alpha^{n-1}\}$ è una base di L/K. Il termine di sinistra è il prodotto topologico ristretto dei $K_v \otimes_K L \cong K_v \oplus K_v\alpha \oplus \dots \oplus K_v\alpha^{n-1}$ relativo agli aperti $\mathscr{O}_{K_v} \oplus \mathscr{O}_{K_v}\alpha \oplus \dots \oplus \mathscr{O}_{K_v}\alpha^{n-1}$.
Inoltre $K_v \otimes_K L = L_{w_1} \oplus \dots \oplus L_{w_j}$, dove le w_i sono le estensioni di v a L, e quasi tutti gli aperti precedenti si identificano in questo spazio come $\mathscr{O}_{L_{w_1}} \oplus \dots \oplus \mathscr{O}_{L_{w_j}}$ (infatti si applica la teoria di Kummer, in quanto α è un generatore per quasi tutti i primi di K). Ma allora $V_K \otimes_K L$, che è il prodotto topologico ristretto dei $K_v \otimes_K L$ relativo agli $\mathscr{O}_{K_v} \oplus \mathscr{O}_{K_v}\alpha \oplus \dots \oplus \mathscr{O}_{K_v}\alpha^{n-1}$ coincide con il prodotto topologico ristretto dei L_w relativo agli aperti $\mathscr{O}_{L_w}$, con w che varia fra tutte le valutazioni di L, che non è altro che V_L.
Questo conclude che l'isomorfismo vale dal punto di vista topologico. Che valga dal punto di vista algebrico è invece evidente. $\square$

Corollario 3.1.4. *Indichiamo con V_K^+ il gruppo additivo ottenuto da V_K togliendo l'operazione di moltiplicazione. Allora:*

$$V_L^+ \cong \bigoplus_1^n V_K^+,$$

dove n è il grado dell'estensione L/K.

Dimostrazione. Preso un qualunque $\beta \in K$ diverso da 0, βV_K^+ è isomorfo a V_K^+ come gruppo topologico, quindi basta prendere la decomposizione $V_L^+ \cong V_K^+ \oplus V_K^+\alpha \oplus \dots \oplus V_K^+\alpha^{n-1}$ dalla proposizione precedente per giungere alla tesi. $\square$

Il seguente teorema dà un'importante informazione sul sottoinsieme degli adeli principali:

Teorema 3.1.5. *K (visto come immagine di K in V_K) è un sottoinsieme discreto di V_K. Inoltre V_K^+/K è compatto con la topologia quoziente.*

Dimostrazione. Per la decomposizione del corollario precedente è sufficiente mostrare la tesi solo per $\mathbb{Q}$ (in realtà questi risultati valgono per un qualsiasi campo globale, cioè anche per estensioni finite di $\mathbb{F}(t)$, con $\mathbb{F}$ un campo finito e t un'indeterminata).
Per vedere che $\mathbb{Q}$ è discreto in $V_\mathbb{Q}$ basta vedere che 0 ha un intorno U che non contiene nessun altro punto di $\mathbb{Q}$, in quanto le traslazioni sono omeomorfismi.
Indicato con $|\cdot|_\infty$ il valore assoluto usuale su $\mathbb{Q}$, consideriamo:

$$U = \{\alpha \in V_\mathbb{Q}^+ \mid |\alpha_\infty|_\infty < 1,\ |\alpha_p|_p \leq 1\}.$$

Questo insieme è chiaramente aperto e $U \cap \mathbb{Q} = \{0\}$, in quanto sappiamo che $\prod_{v \in M_\mathbb{Q}} |\alpha_v|_v = 1$ per ogni $\alpha \neq 0$.
Per vedere la parte relativa alla compattezza, vogliamo trovare un compatto $W \subseteq V_\mathbb{Q}^+$ tale che la proiezione $\pi : W \to V_\mathbb{Q}^+/\mathbb{Q}^+$ è surgettiva. Consideriamo:

$$W = \left\{ \alpha \in V_\mathbb{Q}^+ \;\middle|\; |\alpha_\infty|_\infty \leq \frac{1}{2},\ |\alpha_p|_p \leq 1 \right\}.$$

Per la surgettività, devo vedere che ogni adele β è della forma $\beta = b + \alpha$, con $b \in \mathbb{Q}$ e $\alpha \in W$. Se p è primo, $\beta_p \in \mathbb{Q}_p$, dunque β_p ammette una scrittura:

$$\beta_p = \underbrace{\frac{a_k}{p^k} + \dots}_{=r_p} + a_0 + a_1 p + \dots;$$

$\beta_p - r_p$ è intero, quindi $|\beta_p - r_p|_p \leq 1$. Visto che $\beta_p \in \mathbb{Z}_p$ per quasi tutti i p, cioè $r_p = 0$ per quasi tutti i p, possiamo definire $r = \sum_p r_p$.
Dato che $\left|\sum_{q \neq p} r_q\right|_q \leq 1$ per ogni q, in quanto gli r_q stanno in $\mathbb{Z}_p$, allora:

$$|\beta_p - r|_p \leq \max\left\{|\beta_p - r_p|_p, \left|\sum_{q \neq p} r_q\right|_q\right\} \leq 1$$

per ogni p.
Per la componente all'infinito, scelgo $s \in \mathbb{Z}$ tale che $|\beta_\infty - r - s|_\infty \leq \frac{1}{2}$; $b = r + s$ dà la tesi. □

Corollario 3.1.6. *Esiste un sottoinsieme W di V_K definito da disuguaglianze del tipo $|\xi_v|_v \leq \delta_v$, con $\delta_v = 1$ quasi sempre, tale che per ogni $\varphi \in V_K$ esistono $\theta \in W$ e $\gamma \in K$ tali che $\varphi = \theta + \gamma$.*

Dimostrazione. La tesi facilmente usando l'insieme W definito nella precedente dimostrazione e la decomposizione del corollario 3.1.4. □

Corollario 3.1.7. *La misura prodotto μ su V_K induce, per proiezione, una misura finita su V_K^+/K^+. Inoltre il W della dimostrazione ha misura 1.*

Dimostrazione. Visto che V_K^+/K^+ è compatto, possiamo ricoprirlo con i traslati di un aperto F di misura finita ed estrarne un sottoricoprimento finito; questo giustifica la finitezza della misura quoziente su V_K^+/K^+.
Inoltre, per calcolare la misura di W, ci si può ricondurre al caso $K = \mathbb{Q}$ con la solita decomposizione del corollario 3.1.4; in questo caso è facile vedere che $\mu(W) = 1$, in quanto $\mu_\infty\left(\left[-\frac{1}{2}, \frac{1}{2}\right]\right) = 1$ e $\mu_p(\mathbb{Z}_p) = 1$ per definizione. □

Lemma 3.1.8. *Esiste una costante $C > 0$ dipendente solo dal campo K con la seguente proprietà: se $\alpha \in V_K$ è tale che $\prod_v |\alpha_v|_v > C$, allora esiste un adele principale $\beta \in K$ diverso da 0 tale che $|\beta|_v \leq |\alpha_v|_v$ per ogni $v \in M_K$.*

Dimostrazione. Visto che $\alpha \in V_K$, allora $|\alpha_v|_v \leq 1$ per quasi tutte le v; la condizione $\prod_v |\alpha_v|_v > C$ implica però che $|\alpha_v|_v = 1$ per quasi tutte le v.
Denotiamo con C_0 la misura (di Haar) di V_K^+/K^+ e con C_1 la misura di:

$$W_1 = \left\{\gamma \in V_K^+ \;\middle|\; |\gamma_v|_v \leq \frac{1}{2C'} \text{ se } v \text{ è arch.}, |\gamma_v|_v \leq 1 \text{ se } v \text{ è non arch.}\right\},$$

dove C' è la costante tale che $|x + y|_v \leq C'(|x|_v + |y|_v)$ per tutte le v. Chiaramente, data la finitezza delle valutazioni archimedee, sia C_0 che C_1 sono numeri reali compresi strettamente fra 0 e ∞; posto $C = \frac{C_0}{C_1}$, vogliamo vedere che tale scelta funziona.
Consideriamo l'insieme T:

$$T = \left\{\gamma \in V_K^+ \;\middle|\; |\gamma_v|_v \leq \frac{1}{2C'}|\alpha_v|_v \text{ se } v \text{ è arch.}, |\gamma_v|_v \leq |\alpha_v|_v \text{ se } v \text{ è non arch.}\right\};$$

tale insieme ha misura $C_1 \prod_v |\alpha_v|_v > C_1 C = C_0$, dunque la proiezione $V_K^+ \to V_K^+/K^+$ non può essere iniettiva. Siano $\tau', \tau'' \in T$ tali che $\tau' - \tau'' = \beta \in K^+$; allora $|\beta|_v = |\tau'_v - \tau''_v|_v \leq |\alpha_v|_v$ per ogni v, in quanto lo è evidentemente se v è archimedea, mentre $|\tau'_v - \tau''_v|_v \leq 2C' \frac{1}{2C'}|\alpha_v|_v = |\alpha_v|_v$ se v è non archimedea. □

Corollario 3.1.9. *Sia v_0 una valutazione normalizzata di K e siano $\delta_v > 0$ numeri dati per $v \neq v_0$, con $\delta_v = 1$ per quasi tutte le v. Allora esiste $\beta \in K$ non nullo tale che $|\beta|_v \leq \delta_v$ per tutte le v diverse da v_0.*

Dimostrazione. Scegliamo $\alpha_v \in K_v$ tale che $0 < |\alpha_v|_v \leq \delta_v$ e $|\alpha_v|_v = 1$ se $\delta_v = 1$ per ogni $v \neq v_0$. Possiamo quindi scegliere un $\alpha_{v_0} \in K_{v_0}$ tale che $\prod_v |\alpha_v|_v > C$. Il lemma precedente permette di concludere. $\square$

Teorema 3.1.10 (di approssimazione forte). *Sia v_0 una valutazione normalizzata di K e sia U il prodotto topologico ristretto dei K_v relativo agli aperti $\mathscr{O}_{K_v}$ per $v \neq v_0$. Allora K è denso in U.*

Dimostrazione. È piuttosto facile vedere che l'enunciato è equivalente alla seguente proposizione: supponiamo di avere un sottoinsieme S di valutazioni $v \neq v_0$, degli elementi $\alpha_v \in K_v$ per $v \in S$ e un $\varepsilon > 0$; allora esiste un $\beta \in K$ tale che $|\beta - \alpha_v|_v < \varepsilon$ per tutti i $v \in S$ e $|\beta|_v \leq 1$ per i $v \notin S$, $v \neq v_0$ (infatti una implicazione è ovvia, mentre per l'altra basta porre $\alpha_v = 0$ per $v \notin S$, $v \neq v_0$).
Per il corollario 3.1.6 esiste un sottoinsieme $W \subseteq V_K$ definito da disuguaglianze del tipo $|\xi_v|_v \leq \delta_v$, con $\delta_v = 1$ per quasi tutti i v tale che ogni $\varphi \in V_K$ si può scrivere nella forma $\varphi = \theta + \gamma$, $\theta \in W$, $\gamma \in K$; inoltre, per l'ultimo corollario, esiste $\lambda \in K$ diverso da 0 tale che $|\lambda|_v < \delta_v^{-1}\varepsilon$ per $v \in S$ e $|\lambda|_v \leq \delta_v^{-1}$ per $v \notin S$, $v \neq v_0$. Dunque, ponendo $\varphi = \lambda^{-1}\alpha$, si vede che ogni $\alpha \in V_K$ è della forma $\alpha = \psi + \beta$, con $\psi \in \lambda W$ e $\beta \in K$. A questo punto, se denotiamo α l'adele con componenti i numeri dati α_v per $v \in S$ e 0 altrimenti, è facile vedere che il β precedente soddisfa le proprietà richieste. $\square$

A questo punto vorremmo studiare gli invertibili dell'anello topologico commutativo V_K, ma purtroppo V_K^* non è un gruppo topologico dotato della topologia di sottospazio, in quanto la mappa $x \mapsto x^{-1}$ non è continua. Per ovviare a ciò, diamo a V_K^* la seguente topologia: considerata l'immersione:

$$\begin{array}{ccc} V_K^* & \hookrightarrow & V_K \times V_K \\ x & \longmapsto & (x, x^{-1}) \end{array}$$

mettiamo su V_K^* la topologia di sottospazio rispetto a $V_K \times V_K$. È evidente che V_K^* sia un gruppo topologico con tale topologia e che l'inclusione $V_K^* \hookrightarrow V_K$ sia continua.

Definizione 3.1.3. Il **gruppo degli ideli** J_K di K è il gruppo V_K^* dotato della precedente topologia.

È importante sottolineare che le topologie su J_K indotte da V_K e $V_K \times V_K$ non coincidono; per questo ci riferiremo alla prima come la V_K-topologia di J_K e alla seconda come la J_K-topologia. Il prossimo esempio esibisce un caso concreto in cui le due topologie sono diverse.

Esempio. Sia $K = \mathbb{Q}$ e consideriamo la successione $\alpha^{(p)}$ tale che $\alpha_p^{(p)} = p$ e $\alpha_v^{(p)} = 1$ per $v \neq p$. Chiaramente tale successione converge a 1 nella $V_\mathbb{Q}$-topologia. Però essa non converge nella $J_\mathbb{Q}$-topologia: infatti un intorno di 1 nella $J_\mathbb{Q}$-topologia è del tipo $(U \times V) \cap V_K^*$, dove U e V sono del tipo $\prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p$, con $S \subseteq M_\mathbb{Q}$ finito, dunque definitivamente la successione $\left\{(\alpha^{(p)})^{-1}\right\}$ non sta in V.

Visto che K si immerge in modo naturale in V_K, allo stesso modo K^* si immerge in modo naturale in J_K; consideremo quindi K^* come sottogruppo di J_K, che chiameremo sottogruppo degli **ideli principali**.

Osservazioni. 1. K^* è un sottogruppo discreto di J_K. Infatti K è discreto in V_K, dunque K^* si immerge in $V_K \times V_K$ tramite la composizione:

$$\begin{array}{ccccc} K^* & \hookrightarrow & J_K & \hookrightarrow & V_K \times V_K \\ x & \longmapsto & x = \{x_v\}_{v \in M_K} & \longmapsto & (x, x^{-1}) \end{array}$$

come un sottogruppo discreto.

2. J_K è il prodotto topologico ristretto dei K_v^* relativo agli aperti $U(K_v)$ delle unità.

Definizione 3.1.4. Preso un idele α, si definisce **contenuto** di α il numero $c(\alpha) = \prod_v |\alpha_v|_v$.

Osservazione. La mappa $c : \alpha \mapsto c(\alpha)$ è un omomorfismo continuo da J_K al gruppo $\mathbb{R}_+$. Infatti sicuramente è un omomorfismo; per vedere che è continuo basta vedere che lo è in 1.
Dato un intorno U di 1 in $\mathbb{R}_+$, diciamo $U = \{|x-1| < \varepsilon\}$, denotiamo con V il sottoinsieme di J_K formato dagli α tali che $|\alpha_v|_v = 1$ per v non archimedeo e $|\alpha_v - 1|_v < \delta$ per v non archimedeo, con $\delta = \delta(\varepsilon)$ oppurtuno. Allora basta studiare la mappa c ristretta a $J_K \cap \prod_{v \text{ arch.}} K_v$, che può essere vista come la moltiplicazione $\mathbb{R}_+^n \to \mathbb{R}_+$, che è continua.

Denotiamo con J_K^1 il nucleo della mappa c dotato della topologia di sottospazio di J_K.

Lemma 3.1.11. *1. J_K^1, considerato come sottospazio di V_K, è chiuso.*

2. La V_K-topologia di J_K^1 coincide con la J_K-topologia.

Dimostrazione. 1. Sia $\alpha \in V_K \backslash J_K^1$; cerchiamo un intorno $W \subseteq V_K$ di α che non intersechi J_K^1. Separiamo due casi:

$c(\alpha) < 1$: Esiste un sottoinsieme finito delle valutazioni che contiene tutti i v per cui $|\alpha_v|_v > 1$ e tale che $\prod_{v \in S} |\alpha_v|_v < 1$. Allora W può essere scelto:

$$W = \{\xi \in V_K \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ se } v \in S, |\xi|_v \leq 1 \text{ se } v \notin S\},$$

con ε sufficientemente piccolo, in quanto la moltiplicazione in $\mathbb{R}^n$ è continua.

$c(\alpha) > 1$: Sia $c(\alpha) = C$ e s il numero delle valutazioni v di K per cui $|\alpha_v|_v < 1$. Esiste un insieme S finito di valutazioni tali che S contiene tutte le v per cui $|\alpha_v|_v > 1$, tutte le valutazioni archimedee e tutte le v con la proprietà che, se $v \notin S$ e $|\xi_v|_v < 1$, allora $|\xi_v|_v \leq \frac{1}{(2C)^{s+1}}$. Infatti, detto $n = [K : \mathbb{Q}]$, se v è una valutazione di K che estende la valutazione p-adica, allora $|\alpha_v|_v < 1 \Rightarrow |\alpha_v|_v \leq \frac{1}{p^{1/n}}$, dunque mi basta mettere in S tutte le v che estendono le valutazioni p-adiche per $p \leq (2C)^{n(s+1)}$. Può essere scelto un $\varepsilon > 0$ abbastanza piccolo in modo che, se $|\xi_v - \alpha_v|_v < \varepsilon$, allora $1 < \prod_{v \in S} |\xi_v|_v < (2C)^{s+1}$; consideriamo dunque:

$$W = \{\xi \in V_K \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ se } v \in S, |\xi_v|_v \leq 1 \text{ se } v \notin S\}.$$

Tale W funziona, perchè, se $\xi \in W$ è tale che $|\xi_v|_v = 1$ per ogni $v \notin S$, allora $c(\xi) > 1$; se invece esiste $v \notin S$ per cui $|\xi_v|_v < 1$, allora $|\xi_v|_v \leq \frac{1}{(2C)^{s+1}}$ e dunque $c(\xi) < 1$.

2. Se $\alpha \in J_K^1$, dobbiamo mostrare che ogni J_K-intorno di α contiene un suo V_K-intorno e viceversa. Sia $W \subseteq J_K^1$ un V_K-intorno di α. Allora sicuramente W contiene un V_K-intorno di α del tipo:

$$W_1 = \{\xi \in J_K^1 \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ se } v \in S, |\xi_v|_v \leq 1 \text{ se } v \notin S\},$$

dove $\varepsilon > 0$ è abbastanza piccolo e S è un certo sottoinsieme finito di M_K. Ma W_1 contiene il J_K-intorno W_2 di α definito da:

$$W_2 = \{\xi \in J_K^1 \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ se } v \in S, |\xi_v|_v = 1 \text{ se } v \notin S\}.$$

Sia viceversa $H \subseteq J_K^1$ un J_K-intorno di α. Come sopra H contiene un J_K-intorno H_1 di α del tipo:

$$H_1 = \{\xi \in J_K^1 \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ se } v \in S, |\xi_v|_v = 1 \text{ se } v \notin S\},$$

dove $\varepsilon > 0$ è abbastanza piccolo e contiene tutte le valutazioni archimedee e tutte le valutazioni v per cui $|\alpha_v|_v \neq 1$. Visto che $c(\alpha) = 1$, può essere scelto ε abbastanza piccolo in modo che $c(\xi) < 2$ per oogni $\xi \in H_1$. Ma allora l'intersezione di H_1 con J_K^1 coincide con l'intersezione del W_1 definito prima con J_K^1, dunque H_1 è un V_K-intorno di α.

□

Teorema 3.1.12. *J_K^1/K^* con la topologia quoziente è compatto.*

Dimostrazione. Per il lemma precedente basta trovare un W compatto in V_K tale che la proiezione $\pi : W \cap J_K^1 \to J_K^1/K^*$ sia surgettiva. Consideriamo:

$$W = \{\xi \in V_K \mid |\xi_v|_v \leq |\alpha_v|_v \ \forall \alpha \text{ tale che } c(\alpha) > C\},$$

dove C è la costante del lemma 3.1.8.
Sia $\beta \in J_K^1$. Per il lemma 3.1.8 esiste $\eta \in K^*$ tale che $|\eta|_v \leq |\beta_v^{-1}\alpha_v|_v$ per ogni v, dunque $\eta\beta \in W$, cioè $\beta \in \eta^{-1}W$, cioè $\beta K^* \in \pi(W)$. □

A questo punto vogliamo vedere in che modo gli strumenti appena introdotti si applicano allo studio del gruppo delle classi di ideali di un certo campo di numeri K e del suo gruppo delle unità.

Se K è un campo di numeri, possiamo indicare il suo ideale frazionario $\prod_P P^{n_P}$ come la somma formale $\sum_{v \text{ non arch.}} n_v v$, dove v è la valutazione associata a P e $n_P = n_v$. In questo modo il gruppo I_K degli ideali di K non è altro che il gruppo delle somme $\sum_{v \text{ non arch.}} n_v v$ tali che $n_v \in \mathbb{Z}$ e $n_v = 0$ per quasi ogni v. Chiaramente un ideale frazionario $\sum_{v \text{ non arch.}} n_v v$ è intero se e solo se $n_v \geq 0$ per ogni v.
Costruiamo una mappa continua (abbiamo posto in I_K la topologia discreta):

$$\begin{array}{ccc} J_K & \longrightarrow & I_K \\ \alpha & \longmapsto & \sum \operatorname{ord}_v(\alpha) v \end{array}$$

Tramite tale mappa l'immagine di K^* è il gruppo degli ideali principali; da questo si deduce il seguente:

Teorema 3.1.13. *Il gruppo delle classi di ideali è finito.*

Dimostrazione. La restrizione della mappa precedente a J_K^1 è surgettiva su I_K, quindi il gruppo delle classi di ideali, essendo l'immagine continua del compatto J_K^1/K^*, è compatto. Ma un compatto discreto è necessariamente finito. □

Tramite il linguaggio degli adeli e ideli riusciamo a dare una dimostrazione semplificata del teorema delle unità di Dirichlet, addirittura in una versione generalizzata.

Definizione 3.1.5. Sia S un insieme finito di valutazioni contenente le valutazioni archimedee. Si definiscono **S-unità** gli elementi $\eta \in K^*$ tali che $|\eta_v|_v = 1$ per ogni $v \notin S$; l'insieme delle S-unità viene indicato con H_S.

Se S coincide con l'insieme delle valutazioni archimedee, le S-unità non sono altro che le unità usuali.

Lemma 3.1.14. *Siano c_1, c_2 costanti strettamente positive. L'insieme delle S-unità che soddisfano la condizione $c_1 \leq |\eta_v|_v \leq c_2$ per ogni v è finito.*

Dimostrazione. Consideriamo l'insieme:

$$W = \{\alpha \in J_K \mid |\alpha_v|_v = 1 \text{ se } v \notin S, c_1 \leq |\alpha_v|_v \leq c_2 \text{ se } v \in S\}.$$

W è compatto, in quanto è il prodotto di insiemi compatti con la topologia prodotto; visto che l'insieme cercato non è altro che $W \cap K^*$, esso è finito in quanto compatto e discreto. □

Lemma 3.1.15. *L'insieme degli elementi $\varepsilon \in K^*$ tali che $|\varepsilon_v|_v = 1$ per ogni v è finito e coincide con l'insieme delle radici di 1 in K.*

Dimostrazione. Sicuramente le radici di 1 soddisfano tale proprietà. Viceversa, per il lemma precedente, esiste solo un numero finito di $\varepsilon \in K^*$ tali che $|\varepsilon_v|_v = 1$ per ogni v; visto che formano un gruppo moltiplicativo, non possono far altro che coincidere con le radici di 1. □

Teorema 3.1.16 (Dirichlet)**.** *H_S è il prodotto diretto di un gruppo ciclico finito e di $\mathbb{Z}^{s-1}$, dove $[K:\mathbb{Q}] = r + 2t$ è la solita divisione fra immerisioni reali e complesse e $s = r + t$.*

Dimostrazione. Trattiamo prima il caso $S = S_\infty$ in cui S coincide con le valutazioni archimedee di K. Sia J_S l'insieme degli ideli α tali che $|\alpha_v|_v = 1$ per ogni $v \notin S$; se $J_S^1 = J_S \cap J_K^1$, J_S^1 è aperto in J_K^1.
Il sottoinsieme:

$$J_S^1/H_S = J_S^1/(J_S^1 \cap K^*) \cong J_S^1 K^*/K^* \subseteq J_K^1/K^*$$

è aperto in J_K^1/K^*, dunque è chiuso e perciò compatto. Riprendiamo l'immersione logaritmica:

$$\begin{array}{rccc} \lambda: & J_S & \longrightarrow & (\mathbb{R}^+)^s \\ & \alpha & \longmapsto & (\log|\alpha_1|_1, \ldots, \log|\alpha_s|_s) \end{array}$$

essaè continua e surgettiva, inoltre $\mathrm{Ker}(\lambda)$ è l'insieme delle radici di 1.
Per il lemma 3.1.14 esiste un numero finito di elementi $\eta \in H_S$ tali che $\frac{1}{2} \leq |\eta_v|_v \leq 2$ per ogni $v \in S$, quindi il gruppo $\Lambda = \lambda(H_S)$ è discreto.
D'altra parte, $T = \lambda(J_S^1)$ non è altro che l'iperpiano $x_1 + \ldots + x_s = 0$ in $\mathbb{R}^s$, cioè uno spazio vettoriale di dimensione $s - 1$. Visto che T/Λ è compatto, essendo l'immagine continua del precedente J_S^1/H_S, allora necessariamente Λ è libero con $s - 1$ generatori.
Per il caso di un insieme $S \supseteq S_\infty$ generico, la dimostrazione è analoga considerando l'immerisione logaritimica $\lambda : J_S \to \mathbb{R}^{s_0} \times \mathbb{Z}^{s-s_0}$, dove s_0 è il numero delle valutazioni archimedee di K. □