Cenni alla teoria dei valori assoluti

Luca Minutillo Menga

18 giugno 2015

Sommario

Indice

1 Definizioni ed esempi

Presenteremo i concetti basilari della teoria dei valori assoluti, investigandone le prime proprietà.

1.1 Prime definizioni

Definizione 1.1. Dato K campo, $|\cdot| : K \mapsto \mathbb{R}_{\geq 0}$ è detto valore assoluto su K se valgono le seguenti:

1. $|x| = 0 \Leftrightarrow x = 0$.
2. $\forall\ x, y \in K\ |x||y| = |xy|$.
3. $c := \sup\{|1 + x| : |x| \leq 1\} < \infty$.

$|\cdot|$ è detto banale se $|x| = 1$ per ogni $x \in K \setminus \{0\}$.

Osservazione 1.2. Se $\xi \in K$ è una radice dell'unità allora $|\xi| = 1$; in particolare $|1| = 1$.

Dimostrazione. Dato $n > 0$ tale che $\xi^n = 1$, si ha $|\xi|^n = |\xi|^{2n}$; dunque $|\xi| = 1$. □

Corollario 1.3. *Ogni valore assoluto su un campo finito è banale.*

Dimostrazione. In un campo finito ogni elemento è radice dell'unità. □

Osservazione 1.4. Data F/K estensione di campi, la restrizione a K di un valore assoluto su F è un valore assoluto su K.

Definizione 1.5. Dato $|\cdot|$ valore assoluto su K,

$$\Gamma := \{|x| : x \in K \setminus \{0\}\} \subseteq \mathbb{R}_{>0}$$

è detto gruppo dei valori di $|\cdot|$.

Osservazione 1.6. Γ è sottogruppo di $\mathbb{R}^*$, banale se e solo se lo è $|\cdot|$.

Osservazione 1.7. La costante c introdotta nella definizione 1.1 vale almeno 1.

Osservazione 1.8. Sia $|\cdot|$ valore assoluto con costante c. Dato λ reale positivo, $|\cdot|' : x \mapsto |x|^\lambda$ è ancora valore assoluto, con costante c^λ.

Definizione 1.9. $|\cdot|_1, |\cdot|_2$ valori assoluti su K sono equivalenti (scriveremo $|\cdot|_1 \sim |\cdot|_2$) se esiste $\lambda \in \mathbb{R}_{>0}$ tale che $|\cdot|_2 = |\cdot|_1^\lambda$.
Diremo inoltre che $|\cdot|_1$, ..., $|\cdot|_n$ sono indipendenti se sono a due a due non equivalenti.

Osservazione 1.10. Ogni valore assoluto è equivalente ad uno con costante $c \leq 2$.

Proposizione 1.11. *Sia $|\cdot|$ valore assoluto con costante c. $|\cdot|$ soddisfa la disuguaglianza triangolare se e solo se $c \leq 2$.*

Dimostrazione. Supponiamo che valga $|x| \leq 1 \Rightarrow |1+x| \leq 2$ e dimostriamo che allora sussiste la disuguaglianza triangolare (l'altra implicazione è banale).
Dimostriamo preliminarmente che, dati $r \in \mathbb{N},\ a_1,\ ...,\ a_{2^r} \in K$, vale:

$$\left| \sum_{i=1}^{2^r} a_i \right| \leq 2^r \max_{1 \leq i \leq 2^r} |a_i|.$$

Procediamo per induzione su $r \geq 1$. Il passo base segue notando che, supponendo $|a_1| \geq |a_2|$, vale

$$|a_1 + a_2| = |1 + a_1^{-1} a_2||a_1| \leq 2|a_1|.$$

Ipotizzando vera la tesi per $r-1$, si ha:

$$\left| \sum_{i=1}^{2^{r-1}} a_i + \sum_{i=2^{r-1}+1}^{2^r} a_i \right| \leq 2 \max \left\{ \left| \sum_{i=1}^{2^{r-1}} a_i \right|, \left| \sum_{i=2^{r-1}+1}^{2^r} a_i \right| \right\} \leq 2^r \max_{1 \leq i \leq 2^r} |a_i|,$$

come si voleva. Dunque, dati $n \in \mathbb{N},\ a_1,\ ...,\ a_n \in K$, vale:

$$\left| \sum_{i=1}^{n} a_i \right| \leq 2n \max_{1 \leq i \leq n} |a_i|,$$

aggiungendo eventualmente termini nulli alla $n-$upla.
In particolare $|n| \leq 2n$ per ogni $n \in \mathbb{N}$. [1]
Adesso possiamo dimostrare ciò che volevamo: dati comunque $n \in \mathbb{N}, x, y \in K$, si ha per quanto detto:

$$|(x+y)|^n = |(x+y)^n| \leq 2(n+1) \max_{0 \leq i \leq n} \left| \binom{n}{i} x^i y^{n-i} \right| =$$

$$= 2(n+1) \max_{0 \leq i \leq n} \left| \binom{n}{i} \right| |x|^i |y|^{n-i} \leq 4(n+1) \max_{0 \leq i \leq n} \binom{n}{i} |x|^i |y|^{n-i} \leq 4(n+1)(|x|+|y|)^n.$$

Estraendo la radice $n-$esima e portando al limite $n \to \infty$ si ottiene $|x+y| \leq |x| + |y|$. □

Corollario 1.12. *Ogni valore assoluto su K è equivalente ad uno che soddisfi la disuguaglianza triangolare.*

La proprietà della disuguaglianza triangolare è talmente fondamentale che molti autori la richiedono nella definizione di valore assoluto. Da ora in avanti anche noi la assumeremo sempre valida; d'altronde sostituire un valore assoluto con uno equivalente non ne cambia in modo tangibile la natura, in un senso che sarà presto chiaro.
L'intuizione suggerisce che i valori assoluti con costante $c = 1$ abbiano proprietà radicalmente diverse dagli altri.

Definizione 1.13. Un valore assoluto con costante c è detto ultrametrico se $c = 1$; archimedeo altrimenti.

[1] Per alleggerire la notazione identificheremo sempre gli interi in $\mathbb{Z}$ con la propria immagine in K data dall'omomorfismo canonico (anche nel caso in cui la caratteristica di K sia finita).

Osservazione 1.14. Dati $|\cdot|_1$, $|\cdot|_2$ equivalenti su K, $|\cdot|_1$ è ultrametrico se e solo se lo è $|\cdot|_2$.

Osservazione 1.15. $|\cdot|$ è ultrametrico se e solo se soddisfa la disuguaglianza ultrametrica:

$$\forall\, x, y \in K \ |x+y| \leq \max\{|x|, |y|\}.$$

Osservazione 1.16. Sia $|\cdot|$ ultrametrico, $x, y \in K$. Se $|x| > |y|$ allora $|x+y| = |x|$.

Dimostrazione. Vale $|x+y| \leq |x|$; inoltre $|x| = |x+y-y| \leq \max\{|x+y|, |y|\} = |x+y|$. □

Proposizione 1.17. *Sia $|\cdot|$ valore assoluto su K. Le seguenti sono equivalenti:*

1. *$|\cdot|$ è ultrametrico.*
2. *$n \in \mathbb{Z} \Rightarrow |n| \leq 1$.*
3. *$\exists\, B \in \mathbb{R}$ tale che $n \in \mathbb{Z} \Rightarrow |n| \leq B$.*

Dimostrazione. Consideriamo la catena di implicazioni $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$; l'unica non banale è l'ultima, che ci prepariamo a dimostrare. Comunque presi $n \in \mathbb{N}$ e $x, y \in K$ si ha:

$$|(x+y)|^n \leq \sum_{i=0}^{n} \left| \binom{n}{i} x^i y^{n-i} \right| \leq B \sum_{i=0}^{n} |x|^i |y|^{n-i} \leq B(n+1) \max\{|x|, |y|\}^n.$$

Estraendo la radice $n-$esima e portando al limite $n \to \infty$ si ottiene la tesi (ricordando l'osservazione 1.15). □

Corollario 1.18. *Data F/K estensione di campi, $|\cdot|$ valore assoluto su F è ultrametrico se e solo se lo è la sua restrizione a K.*

Corollario 1.19. *Ogni valore assoluto su un campo di caratteristica prima è ultrametrico.*

Dimostrazione. Se $\mathrm{char}(K) = p$ allora $\mathbb{F}_p \subseteq K$, e ogni valore assoluto su $\mathbb{F}_p$ è banale in virtù del corollario 1.3. □

Definizione 1.20. Dato $|\cdot|$ ultrametrico non banale su K, chiamiamo

$$\mathcal{O} := \{x \in K : |x| \leq 1\}$$

anello di valutazione di $|\cdot|$; definiamo inoltre $\mathcal{M} := \{x \in \mathcal{O} : |x| < 1\}$.

Osservazione 1.21. $\mathcal{O}$ e $\mathcal{M}$ dipendono solo dalla classe di equivalenza di $|\cdot|$.

Proposizione 1.22. *$\mathcal{O}$ è un dominio di integrità locale, con K campo dei quozienti e $\mathcal{M}$ unico ideale massimale.*

Dimostrazione. Si verifica facilmente che $\mathcal{O}$ è un anello (quindi dominio, essendo contenuto in K) e che $\mathcal{M}$ è un suo ideale. E' una banale verifica anche che K sia il suo campo dei quozienti. La massimalità di $\mathcal{M}$ e la località di $\mathcal{O}$ seguono osservando che $\mathcal{M} = \mathcal{O} \setminus \mathcal{O}^*$, con $\mathcal{O}^*$ l'insieme degli invertibili di $\mathcal{O}$. □

Osservazione 1.23. Dati $x, y \in \mathcal{O}$, vale $x \mid y \Leftrightarrow |x| \geq |y|$.

Definizione 1.24. Dato $|\cdot|$ ultrametrico non banale su K e $\mathcal{O}$, $\mathcal{M}$ come in 1.20, definiamo $k := \mathcal{O}/\mathcal{M}$ campo residuo di $|\cdot|$.

1.2 Valori assoluti discreti

Definizione 1.25. $|\cdot|$ valore assoluto su K è detto discreto se il suo gruppo dei valori Γ è un sottoinsieme discreto non banale di $\mathbb{R}^*$.

Osservazione 1.26. Dati $|\cdot|_1$, $|\cdot|_2$ equivalenti, $|\cdot|_1$ è discreto se e solo se lo è $|\cdot|_2$.

Proposizione 1.27. *Ogni $|\cdot|$ valore assoluto discreto è ultrametrico.*

Dimostrazione. Essendo $|\cdot|$ discreto, $\exists\ \delta \in \mathbb{R}$ tale che $\Gamma \cap [1-\delta, 1+\delta] = \{1\}$.
Sia per assurdo $g \in \mathbb{Z}$ tale che $|g| > 1$. Allora, preso $m \in \mathbb{N}$ tale che $|g|^m > \delta^{-1}$, dimostriamo per induzione su $n \in \mathbb{N}$ che

$$|1 + ng^{-m}| = 1$$

per ogni $n \in \mathbb{N}$. Il passo base è banale. Supponiamo l'uguaglianza verificata per n. A meno di passare a un valore assoluto equivalente, possiamo supporre (in virtù del corollario 1.12 e delle osservazioni 1.14 e 1.26) che $|\cdot|$ soddisfi la disuguaglianza triangolare. Allora si ha:

$$1 - \delta < |1 + ng^{-m}| - |g|^{-m} \leq |1 + (n+1)g^{-m}| \leq |1 + ng^{-m}| + |g|^{-m} < 1 + \delta,$$

da cui segue che $|1 + (n+1)g^{-m}| = 1$.
Dimostrato ciò, notiamo che in particolare, per $n = g^m(g-1)$, si ha $|g| = 1$. Assurdo. □

Osservazione 1.28. Vedremo più avanti (corollario 4.7) che il viceversa non è sempre vero.

Proposizione 1.29. *Sia $|\cdot|$ ultrametrico non banale su K, Γ gruppo dei valori, $\mathcal{O}$ l'anello di valutazione, $\mathcal{M}$ il suo massimale, $\mu \in \mathcal{O}$. Le seguenti sono equivalenti:*

1. *$\mathcal{M} = \mu\mathcal{O}$.*
2. *μ è primo in $\mathcal{O}$.*
3. *$|\mu| = \max \Gamma \cap (0,1)$.*
4. *$|\mu|$ genera Γ.*

Dimostrazione. Mostriamo la catena di implicazioni $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$.
$1 \Rightarrow 2$. Banale, ricordando che in un qualsiasi anello ogni ideale massimale è primo.
$2 \Rightarrow 3$. In particolare μ è non invertibile, dunque $|\mu| \in (0,1)$. Quindi, comunque preso $x \in \mathcal{M}$, per $n \in \mathbb{N}$ sufficientemente grande $|\mu| \geq |x|^n$; segue dalla 1.23 e dalla primalità di μ che $|\mu| \geq |x|$.
$3 \Rightarrow 4$. Sia $x \in K \setminus \{0\}$ con $|x| \neq 1$. A meno di prendere l'inverso possiamo supporre $|x| < 1$. Esiste quindi $n \in \mathbb{N}$ tale che $|\mu|^{n+1} < |x| \leq |\mu|^n$. Allora $|\mu| < |x\mu^{-n}| \leq 1$, dunque $|x| = |\mu|^n$.
$4 \Rightarrow 1$. Dato $x \in \mathcal{M}$, esiste $n \geq 1$ tale che $|x| = |\mu|^n$; allora in particolare $\mu^{-1}x \in \mathcal{O}$. □

Definizione 1.30. Dato $|\cdot|$ ultrametrico non banale, $\mu \in \mathcal{O}$ è detto uniformizzante per $|\cdot|$ se soddisfa una delle quattro condizioni equivalenti in 1.29.

Osservazione 1.31. Se μ è uniformizzante per un certo valore assoluto, allora lo è per ogni altro ad esso equivalente.

Proposizione 1.32. *Un valore assoluto ultrametrico non banale è discreto se e solo se ammette un uniformizzante.*

Dimostrazione. Se il gruppo dei valori Γ è discreto e non banale allora $\Gamma \cap (0,1)$ ammette massimo; viceversa se Γ è ciclico allora è discreto. □

Proposizione 1.33. *Sia $|\cdot|$ ultrametrico non banale. $|\cdot|$ è discreto se e solo se l'anello di valutazione $\mathcal{O}$ è a ideali principali; inoltre, in tal caso, dato μ uniformizzante, gli ideali di $\mathcal{O}$ diversi da $\{0\}$ sono tutti e soli quelli della forma $\mu^n\mathcal{O}$ con $n \in \mathbb{N}$.*

Dimostrazione. Se $\mathcal{O}$ è a ideali principali in particolare $\mathcal{M}$ è principale, quindi per la 1.32 $|\cdot|$ è discreto. Supponiamo ora $|\cdot|$ discreto e sia $I \neq \{0\}$ ideale di $\mathcal{O}$. Sia $n \in \mathbb{N}$ tale che $|\mu|^n = \max\{|x| : x \in I\}$. Allora $I \subseteq \mu^n\mathcal{O}$ (1.23); inoltre esiste $x_0 \in I$ tale che $|\mu|^n = |x_0|$, da cui segue l'inclusione opposta. □

Osservazione 1.34. Dato $|\cdot|$ discreto e μ uniformizzante, per ogni $n \in \mathbb{N}$ vale

$$\mathcal{M}^n = \mu^n\mathcal{O} = \{x \in K : |x| \leq |\mu|^n\}.$$

Osservazione 1.35. Dato $|\cdot|$ discreto e μ uniformizzante,

$$\tau_n : \mathcal{O} \to \mathcal{M}^n : x \mapsto \mu^n x$$

è isomorfismo di gruppi per ogni $n \in \mathbb{N}$.

Proposizione 1.36. *Sia $|\cdot|$ discreto su K con μ uniformizzante; siano $\mathcal{O}$ l'anello di valutazione e k il campo residuo. Definiamo, per ogni $n \in \mathbb{N}$, $\tilde{\pi}_n : \mathcal{M}^n \to \mathcal{M}^n/\mathcal{M}^{n+1}$, $\pi : \mathcal{O} \to k$ le proiezioni al quoziente; $\tau_n : \mathcal{O} \to \mathcal{M}^n : x \mapsto \mu^n x$.*
Allora per ogni $n \in \mathbb{N}$ esiste (unico)

$$\psi_n : k \to \mathcal{M}^n/\mathcal{M}^{n+1}$$

isomorfismo di campi tale che $\psi_n \circ \pi = \tilde{\pi}_n \circ \tau_n$.

Dimostrazione. τ_n è surgettiva, dunque lo è $\tilde{\pi}_n \circ \tau_n$; inoltre $\ker(\tilde{\pi}_n \circ \tau_n) = \mathcal{M}$. La tesi segue passando al quoziente. □

Definizione 1.37. $v : K \to \mathbb{Z} \cup \{\infty\}$ surgettiva è detta funzione d'ordine su K se valgono le seguenti:

1. $v(x) = \infty \Leftrightarrow x = 0$.
2. $\forall\ x, y \in K\ v(xy) = v(x) + v(y)$.
3. $\forall\ x, y \in K\ v(x+y) \geq \min\{v(x), v(y)\}$.

Proposizione 1.38. *Dato $|\cdot|$ discreto su K con μ uniformizzante, $v : K \to \mathbb{Z} \cup \{\infty\}$ definita da*

$$v(0) = \infty, \quad |x| = |\mu|^{v(x)} \quad \textit{per } x \in K \setminus \{0\}$$

è funzione d'ordine (che chiameremo indotta da $|\cdot|$).
Viceversa, data $v : K \to \mathbb{Z} \cup \{\infty\}$ funzione d'ordine e $b \in (0,1)$, $|\cdot| : K \to \mathbb{R}_{\geq 0}$ definito da

$$|0| = 0, \quad |x| = b^{v(x)} \quad \textit{per } x \in K \setminus \{0\}$$

è valore assoluto discreto su K (che chiameremo indotto da v con base b).

Dimostrazione. L'enunciato segue facilmente dalle definizioni. □

Osservazione 1.39. La funzione d'ordine indotta da un valore assoluto discreto induce (tutti i) valori assoluti equivalenti a quello dato; viceversa un valore assoluto indotto da una funzione d'ordine induce la funzione d'ordine stessa. In particolare funzioni d'ordine distinte inducono valori assoluti non equivalenti e valori assoluti non equivalenti inducono funzioni d'ordine distinte.

Osservazione 1.40. Sia $|\cdot|$ discreto su K, v funzione d'ordine indotta da $|\cdot|$. Per ogni $n \in \mathbb{N}$ vale $\mathcal{M}^n = \{x \in K : v(x) \geq n\}$ (in particolare $\mathcal{O} = \{x \in K : v(x) \geq 0\}$).

L'introduzione delle funzioni d'ordine è dettata dalla maggiore comodità, in molte circostanze, di lavorare con notazione additiva piuttosto che moltiplicativa; tanto più nei casi in cui non siamo interessati alla base b ma soltanto alla classe di equivalenza.
Concludiamo la sezione con una proposizione utile nello studio della struttura moltiplicativa di un campo, come vedremo più avanti in un caso specifico.

Proposizione 1.41. *Sia $|\cdot|$ discreto su K, $\mathcal{O}$ anello di valutazione. Vale l'isomorfismo di gruppi $K^* \cong \mathbb{Z} \oplus \mathcal{O}^*$.*

Dimostrazione. Sia μ uniformizzante, v funzione d'ordine indotta da $|\cdot|$. È immediato verificare che

$$\varphi : K^* \to \mathbb{Z} \oplus \mathcal{O}^* : x \mapsto \left(v(x), \frac{x}{\mu^{v(x)}} \right)$$

è isomorfismo. □

2 Topologia indotta

Stabilire un valore assoluto su un campo permette di dotarlo, in modo del tutto naturale, di una topologia di spazio metrico coerente con la struttura di campo. Per rendere possibile una forma di analisi, però, è imprescindibile la completezza della metrica. Sorprendentemente sarà sempre possibile estendere campo e valore assoluto (in modo unico) guadagnando la completezza e conservando la coerenza con le operazioni.

2.1 Definizione e prime proprietà

Definizione 2.1. Dato $(K, +, \cdot)$ campo e τ topologia su K, chiamiamo (K, τ) campo topologico se

$$+ : (K^2, \tau^2) \to (K, \tau) : (x, y) \mapsto x + y,$$
$$\cdot : (K^2, \tau^2) \to (K, \tau) : (x, y) \mapsto xy,$$
$$g : (K \setminus \{0\}, \tau) \to (K, \tau) : x \mapsto x^{-1}$$

sono continue. Se inoltre τ è indotta da una distanza d, chiamiamo (K, d) campo topologico metrico.

Proposizione 2.2. *Sia K campo, dotato di un valore assoluto $|\cdot|$ (che soddisfi la disuguaglianza triangolare).*

$$d : K^2 \to \mathbb{R} : (x, y) \mapsto |x - y|$$

è una distanza su K, che rende (K, d) campo topologico metrico.

Dimostrazione. Che d sia una distanza segue immediatamente dalla definizione. Se $|\cdot|$ è banale allora d è la distanza discreta e la tesi è ovvia; altrimenti si verificano facilmente la lipschitzianità della somma e la continuità del prodotto e dell'inverso moltiplicativo. □

Per alleggerire la notazione scriveremo $(K, |\cdot|)$ in luogo di (K, d).

Osservazione 2.3. $|\cdot| : (K, |\cdot|) \to (\mathbb{R}, |\cdot|_\infty)$, con $|\cdot|_\infty$ il valore assoluto euclideo, è lipschitziana (con costante 1).

Proposizione 2.4. *$|\cdot|$ è banale se e solo se la topologia indotta è discreta.*

Dimostrazione. Abbiamo già notato che valori assoluti banali inducono la topologia discreta. Viceversa, se esiste $x \in K$ con $0 < |x| < 1$, allora $\{x^n : n \in \mathbb{N}\} \subset K$ non è chiuso, quindi la topologia indotta non è discreta. □

Proposizione 2.5. *Siano $|\cdot|_1, |\cdot|_2$ valori assoluti non banali su K. Le seguenti sono equivalenti:*

1. $|\cdot|_1 \sim |\cdot|_2$.
2. $|\cdot|_1$, $|\cdot|_2$ *inducono la stessa topologia.*
3. $|x|_1 < 1 \Rightarrow |x|_2 < 1$.
4. $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$.

Dimostrazione. Mostriamo la catena di implicazioni $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$.
$1 \Rightarrow 2$. Basta notare che le palle rispetto alle due distanze sono le stesse.
$2 \Rightarrow 3$. Sia $x \in K$, $|x|_1 < 1$. $\lim_{n\to\infty} |x^n|_1 = 0$, quindi anche $\lim_{n\to\infty} |x^n|_2 = 0$, da cui segue che $|x|_2 < 1$.
$3 \Rightarrow 4$. Supponiamo per assurdo che esista $a \in K$ tale che $|a|_2 < 1$, $|a|_1 \geq 1$. Allora, dato $b \in K$ tale che $|b|_1 < 1$, per n sufficientemente grande si ha $|ba^{-n}|_1 < 1$, $|ba^{-n}|_2 > 1$, contro le ipotesi.
$4 \Rightarrow 1$. Siano $x, y \in K$ tali che $|x|_1 \neq 1$. Allora

$$\forall\, a, b \in \mathbb{Z} \;\; \big(|x^a y^b|_1 < 1 \Leftrightarrow |x^a y^b|_2 < 1 \big),$$

da cui, passando al logaritmo,

$$\forall\, q \in \mathbb{Q} \;\; \big(q \log(|x|_1) + \log(|y|_1) < 0 \Leftrightarrow q \log(|x|_2) + \log(|y|_2) < 0 \big).$$

La precedente vale per continuità anche per ogni q reale.
Quindi $|x|_2 \neq 1$ e

$$\frac{\log(|y|_1)}{\log(|x|_1)} = \frac{\log(|y|_2)}{\log(|x|_2)},$$

ovvero $|y|_1 = |y_2|^\lambda$ con $\lambda := \dfrac{\log(|x|_1)}{\log(|x|_2)}$. □

Osservazione 2.6. $(K, |\cdot|)$ è compatto se e solo se K è finito.

Dimostrazione. Supponiamo K non finito (il viceversa è ovvio). Se $|\cdot|$ è banale allora una qualunque successione iniettiva a valori in K non possiede sottosuccessioni convergenti; altrimenti, dato $x \in K$ tale che $|x| > 1$, basta considerare $(x^n)_{n\in\mathbb{N}}$. □

La topologia indotta da un valore assoluto ultrametrico gode di proprietà sorprendenti.

Proposizione 2.7. *Sia $(K, |\cdot|)$ campo topologico con $|\cdot|$ ultrametrico. Valgono le seguenti:*

1. *Ogni triangolo è isoscele acutangolo. Ovvero, comunque presi $x, y, z \in K$, a meno di riordinarli vale $|x - y| = |y - z| \geq |z - x|$.*

2. *Le palle aperte sono chiuse, le palle chiuse sono aperte. In particolare K è totalmente sconnesso.*

3. *Due palle aperte sono disgiunte oppure una contiene l'altra.*

Dimostrazione. La prima asserzione è la chiave per mostrare le altre due.

1. Siano $x, y, z \in K$. Segue dall'ultrametricità (e dall'osservazione 1.15) che $|z - x| \leq \max\{|x - y|, |y - z|\}$. Se $|x - y| = |y - z|$ si ha subito la tesi; altrimenti possiamo supporre $|x - y| > |y - z|$. Allora $|z - x| = |x - y|$ per quanto osservato nella 1.16.

2. Senza perdita di generalità possiamo limitarci alle palle aperte e chiuse centrate nell'origine, che indichiamo rispettivamente con $B(0,r)$ e $B_+(0,r)$, con $r>0$ raggio.
Sia $x \notin B(0,r)$, $y \in B(x,r)$. Allora, per l'enunciato 1, $|y| = |x| \geq r$. Quindi $B(0,r)$ è chiusa. Supponendo come ulteriore ipotesi $x \in B_+(0,r)$ si ha in particolare $|y| = |x| = r$. Allora $B_+(0,r) \setminus B(0,r)$ è aperta, e di conseguenza lo è anche $B_+(0,r)$. La totale sconnessione di K è un immediato risultato di quanto detto.

3. Sia $x \in K,\ R \geq r > 0$. Consideriamo le palle $B(0,R)$, $B(x,r)$.
Se $|x| \geq R$ abbiamo mostrato nel punto 2 che $B(0,R) \cap B(x,R) = \emptyset$, quindi a fortiori $B(0,R) \cap B(x,r) = \emptyset$.
Se invece $|x| < R$, allora, preso $y \in B(x,r)$, si ha $|y| \leq \max\{|x|, |y-x|\} < R$, quindi $B(x,r) \subseteq B(0,R)$.

□

Prima di parlare di completamenti enunciamo e dimostriamo un teorema spesso utile.

Teorema 2.8 (Artin-Whaples)**.** *Siano $|\cdot|_1$, ..., $|\cdot|_n$ valori assoluti non banali e indipendenti su K. Detta*

$$\omega : K \to K^n : x \mapsto (x, ..., x)$$

l'immersione diagonale, $\omega(K)$ è denso in $\bigotimes_{i=1}^n (K, |\cdot|_i)$.

Dimostrazione. Dimostriamo innanzitutto l'esistenza di θ_1, ..., $\theta_n \in K$ tali che

$$|\theta_i|_i > 1,\ |\theta_i|_j < 1 \ \ \forall\ i \neq j.$$

Possiamo limitarci a dimostrare, per induzione su $n \geq 2$, l'esistenza di θ_1.
Passo base. Per la proposizione 2.5 (precisamente per la contronominale a $3 \Rightarrow 1$) esistono $x, y \in K$ tali che $|x|_1 < 1, |x|_2 \geq 1, |y|_2 < 1, |y|_1 \geq 1$; quindi $x^{-1}y$ soddisfa quanto voluto.
Passo induttivo. Supponiamo che esista θ tale che

$$|\theta|_1 > 1,\ |\theta|_j < 1 \ \ \forall\ j \in \{2, ..., n-1\}$$

sia inoltre z tale che $|z|_1 > 1, |z|_n < 1$ (esiste in virtù del passo base).
Se $|\theta|_n \leq 1$ allora, per m sufficientemente grande, $\theta^m z$ risponde a quanto chiesto.
Se invece $|\theta|_n > 1$, osserviamo che

$$\lim_{m\to\infty} \left|\frac{\theta^m}{1+\theta^m}\right|_j = 1 \ \ \forall\ j \in \{1, n\}, \quad \lim_{m\to\infty} \left|\frac{\theta^m}{1+\theta^m}\right|_j = 0 \ \ \forall\ j \in \{2, ..., n-1\};$$

quindi $\theta^m(1+\theta^m)^{-1}z$, per m abbastanza grande, è ciò che cercavamo.
A questo punto siamo pronti per dimostrare il teorema: comunque preso $(a_1, ..., a_n) \in K^n$ vale infatti, nella metrica prodotto,

$$\lim_{m\to\infty} \omega\left(\sum_{i=1}^n a_i \frac{\theta_i^m}{1+\theta_i^m} \right) = (a_1, ..., a_n).$$

□

2.2 Esistenza e unicità del completamento

Definizione 2.9. Dati $(K, |\cdot|)$, $(K', |\cdot|')$ campi topologici, $(K', |\cdot|')$ è detto completamento di $(K, |\cdot|)$ se valgono le seguenti:

1. $(K', |\cdot|')$ è completo.
2. Esiste $i : K \to K'$ immersione (omomorfismo iniettivo) tale che $|\cdot|' \circ i = |\cdot|$ e $i(K)$ è denso in $(K', |\cdot|')$.

Teorema 2.10 (Esistenza e unicità del completamento)**.** *Ogni $(K, |\cdot|)$ con $|\cdot|$ non banale ammette un completamento $(K', |\cdot|')$.*
Inoltre, se $(K'', |\cdot|'')$ è un altro campo topologico, $(K'', |\cdot|'')$ è completamento di $(K, |\cdot|)$ se e solo se esiste $\varphi : (K', |\cdot|') \to (K'', |\cdot|'')$ isomorfismo tale che $|\cdot|'' \circ \varphi = |\cdot|'$.

Dimostrazione. La dimostrazione è divisa in 4 parti.

Costruzione di $(K', |\cdot|')$. Sia Σ l'anello delle successioni di Cauchy a valori in K (con le operazioni indotte da K componente per componente). Sia $\Sigma_0 \subset \Sigma$ il sottoinsieme delle successioni che tendono a zero. Dalla limitatezza delle successioni di Cauchy segue che Σ_0 è ideale di Σ; inoltre è massimale. Si verifica infatti che una successione in $\Sigma \setminus \Sigma_0$ prende definitivamente valori in $K \setminus \{0\}$, ed è dunque somma di una successione infinitesima e di una invertibile. Possiamo quindi definire $K' = \Sigma/\Sigma_0$.
Chiamiamo $\Pi : \Sigma \to K'$ la proiezione al quoziente. Data $(x)_{n\in\mathbb{N}} \in \Sigma$, per la disuguaglianza triangolare anche $(|x|)_{n\in\mathbb{N}}$ è di Cauchy in $\mathbb{R}$, e per completezza ammette limite, dipendente solo da $\Pi((x)_{n\in\mathbb{N}})$. Si verifica facilmente che

$$|\cdot|' : K' \to \mathbb{R} : \Pi((x_n)_{n\in\mathbb{N}}) \mapsto \lim_{n\to\infty} |x_n|$$

è un valore assoluto non banale su K'.

Costruzione di i. Definiamo

$$i : K \to K' : x \mapsto \Pi((x)_{n\in\mathbb{N}}).$$

Chiaramente i è omomorfismo iniettivo tale che $|\cdot|' \circ i = |\cdot|$. La densità di $i(K)$ in $(K', |\cdot|')$ segue notando che, comunque preso $\Pi((x_n)_{n\in\mathbb{N}}) \in K'$, la successione $(i(x_m))_{m\in\mathbb{N}}$ a valori in $i(K)$ verifica

$$\lim_{m\to\infty} |i(x_m) - \Pi((x_n)_{n\in\mathbb{N}})|' = \lim_{m\to\infty} \lim_{n\to\infty} |x_m - x_n| = 0.$$

Completezza di $(K', |\cdot|')$. Sia $(\sigma_n)_{n\in\mathbb{N}}$ successione di Cauchy a valori in K'.
Per la densità di $i(K)$ in $(K', |\cdot|')$ esiste $(x_n)_{n\in\mathbb{N}}$ a valori in K tale che $(i(x_n) - \sigma_n)_{n\in\mathbb{N}}$ sia infinitesima. Osserviamo innanzitutto che

$$0 \leq \lim_{\min\{n,m\}\to\infty} |x_n - x_m| = \lim_{\min\{n,m\}\to\infty} |i(x_n) - i(x_m)|' \leq$$

$$\leq \lim_{n\to\infty} |i(x_n) - \sigma_n|' + \lim_{\min\{n,m\}\to\infty} |\sigma_n - \sigma_m|' + \lim_{m\to\infty} |\sigma_m - i(x_m)|' = 0,$$

quindi $(x_n)_{n\in\mathbb{N}} \in \Sigma$. Possiamo allora definire $\sigma := \Pi((x_n)_{n\in\mathbb{N}})$. Vale:

$$0 \leq \lim_{n\to\infty} |\sigma_n - \sigma|' \leq \lim_{n\to\infty} |\sigma_n - i(x_n)|' + \lim_{n\to\infty} |i(x_n) - \sigma|' =$$

$$= \lim_{n\to\infty} |\sigma_n - i(x_n)|' + \lim_{n\to\infty} \lim_{m\to\infty} |x_n - x_m| = 0.$$

Segue che $\lim_{n\to\infty} \sigma_n = \sigma$.

Unicità di $(K', |\cdot|')$. Se $\varphi : (K', |\cdot|') \to (K'', |\cdot|'')$ è isomorfismo tale che $|\cdot|'' \circ \varphi = |\cdot|'$, allora $\varphi \circ i$ è isomorfismo tale che $|\cdot|'' \circ \varphi \circ i = |\cdot|$, e $\varphi \circ i(K)$ è denso in $(K'', |\cdot|'')$. Supponiamo ora che $(K'', |\cdot|'')$ sia un altro completamento di $(K, |\cdot|)$, con $j : K \to K''$ immersione. Definiamo

$$\varphi : (K', |\cdot|') \to (K'', |\cdot|'') : \lim_{n\to\infty} i(x_n) \mapsto \lim_{n\to\infty} j(x_n).$$

La buona definizione e l'iniettività di φ seguono dalla densità di $i(K)$ in $(K', |\cdot|')$ e dal fatto che $|\cdot|' \circ i = |\cdot|'' \circ j$; la surgettività dalla densità di $i(K)$ in $(K', |\cdot|')$. La conservazione del valore assoluto è assicurata dalla continuità di $|\cdot|'$, $|\cdot|''$ (2.3); la continuità delle operazioni in $(K', |\cdot|')$, $(K'', |\cdot|'')$, infine, fa sì che φ estenda l'isomorfismo $j \circ i^{-1}$ fra le immagini di K ad un isomorfismo tra K', K''. □

Osservazione 2.11. Siano $(K, |\cdot|)$, $(F, |\cdot|')$ campi topologici ($|\cdot|$ non banale) con $(F, |\cdot|')$ completo, $i : K \to F$ immersione tale che $|\cdot|' \circ i = |\cdot|$. Allora la chiusura topologica di K in $(F, |\cdot|')$, dotata della restrizione di $|\cdot|'$, è completamento di $(K, |\cdot|)$.

Dimostrazione. Segue dalla continuità delle operazioni in $(F, |\cdot|')$ che la chiusura di K in $(F, |\cdot|')$ è campo; è completa con la topologia indotta in quanto chiusa in uno spazio completo. □

Proposizione 2.12. *Sia $(K', |\cdot|')$ completamento di $(K, |\cdot|)$. $|\cdot|'$ è ultrametrico se e solo se lo è $|\cdot|$.*

Dimostrazione. Basta notare che, per il corollario 1.18, chiamando $i : K \to K'$ l'immersione, $|\cdot|'$ è ultrametrico se e solo se lo è la sua restrizione a $i(K)$. □

Lemma 2.13. *Se $|\cdot|$ è ultrametrico su K, data $(x_n)_{n\in\mathbb{N}}$ successione di Cauchy non infinitesima a valori in K, $(|x_n|)_{n\in\mathbb{N}}$ è stazionaria.*

Dimostrazione. Per $\min\{n, m\}$ abbastanza grande vale $|x_n - x_m| < |x_m|$; la tesi segue sulla base dell'osservazione 1.16. □

Corollario 2.14. *Dato $(K', |\cdot|')$ completamento di $(K, |\cdot|)$, se $|\cdot|$ e $|\cdot|'$ sono ultrametrici allora hanno lo stesso gruppo dei valori.*

Dimostrazione. Comunque preso $\sigma = \lim_{n\to\infty} i(x_n) \in K' \setminus \{0\}$, $(|x_n|)_{n\in\mathbb{N}}$ è stazionaria; la tesi segue dalla continuità di $|\cdot|'$. □

Corollario 2.15. *Sia $(K', |\cdot|')$ completamento di $(K, |\cdot|)$ con $|\cdot|$, $|\cdot|'$ ultrametrici. Chiamiamo $i : K \to K'$ l'immersione e $\mathcal{O}$, $\mathcal{O}'$ gli anelli di valutazione rispettivamente di $|\cdot|$, $|\cdot|'$. Allora $i(\mathcal{O})$ è denso in $\mathcal{O}'$.*

Dimostrazione. Comunque preso $\sigma = \lim_{n\to\infty} i(x_n) \in \mathcal{O}' \setminus \{0\}$, $(|x_n|)_{n\in\mathbb{N}}$ è stazionaria; dunque, per la continuità di $|\cdot|'$, $(x_n)_{n\in\mathbb{N}}$ prende definitivamente valori in $\mathcal{O}$. □

Proposizione 2.16. *Sia $(K', |\cdot|')$ completamento di $(K, |\cdot|)$. $|\cdot|'$ è discreto se e solo se lo è $|\cdot|$. Inoltre, in tal caso, μ è uniformizzante per $|\cdot|'$ se e solo se lo è per $|\cdot|$.*

Dimostrazione. Se $|\cdot|$ (oppure $|\cdot|'$) è discreto in particolare è ultrametrico (1.27), quindi per la 2.14 ha lo stesso gruppo dei valori di $|\cdot|'$ (oppure $|\cdot|$). La seconda parte è ancora immediata conseguenza della conservazione del gruppo dei valori. □

Proposizione 2.17. *Sia $(K', |\cdot|')$ completamento di $(K, |\cdot|)$ con $|\cdot|$ ultrametrico. Chiamiamo $\mathcal{O}$ e $\mathcal{O}'$ gli anelli di valutazione rispettivamente di K e K', $\mathcal{M}$ e $\mathcal{M}'$ i rispettivi ideali massimali, k e k' i rispettivi campi residui. Definiamo inoltre $i : \mathcal{O} \to \mathcal{O}'$ l'immersione e $\pi : \mathcal{O} \to k$, $\pi' : \mathcal{O}' \to k'$ le proiezioni al quoziente. Allora esiste (unico)*

$$\phi : k \to k'$$

isomorfismo tale che $\phi \circ \pi = \pi' \circ i$.
Inoltre, se $|\cdot|$ è discreto, chiamando $\pi_n : \mathcal{O} \to \mathcal{O}/\mathcal{M}^n$, $\pi'_n : \mathcal{O}' \to \mathcal{O}'/\mathcal{M}'^n$ le proiezioni al quoziente, per ogni $n \in \mathbb{N}$ esiste (unico)

$$\phi_n : \mathcal{O}/\mathcal{M}^n \to \mathcal{O}'/\mathcal{M}'^n$$

isomorfismo tale che $\phi_n \circ \pi_n = \pi'_n \circ i$.

Dimostrazione. Comunque preso $\sigma \in \mathcal{O}'$, per il corollario 2.15 esiste $x \in \mathcal{O}$ tale che valga $|\sigma - i(x)|' < 1$, quindi $\pi' \circ i$ è surgettiva; inoltre $\ker(\pi' \circ i) = \mathcal{M}$. passando al quoziente si ha la tesi.
Se $|\cdot|$ è discreto, comunque preso $\sigma \in \mathcal{O}'$, per lo stesso corollario (e per l'osservazione 1.34) esiste $x \in \mathcal{O}$ tale che $x - \sigma \in \mathcal{M}'^n$. Si conclude come prima. □

Il completamento che abbiamo costruito esplicitamente ha un evidente difetto, che ci lascia insoddisfatti: non è maneggevole. Possiamo trovare una costruzione più comoda? Per i valori assoluti archimedei la questione avrà un epilogo del tutto inatteso; per i valori discreti la risposta è subito: si. La prossima proposizione ci suggerirà come fare.

Proposizione 2.18. *Sia $(K, |\cdot|)$ campo topologico con $|\cdot|$ discreto, μ uniformizzante, $\mathcal{O}$ anello di valutazione, v funzione d'ordine indotta. Sia $\{0\} \subset \mathcal{R} \subset \mathcal{O}$ un sistema di rappresentanti per il campo residuo k (ovvero l'immagine di una inversa destra della proiezione al quoziente). Dato $x \in K \setminus \{0\}$, esiste unica una successione $(a_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{R}$ tale che:*

$$x = \mu^{v(x)} \sum_{n=0}^{\infty} a_n \mu^n \quad \textit{con} \;\; a_0 \neq 0.$$

Dimostrazione. Siano $\pi : \mathcal{O} \to k$, $\tilde{\pi}_n : \mathcal{M}^n \to \mathcal{M}^n/\mathcal{M}^{n+1}$ le proiezioni al quoziente e $\psi_n : k \to \mathcal{M}^n/\mathcal{M}^{n+1}$ isomorfismo come nella 1.36. Sia $\tilde{x} := \mu^{-v(x)} x \in \mathcal{O} \setminus \mathcal{M}$. Sia $a_0 \in \mathcal{R}$ l'unico rappresentante (non nullo) per $\pi(\tilde{x})$. Dimostriamo per induzione su $n \in \mathbb{N}$ che

$$\tilde{x} - \sum_{i=0}^{n} a_i \mu^i \in \mathcal{M}^{n+1}$$

definendo ricorsivamente $a_{n+1} \in \mathcal{R}$ come l'unico rappresentante per

$$\psi_{n+1}{}^{-1} \circ \tilde{\pi}_{n+1}\left(\tilde{x} - \sum_{i=0}^{n} a_i \mu^i\right).$$

Il passo base è immediato. Supposta verificata la tesi per n, ricordando la 1.36 si ha

$$\tilde{\pi}_{n+1}\left(\tilde{x} - \sum_{i=0}^{n+1} a_i \mu^i\right) = \tilde{\pi}_{n+1}\left(\tilde{x} - \sum_{i=0}^{n} a_i \mu^i\right) - \tilde{\pi}_n \circ \tau_n(a_{n+1}) =$$

$$= \tilde{\pi}_{n+1}\left(\tilde{x} - \sum_{i=0}^{n} a_i \mu^i\right) - \psi_{n+1} \circ \tilde{\pi}(a_{n+1}) = 0.$$

Alla luce della 1.40 si ha quindi

$$v\left(x - \mu^{v(x)} \sum_{i=0}^{n} a_i \mu^i\right) = v\left(\tilde{x} - \sum_{i=0}^{n} a_i \mu^i\right) + v(x) \geq n + 1 + v(x),$$

Da cui segue la convergenza della serie. L'unicità si verifica facilmente. □

Viceversa, non necessariamente tutte le serie della forma descritta convergono; la colpa va attribuita proprio alla non completezza del campo. E allora noi le faremo convergere con la forza.

2.3 Completamento per valori assoluti discreti

Ci sono d'aiuto i seguenti lemmi (il primo dei quali, di cui ora ci serve solo una parte, sarà fondamentale più avanti).

Lemma 2.19. *Sia $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, $(x_n)_{n\in\mathbb{N}}$ a valori in K.*

$$\sum_{n=0}^{\infty} x_n \text{ converge} \quad \Leftrightarrow \quad \lim_{n\to\infty} x_n = 0.$$

Inoltre, in caso di convergenza, vale

$$\left|\sum_{n=0}^{\infty} x_n\right| \leq \max_{n\in\mathbb{N}} |x_n|$$

e, se esiste n_0 tale che $|x_{n_0}| > |x_n|$ per ogni $n \neq n_0$, allora sussiste l'uguaglianza.

Dimostrazione. Chiaramente se la serie converge allora $(x_n)_{n\in\mathbb{N}}$ è infinitesima (qualunque sia il valore assoluto); l'implicazione opposta segue dalla completezza di $(K, |\cdot|)$ e dal fatto che, comunque presi $n < m$, vale

$$\left|\sum_{i=n}^{m} x_i\right| \leq \max_{i\geq n} |x_i|.$$

In particolare

$$\left|\sum_{i=0}^{m} x_i\right| \leq \max_{n\in\mathbb{N}} |x_n|,$$

dunque per la continuità del valore assoluto si ha la disuguaglianza finale. L'uguaglianza sotto la particolare ipotesi indicata segue dall'osservazione 1.16. □

Lemma 2.20. *Sia $(K', |\cdot|')$ completamento di $(K, |\cdot|)$, con i immersione. Data $\sum_{n=0}^{\infty} x_n$ serie convergente in $(K, |\cdot|)$, vale*

$$i\left(\sum_{n=0}^{\infty} x_n\right) = \sum_{n=0}^{\infty} i(x_n).$$

Dimostrazione. Segue dalla continuità di i. □

Lemma 2.21. *Sia $(K, |\cdot|)$ campo topologico con $|\cdot|$ ultrametrico, x in K con $|x| < 1$. Data $(a_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{O}$, con $|a_0| = 1$, se la serie*

$$y := \sum_{n=0}^{\infty} a_n x^n$$

converge allora $|y| = 1$.

Dimostrazione. Chiamando $(y_n)_{n\in\mathbb{N}}$ la successione delle somme parziali, vale $|y_n| = 1$ identicamente (1.16); la tesi segue dalla continuità di $|\cdot|$. □

Proposizione 2.22 (Completamento per i valori assoluti discreti)**.** *Sia $|\cdot|$ discreto su K, μ uniformizzante, $\mathcal{O}$ l'anello di valutazione. Sia $\{0\} \subset \mathcal{R} \subset \mathcal{O}$ un sistema di rappresentanti per il campo residuo. Definiamo formalmente l'insieme*

$$\hat{K} := \{0\} \cup \left\{ \sum_{n=m}^{\infty} a_n \mu^n : m \in \mathbb{Z},\ a_n \in \mathcal{R}\ \forall\ n \geq m,\ a_m \neq 0 \right\}.$$

$\hat{K}$ possiede una naturale struttura di campo che estende K; inoltre

$$\hat{|\cdot|} : K \to \mathbb{R}_{\geq 0} : \quad 0 \mapsto 0, \quad \sum_{n=m}^{\infty} a_n \mu^n \mapsto |\mu|^m$$

è valore assoluto su $\hat{K}$ che estende $|\cdot|$. $(\hat{K}, \hat{|\cdot|})$ è completamento di $(K, |\cdot|)$.

Dimostrazione. Dalla 2.18 segue che $K \subseteq \hat{K}$.
Sia $(K', |\cdot|')$ completamento di $(K, |\cdot|)$, con i immersione. Consideriamo la mappa

$$\hat{i} : \hat{K} \to K' : \quad 0 \mapsto 0, \quad \sum_{n=m}^{\infty} a_n \mu^n \mapsto \sum_{n=m}^{\infty} i(a_n) i(\mu)^n$$

estensione di i (2.20). $|i(\mu)|' < 1$, quindi $\hat{i}$ è ben definita (2.19). i mappa uniformizzanti per $|\cdot|$ in uniformizzanti per $|\cdot|'$ e, in virtù della 2.17, mappa un sistema di rappresentanti per

k in un sistema di rappresentanti per $\mathcal{O}'/\mathcal{M}'$ (campo residuo di K'); alla luce della 2.18, quindi, concludiamo che $\hat{i}$ è bigettiva. Possiamo dunque stabilire su $\hat{K}$ la struttura di campo che rende $\hat{i}$ isomorfismo (e che rende $\hat{K}$ estensione di K, essendo $\hat{i}$ estensione di i). Il lemma 2.21 assicura che $|\hat{\cdot}| = |\cdot| \circ \hat{i}$; dunque $|\hat{\cdot}|$ è valore assoluto ben definito su $\hat{K}$, e inoltre K è denso in $(\hat{K}, |\cdot|)$. La tesi segue dal teorema di unicità del completamento. □

Corollario 2.23. *Sia $(K, |\cdot|)$ campo topologico con $|\cdot|$ discreto, μ uniformizzante. $(K, |\cdot|)$ è completo se e solo se, comunque presa $(a_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{O}$ anello di valutazione, la serie*

$$\sum_{n=0}^{\infty} a_n \mu^n$$

converge.

Dimostrazione. Se tutte le serie della forma descritta convergono allora $(K, |\cdot|)$ è uguale al proprio completamento; l'implicazione opposta è data dal lemma 2.19. □

Adesso abbiamo davanti delle gradevoli serie piuttosto che classi di equivalenza di successioni di Cauchy, e per di più l'immersione nel completamento è ora una tranquilla inclusione. Il problema adesso è la struttura di campo, che esiste (lo abbiamo dimostrato) ma non è esplicita. La prossima proposizione può' esserci d'aiuto.

Proposizione 2.24 (Prodotto di Cauchy)**.** *Sia $(K, |\cdot|)$ campo topologico con $|\cdot|$ ultrametrico, x in K con $|x| < 1$. Date $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ a valori in K, sia $(c_n)_{n\in\mathbb{N}}$ così definita:*

$$c_n = \sum_{i+j=n} a_i b_j.$$

Se le seguenti serie convergono, vale

$$\sum_{n=0}^{\infty} a_n x^n \ \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} c_n x^n.$$

Dimostrazione. Supponiamo che le serie convergano. Per il lemma 2.19, comunque dato $\varepsilon > 0$ esistono $B > 0$ (non dipendende da ε), $N \in \mathbb{N}$; tali che

$$|a_n x^n| < B, \ |b_n x^n| < B \ \ \forall\, n \in \mathbb{N};$$

$$|a_n x^n| < \frac{\varepsilon}{B}, \ |b_n x^n| < \frac{\varepsilon}{B} \ \ \forall\, n \in \mathbb{N}, n > N.$$

Allora per $n > 2N$

$$\left| \sum_{m=0}^{\infty} c_m x^m - \sum_{i=0}^{n} a_i x^i \ \sum_{j=0}^{n} b_j x^j \right| = \left| \sum_{m=0}^{\infty} \sum_{\substack{i+j=m \\ \max\{i,j\}>n}} a_i b_j x^m \right| \leq$$

$$\leq \max_{\substack{m>n \\ i+j=m}} |a_i b_j x^m| \leq \max_{\substack{m\geq 2N \\ i+j=m}} |a_i x^i||b_j x^j| < \varepsilon.$$

Segue la tesi. □

Dunque, dati due elementi

$$\sum_{n=0}^{\infty} a_n\mu^n, \quad \sum_{n=0}^{\infty} b_n\mu^n \in \hat{K}$$

con $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{R}$ (per comodità li prendiamo di valore assoluto 1, ma la generalizzazione è immediata), abbiamo le seguenti scritture per la somma e il prodotto:

$$\sum_{n=0}^{\infty} a_n\mu^n + \sum_{n=0}^{\infty} b_n\mu^n = \sum_{n=0}^{\infty} (a_n + b_n)\mu^n;$$

$$\sum_{n=0}^{\infty} a_n\mu^n \sum_{n=0}^{\infty} b_n\mu^n = \sum_{n=0}^{\infty} c_n\mu^n;$$

con i c_n determinati come descritto nella 2.24.
Questo, però, ci fornisce una descrizione solo parzialmente esplicita della struttura del nostro campo, perché le successioni $(a_n + b_n)_{n\in\mathbb{N}}$, $(c_n)_{n\in\mathbb{N}}$ possono non essere in $\mathcal{R}$. In tal caso, per avere un algoritmo completo che determini la forma canonica di somma e prodotto (e con un po' di lavoro in più, che lasciamo all'intraprendenza del lettore, dell'inverso moltiplicativo) non possiamo prescindere dall'algoritmo descritto nella proposizione 2.18, che può' essere molto semplificato avendo cura di scegliere, in casi specifici, un sistema di rappresentanti abbastanza comodo.
Chiaramente, l'ideale sarebbe poter scegliere un sistema di rappresentanti del campo residuo k che sia chiuso rispetto alle operazioni del campo; ovvero trovare una sezione della proiezione $\pi : \mathcal{O} \to k$. Sfortunatamente in generale non ci riusciamo; vedremo invece più in avanti un importante caso in cui abbiamo fortuna.
Un buon compromesso sarebbe anche un sistema di generatori chiuso per prodotto, ovvero una sezione della proiezione $\pi^* : \mathcal{O}^* \to k^*$; vedremo un esempio anche di questo.

Investighiamo ora in maggior dettaglio la struttura topologica di un campo dotato di un valore assoluto discreto.

2.4 $\mathcal{O}$ come limite proiettivo

Lemma 2.25. *Dato $(K, |\cdot|)$ con $|\cdot|$ discreto, $\{x + \mathcal{M}^n : n \in \mathbb{N}\}$ è sistema fondamentale di intorni di $x \in K$, tutti omeomorfi a $\mathcal{O}$.*

Dimostrazione. $f : \mathcal{O} \to x + \mathcal{M}^n : y \mapsto x + \mu^n y$, con μ uniformizzante, è omeomorfismo. □

Lemma 2.26. *Dato $(K, |\cdot|)$ con $|\cdot|$ discreto, $\mathcal{O}/\mathcal{M}^n$ è discreto rispetto alla topologia quoziente per ogni $n \in \mathbb{N}$.*

Dimostrazione. Le fibre della proiezione al quoziente sono tutte omeomorfe a $\mathcal{O}$ (2.25), che è aperto in $(K, |\cdot|)$ (2.18). □

Lemma 2.27. *Sia $f : X \to Y$ un omomorfismo continuo fra gruppi topologici. f è una mappa aperta se e solo se esiste $\{B_n : n \in \mathbb{N}\}$ sistema fondamentale di intorni di 0 in X tale che $f(B_n)$ sia aperto in Y per ogni $n \in \mathbb{N}$.*

Dimostrazione. Sia $A \subset X$ aperto, $x \in A$. $-x + A$ è aperto e include 0, quindi esiste $n \in \mathbb{N}$ tale che $B_n \subseteq -x + A$. $f(x) + f(B_n) \subset f(A)$, segue che $f(A)$ è intorno di $f(x)$ in Y; data la generalità di $x \in A$ concludiamo che $f(A)$ è aperto. L'implicazione opposta è banale. □

Definizione 2.28. Sia $(A_n)_{n\in\mathbb{N}}$ una successione di anelli topologici, $\lambda_{n,m} : A_n \to A_m$ omomorfismo continuo per ogni $n, m \in \mathbb{N}, n > m$. $((A_n)_{n\in\mathbb{N}}, \{\lambda_{n,m}\})$ è detto sistema inverso di anelli topologici se vale $\lambda_{m,l} \circ \lambda_{n,m} = \lambda_{n,l}$ per ogni $n > m > l$.
Definiamo limite inverso del sistema inverso $((A_n)_{n\in\mathbb{N}}, \{\lambda_{n,m}\})$ l'anello topologico

$$\varprojlim A_n := \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} A_n : \lambda_{n,m}(x_n) = x_m \ \forall\ n > m \right\}.$$

La definizione sussiste per sistemi inversi di semplici anelli o gruppi (nel qual caso i $\lambda_{n,m}$ sono semplici omomorfismi).

Proposizione 2.29. *Sia $(K, |\cdot|)$ completo con $|\cdot|$ discreto, $\mathcal{O}$ l'anello di valutazione, $\mathcal{M}$ il suo massimale. Definendo $\pi_n : \mathcal{O} \to \mathcal{M}^n$ le proiezione al quoziente, per ogni $n > m$ esiste unico $\lambda_{n,m} : \mathcal{O}/\mathcal{M}^n \to \mathcal{O}/\mathcal{M}^m$ omomorfismo tale che $\lambda_{n,m} \circ \pi_n = \pi_m$.*
$((\mathcal{O}/\mathcal{M}^n)_{n\in\mathbb{N}}\{\lambda_{n,m}\})$ è un sistema inverso di anelli topologici; inoltre

$$\varphi : \mathcal{O} \to \varprojlim \mathcal{O}/\mathcal{M}^n : x \mapsto (\pi_n(x))_{n\in\mathbb{N}}$$

è isomorfismo e omeomorfismo.

Dimostrazione. L'esistenza e unicità delle $\lambda_{n,m}$ segue dal fatto che $\ker(\pi_n) \subset \ker(\pi_m)$ per ogni $n > m$. Dati $n > m > l$, si ha:

$$\lambda_{m,l} \circ \lambda_{n,m} \circ \pi_n = \lambda_{m,l} \circ \pi_m = \pi_l = \lambda_{n,l} \circ \pi_n$$

da cui, data l'unicità di $\lambda_{n,l}$, concludiamo che $\lambda_{m,l} \circ \lambda_{n,m} = \lambda_{n,l}$.
La buona definizione di φ segue immediatamente dalla definizione stessa delle $\lambda_{n,m}$; resta da dimostrare che è isomorfismo e omeomorfismo.

$$\ker(\varphi) = \bigcap_{n\in\mathbb{N}} \ker \pi_n = \bigcap_{n\in\mathbb{N}} \mathcal{M}^n = \{0\}.$$

Inoltre, dato $(y_n)_{n\in\mathbb{N}} \in \varprojlim \mathcal{O}/\mathcal{M}^n$, sia $(x_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{O}$ tale che $\pi_n(x_n) = y_n$ per ogni $n \in \mathbb{N}$. Per ogni $n > m$ si ha $\pi_m(x_n) = \lambda_{n,m} \circ \pi_n(x_n) = \pi_m(x_m)$, ovvero $x_n - x_m \in \mathcal{M}^m$. Segue dalla 1.34 che $(x_n)_{n\in\mathbb{N}}$ è di Cauchy, e converge a $x \in \mathcal{O}$. Comunque dato $m \in \mathbb{N}$, per $n > m$ sufficientemente grande $x - x_n \in M^m$; d'altronde $x_n - x_m \in \mathcal{M}^m$, quindi $\pi_m(x) = \pi_m(x_m) = y_m$. Concludiamo che φ è isomorfismo.
Dimostriamo ora che φ è omeomorfismo. Gli spazi metrici $\mathcal{O}/\mathcal{M}^n$ sono discreti (2.26), quindi, per definizione di topologia prodotto, per ogni $m \in \mathbb{N}$ l'insieme

$$V_m := \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathcal{O}/\mathcal{M}^n \;\middle|\; x_n = 0 \ \forall\ n \leq m \right\}$$

è aperto in $\prod_{n\in\mathbb{N}} \mathcal{O}/\mathcal{M}^n$. D'altronde, per ogni $m \in \mathbb{N}$, $\varphi(\mathcal{M}^m) = V_m \cap \varprojlim \mathcal{O}/\mathcal{M}^n$. Segue che φ è aperta (2.27), e dunque omeomorfismo. □

Osservazione 2.30. $\{V_m : m \in \mathbb{N}\}$ è un sistema fondamentale di intorni di 0 in $\varprojlim \mathcal{O}/\mathcal{M}^n$.

Chiudiamo con una caratterizzazione dei campi localmente compatti sotto un valore assoluto ultrametrico.

2.5 Locale compattezza per valori assoluti ultrametrici

Lemma 2.31. *Sia $|\cdot|$ ultrametrico non banale su K, $\mathcal{O}$ anello di valutazione. $(K, |\cdot|)$ è localmente compatto se e solo se $\mathcal{O}$ è compatto con la topologia indotta.*

Dimostrazione. Se K è localmente compatto allora, per $r \in \Gamma$ abbastanza piccolo (con Γ gruppo dei valori), la palla chiusa $\{x \in K : |x| \leq r\}$ è compatta. Dato $\gamma \in K$ tale che $|\gamma| = r$,

$$f : \mathcal{O} \to \{x \in K : |x| \leq r\} : x \mapsto \gamma x$$

è omeomorfismo, dunque $\mathcal{O}$ è compatto.
Viceversa, supponiamo $\mathcal{O}$ compatto. Comunque preso $x \in K$, la traslazione $\tau : \mathcal{O} \to x + \mathcal{O}$ è omeomorfismo; segue la locale compattezza di K. □

Teorema 2.32. *Sia $|\cdot|$ ultrametrico non banale su K, con k campo residuo. $(K, |\cdot|)$ è localmente compatto se e solo se valgono le seguenti:*

1. *$|\cdot|$ è discreto;*
2. *$(K, |\cdot|)$ è completo;*
3. *k è finito.*

Dimostrazione. Supponiamo che $(K, |\cdot|)$ sia localmente compatto, ovvero che l'anello di valutazione $\mathcal{O}$ sia compatto (2.31), e mostriamo una alla volta le tre asserzioni.

1. Se per assurdo $|\cdot|$ non fosse discreto, detto Γ il gruppo dei valori, $\Gamma \cap (0, 1)$ non ammetterebbe massimo per le proposizioni 1.29 e 1.32; ovvero esisterebbe una successione $(x_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{O}$ tale che $(|x_n|)_{n\in\mathbb{N}}$ sia strettamente crescente. Allora (x_n) ammetterebbe una sottosuccessione convergente, contraddicendo il lemma 2.13.

2. Sia $(x_n)_{n\in\mathbb{N}}$ di Cauchy a valori in K. Essendo tale successione limitata, esiste $\gamma \in K$ (di valore assoluto abbastanza piccolo) tale che $(\gamma x_n)_{n\in\mathbb{N}}$, ancora di Cauchy, prenda valori in $\mathcal{O}$. Essendo $\mathcal{O}$ compatto, in particolare è completo; dunque $(\gamma x_n)_{n\in\mathbb{N}}$ converge, così come $(x_n)_{n\in\mathbb{N}}$.

3. Se k non fosse finito, chiamando $\pi : \mathcal{O} \to k$ la proiezione al quoziente, ogni successione $(x_n)_{\in\mathbb{N}}$ a valori in $\mathcal{O}$ tale $\pi \circ x$ sia iniettiva non avrebbe sottosuccessioni convergenti, contro la compattezza di $\mathcal{O}$.

Supponiamo ora che valgano le condizioni $1, 2, 3$ e mostriamo allora la compattezza di $\mathcal{O}$, ovvero la compattezza di $\varprojlim \mathcal{O}/\mathcal{M}^n$ (2.29). Sia dunque $(x_n)_{n\in\mathbb{N}}$ a valori in $\varprojlim \mathcal{O}/\mathcal{M}^n$. Essendo k finito, esiste una sottosuccessione $(x_{l_1(n)})_{n\in\mathbb{N}}$ costante nella prima componente. Supponendo di avere $(x_{l_m(n)})_{n\in\mathbb{N}}$ sottosuccessione costante nelle prime m componenti, osservando che $\ker(\lambda_{m+1,m}) = \mathcal{M}^m/\mathcal{M}^{m+1} \cong k$ (1.36), possiamo estrarre un'ulteriore sottosuccessione $(x_{l_{m+1}(n)})_{n\in\mathbb{N}}$ di $(x_{l_m(n)})_{n\in\mathbb{N}}$ che sia costante nelle prime $m + 1$ componenti. La sottosuccessione diagonale $(x_{l_n(n)})_{n\in\mathbb{N}}$ è convergente (2.30). □

Osservazione 2.33. Ogni campo è localmente compatto rispetto alla topologia indotta dal valore assoluto banale.

3 Valori assoluti archimedei: classificazione

Il lettore avrà notato che fino a questo momento ci siamo poco soffermati sul caso dei valori assoluti archimedei, quasi eludendolo. Nelle prossime pagine scopriremo il sorprendente motivo di tale mancanza di interesse; prima, però, abbiamo bisogno di nuovi strumenti e di ulteriore teoria.

3.1 Norme su spazi vettoriali

Definizione 3.1. Sia V spazio vettoriale su K, $|\cdot|$ valore assoluto non banale su K. $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ è detta norma su V (rispetto a $|\cdot|$) se valgono le seguenti:

1. $\|v\| = 0 \Leftrightarrow v = 0$.
2. $\forall\ x \in K,\ \forall\ v \in V\ \ \|xv\| \leq |x|\|v\|$.
3. $\forall\ v, w \in V\ \ \|v + w\| \leq \|v\| + \|w\|$.

Osservazione 3.2. La condizione 2 è equivalente alla seguente:

$$\forall\ x \in K,\ \forall\ v \in V\ \ \|xv\| = |x|\|v\|.$$

Dimostrazione. Supponendo verificata la 2 in 3.1, presi comunque $x \in K \setminus \{0\}$, $v \in V$ si ha

$$\|xv\| \leq |x|\|v\| \leq |x||x|^{-1}\|xv\| = \|xv\|.$$

□

Osservazione 3.3. Se $\|\cdot\|$ è norma su V rispetto a $|\cdot|$ e W è sottospazio di V, allora la restrizione di $\|\cdot\|$ a W è norma su W rispetto a $|\cdot|$.

Osservazione 3.4. Se $V = K$ l'unica norma ammissibile rispetto a $|\cdot|$, a meno di una costante moltiplicativa, è $|\cdot|$ stesso.

Osservazione 3.5. Dati F/K estensione di campi e $|\cdot|$ valore assoluto su F, $|\cdot|$ è anche norma su F rispetto alla restrizione di $|\cdot|$ a K.

Osservazione 3.6. Dati F/K estensione di campi, $|\cdot|$ valore assoluto su F, V spazio vettoriale su F dotato di norma $\|\cdot\|$ rispetto a $|\cdot|$, $\|\cdot\|$ è norma anche rispetto alla restrizione di $|\cdot|$ a K.

Osservazione 3.7. Se V ha dimensione finita, data una base $\beta = (b_1, ..., b_n)$ di V su K,

$$\|\cdot\| : V \to \mathbb{R} : \sum_{i=1}^{n} x_i b_i \mapsto \max\{|x_i| : 1 \leq i \leq n\}$$

è una norma su V rispetto a $|\cdot|$, che chiamiamo norma del sup (per la base β).

Definizione 3.8. Dato V spazio vettoriale su K, due norme $\|\cdot\|_1,\ \|\cdot\|_2$ su V (rispetto allo stesso valore assoluto) sono dette equivalenti ($\|\cdot\|_1 \sim\ \|\cdot\|_2$) se esiste $c > 0$ tale che valga identicamente

$$\frac{1}{c}\|v\|_2 \leq \|v\|_1 \leq c\|v\|_2.$$

Proposizione 3.9. *Sia V spazio vettoriale su K, $\|\cdot\|$ norma su V.*

$$d : V^2 \to \mathbb{R} : (v, w) \mapsto \|v - w\|$$

è distanza su V, rispetto alla quale le operazioni di somma e moltiplicazione per scalare sono continue.

Dimostrazione. La verifica è semplice e viene omessa. □

Osservazione 3.10. $\|\cdot\| : V \to \mathbb{R}$ è lipschitziana (con costante 1) rispetto alla topologia indotta da $\|\cdot\|$ su V e a quella euclidea su $\mathbb{R}$.

Proposizione 3.11. *Dato V spazio vettoriale su K siano $\|\cdot\|_1$, $\|\cdot\|_2$ norme su V (rispetto allo stesso valore assoluto). Le seguenti sono equivalenti:*

1. $\|\cdot\|_1 \sim \|\cdot\|_2$.
2. $\|\cdot\|_1$, $\|\cdot\|_2$ *inducono la stessa topologia.*
3. *Esiste $\varepsilon > 0$ tale che* $\|v\|_1 \leq \varepsilon \Rightarrow \|v\|_2 \leq 1$; $\|v\|_2 \leq \varepsilon \Rightarrow \|v\|_1 \leq 1$.

Dimostrazione. L'equivalenza $2 \Leftrightarrow 3$ è molto semplice; mostriamo dunque $1 \Leftrightarrow 3$.
$1 \Rightarrow 3$. Basta porre $\varepsilon := c^{-1}$, in riferimento alla definizione 3.8.
$3 \Rightarrow 1$. A meno di prendere un ε minore, possiamo supporre che esista $x \in K$ con $|x| = \varepsilon \in (0, 1)$. Comunque preso $v \in V \setminus \{0\}$ esiste $n \in \mathbb{Z}$ tale che $\varepsilon^{n+1} < \|v\|_1 \leq \varepsilon^n$. Allora $\|vx^{-n+1}\|_1 \leq \varepsilon$, dunque $\|vx^{-n+1}\|_2 \leq 1$; segue che $\|v\|_1 > \varepsilon^{n+1} \geq \varepsilon^2 \|v\|_2$. Intercambiando le norme si ha la disuguaglianza opposta. Dunque $\|\cdot\|_1 \sim \|\cdot\|_2$ con costante $c := \varepsilon^{-2}$. □

Proposizione 3.12. *Se $(K, |\cdot|)$ è completo, dato V spazio vettoriale su K di dimensione finita, tutte le norme su V rispetto a $|\cdot|$ sono equivalenti. Inoltre V è completo con la topologia indotta da ognuna di esse.*

Dimostrazione. Dimostriamo la tesi per induzione su $n := \dim(V)$. Se $n = 1$ la tesi è banale (3.4). Supponiamola verificata per $n - 1$.
Sia $\beta = (b_1, ..., b_n)$ base di V su K, $\|\cdot\|_\beta$ norma del sup per β. Osserviamo preliminarmente che V è completo con la topologia indotta da $\|\cdot\|_\beta$. Infatti, data una successione $\left(\sum_{i=1}^n y_{i,m} b_i\right)_{m\in\mathbb{N}}$ a valori in V di Cauchy rispetto a $\|\cdot\|_\beta$, è immediato verificare che per ogni $1 \leq i \leq n$ la successione $(y_{i,m})_{m\in\mathbb{N}}$ è di Cauchy in $(K, |\cdot|)$ e dunque convergente a un certo y_i; inoltre

$$\lim_{m\to\infty} \left\| \sum_{i=1}^n y_{i,m} b_i - \sum_{i=1}^n y_i b_i \right\|_\beta = \lim_{m\to\infty} \max_{1\leq i\leq n} |y_{i,m} - y_i| = 0.$$

Dimostriamo ora che qualunque altra norma $\|\cdot\|$ su V (rispetto a $|\cdot|$) è equivalente a $\|\cdot\|_\beta$. Per ogni $v \in V$ vale

$$\|v\| \leq \left(\sum_{i=1}^n \|b_i\| \right) \|v\|_\beta.$$

Resta da verificare l'esistenza di una costante $c > 0$ tale che $\|v\|_\beta \leq c\|v\|$ per ogni $v \in V$. Supponiamo per assurdo che ciò non sia vero, ovvero che esista una successione

$$(v_m)_{m\in\mathbb{N}} = \left(\sum_{i=1}^{n} x_{1,m} b_i\right)_{m\in\mathbb{N}}$$

a valori in $V \setminus \{0\}$ tale che

$$\lim_{m\to\infty} \frac{\|v_m\|}{\|v_m\|_\beta} = 0.$$

A meno di passare ad una sottosuccessione e di riordinare i vettori di β, possiamo supporre che valga $|x_{1,m}| = \|v_m\|_\beta$ per ogni $m \in \mathbb{N}$. Allora

$$\lim_{m\to\infty} \left\| \frac{v_m}{x_{i,m}} \right\| = 0,$$

dunque la successione $(w_m)_{m\in\mathbb{N}} := (x_{1,m}^{-1} v_m)_{m\in\mathbb{N}}$ converge a 0 nella topologia indotta da $\|\cdot\|$. Segue in particolare che $(b_1 - w_m)_{m\in\mathbb{N}}$, che prende valori nel sottospazio W di V generato dai vettori $(b_2, ..., b_n)$, è di Cauchy. Per ipotesi induttiva W è completo con la topologia indotta dalla restrizione di $\|\cdot\|$ a W (3.3), perciò $(b_1 - w_m)_{m\in\mathbb{N}}$ converge in W; si trova l'assurdo notando che, però, il suo limite è b_1. □

Corollario 3.13. *Data F/K estensione finita e $(K, |\cdot|)$ completo, esiste al più un valore assoluto su F che estenda $|\cdot|$.*

Dimostrazione. Siano $|\cdot|'$, $|\cdot|''$ valori assoluti su F che estendano $|\cdot|$. $|\cdot|'$, $|\cdot|''$ sono norme equivalenti su F rispetto a $|\cdot|$ (3.5), dunque inducono la stessa topologia su F (3.11); ne segue che sono equivalenti anche come valori assoluti (2.5) e, coincidendo su K, sono uguali. □

Lemma 3.14. *Data A algebra [2] su K e $\|\cdot\|$ norma submoltiplicativa [3] su A, le operazioni di prodotto di algebra e inverso moltiplicativo (definito sul gruppo degli invertibili di A) sono continue rispetto alla topologia indotta da $\|\cdot\|$.*

Dimostrazione. Presi $x,\ y,\ \delta_x,\ \delta_y \in A$ si ha

$$\|xy - (x+\delta_x)(y+\delta_y)\| \leq \|x\|\|\delta_x\| + \|y\|\|\delta_y\| + \|\delta_x\|\|\delta_y\|;$$

ciò prova la continuità del prodotto.
Consideriamo ora l'inverso moltiplicativo. Siano $x, \delta \in A$; supponiamo che $x, x+\delta$ siano invertibili e che $\|\delta\|\|x^{-1}\| < 1$. Allora

$$\left\|\frac{1}{x} - \frac{1}{x+\delta}\right\| \left(\frac{1}{\|\delta\|\|x^{-1}\|} - 1\right) \leq \left\|\left(\frac{1}{x} - \frac{1}{x+\delta}\right)\frac{x}{\delta}\right\| - \left\|\frac{1}{x} - \frac{1}{x+\delta}\right\| =$$

$$= \left\|\frac{1}{x+\delta}\right\| - \left\|\frac{1}{x} - \frac{1}{x+\delta}\right\| \leq \left\|\frac{1}{x}\right\| \leq \|1\|\|x^{-1}\|;$$

[2] Sottintendiamo (sempre) che sia associativa, commutativa e con identità.
[3] Ovvero tale che $\|xy\| \leq \|x\|\|y\|$ per ogni $x, y \in A$.

ovvero

$$\left\| \frac{1}{x} - \frac{1}{x+\delta} \right\| \leq \frac{\|1\|\|\delta\|\|x^{-1}\|^2}{1 - \|\delta\|\|x^{-1}\|},$$

da cui segue la continuità dell'inverso. □

Osservazione 3.15. Data A algebra di dimensione finita su K e $|\cdot|$ non banale su K, esiste sempre una norma submoltiplicativa su A rispetto a $|\cdot|$.

Dimostrazione. Presa $\beta = (b_1, ..., b_n)$ base di A su K e $\|\cdot\|_\beta$ norma del sup rispetto a β, si verifica facilmente che

$$\|\cdot\| : A \to \mathbb{R} : \ x \mapsto \|x\|_\beta \sum_{i=1}^{n} \sum_{j=1}^{n} \|b_i b_j\|_\beta$$

è una norma equivalente a $\|\cdot\|_\beta$ che soddisfa la disuguaglianza voluta. □

Teorema 3.16 (Gelfand-Mazur)**.** *Sia A un'algebra su $\mathbb{R}$, dotata di una norma $\|\cdot\|$ submoltiplicativa rispetto al valore assoluto euclideo. Supponiamo che esista $j \in A$ tale che $j^2+1=0$ e chiamiamo $C := \mathbb{R} + \mathbb{R}j$. Allora per ogni $x \in A \setminus \{0\}$ esiste $z \in C$ tale che $x - z$ non sia invertibile in A.*
In particolare se A è campo allora $A = C$.

Dimostrazione. Notiamo innanzitutto che $C \cong \mathbb{C}$; in particolare C è campo e, in virtù delle proposizioni 3.12, 3.11, la topologia indotta su C da $\|\cdot\|$ è quella euclidea abituale. Nel seguito faremo dunque uso delle proprietà topologiche proprie di $\mathbb{C}$, quali la locale compattezza e la connessione.
Supponiamo per assurdo che esista $a \in A$ tale che $z-a$ sia invertibile per ogni $z \in C$. Allora

$$f : C \to \mathbb{R} : \ z \mapsto \|(z-a)^{-1}\|$$

è continua per la continuità somma (3.9), inverso moltiplicativo (3.14) e norma (3.10). Inoltre

$$\lim_{z\to\infty} f(z) \leq \lim_{z\to\infty} \left\| \frac{1}{z} \right\| \lim_{z\to\infty} \left\| \left(1 - \frac{a}{z}\right)^{-1} \right\| = 0,$$

essendo il primo limite nullo (perché lo è in $\mathbb{C}$ con la topologia euclidea) e valendo il secondo 1 per la continuità del prodotto in A e dell'inverso moltiplicativo. Dunque f assume massimo M. Arriveremo ad un assurdo, data la connessione di C, mostrando che la controimmagine di M (non vuota, chiusa e limitata) è aperta.
Sia $z_0 \in f^{-1}(M)$. Vogliamo mostrare che la palla in C (rispetto alla distanza euclidea) di centro z_0 e raggio $\|(z_0-a)^{-1}\|^{-1}$ è contenuta in $f^{-1}(M)$. A tal fine, dato $r > 0$ reale tale che $r\|(z_0-a)^{-1}\| < 1$, per ogni $n \in \mathbb{N}$ consideriamo il polinomio

$$g_n(X) = X^n - r^n = \prod_{i=0}^{n-1} (X - r\xi_n^i) \in A[X],$$

dove ξ_n, in analogia con $\mathbb{C}$, definisce una radice n-esima primitiva dell'unità.
Si ha

$$\frac{g_n'(X)}{g_n(X)} = \frac{nX^{n-1}}{X^n - r^n} = \sum_{i=0}^{n-1} \frac{1}{X - r\xi_n^i}.$$

Valutando in $z_0 - a$, otteniamo

$$S_n := \frac{1}{n} \sum_{i=0}^{n-1} \frac{1}{z_0 - a - r\xi_n^i} = \frac{1}{z_0 - a - r(r(z_0 - a)^{-1})^{n-1}}.$$

Dunque, ricordando che $r\|(z_0-a)^{-1}\| < 1$ (e usando ancora la continuità di somma e inverso), concludiamo che

$$\lim_{n\to\infty} \|S_n\| = f(z_0) = M.$$

Supponiamo per assurdo che esista $\gamma \in C$, di norma euclidea unitaria, tale che $f(z_0 + r\gamma) < M$. Allora, per continuità di f, esiste $\varepsilon > 0$ e un intorno di $z_0 + r\gamma$ la cui immagine sia contenuta in $(0, M - \varepsilon)$. In particolare è facile convincersi che, definendo t_n la cardinalità dell'insieme

$$\{i : f(z_0 - r\xi_n^i) < M - \varepsilon\} \subset \{0, ..., n-1\},$$

esiste una costante $c > 0$ tale che si abbia definitivamente

$$\frac{t_n}{n} > c.$$

Dunque, per n sufficientemente grande, vale la stima

$$\|S_n\| = \left\| \frac{1}{n} \sum_{i=0}^{n-1} \frac{1}{z_0 - a - r\xi_n^i} \right\| \leq \frac{1}{n} \sum_{i=0}^{n-1} f(z_0 - r\xi_n^i) <$$

$$< \frac{1}{n}\big(t_n(M - \epsilon) + (n - t_n)M\big) < M - c,$$

in contraddizione con quanto asserito precedentemente.
Concludiamo che $f^{-1}(M)$ è non vuoto, chiuso, aperto e limitato, contro la connessione di C. Ancora una volta, assurdo. □

Corollario 3.17 (Teorema fondamentale dell'algebra)**.** $\mathbb{C}$ *è algebricamente chiuso.*

Dimostrazione. Sia $K/\mathbb{C}$ estensione algebrica. Comunque preso $x \in K$, alla luce dell'osservazione 3.15, possiamo trovare una norma submoltiplicativa su $\mathbb{C}(x)$ rispetto al valore assoluto euclideo di $\mathbb{R}$. Possiamo allora applicare il teorema concludendo che $\mathbb{C}(x) = \mathbb{C}$; data l'arbitrarietà di $x \in K$, segue che $K = \mathbb{C}$. □

Abbiamo tutto ciò che ci serve (e più) per fornire, in un certo senso, una completa classificazione dei valori assoluti archimedei.

3.2 Classificazione dei valori assoluti archimedei

Definizione 3.18. Chiamiamo $|\cdot|_\infty$ il valore assoluto archimedeo standard su $\mathbb{C}$; ne denotiamo allo stesso modo la restrizione a $\mathbb{R}$ e a $\mathbb{Q}$.[4]

La seguente osservazione, sebbene ovvia, è utile perché sarà centrale in alcune future dimostrazioni.

Osservazione 3.19. Dato A dominio e K campo dei quozienti, valori assoluti su K che coincidano su A sono uguali.

Lemma 3.20. *Ogni valore assoluto archimedeo su $\mathbb{Q}$ è equivalente a $|\cdot|_\infty$.*

Dimostrazione. Sia $|\cdot|$ archimedeo su $\mathbb{Q}$. Per quanto visto nella 1.17, esiste $g \in \mathbb{N}$ con $|g| > 1$. Comunque preso $x \in \mathbb{N},\ x > 1$, esistono unici $n \in \mathbb{N},\ a_0, ..., a_n \in \mathbb{N}$ tali che:

$$g = \sum_{i=0}^{n} a_i x^i, \quad a_i < x \ \forall\ i \in \{0, ..., n\},\ a_n \neq 0.$$

Posto $c := \max\{|j| : j \in \mathbb{N}, 0 < j < x\}$, vale

$$|g| \leq c \sum_{i=0}^{n} |x|^i \leq c(n+1)\max\{1,\ |x|^n\} \leq c\left(\frac{\log(g)}{\log(x)} + 1\right)\max\left\{1,\ |x|^{\frac{\log(g)}{\log(x)}}\right\}.$$

In particolare, comunque preso $m \in \mathbb{N}$, si ha

$$|g|^m \leq c\left(\frac{m\log(g)}{\log(x)} + 1\right)\max\left\{1,\ |x|^{\frac{m\log(g)}{\log(x)}}\right\}.$$

Estraendo la radice $m-$esima, al limite per $m \to \infty$ si ottiene

$$|g| \leq \max\left\{1,\ |x|^{\frac{\log(g)}{\log(x)}}\right\};$$

ovvero, essendo $g > 1$,

$$|g| \leq |x|^{\frac{\log(g)}{\log(x)}}.$$

Segue in particolare che $|x| > 1$. Possiamo quindi intercambiare $g,\ x$ nella disuguaglianza precedente, ottenendo

$$|x|^{\frac{1}{\log(x)}} = |g|^{\frac{1}{\log(g)}} =: e^\lambda,$$

ovvero $|x| = |x|_\infty^\lambda$ identicamente su $\mathbb{N}$, dunque su tutto $\mathbb{Z}$. Tenendo a mente l'osservazione 3.19, concludiamo che $|\cdot| \sim |\cdot|_\infty$. □

Lemma 3.21. *Data $(K, |\cdot|)$ estensione $(\mathbb{R}, |\cdot|_\infty)$, esiste $i : K \to \mathbb{C}$ immersione tale che $|\cdot|_\infty \circ i = |\cdot|$.*

[4] Chiamare un valore assoluto ed una sua restrizione nello stesso modo è una scelta convenzionale (che attueremo ancora) che non genera confusione in un lettore attento; il campo in questione sarà sempre chiaro dal contesto.

Dimostrazione. Preso j in un'estensione di K tale che $j^2+1=0$, esiste una norma $\|\cdot\|$ submoltiplicativa su $K(j)$ rispetto a $|\cdot|$ (3.15). Possiamo applicare il teorema 3.16 considerando $\|\cdot\|$ come norma rispetto a $|\cdot|_\infty$ (3.22), concludendo che $K(j)=\mathbb{R}(j)\cong\mathbb{C}$; abbiamo dunque trovato un'immersione $i:K\to\mathbb{C}$, tale che $|\cdot|_\infty\circ i=|\cdot|$ (3.13). □

Teorema 3.22 (Classificazione dei valori assoluti archimedei)**.** *Dato $|\cdot|$ archimedeo su K, esiste $i:K\to\mathbb{C}$ immersione tale che $|\cdot|_\infty\circ i\sim|\cdot|$ e, in caso di completezza di $(K,|\cdot|)$, tale che $i(K)=\mathbb{R}$ oppure $i(K)=\mathbb{C}$.*

Dimostrazione. Sia $(K',|\cdot|')$ completamento di $(K,|\cdot|)$, con i immersione. $\mathrm{char}(K')=0$ (1.19), dunque a meno di cambiare completamento possiamo assumere che $Q\subset K'$. La restrizione di $|\cdot|'$ a $\mathbb{Q}$ è un valore assoluto archimedeo su $\mathbb{Q}$ (1.18), ovvero $|\cdot|_\infty^\lambda$ per qualche $\lambda>0$ (3.20). La chiusura topologica di $\mathbb{Q}$ in $(K',|\cdot|'^{-\lambda})$ è completamento di $(\mathbb{Q},|\cdot|_\infty)$ (2.11), come anche $(\mathbb{R},|\cdot|_\infty)$; dunque possiamo assumere che $\mathbb{R}\subseteq K'$ (e $|\cdot|'^{-\lambda}$ estenda $|\cdot|_\infty$ su $\mathbb{R}$). Concludiamo per il lemma 3.21 che $K'=\mathbb{R}$ oppure (a meno di cambiare ancora una volta completamento) $K'=\mathbb{C}$, e in entrambi i casi $|\cdot|'=|\cdot|_\infty^\lambda$. Segue in particolare che $|\cdot|_\infty\circ i\sim|\cdot|'\circ i=|\cdot|$. Osserviamo infine che se $(K,|\cdot|)$ è completo allora i è isomorfismo, dunque $i(K)=K'$. □

Corollario 3.23. *Sia $K:=\mathbb{Q}(\alpha)$ campo di numeri. Sia $f(X)\in\mathbb{Q}[X]$ polinomio minimo di α su $\mathbb{Q}$. Siano α_1, ..., α_n le radici di $f(X)$ contenute nel semipiano complesso $\{z\in\mathbb{C}:\mathrm{Im}(z)\geq 0\}$. Allora esistono esattamente n possibili valori assoluti archimedei $|\cdot|_1$, ..., $|\cdot|_n$ indipendenti su K; precisamente*

$$|\cdot|_j:K\to\mathbb{R}:h(\alpha)\mapsto|h(\alpha_j)|_\infty$$

per ogni $j\in\{1,\ldots,n\}$, e $h(X)$ variabile in $\mathbb{Q}[X]$.

Dimostrazione. Sia $|\cdot|$ valore assoluto archimedeo su K. Per il teorema di classificazione esiste $i:K\to\mathbb{C}$ immersione tale che $|\cdot|_\infty\circ i\sim|\cdot|$. Sappiamo che immersioni di K in $\mathbb{C}$ sono tutte e sole quelle della forma

$$i:K\to\mathbb{C}:h(\alpha)\to h(\alpha')$$

con α' radice di $f(X)$ e $h(X)$ variabile in $\mathbb{Q}[X]$; inoltre α' è radice di $f(X)$ se e solo se lo è $\overline{\alpha'}$, e notiamo che

$$|h(\alpha')|_\infty=|h(\overline{\alpha'})|_\infty\ \ \forall\ h(X)\in\mathbb{Q}[X].$$

Concludiamo che i possibili valori assoluti archimedei su K, a meno di equivalenza, sono proprio $|\cdot|_1$, ..., $|\cdot|_n$. Resta da verificarne l'indipendenza. Essendo tutti estensione di $|\cdot|_\infty$ su $\mathbb{Q}$, sono indipendenti se e solo se sono a due a due distinti. Siano $j,l\in\{1,\ldots,n\}$ tali che $|\cdot|_j=|\cdot|_l$; dunque comunque presi $x,y\in\mathbb{Q}$ si ha

$$(x+\alpha_j y)(x+\overline{\alpha}_j y)=(x+\alpha_l y)(x+\overline{\alpha}_l y);$$

ovvero

$$2xy(\mathrm{Re}(\alpha_j)-\mathrm{Re}(\alpha_l))+y^2(|\alpha_j|_\infty^2-|\alpha_l|_\infty^2)=0$$

Data la generalità di x,y, ricordando che α_j,α_l hanno parte immaginaria non negativa, concludiamo che sono uguali. □

Corollario 3.24. *Sia K campo di numeri. $|\cdot|_\infty$ su $\mathbb{Q}$ ammette un'unica estensione ad un valore assoluto su K se e solo se $K = \mathbb{Q}(\sqrt{-n})$ per qualche $n \in \mathbb{N}$ libero da quadrati.*

Osservazione 3.25. Alla luce degli ultimi risultati, notiamo che l'ipotesi di completezza in 3.12 non è ridondante.

Concludiamo con la controparte archimedea del teorema 2.32.

Proposizione 3.26. *Sia $|\cdot|$ archimedeo K. $(K, |\cdot|)$ è localmente compatto se e solo se è completo.*

Dimostrazione. Se $(K, |\cdot|)$ è completo, allora, per il teorema precedente, è omeomorfo a $\mathbb{R}$ o a $\mathbb{C}$ e dunque è localmente compatto.
Supponiamo ora che $(K, |\cdot|)$ sia localmente compatto. Allora per r abbastanza piccolo la palla chiusa di centro 0 e raggio r è compatta, in particolare completa. Si conclude riscalando ogni successione di Cauchy a valori in K per un fattore di valore assoluto abbastanza piccolo, come nella dimostrazione del teorema 2.32. □

4 Estensioni

È naturale chiedersi se ci sia un modo di estendere un valore assoluto ad un'estensione del campo. Affronteremo prima il caso di estensioni algebriche di campi completi, che ci riserveranno una piacevole sorpresa.
Seguiranno alcune considerazioni sulle estensioni puramente trascendenti di campi sotto valori assoluti ultrametrici, a conclusione delle quali esibiremo degli esempi di valori assoluti ultrametrici che non siano discreti.

4.1 Estensioni algebriche di campi completi

Presentiamo innanzitutto un utile lemma, noto (così come una diversa versione, che vedremo più avanti) sotto il nome di lemma di Hensel.

Lemma 4.1 (Hensel)**.** *Sia $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, $\mathcal{O}$ l'anello di valutazione, k il campo residuo. Definiamo $\pi : \mathcal{O} \to k$ la proiezione al quoziente e $\hat{\pi} : \mathcal{O}[X] \to k[X]$ la riduzione modulo l'ideale massimale. Sia $f \in \mathcal{O}[X]$ tale che valga*

$$\hat{\pi}(f)(X) = \bar{g}(X)\bar{h}(X)$$

per due polinomi coprimi $\bar{g}(X), \bar{h}(X) \in k[X]$.
Allora esistono $g(X), h(X) \in \mathcal{O}[X]$ tali che:

$$\hat{\pi}(g)(X) = \bar{g}(X); \quad \hat{\pi}(h)(X) = \bar{h}(X);$$

$$\deg(g) = \deg(\bar{g});$$
$$f(X) = g(X)h(X).$$

Dimostrazione. Definiamo $d := \deg(f),\ m := \deg(\bar{g})$.
Siano $g_0(X), h_0(X) \in \mathcal{O}[X]$ con $\deg(g_0) = m$, $\deg(h_0) \leq d - m$, tali che

$$\hat{\pi}(g_0)(X) = \bar{g}(X),\ \hat{\pi}(h_0)(X) = \bar{h}(X).$$

Essendo $\bar{g}(X), \bar{h}(X)$ coprimi, esistono $a(X), b(X) \in \mathcal{O}[X]$ tali che

$$a(X)g_0(X) + b(X)h_0(X) \equiv 1 \pmod{\mathcal{M}},$$

con $\mathcal{M}$ l'ideale massimale di $\mathcal{O}$. Sia $\gamma \in \mathcal{M}$ tale che

$$f(X) - g_0(X)h_0(X) \equiv 0 \pmod{\gamma\mathcal{O}};$$

$$a(X)g_0(X) + b(X)h_0(X) - 1 \equiv 0 \pmod{\gamma\mathcal{O}}$$

(γ può' essere scelto ad esempio fra i coefficienti dei due polinomi appena considerati, purché abbia valore assoluto massimo). Vogliamo determinare ricorsivamente delle successioni $(g_n(X))_{n\in\mathbb{N}}$, $(h_n(X))_{n\in\mathbb{N}}$ a valori in $\mathcal{O}[X]$ che soddisfino le condizioni

$$g_n(X) = \sum_{i=0}^{n} \gamma^i p_i(X), \qquad h_n(X) = \sum_{i=0}^{n} \gamma^i q_i(X),$$

$$f(X) - g_n(X)h_n(X) = \gamma^{n+1} f_n(X)$$

per opportune successioni $(p_i(X))_{i\in\mathbb{N}},\ (q_i(X))_{i\in\mathbb{N}},\ (f_n(X))_{n\in\mathbb{N}}$ in $\mathcal{O}[X]$ con

$$\deg(p_i) < m, \quad \deg(q_i) \leq d - m \quad \forall\ i \in \mathbb{N}_{>0}.$$

$g_0(X)$, $h_0(X)$ sono stati già scelti opportunamente.
Supponiamo di aver determinato $g_{n-1}(X), h_{n-1}(X)$.
Siano $\tau(X),\ p_n(X) \in K[X]$ quoziente e resto della divisione euclidea

$$b(X)f_{n-1}(X) = \tau(X)g_0(X) + p_n(X).$$

Dato che $\hat{\pi}(g_0)(X) = \bar{g}(X)$ e $\deg(g_0) = \deg(\bar{g})$, il coefficiente direttivo di $g_0(X)$ è in $\mathcal{O}^*$; ne consegue che $\tau(X) \in \mathcal{O}[X]$; dunque anche $p_n(x) \in \mathcal{O}[X]$.
Sia inoltre $q_n(X) \in \mathcal{O}[X]$ di grado minimo che soddisfi

$$q_n(X) \equiv a(X)f_{n-1}(X) + \tau(X)h_0(X) \pmod{\gamma\mathcal{O}}.$$

Mostriamo che i polinomi

$$g_n(X) := g_{n-1}(X) + \gamma^n p_n(X), \quad h_n(X) := h_{n-1}(X) + \gamma^n q_n(X)$$

soddisfano quanto richiesto. Si ha

$$f(X) - g_n(X)h_n(X) \equiv \gamma^n\big(f_{n-1}(X) - g_{n-1}(X)q_n(X) - h_{n-1}(X)p_n(X)\big) \pmod{\gamma^{n+1}\mathcal{O}};$$

d'altronde, notando che

$$g_{n-1}(X) \equiv g_0(X),\ h_{n-1}(X) \equiv h_0(X) \pmod{\gamma\mathcal{O}},$$

e usando tutte le equazioni in nostro possesso, otteniamo

$$f_{n-1}(X) \equiv \big(a(X)g_0(X) + b(X)h_0(X)\big)f_{n-1}(X) \equiv$$
$$\equiv g_0(X)\big(a(X)f_{n-1}(X) + \tau(X)h_0(X)\big) + h_0(X)p_n(X) \equiv$$
$$\equiv g_0(X)q_n(X) + h_0(X)p_n(X) \equiv$$
$$\equiv g_{n-1}(X)q_n(X) + h_{n-1}(X)p_n(X) \pmod{\gamma\mathcal{O}};$$

ovvero

$$f(X) - g_n(X)h_n(X) \equiv 0 \pmod{\gamma^{n+1}\mathcal{O}}.$$

Dato che

$$\deg(p_n) < \deg(g_0) = m$$

per definizione, resta solo da verificare la condizione sul grado di $g_n(X)$.
Per ipotesi induttiva $\deg(p_i) < m$ per ogni $0 < i < n$, dunque $\deg(g_{n-1}) = \deg(g_0) = m$; inoltre $\deg(q_i) \leq d - m$ per ogni $0 \leq i < n$, quindi $\deg(h_{n-1}) \leq d - m$. Allora, ricordando che $\gamma^n f_{n-1}(X) = f(X) - g_{n-1}(X)h_{n-1}(X)$, si ha $\deg(f_{n-1}) \leq d$. A questo punto è facile, usando la minimalità di $\deg(q_n)$ e l'equazione (già provata)

$$f_{n-1}(X) - g_0(X)q_n(X) - h_0(X)p_n(X) \equiv 0 \pmod{\gamma\mathcal{O}},$$

concludere che

$$\deg(q_n) \leq d - m,$$

come si voleva.
Finalmente abbiamo tutto ciò che ci serve per dimostrare il lemma.
Di seguito, la convergenza di polinomi in $\mathcal{O}[X]$ sarà intesa coeffiente per coefficiente.
Abbiamo già notato che $\deg(g_n) = m$, $\deg(h_n) \leq d - m$ identicamente. Le successioni $(g_n(X))_{n\in\mathbb{N}}$, $(h_n(X))_{n\in\mathbb{N}}$ sono di Cauchy (coefficiente per coefficiente) e dunque, data la completezza di K e la chiusura di $\mathcal{O}$ in esso, sono ben definiti

$$g(X) := \lim_{n\in\mathbb{N}} g_n(X),\ h(X) := \lim_{n\in\mathbb{N}} h_n(X) \in \mathcal{O}[X],$$

con $\deg(g_n) = m$ (in quanto $\deg(p_n) < m$ per ogni $n > 1$) e $\deg(h_n) \leq d - m$.
Infine, usando la linearità dell'operatore di limite, si verifica facilmente che

$$g(X)h(X) = \lim_{n\to\infty} g_n(X)h_n(X) = f(X),$$

il ché conclude la dimostrazione del lemma di Hensel. □

Corollario 4.2. *Sia $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, $\mathcal{O}$ l'anello di valutazione. Sia $f(X) \in \mathcal{O}[X]$ irriducibile di grado n, con $\max_{0\leq i\leq n} |f_i| = 1$.*[5] *Allora*

$$\max\{|f_0|, |f_n|\} = 1.$$

Dimostrazione. Chiamando $r := \min\{0 \leq i \leq n : |f_i| = 1\}$, si ha

$$\hat{\pi}(f)(X) = X^r \bar{h}(X),$$

con

$$\bar{h}(X) = \sum_{i=0}^{n-r} \pi(f_i + r)X^i.$$

Essendo $\pi(f_r) \neq 0$, i polinomi X^r, $\bar{h}(X)$ sono coprimi in $k[X]$; dunque, per il lemma di Hensel, esiste $g(X) \in \mathcal{O}[X]$, di grado r, che divide $f(X)$. Essendo $f(X)$ irriducibile, deve valere $r \in \{0, n\}$. □

Corollario 4.3. *Sia $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, $\mathcal{O}$ l'anello di valutazione. Sia $f(X) \in K[X]$ monico irriducibile. Se $|f_0| \leq 1$ allora $f(X) \in \mathcal{O}[X]$.*

Teorema 4.4. *Data F/K estensione algebrica e $(K, |\cdot|)$ completo,*

$$|\cdot|' : F \to \mathbb{R} : x \to |N_{K(x)/K}(x)|^{1/[K(x):K]}$$

è valore assoluto su F ed è l'unico che estenda $|\cdot|$. $|\cdot|'$ è ultrametrico se e solo se lo è $|\cdot|$; inoltre se l'estensione è finita allora $(F, |\cdot|')$ è ancora completo.

[5] Qui e nel seguito, per semplicità notazionale, chiameremo sempre i coefficienti di un polinomio con lo stesso nome della serie stessa (ad esempio $(f_n)_{n\in\mathbb{N}}$ sarà la successione dei coefficienti di $f(X)$).

Dimostrazione. L'unicità dell'estensione segue dal corollario 3.13, notando che vale su $K(x)/K$ per ogni $x \in F$. Mostriamone dunque l'esistenza.
Se $|\cdot|$ è archimedeo allora, tenendo a mente i risultati della precedente sezione (in particolare i teoremi 3.22 e 3.17), ci si accorge facilmente che F è estensione algebrica propria di K solo nel caso in cui, a meno di isomorfismi, $K = \mathbb{R}$ e $F = \mathbb{C}$. In tal caso $|\cdot| = |\cdot|_\infty^\lambda$ per qualche $\lambda > 0$, ed è immediato verificare che $|\cdot|' = |\cdot|_\infty^\lambda$ su $\mathbb{C}$.
Supponiamo ora $|\cdot|$ ultrametrico. Vogliamo dimostrare che:

1. $x \in K \to |x|' = |x|$;
2. $|x|' = 0 \Leftrightarrow x = 0$;
3. $\forall\ x, y \in F\ |xy|' = |x|'|y|'$;
4. $|x|' \leq 1 \Rightarrow |1 + x|' \leq 1$.

Le prime tre condizioni seguono banalmente dalle proprietà di N, osservando che

$$|xy|' \ = \ |N_{K(xy)/K}(xy)|^{1/[K(xy):K]} \ =$$

$$= \ |N_{K(xy)/K}(x)|^{1/[K(xy):K]} \ |N_{K(xy)/K}(y)|^{1/[K(xy):K]} \ =$$

$$= \ |N_{K(x)/K}(x)|^{1/[K(x):K]} \ |N_{K(y)/K}(y)|^{1/[K(y):K]} \ = \ |x|'|y|'.$$

Resta da mostrare la quarta. Se $|x|' \leq 1$, ovvero $|N_{K(x):K}(x)| \leq 1$, allora per il corollario 4.3 x è nella chiusura integrale di $\mathcal{O}$ in $K(x)$; lo è dunque anche $1 + x$; in particolare $|N_{K(x):K}(1 + x)| \leq 1$, ovvero $|1 + x|' \leq 1$.

Notiamo infine che, nel caso in cui F/K sia estensione finita, la completezza di $(F, |\cdot|')$ segue ancora dalla 3.12. □

4.2 Estensioni trascendenti

Consideriamo ora un fissato un campo K dotato di un valore assoluto ultrametrico $|\cdot|$ (non necessariamente completo).

Proposizione 4.5. *Comunque preso $c \in \mathbb{R}_{>0}$, esiste $|\cdot|'$ valore assoluto ultrametrico su $K(X)$, estensione di $|\cdot|$, tale che $|X|' = c$.*

Dimostrazione. Definiamo così $|\cdot|' : K(X) \to \mathbb{R}_{>0}$:

$$0 \mapsto 0;$$

$$\sum_{i=0}^{n} f_i(X) \mapsto \max_{0 \leq i \leq \deg(f)} c^i |f_i| \quad \forall\ f(X) \in K[X] \setminus \{0\};$$

$$\frac{f(X)}{g(X)} \mapsto \frac{|f(X)|'}{|g(X)|'} \quad \forall\ f(X), g(X) \in K[X] \setminus \{0\}.$$

Comunque presi $f(X), g(X) \in K[X] \setminus \{0\}$, con $n := \deg(f)$, $m := \deg(g)$, vale

$$|f(X)g(X)|' = \max_{0\le l\le n+m} c^l \left| \sum_{i+j=l} f_i g_j \right| \le$$

$$\le \max_{0\le i\le n} c^i |f_i| \max_{0\le j\le m} c^j |g_j| = |f(X)|'|g(X)|'.$$

D'altronde, definendo $r \in \{0, ..., n\}$ $s \in \{0, ..., m\}$ come i minimi indici tali che valga

$$|f(X)|' = c^r |f_r|; \quad |g(X)|' = c^s |g_s|,$$

si ha

$$|f(X)g(X)|' = \max_{0\le l\le n+m} c^l \left| \sum_{i+j=l} f_i g_j \right| \ge$$

$$\ge c^{r+s} \left| \sum_{i+j=r+s} f_i g_j \right| = c^{r+s} |f_r||g_s| = |f(X)|'|g(X)|'.$$

La penultima uguaglianza si ottiene ricordando la 1.16 e notando che, presa una coppia di indici $(i,\, j) \neq (r,\, s)$ tale che $i + j = r + s$, vale $i < r$ oppure $j < s$, quindi si ha

$$|f_i||g_j| < |f_r||g_s|.$$

Abbiamo dunque mostrato la moltiplicatività di $|\cdot|'$ su $K[X]$, dalla quale segue la buona definizione di $|\cdot|$ (nonché la moltiplicatività) su tutto $K(X)$.
Si verifica molto facilmente, infine, che

$$|f(X) + g(X)|' \le \max\{|f(X)|', |g(X)|'\};$$

è immediato dedurne, usando la moltiplicatività, la validità della disuguaglianza ultrametrica su tutto $K(X)$. □

Corollario 4.6. *Comunque presa $(c_n)_{n\in\mathbb{N}}$ una successione di reali positivi, esiste $|\cdot|'$ valore assoluto ultrametrico su $K(\{X_n : n \in \mathbb{N}\})$ tale che*

$$|X_n|' = c_n \quad \forall\ n \in \mathbb{N}.$$

Dimostrazione. Una facile induzione mostra, per ogni $n > 1$, l'esistenza di $|\cdot|_n$ valore assoluto su $K(X_1, ..., X_n)$, estensione di $|\cdot|_{n-1}$ (ponendo $|\cdot|_1 = |\cdot|$), tale che $|X_n| = c_n$. Allora

$$|\cdot|' := \bigcup_{n>0} |\cdot|_n$$

è valore assoluto ben definito su $K(\{X_n : n \in \mathbb{N}\})$, che soddisfa quanto richiesto. □

Corollario 4.7. *Esiste $(F, |\cdot|')$ estensione di $(K, |\cdot|)$ tale che $|\cdot|'$ sia ultrametrico non discreto.*

Dimostrazione. Segue dal precedente ponendo $F := K(\{X_n : n \in \mathbb{N}\})$, scegliendo $(c_n)_{n\in\mathbb{N}}$ convergente non infinitesima. □

5 Funzioni d'ordine $\mathfrak{p}$-adiche

La trattazione sui valori assoluti ultrametrici è stata finora piuttosto astratta e priva di esempi concreti. Adesso che abbiamo alle spalle un apparato teorico soddisfacente possiamo iniziare a scendere gradualmente nel particolare. In questa sezione descriveremo una tecnica per fabbricare letteralmente valori assoluti discreti, avendo a disposizione un dominio a ideali principali. Quanto vedremo troverà immediata applicazione in due diverse direzioni, entrambe di importanza capitale.

Proposizione 5.1. *Sia A dominio a ideali principali, $\mathcal{P}$ insieme degli ideali primi di A, K campo dei quozienti. Per ogni $\mathfrak{p} \in \mathcal{P}$ esiste unica $v_\mathfrak{p}$ funzione d'ordine su K tale che per ogni $x \in A \setminus \{0\}$ valga*

$$xA = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(x)}.$$

Inoltre, dato $\mu \in A$ generatore di $\mathfrak{p}$, μ è uniformizzante per ogni valore assoluto indotto da $v_\mathfrak{p}$. Infine, dati $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathcal{P}$ distinti, $v_{\mathfrak{p}_1}$ e $v_{\mathfrak{p}_2}$ inducono valori assoluti su K non equivalenti.

Dimostrazione. La dimostrazione è molto semplice ed è omessa. Se $\mathfrak{p}_1 \neq \mathfrak{p}_2$ allora $v_{\mathfrak{p}_1}, v_{\mathfrak{p}_2}$ sono distinte, quindi inducono valori assoluti distinti (1.39). □

Nei prossimi enunciati sia A un dominio a ideali principali con campo dei quozienti K, $\mathfrak{p}$ un suo ideale primo, $v_\mathfrak{p}$ la funzione d'ordine (che chiamiamo $\mathfrak{p}$-adica) definita nella 5.1, $\mathcal{O}$ l'anello di valutazione per $v_\mathfrak{p}$, $\mathcal{M}$ il suo ideale massimale, k il campo residuo.

Lemma 5.2. *Chiamando $j : A \to \mathcal{O}$ l'inclusione e $\bar{\pi} : A \to A/\mathfrak{p}$, $\pi : \mathcal{O} \to k$ le proiezioni al quoziente, esiste (unico) $\varphi : A/\mathfrak{p} \to k$ isomorfismo tale che $\varphi \circ \bar{\pi} = \pi \circ j$.*

Dimostrazione. Sia $\mu \in A$ tale che $\mathfrak{p} = \mu A$, $\mathcal{M} = \mu\mathcal{O}$ (5.1, 1.33). Comunque dato $a/b \in \mathcal{O} \setminus \mathcal{M}$, con $a \in A,\ b \in A \setminus \mathfrak{p}$, per la massimalità di $\mathfrak{p}$ esiste $c \in A$ tale che $bc - 1 \in \mathfrak{p}$. Si ha $abc - a \in \mu A$, ovvero $ac - a/b \in \mu\mathcal{O}$. Quindi $\pi \circ j$ è surgettiva; inoltre $\ker(\pi \circ j) = \mathfrak{p}$. Passando al quoziente si ha la tesi. □

Lemma 5.3. *A è denso nell'anello di valutazione $\mathcal{O}$.*

Dimostrazione. Per il lemma 5.2 esiste $\{0\} \subset \mathcal{R} \subset A$ sistema di rappresentanti per il campo residuo k. Dunque, preso $x \in \mathcal{O}$, per la 2.18 esiste $(a_n)_{n\in\mathbb{N}}$ a valori in A tale che

$$x = \sum_{n=0}^{\infty} a_n \mu^n$$

La tesi segue notando che la successione delle somme parziali prende valori in A. □

Proposizione 5.4. *Chiamando $j : A \to \mathcal{O}$ l'inclusione e $\bar{\pi}_n : A \to A/\mathfrak{p}^n$, $\pi_n : \mathcal{O} \to \mathcal{O}/\mathcal{M}^n$ le proiezioni al quoziente, per ogni $n \in \mathbb{N}$ esiste (unico) $\varphi_n : A/\mathfrak{p}^n \to \mathcal{O}/\mathcal{M}^n$ isomorfismo tale che $\varphi \circ \bar{\pi}_n = \pi_n \circ j$.*

Dimostrazione. Comunque preso $x \in \mathcal{O}$, per il lemma 5.3 (e il corollario 1.34) esiste $a \in A$ tale che $a - x \in \mathcal{M}^n$. Quindi $\pi_n \circ j$ è surgettiva; inoltre $\ker(\pi_n \circ j) = \mathfrak{p}^n$. Passando al quoziente si ha la tesi. □

Corollario 5.5. *Sia $(K', |\cdot|'_{\mathfrak{p}})$ completamento di $(K, |\cdot|_{\mathfrak{p}})$ con i immersione, $\mathcal{O}'$ anello di valutazione in K', $\mathcal{M}'$ suo massimale. Allora $i(A)$ è denso in $\mathcal{O}'$; inoltre, per ogni $n \in \mathbb{N}$, $A/\mathfrak{p}^n \cong \mathcal{O}'/\mathcal{M}'^n$.*

Dimostrazione. La densità di $i(A)$ in $\mathcal{O}'$ è immediata conseguenza della densità di A in $\mathcal{O}$ (5.3) e della densità di $i(\mathcal{O})$ in $\mathcal{O}'$ (2.15). L'isomorfismo $A/\mathfrak{p}^n \cong \mathcal{O}'/\mathcal{M}'^n$ segue da 2.17, 5.4. □

Proposizione 5.6. *Sia A dominio a ideali principali con K campo dei quozienti, $|\cdot|$ valore assoluto non banale su K. Se $|x| \leq 1$ per ogni $x \in A$ allora $|\cdot|$ è discreto e induce la funzione d'ordine $v_{\mathfrak{p}}$ per qualche $\mathfrak{p} \in A$ ideale primo.*

Dimostrazione. $\mathbb{N} \subset A$, quindi per la 1.17 $|\cdot|$ è ultrametrico. Segue che $\mathfrak{p} := \{x \in A : |x| < 1\}$ è un ideale primo non banale di A; poniamo $\mathfrak{p} =: pA$. Dato che $|x| = 1$ per ogni $x \in A \setminus M$, comunque preso $y \in A$ si ha $|y| = |p|^{v_{\mathfrak{p}}(y)}$, dunque $|\cdot|$ coincide su A con il valore assoluto indotto da $v_{\mathfrak{p}}$ con base $|p|$. Segue la tesi (3.19, 1.39). □

Come anticipato, presentiamo subito due fondamentali applicazioni della tecnica che abbiamo descritto, l'importanza delle quali è tale da giustificare la grande attenzione che abbiamo mostrato, finora, nei riguardi dei valori assoluti discreti.

5.1 Valori assoluti p-adici

Definizione 5.7. Dato $p \in \mathbb{N}$ primo, chiamiamo $p-$adica la funzione d'ordine v_p su $\mathbb{Q}$ associata all'ideale $p\mathbb{Z}$ come descritto nella 5.1; chiamiamo altresì $p-$adico il valore assoluto discreto $|\cdot|_p$ su $\mathbb{Q}$ indotto da v_p, con base convenzionalmente $1/p$.

Proposizione 5.8. *$|\cdot|_p$ ha uniformizzante p e campo residuo (isomorfo a) $\mathbb{F}_p$.*
Inoltre, dati p_1, p_2 primi distinti, $|\cdot|_{p_1}, |\cdot|_{p_2}$ sono non equivalenti.

Dimostrazione. Diretta applicazione di 5.1, 5.2. □

Il prossimo teorema completa la classificazione dei valori assoluti su $\mathbb{Q}$.

Teorema 5.9 (Ostrowsky)**.** *Dato $|\cdot|$ valore assoluto non banale su $\mathbb{Q}$, vale $|\cdot| \sim |\cdot|_\infty$ oppure $|\cdot| \sim |\cdot|_p$ per qualche p primo.*

Dimostrazione. Se $|\cdot|$ è archimedeo allora $|\cdot| \sim |\cdot|_\infty$ (3.20); altrimenti $|x| \leq 1$ per ogni $x \in \mathbb{Z}$ (1.17), quindi per la 5.6 vale $|\cdot| \sim |\cdot|_p$ per qualche p primo. □

Definizione 5.10. Dato p primo, chiamiamo $(\mathbb{Q}_p, |\cdot|_p)$ il completamento di $(\mathbb{Q}, |\cdot|_p)$ e $\mathbb{Z}_p$ l'anello di valutazione di $\mathbb{Q}_p$.

Proposizione 5.11. *$|\cdot|_p$ su $\mathbb{Q}_p$ ha uniformizzante p e campo residuo (isomorfo a) $\mathbb{F}_p$; l'insieme $\{i : 0 \leq i < p\} \subset \mathbb{Z}_p$ è un sistema di rappresentanti per $\mathbb{F}_p$.*
$\mathbb{Q}_p$ è localmente compatto, $\mathbb{Z}_p$ è compatto; $\mathbb{Z}$ è denso in $\mathbb{Z}_p$.
Inoltre $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ per ogni $n \in \mathbb{N}$.

Dimostrazione. Immediata conseguenza di 2.16, 2.17, 2.32, 5.5 (salvo la semplice verifica che l'insieme indicato è sistema di rappresentanti). □

Un modo classico di costruire $\mathbb{Q}_p$ è quello descritto nella proposizione 2.22 scegliendo come sistema di rappresentanti gli interi fra 0 e $p-1$; vedremo che sono possibili scelte più interessanti.

L'importanza dei valori assoluti p-adici risiede, in parte, nella seguente:

Proposizione 5.12. *Sia $|\cdot|$ ultrametrico su K di caratteristica 0. Allora $(K, |\cdot|)$ è estensione di $(\mathbb{Q}, |\cdot|_p)$; inoltre se $(K, |\cdot|)$ è completo è anche estensione di $(\mathbb{Q}_p, |\cdot|_p)$. Le estensioni sono intese a meno di isomorfismo.*

Dimostrazione. Se $\mathrm{char}(K) = 0$ allora K contiene (a meno di isomorfismo) $\mathbb{Q}$ e la restrizione di $|\cdot|$ a $\mathbb{Q}$ è ultrametrica (1.18); si conclude con il teorema di Ostrowsky (5.9). Se $(K, |\cdot|)$ è completo allora la chiusura topologica di $\mathbb{Q}$ in $(K, |\cdot|)$, con la restrizione di $|\cdot|$, è completamento di $(\mathbb{Q}, |\cdot|_p)$ (2.11); segue la tesi. □

Approfondiremo questo argomento più avanti; adesso veniamo alla seconda applicazione.

5.2 Serie formali di potenze

Consideriamo un campo K e chiamiamo $K[X]$, $K(X)$ rispettivamente l'anello dei polinomi in un'indeterminata su K e il campo delle funzioni razionali in una indeterminata su K. [6]

Lemma 5.13. *Esiste unica la funzione d'ordine v_∞ su $K(X)$ tale che per ogni $f \in K[X]$ valga $v_\infty(f) = \deg(f)$.*

Dimostrazione. Dati $f \in K[X]$, $g \in K[X] \setminus \{0\}$, deve valere

$$v_\infty\left(\frac{f(X)}{g(X)}\right) = \deg(f) - \deg(g).$$

D'altronde è banale verificare che la funzione così definita è funzione d'ordine su $K(X)$. □

Teorema 5.14. *Ogni valore assoluto su $K(X)$ la cui restrizione a K sia banale è discreto e induce v_∞ oppure la funzione d'ordine $v_\mathfrak{p}$ associata a qualche ideale primo $\mathfrak{p}$ di $K[X]$ (definita come nella 5.1).*

Dimostrazione. Sia $|\cdot|$ valore assoluto su $K(X)$, banale su K. In particolare $|\cdot|$ è ultrametrico su K, quindi per la 1.18 lo è anche su $K(X)$. Se $|X| \leq 1$ allora, per ultrametricità, $|f(X)| \leq 1$ per ogni $f(X) \in K[X]$; quindi per la 5.6 $|\cdot|$ è discreto e induce $v_\mathfrak{p}$ per qualche $\mathfrak{p}$ ideale primo di $K[X]$.
Se invece $|X| > 1$ allora $|f(X^{-1})| \leq 1$ per ogni $f(X) \in K[X]$, e in particolare $|f(X^{-1})| = 1$ per ogni $f \in K[X] \setminus XK[X]$; segue che, comunque preso $g(X) \in K[X]$, vale $|g(X)| = |X|^{\deg(g)}$. Dunque $|\cdot|$ coincide su $K[X]$ con il valore assoluto indotto da v_∞ con base $|X|$, di conseguenza è discreto e induce v_∞ (3.19, 1.39). □

Osservazione 5.15. Se K è algebricamente chiuso allora gli ideali primi di $K[X]$ sono tutti e soli quelli della forma $(X - x)X[X]$ per $x \in K$; esiste quindi, in tal caso, una naturale corrispondenza biunivoca fra i valori assoluti di $K[X]$ e i punti del proiettivo $\mathbb{P}^1(K)$.

[6] Useremo sempre la convenzione di riservare le lettere maiuscole (solo) alle varie variabili indeterminate.

Definizione 5.16. Sia $|\cdot|_0$ il valore assoluto su $K(X)$ indotto dalla funzione d'ordine associata all'ideale $XK[X]$ di $K[X]$, con base convenzionalmente $1/2$.

Proposizione 5.17. *$|\cdot|_0$ ha uniformizzante X e campo residuo (isomorfo a) K.*

Dimostrazione. Come per la 5.8. □

Definizione 5.18. Definiamo $(K((X)), |\cdot|_0)$ il completamento di $(K(X), |\cdot|_0)$ e $K[[X]]$ l'anello di valutazione. $K[[X]]$ e $K((X))$ sono chiamati rispettivamente anello delle serie formali di potenze e campo delle serie formali di Laurent (in un'indeterminata su K).

Proposizione 5.19. *$|\cdot|_0$ su $K((X))$ ha uniformizzante X e campo residuo (isomorfo a) K; $K \subset K[[X]]$ è un sistema di rappresentanti per il campo residuo.*
$K((X))$ è localmente compatto (ovvero $K[[X]]$ è compatto) se e solo se K è finito; $K[X]$ è denso in $K[[X]]$.
Inoltre $K[X]/X^nK[X] \cong K[[X]]/X^nK[[X]]$ per ogni $n \in \mathbb{N}$.

Dimostrazione. Come per la 5.11. □

La costruzione standard di $K((X))$ è quella descritta nella proposizione 2.22 scegliendo come sistema di rappresentanti il campo K, isomorfo al campo residuo. Abbiamo già accennato ai vantaggi pratici di avere un sistema di rappresentanti chiuso rispetto alle operazioni del campo; in particolare abbiamo a disposizione semplici algoritmi, già descritti, per il calcolo dei coefficienti di somme e prodotti a partire da quelli di addendi e fattori (anche il calcolo dell'inverso moltiplicativo non presenta alcuna difficoltà).

L'importanza delle serie formali di potenze e di Laurent, evidente in ogni ambito dell'analisi, sarà resa intuibile nella prossima sezione.

6 Valori assoluti ultrametrici: analisi elementare

Abbiamo finalmente tutti gli strumenti per iniziare a parlare, in modo elementare e introduttivo, di analisi su campi completi sotto valori assoluti ultrametrici.

6.1 Funzioni definite da serie formali di potenze

Consideriamo un fissato $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, e sia $\mathcal{O}$ l'anello di valutazione.

Definizione 6.1. Data $f(X) \in K[[X]]$, l'insieme $\mathcal{D} \subset K$ dei punti x tali che la serie [7]

$$\sum_{n\in\mathbb{N}} f_n x^n$$

converga è detto dominio di convergenza di $f(X)$ su K (rispetto a $|\cdot|$).

In analogia con i polinomi, si usa denotare la funzione

$$f : \mathcal{D} \to K : x \mapsto \sum_{n\in\mathbb{N}} f_n x^n,$$

definita dalla serie formale $f(X)$, con la stessa lettera con cui denotiamo la serie formale stessa; sarà chiaro dal contesto ciò a cui ci riferiamo.

Definizione 6.2. Data $f(X) \in K[[X]]$, chiamiamo

$$R := \left(\limsup_{n\to\infty} \left(|f_n|^{1/n}\right) \right)^{-1} \in [0, +\infty]$$

raggio di convergenza di $f(X)$ su K (rispetto a $|\cdot|$).

Proposizione 6.3. *Sia $f(X) \in K[[X]]$, $\mathcal{D} \subseteq K$ il dominio di convergenza di $f(X)$, R il raggio di convergenza.*

1. *Se $R = 0$ allora $\mathcal{D} = \{0\}$.*
2. *Se $R = \infty$ allora $\mathcal{D} = K$.*
3. *Se $R \in (0, \infty)$ e $\lim_{n\to\infty} |f_n| R^n = 0$ allora $\mathcal{D} = \{x \in K : |x| \leq R\}$.*
4. *Altrimenti $\mathcal{D} = \{x \in K : |x| < R\}$.*

Dimostrazione. Se $R = \infty$, ovvero $(f_n^{1/n})_{n\in\mathbb{N}}$ è infinitesima, lo è anche $(f_n b^n)_{n\in\mathbb{N}}$ per qualunque $b \in K$. Supponiamo ora R finito e sia $b \in K$. Se $|b| < R$, valendo $|f_n|^{1/n} R \leq 1$ definitivamente, si ha

$$\lim_{n\to\infty} f_n b^n = \lim_{n\to\infty} (|f_n|^{1/n} R)^n \left(\frac{|b|}{R}\right)^n = 0.$$

Se invece $|b| > R$ allora $|f_n|^{1/n}|b| > 1$ per infiniti valori di n, dunque non c'è convergenza. Il caso $|b| = R$, infine, è diretta applicazione del lemma 2.19. □

[7] come per i polinomi, chiameremo sempre i coefficienti di una serie formale di potenze con lo stesso nome della serie stessa.

Corollario 6.4. *Data $f(X) \in K[[X]]$ con dominio di convergenza $\mathcal{D}$, si ha*

$$\mathcal{O} \subseteq \mathcal{D} \Leftrightarrow \lim_{n\to\infty} f_n = 0.$$

Lemma 6.5. *Siano $f(X),\ g(X) \in K[[X]]$ aventi domini di convergenza $\mathcal{D}_1$, $\mathcal{D}_2$. Sia $\mathcal{D}_3$ il dominio di convergenza di $f(X)g(X)$ e $h : \mathcal{D}_3 \to K$ la funzione da essa definita. Allora*

$$\mathcal{D}_1 \cap \mathcal{D}_2 \subseteq \mathcal{D}_3;$$

$$h(x) = f(x)g(x) \quad \forall\ x \in \mathcal{D}_1 \cap \mathcal{D}_2.$$

Dimostrazione. Sia $(c_n)_{n\in\mathbb{N}}$ a valori in K così definita:

$$c_n = \sum_{i+j=n} f_i g_j.$$

Dato $x \in \mathcal{D}_1 \cap \mathcal{D}_2$, per la proposizione 2.24 si ha

$$f(x)g(x) = \sum_{n\in\mathbb{N}} c_n x^n;$$

ancora per la 2.24, applicata questa volta in $K((X))$, si ha

$$f(X)g(X) = \sum_{n\in\mathbb{N}} c_n X^n;$$

segue la tesi. □

Lemma 6.6. *La funzione definita da una serie formale di potenze con raggio di convergenza non nullo è continua in* 0.

Dimostrazione. Data $f(X) \in K[[X]]$, di raggio R, sia $b \in K$ tale che $|b| < R$. $f(b)$ converge e vale

$$|f(b) - f(0)| = \left|\sum_{n=1}^{\infty} f_n b^n\right| \leq \max_{n\geq 1} |f_n||b|^n \leq \frac{|b|}{R} \max_{n\geq 1}(|f_n|^{1/n}R)^n.$$

Valendo definitivamente $|f_n|^{1/n}R \leq 1$, tale massimo esiste. Segue la tesi. □

Proposizione 6.7. *La funzione definita da una serie formale di potenze con raggio di convergenza non nullo è continua su tutto il dominio di convergenza.*

Dimostrazione. Sia $\mathcal{D}$ il dominio di convergenza di $f(X) \in K[[X]]$; sia $x \in \mathcal{D}$. Vogliamo dimostrare che $f(X)$ è continua in x. Se $x = 0$ la tesi è già dimostrata (6.6); supponiamo dunque $x \neq 0$. Sia $y \in \mathcal{D}$ tale che $|x-y| < |x|$; dunque in particolare $|x| = |y|$ (1.16). Allora, ricordando il lemma 2.19, si ha:

$$|f(x) - f(y)| \leq \max_{n\in\mathbb{N}} |f_n x^n - f_n y^n| = \max_{n\in\mathbb{N}} |f_n||x-y| \left|\sum_{i=0}^{n-1} x^i y^{n-1-i}\right| \leq$$

$$\leq \max_{n\in\mathbb{N}} |f_n||x-y||x^{n-1}| = \frac{|x-y|}{|x|} \max_{n\in\mathbb{N}} |f_n x^n|.$$

Essendo $x \in \mathcal{D}$, la successione $f_n x^n$ è infinitesima (1.16); è quindi ben definito $\max_{n\in\mathbb{N}} |f_n x^n|$. Quindi

$$\lim_{y\to x} f(y) = f(x),$$

come si voleva. □

Teorema 6.8 (Strassmann)**.** *Sia $f(X) \in K[[X]] \setminus \{0\}$ con dominio di convergenza $\mathcal{D} \supseteq \mathcal{O}$. Allora la funzione definita da $f(X)$ ammette al più*

$$N := \max\{n \in \mathbb{N} : |f_n| \geq |f_m| \ \forall\ m \in \mathbb{N}\}$$

zeri in $\mathcal{O}$.

Dimostrazione. Notiamo innanzitutto che N esiste perché $(f_n)_{n\in\mathbb{N}}$ è infinitesima (6.4).
Procediamo per induzione su $N \in \mathbb{N}$.
Se $N = 0$, ovvero $|f_0| > |f_n|$ per ogni $n \in \mathbb{N}$, comunque preso $x \in \mathcal{O}$ si ha $|f(x)|=|f_0| \neq 0$ per il lemma 2.19.
Supponiamo ora $N > 0$ e sia $b \in \mathcal{O}$, $f(b) = 0$. Allora, comunque dato $x \in \mathcal{O}$, si ha:

$$f(x) = f(x) - f(b) = \sum_{n=1}^{\infty} f_n(x^n - b^n) = (x-b) \sum_{n=1}^{\infty} \sum_{m=0}^{n-1} f_n x^m b^{n-1-m} =$$

$$= (x-b) \sum_{m=0}^{\infty} \sum_{n=m+1}^{\infty} f_n x^m b^{n-1-m} = (x-b)g(x)$$

avendo posto

$$g(X) = \sum_{m=0}^{\infty} g_n X^n, \qquad g_m = \sum_{i=0}^{\infty} f_{m+i+1} b^i \ \ \forall\ m \in \mathbb{N}.$$

Notiamo che, per il lemma 2.19,

$$|g_m| \leq \max_{i\in\mathbb{N}} |f_{m+i+1}||b|^i \leq \max_{i\in\mathbb{N}} |f_{m+i+1}| \leq |f_N| \quad \forall\ m \in \mathbb{N};$$

$$|g_{N-1}| = |f_N|; \qquad |g_m| < |f_N| \quad \forall\ m > N-1.$$

Quindi $g(X)$ soddisfa le ipotesi del teorema nel caso $N-1$, e per ipotesi induttiva la funzione da essa definita ammette al più $N-1$ zeri in $\mathcal{O}$. Segue che f ne ammette al più N. □

Corollario 6.9. *Data $f(X) \in K[[X]]$ con dominio di convergenza $\mathcal{D} \supseteq \mathcal{O}$, se la funzione definita da $f(X)$ ammette infinite radici in $\mathcal{O}$ allora $f(X) = 0$.*

Corollario 6.10. *Date $f(X), g(X) \in K[[X]]$ con domini di convergenza contenenti $\mathcal{O}$, se $f(b) = g(b)$ per infiniti $b \in \mathcal{O}$ allora $f(X) = g(X)$.*

Corollario 6.11. *Supponiamo* $\mathrm{char}(K) = 0$. *Data $f(X) \in K[[X]]$ con dominio di convergenza $\mathcal{D} \supseteq \mathcal{O}$, se la funzione definita da $f(X)$ ammette periodo $b \in \mathcal{O}$ (ovvero soddisfa $f(x+b) = f(x)$ per ogni $x \in \mathcal{O}$) allora $f(X) \in K$.*

6.2 Composizione di serie formali di potenze

Nulla ci vieta di parlare di funzioni definite da serie formali di potenze su campi di serie formali di Laurent. Questa idea porta a definire un'operazione fra serie formali di potenze, che, ristretta agli anelli di polinomi, diventa l'abituale composizione polinomiale.

Lemma 6.12. *Sia $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, $(x_{n,m})_{n,m\in\mathbb{N}}$ a valori in K. Se*

$$\lim_{\max\{n,m\}\to\infty} x_{n,m} = 0$$

allora entrambe le serie

$$\sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x_{n,m}, \quad \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} x_{n,m}$$

convergono, e sono uguali.

Dimostrazione. Per il lemma 2.19 la serie $\displaystyle\sum_{m=0}^{\infty} x_{n,m}$ converge per ogni $n \in \mathbb{N}$ ed è maggiorata in valore assoluto da $\max_{m\in\mathbb{N}} |x_{n,m}|$; la convergenza di $\displaystyle\sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x_{n,m}$ segue dallo stesso lemma notando che $\lim_{n\to\infty} \max_{m\in\mathbb{N}} |x_{n,m}| = 0$. La seconda serie converge per lo stesso motivo. Inoltre

$$\lim_{N\to\infty} \left| \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x_{n,m} - \sum_{n=0}^{N}\sum_{m=0}^{N} x_{n,m} \right| =$$

$$= \lim_{N\to\infty} \left| \sum_{n=N+1}^{\infty}\sum_{m=0}^{\infty} x_{n,m} + \sum_{n=0}^{N}\sum_{m=N+1}^{\infty} x_{n,m} \right| \leq$$

$$\leq \lim_{N\to\infty} \left(\max_{n>N,\ m\geq 0} |x_{n,m}| + \max_{n\geq 0,\ m>N} |x_{n,m}| \right) = 0.$$

Quindi

$$\sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x_{n,m} = \lim_{N\to\infty} \sum_{n=0}^{N}\sum_{m=0}^{N} x_{n,m} = \lim_{N\to\infty} \sum_{m=0}^{N}\sum_{n=0}^{N} x_{n,m} = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} x_{n,m}.$$

□

Lemma 6.13. *Ogni $f(Y) \in K[[Y]]$ ha dominio di convergenza $XK[[X]]$ su $K((X))$.*

Dimostrazione. Tutti i coefficienti di $f(Y)$ hanno valore assoluto unitario in $K((X))$, dunque il raggio di convergenza è 1; segue la tesi (6.3). □

Definizione 6.14. Date $f(Y) \in K[[Y]], g(X) \in XK[[X]]$, definiamo

$$f \circ g(X) := f(g(X)) \in K[[X]]$$

composizione di $f(Y)$ e $g(X)$.

Proposizione 6.15. *Date $f(Y) \in K[[Y]], g(X) \in XK[[X]]$, siano*

$$c_{i,j} := \sum_{k_1+\ldots+k_i=j} \prod_{l=1}^{i} g_{k_l} \quad \forall\ j \geq i.$$

Allora

$$f \circ g(X) = \sum_{j=0}^{\infty} \sum_{i=0}^{j} a_i c_{i,j} X^j.$$

Dimostrazione. Per la 2.24 vale

$$g(x)^i = \left(\sum_{j=0}^{\infty} g_j x^j \right)^i = \sum_{j=i}^{\infty} c_{i,j} x^j;$$

dunque

$$f \circ g(X) = \sum_{i=0}^{\infty} \sum_{j=i}^{\infty} a_i c_{i,j} X^j.$$

Si conclude facilmente applicando il lemma 6.12. □

È naturale chiedersi se la composizione di funzioni definite da serie formali di potenze sia definita dalla composizione delle serie formali. In generale no (può' essere istruttivo cercare varie forme di controesempi), ma con qualche ulteriore ipotesi la risposta diventa affermativa, come mostra il seguente lemma.

Lemma 6.16. *Siano $f(X) \in K[[Y]]$, $g(X) \in XK[[X]]$. Sia x nel dominio di convergenza di $g(X)$ e di $f \circ g(X)$, e supponiamo che $g(x)$ sia nel dominio di convergenza di $f(Y)$. Supponiamo, inoltre, che valga*

$$|g_1 x| > |g_k x^k| \quad \forall\ k > 1.$$

Allora sussiste l'uguaglianza

$$f(g(x)) = f \circ g(x).$$

Dimostrazione. Ponendo

$$c_{i,j} := \sum_{k_1+\ldots+k_i=j} \prod_{l=1}^{i} g_{k_l} \quad \forall\ j \geq i,$$

si ha per definizione

$$f \circ g(x) = \sum_{j=0}^{\infty} \sum_{i=0}^{j} a_i c_{i,j} x^j.$$

Inoltre per la 2.24 vale

$$g(x)^i = \left(\sum_{j=0}^{\infty} g_j x^j \right)^i = \sum_{j=i}^{\infty} c_{i,j} x^j.$$

Segue dalle ipotesi che, comunque presi k_1, ..., k_i interi positivi, vale

$$|g_1 x|^i > \prod_{l=1}^{i} |g_{k_l} x^{k_l}|$$

e per la 2.17

$$|g(x)| = |g_1 x|.$$

Di conseguenza

$$|g(x)|^i \geq \max_{k_1+\ldots+k_i=j} \left(\prod_{l=1}^{i} |g_{k_l}| \right) |x|^j \geq |c_{i,j} x^j| \quad \forall\ j \geq i.$$

Allora:

$$|f \circ g(x) - \sum_{i=0}^{n} f_i g(x)^i| = |\sum_{j=n+1}^{\infty} \sum_{i=n+1}^{j} f_i c_{i,j} x^j| < \max_{j \geq i > n} |f_i c_{i,j} x^j| = \max_{i>n} |f_i g(x)^i|.$$

□

6.3 Esponenziale e logaritmo

Presentiamo ora due esempi fondamentali (in parte per applicazione di quanto detto, in parte perché ci saranno utili più avanti) di serie formali di potenze su $K[[X]]$, supponendo $\mathrm{char}(K) = 0$.

Definizione 6.17. Dato K campo con $\mathrm{char}(K) = 0$, definiamo

$$\log(1+X) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} \in K[[X]];$$

$$\exp(X) := \sum_{n=1}^{\infty} \frac{X^n}{n!} \in K[[X]].$$

$\log(1+X)$ e $\exp(X)$ godono di alcune proprietà fondamentali, che enunciamo lasciandole indimostrate.

Proposizione 6.18. *Valgono le seguenti identità:*

1. $\forall\ x, y \in K \quad \log(1 + xX + yX + xyX^2) = \log(1+xX)\log(1+yX)$;
2. $\forall\ x, y \in K \quad \exp(xX + yX) = \exp(xX)\exp(yX)$;
3. $\exp \circ \log(1+X) = 1 + X$.

Concludiamo enunciando una variante del lemma 4.1, spesso utile, nota anch'essa come lemma di Hensel.

6.4 Lemma di Hensel

Lemma 6.19. *Sia $|\cdot|$ ultrametrico su K, $\mathcal{O}$ anello di valutazione. Per ogni $f(X) \in \mathcal{O}[X]$ esiste $g(X,Y) \in \mathcal{O}[X,Y]$ tale che*

$$f(x+y) = f(x) + f'(x)y + g(x,y)y^2$$

per ogni $x, y \in \mathcal{O}$.

Dimostrazione.

$$f(x+y) = \sum_{i=0}^{n} f_i(x+y)^i = f(x) + f'(x)y + \left(\sum_{j=2}^{n} \sum_{i=j}^{n} \binom{i}{j} f_i x^{i-j} y^{j-2} \right) y^2.$$

□

Corollario 6.20. *Sia $|\cdot|$ ultrametrico su K, $\mathcal{O}$ anello di valutazione. Dati $a, \delta \in \mathcal{O}$ e $f(X) \in \mathcal{O}[X]$, valgono le seguenti:*

1. $|f(a+\delta) - f(a)| \leq |\delta|$.
2. $|f(a+\delta) - f(a) - f'(a)\delta| \leq |\delta|^2$.

Lemma 6.21 (Hensel)**.** *Sia $(K, |\cdot|)$ completo con $|\cdot|$ ultrametrico, $\mathcal{O}$ anello di valutazione. Siano $f(X) \in \mathcal{O}[X]$, $a \in \mathcal{O}$ tali che $|f(a)| < |f'(a)|^2$. Allora esiste unico $\theta \in \mathcal{O}$ tale che:*

1. $f(\theta) = 0$;
2. $|\theta - a| < |f'(a)|$.

Inoltre vale la disuguaglianza più forte $|\theta - a| < \dfrac{|f(a)|}{|f'(a)|}$.

Dimostrazione. Siano $(a_n)_{n\in\mathbb{N}}$, $(\delta_n)_{n\in\mathbb{N}}$ a valori in K e $(c_n)_{n\in\mathbb{N}}$ a valori in $\mathbb{R}$ così definite:

$$a_0 := a; \quad a_{n+1} := a_n - \delta_n; \quad \delta_n := \frac{f(a_n)}{f'(a_n)}; \quad c_n = \frac{|f(a_n)|}{|f'(a_n)|^2} \quad \forall\, n \in \mathbb{N}.$$

Vogliamo dimostrare per induzione su $n \in \mathbb{N}$ le seguenti:

i. $a_n \in \mathcal{O}$.

ii. $f'(a_n) = f'(a)$.

iii. $c_n \leq c_0^{2^n}$.

Il passo base è banale per tutte le asserzioni. Supponendole vere per n proviamole, una per volta, per $n+1$.

i. $|f'(a_n)| \leq 1$, quindi $|\delta_n| = |f'(a_n)|c_n < 1$. Dunque $|a_{n+1}| \leq \max\{a_n, \delta_n\} \leq 1$.

ii. Essendo $|\delta_n| < 1$, per il corollario 6.20 vale $|f'(a_{n+1}) - f'(a_n)| \leq |\delta_n|$. Inoltre $|\delta_n| = |f'(a_n)|c_n < |f'(a_n)|$; segue che $|f'(a_{n+1})| = |f'(a_n)|$ (1.16).

iii. Ancora per il 6.20, $|f(a_{n+1})| = |f(a_{n+1}) - f(a_n) + \delta_n f'(a_n)| \leq |\delta_n|^2$. Quindi $c_{n+1} \leq |\delta_n|^2 |f'(a_{n+1})|^{-2} = |\delta_n|^2 |f'(a_n)|^{-2} = c_n^2 \leq c_0^{2^{n+1}}$.

In particolare, dunque, $(c_n)_{n\in\mathbb{N}}$ è infinitesima. Essendo identicamente $|\delta_n| = |f'(a)|c_n$ e $|f(a_n)| = |f'(a)|^2 c_n$, anche le successioni $(\delta_n)_{n\in\mathbb{N}}$, $(f(a_n))_{n\in\mathbb{N}}$ sono infinitesime. Allora per il lemma 2.19 la successione $(a_n)_{n\in\mathbb{N}}$ a valori in $\mathcal{O}$ converge a un certo θ, che per continuità è radice di f. Inoltre, valendo identicamente $|\delta_n| \leq |f'(a)|c_0 = |f(a)|/|f'(a)|$, ancora per il 2.19 si ha

$$|\theta - a| \leq |f(a)|/|f'(a)| < |f'(a)|$$

($\theta \in \mathcal{O}$ in quanto $a,\ \theta - a \in \mathcal{O}$).
Mostriamo ora l'unicità di θ. Supponiamo per assurdo che esista $\tilde{\theta}$ radice di $f(X)$, distinta da θ, tale che $|\tilde{\theta} - a| < |f'(a)|$ (quindi $\tilde{\theta} \in \mathcal{O}$). Allora

$$|\tilde{\theta} - \theta| \leq \max\{|\tilde{\theta} - a|, |\theta - a|\} < |f'(a)|.$$

Per il 6.20

$$|f'(\theta)(\tilde{\theta} - \theta)| = |f(\tilde{\theta}) - f(\theta) - f'(\theta)(\tilde{\theta} - \theta)| \leq (\tilde{\theta} - \theta)^2,$$

ovvero $|f'(\theta)| \leq |\tilde{\theta} - \theta|$. Assurdo. □

7 $\mathbb{Q}_p$

Vediamo ora in maggior dettaglio le proprietà di Q_p, topologiche e algebriche.

7.1 Struttura topologica

Proposizione 7.1. *$(\mathbb{Z}_2, |\cdot|_2)$ è omeomorfo all'insieme di Cantor.*

Dimostrazione. Chiamando $C \subset [0,1]$ il ben noto insieme di Cantor (dotato della topologia euclidea), consideriamo la funzione

$$\varphi : \mathbb{Z}_2 \to C : \sum_{n \in X \subseteq \mathbb{N}} 2^n \mapsto 2 \sum_{n \in X \subseteq \mathbb{N}} 3^{-n+1}.$$

φ è ben definita in virtù della proposizione 2.22 (prendendo $\{0,1\}$ come sistema di rappresentanti) e bigettiva. Inoltre è semplice verificare che

$$|x-y|_2 \leq 2^{-n} \Rightarrow |\varphi(x) - \varphi(y)|_\infty \leq 3^{-n},$$

dunque φ è continua; il fatto che vada da un compatto ad uno spazio di Hausdorff assicura, infine, che sia chiusa, e dunque omeomorfismo. □

Useremo un teorema di topologia mostrato nel 1910 da Brouwer, che enunciamo senza dimostrazione.

Teorema 7.2 (Brouwer)**.** *Ogni spazio metrico non vuoto, compatto, totalmente sconnesso e perfetto (ovvero privo di punti isolati) è omeomorfo all'insieme di Cantor*

Corollario 7.3. *Sia $(K, |\cdot|)$ completo con $|\cdot|$ discreto; sia $\mathcal{O}$ l'anello di valutazione, k il campo residuo; supponiamo k finito. Allora, chiamando C l'insieme di Cantor, valgono gli omeomorfismi:*

$$\mathcal{O} \simeq C; \quad K \simeq C \setminus \{1\}.$$

Dimostrazione. L'omeomorfismo tra l'anello di valutazione e l'insieme di Cantor segue dal teorema di Brouwer, ricordando il teorema 2.32 e la proposizione 2.7 e osservando che, comunque dato $x \in \mathcal{O}$, la successione $(x + \mu^n)_{n\in\mathbb{N}}$ a valori in K (con μ uniformizzante) converge a x.
Considerazioni simili portano a concludere che anche $\mathcal{O}^*$ (chiuso in $\mathcal{O}$) è omeomorfo a C; inoltre

$$f_n : \mathcal{O}^* \to \mu^{-n}\mathcal{O}^* : x \mapsto \mu^{-n}x$$

è omeomorfismo per ogni $n \in \mathbb{N}_{>0}$. Dunque che l'insieme

$$\{\mathcal{O}\} \cup \{\mu^{-n}\mathcal{O}^* : n \in \mathbb{N}_{>0}\}$$

è una partizione numerabile di K costituita da aperti (2.7) tutti omeomorfi a C.
Similmente,

$$\{3^{-1}C\} \cup \{3^{-n-1}C + 1 - 3^{-n} : n \in \mathbb{N}_{>0}\}$$

è una partizione numerabile di $C \setminus \{1\}$ costituita da aperti tutti omeomorfi a C.
L'unione degli omeomorfismi

$$\varphi_0 : \mathcal{O} \to 3^{-1}C;$$
$$\varphi_n : \mu^{-n}\mathcal{O}^* \to 3^{-n-1}C + 1 - 3^{-n}$$

stabilisce un omeomorfismo tra K e $C \setminus \{1\}$. □

Corollario 7.4. *Tutti i campi $(K, |\cdot|)$ localmente compatti (con $|\cdot|$ non banale) sono tra loro omeomorfi; in particolare lo sono $(\mathbb{Q}_p, |\cdot|_p)$ al variare di p primo.*

Dimostrazione. Siano $(K_1, |\cdot|_1)$, $(K_2, |\cdot|_2)$ localmente compatti (dunque completi, con valori assoluti discreti, con campi residui finiti, in virtù del teorema 2.32). Per il teorema di Brouwer esiste $\varphi : \mathcal{O}_1 \to \mathcal{O}_2$ omeomorfismo tra i rispettivi anelli di valutazione. Detti μ_1, μ_2 i rispettivi uniformizzanti, sia

$$\tilde{\varphi} : K_1 \to K_2 : \mu_1^n x \to \mu_2^n \varphi(x),$$

per $n \in \mathbb{Z}, x \in \mathcal{O}_1^*$. Lasciamo al lettore la semplice verifica che $\tilde{\varphi}$ è un ben definito omeomorfismo che estende φ. □

7.2 Struttura moltiplicativa

Definizione 7.5. Per ogni $m \in \mathbb{N}_{>0}$ definiamo

$$U_p^{(m)} := 1 + p^m\mathbb{Z}_p.$$

Osservazione 7.6. $\left(U_p^{(m)}\right)_{m\in\mathbb{N}_{>0}}$ è una catena discendente di sottogruppi di $\mathbb{Z}_p^*$, nonché un sistema fondamentale di intorni di 1.

Dimostrazione. La prima asserzione è banale, la seconda discende dal lemma 2.25 e dalla compattezza di $\mathbb{Z}_p$ (5.11). □

Lemma 7.7. *Dato $n \in \mathbb{N}$, valgono le stime:*

$$1 \leq |n|_p^{-1} \leq n;$$

$$1 \leq |n!|_p^{-1} < p^{n/(p-1)}.$$

Inoltre

$$\lim_{n\to\infty} |n|_p^{-1/n} = 1;$$

$$\limsup_{n\to\infty} |n!|_p^{-1/n} = p^{1/(p-1)}.$$

Dimostrazione. La prima stima è molto semplice, e il primo limite ne segue immediatamente. Non è difficile, inoltre, verificare che

$$v_p(n!) = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Dunque

$$v_p(n!) < \sum_{i=0}^{\infty} \frac{n}{p^i} = \frac{n}{p-1},$$

da cui

$$\limsup_{n\to\infty} |n!|_p^{-1/n} \leq p^{1/(p-1)}.$$

D'altronde, per la precedente identità,

$$v_p(p^m!) = \sum_{i=0}^{m-1} p^i = \frac{p^m - 1}{p-1};$$

quindi

$$\lim_{m\to\infty} |p^m!|^{-p^{-m}} = \lim_{m\to\infty} p^{(1-p^{-m})/(1-p)} = p^{1/(p-1)},$$

da cui segue la tesi. □

Lemma 7.8. *Dati $n, m \in \mathbb{N}$ tali che $n \geq 2$, $p^m \geq 3$, valgono le seguenti disuguaglianze:*

$$\frac{n}{p^{m(n-1)}} < 1;$$

$$\frac{n}{p-1} + m \leq nm.$$

Dimostrazione. Semplice induzione. □

Proposizione 7.9. *Sia $m \in \mathbb{N}$ tale che $p^m \geq 3$. Allora vale l'isomorfismo di gruppi*

$$U_p^{(m)} \cong \mathbb{Z}_p.$$

Dimostrazione. In virtù dell'osservazione 1.35, basta mostrare l'isomorfismo di gruppi

$$U_p^{(m)} \cong p^m\mathbb{Z}_p.$$

Applicando le stime in 7.7 e le disuguaglianze in 7.8, otteniamo che

$$\left|\frac{p^{mn}}{n}\right|_p \leq \frac{n}{p^{mn}} < \frac{1}{p^m} \quad \forall\ n \geq 2;$$

$$\left|\frac{p^{mn}}{n!}\right|_p < \frac{p^{n/(p-1)}}{p^{mn}} \leq \frac{1}{p^m} \quad \forall\ n \geq 2.$$

Dunque, alla luce del lemma 2.19, sono ben definite le funzioni

$$\log : U_p^{(m)} \to p^m\mathbb{Z}_p : \quad 1 + p^m x \mapsto \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(p^m x)^n}{n};$$

$$\exp : p^m\mathbb{Z}_p \to U_p^{(m)} : \quad p^m x \mapsto 1 + \sum_{n=1}^{\infty} \frac{(p^m x)^n}{n!}.$$

Utilizzando il lemma 6.5 e le prime due proprietà in 6.18, non è difficile dimostrare che tali funzioni sono omomorfismi di gruppi; sono inoltre iniettivi per il teorema di Strassmann, applicato per l'esattezza alle serie formali

$$\sum_{n=1}^{\infty}(-1)^{n+1}\frac{(p^mX)^n}{n},\quad \sum_{n=1}^{\infty}\frac{(p^mX)^n}{n!}\quad \in \mathbb{Z}_p[[X]],$$

tenendo conto delle due disuguaglianza iniziali. Infine, per il lemma 6.16, servendoci ancora una volta della prima di tali disuguaglianze e ricordando la terza proprietà in 6.18, concludiamo che $\exp\circ\log$ è l'identità su $U_p^{(m)}$. Segue la tesi. □

Lemma 7.10. *Vale l'isomorfismo di gruppi*

$$\mathbb{Z}_p^* \cong U_p^{(1)} \oplus \mathbb{F}_p^*.$$

Dimostrazione. Consideriamo la successione esatta (semplice verifica) di gruppi abeliani

$$\{0\} \to U_p^{(1)} \xrightarrow{i} \mathbb{Z}_p^* \xrightarrow{\pi} \mathbb{F}_p^* \to \{0\},$$

con i inclusione e π proiezione al quoziente. Basta dimostrare l'esistenza di una sezione $\sigma : \mathbb{F}_p^* \to \mathbb{Z}_p^*$ per π.
Consideriamo dapprima una generica inversa destra σ di π. Sia $f(X) = X^{p-1} - 1 \in \mathcal{O}[X]$. Dato $x \in \mathbb{F}_p^*$, $\pi \circ f \circ \sigma(x) = f(x) = 0$; $\pi \circ f' \circ \sigma(x) = f'(x) = (p-1)x^{p-2} \neq 0$. Quindi $|f(\sigma(x))| < 1 = |f'(\sigma(x))|^2$. Per il lemma di Hensel esiste un'unica radice di f in $\pi^{-1}(x)$, e possiamo assumere che sia $\sigma(x)$ (e che ciò valga per ogni $x \in \mathbb{F}_p^*$).
Mostriamo che σ così costruito è omomorfismo: comunque presi $x, y \in \mathbb{F}_p^*$, $\sigma(x)\sigma(y)$ e $\sigma(xy)$ sono due radici di $f(x)$ in $\pi^{-1}(xy)$ e quindi sono uguali. □

In riferimento all'ultimo lemma, osserviamo che $\{0\}\cup\sigma(\mathbb{F}_p^*)$ è un sistema di rappresentanti per il campo residuo $\mathbb{F}_p$ chiuso per moltiplicazione. Il fatto che $\mathbb{Q}_p$ abbia caratteristica diversa dal campo residuo stronca ogni speranza di trovarne uno chiuso anche per moltiplicazione, ovvero isomorfo a $\mathbb{F}_p$.

Lemma 7.11. *Vale l'isomorfismo di gruppi*

$$\mathbb{Z}_2^* \cong U_2^{(2)} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Dimostrazione. Consideriamo la successione esatta di gruppi abeliani

$$\{0\} \to U_2^{(2)} \xrightarrow{i} \mathbb{Z}_2^* \xrightarrow{\pi_2} (\mathbb{Z}/4\mathbb{Z})^* \to \{0\}$$

con i inclusione e π_2^* proiezione al quoziente, ricordando che

$$\mathbb{Z}_2/4\mathbb{Z}_2 \cong \mathbb{Z}/4\mathbb{Z}$$

(5.11). La tesi segue osservando che

$$\sigma : (\mathbb{Z}_2/4\mathbb{Z}_2)^* \to \mathbb{Z}_2^* :\ 1 \mapsto 1,\ -1 \mapsto -1$$

è sezione per π_2. □

Teorema 7.12 (Struttura moltiplicativa di $\mathbb{Q}_p$)**.** *Per $p \neq 2$ valgono gli isomorfismi di gruppi*

$$\mathbb{Z}_p^* \cong \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z};$$

$$\mathbb{Q}_p^* \cong \mathbb{Z} \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}.$$

Invece, per $p = 2$, si ha

$$\mathbb{Z}_2^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z};$$

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

Dimostrazione. La prima parte del teorema segue dal lemma 7.10 e dalla proposizione 7.9 nel caso $p \neq 2, m = 1$; la seconda parte dal lemma 7.11 e dalla proposizione 7.9 nel caso particolare $p = 2, m = 2$. □

Corollario 7.13. *Per $p \neq 2$, $\mathbb{Z}_p^*$ e $\mathbb{Q}_p^*$ hanno sottogruppo di torsione isomorfo a $\mathbb{Z}/(p-1)\mathbb{Z}$; invece $\mathbb{Z}_2^*$ e $\mathbb{Q}_2^*$ hanno sottogruppo di torsione isomorfo a $\mathbb{Z}/2\mathbb{Z}$*

Corollario 7.14. *Dati p, q primi distinti, $\mathbb{Q}_p^*$ e $\mathbb{Q}_q^*$ non sono isomorfi (dunque in particolare non lo sono $\mathbb{Q}_p$ e $\mathbb{Q}_q$ come campi)*

Dimostrazione. Notiamo che

$$\bigcap_{n \in \mathbb{N}_{>0}} 2^n(\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}) = \bigcap_{n \in \mathbb{N}_{>0}} 2^n\mathbb{Z} \oplus 2^n\mathbb{Z}_2 = \{0\};$$

invece

$$\bigcap_{n \in \mathbb{N}_{>0}} 2^n(\mathbb{Z} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}/2\mathbb{Z}) = \bigcap_{n \in \mathbb{N}_{>0}} 2^n\mathbb{Z} \oplus \mathbb{Z}_3 = \mathbb{Z}_3;$$

dunque $\mathbb{Q}_2^* \ncong \mathbb{Q}_3^*$. D'altronde, in qualunque altro caso, $\mathbb{Q}_p^*$ e $\mathbb{Q}_q^*$ hanno sottogruppi di torsione non isomorfi, e dunque non lo sono essi stessi. □

7.3 Automorfismi

Lemma 7.15. *Per $p \neq 2$ l'addendo diretto $\mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}$ è un sottogruppo caratteristico in $\mathbb{Z} \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}$; così come $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$ in $\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$.*

Dimostrazione. Consideriamo il caso $p > 2$; l'altro è analogo.
Notiamo che, dato $n \in \mathbb{Z}$, se n è coprimo con p allora $n\mathbb{Z}_p = \mathbb{Z}_p$; se n è coprimo con $(p-1)$ allora $n\mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z}$. Dunque

$$\bigcap_{(n,\,(p(p-1)))=1} n(\mathbb{Z} \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}) = \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z};$$

segue che $\mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}$ è un sottogruppo caratteristico, in quanto intersezione di caratteristici. □

Osservazione 7.16. Per $p \neq 2$ anche $\mathbb{Z}/(p-1)\mathbb{Z}$ è caratteristico in $\mathbb{Z} \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}$ in quanto sottogruppo di torsione; così come $\mathbb{Z}/2\mathbb{Z}$ in $\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$.

Proposizione 7.17. *Il gruppo degli automorfismi di $\mathbb{Q}_p$ è banale.*

Dimostrazione. Sia $\varphi \in \mathrm{Aut}(\mathbb{Q}_p)$. φ in particolare è automorfismo del gruppo moltiplicativo $\mathbb{Q}_p^*$, dunque per il lemma 7.15, ricordando che l'isomorfismo stabilito nel teorema di struttura moltiplicativa manda $\mathbb{Z}_p^*$ in $\mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}$ (o in $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$ nel caso $p = 2$), si ha $\varphi(\mathbb{Z}_p^*) = \mathbb{Z}_p^*$. Allora, essendo φ l'identità su $\mathbb{Q}$,

$$\varphi(p^n\mathbb{Z}_p^*) = \varphi(p^n\mathbb{Z}_p^*) \ \ \forall\, n \in \mathbb{N};$$

dunque φ conserva il valore assoluto, in particolare è continuo.
Essendo $\mathbb{Q}$ denso in $\mathbb{Q}_p$, per continuità φ è l'identità su tutto $\mathbb{Q}_p$. □

7.4 Sottoestensioni

Lemma 7.18. *Sia*

$$\{f_i(X_1, ..., X_n) : 1 \leq i \leq m\} \subset \mathbb{Z}[X_1, ..., X_n] \setminus \{0\}$$

un insieme finito di polinomi nelle indeterminate X_1, ..., X_n. Allora esistono a_1, ..., $a_n \in \mathbb{Z}$ tali che

$$f_i(X_1, ..., X_n) \neq 0$$

per ogni $1 \leq i \leq m$.

Dimostrazione. Procediamo per induzione su n. Per $n = 1$ basta prendere a_1 distinto dalle finite radici dei $f_i(X_1)$. Supponendo vera la tesi per $n-1$, possiamo prendere a_2, ..., $a_n \in \mathbb{Z}$ tali che $f_i(X_1, a_2, ..., a_n) \neq 0$ per ogni $1 \leq i \leq m$; allora per il passo base esiste a_1 tale che l'n-upla a_1, ..., a_n soddisfa quanto chiesto. □

Lemma 7.19. *Dato $f(X) \in \mathbb{Z}[X] \setminus \mathbb{Z}$, esistono infiniti primi p tali che valga*

$$f(b) \equiv 0 \pmod{p}$$

per qualche $b \in \mathbb{Z}$.

Dimostrazione. Se $g(0) = 0$ allora p divide $g(0)$ qualunque sia p.
Consideriamo ora $g(0) \neq 0$. Supponiamo per assurdo che l'insieme P dei primi per i quali $g(X)$ ammetta una radice in modulo p sia finito (eventualmente vuoto). Essendo $g(X)$ non costante, possiamo trovare $c \in \mathbb{Z}$ divisibile per tutti i primi in P tale che

$$g(g(0)c) = g(0)r$$

per qualche $r \in \mathbb{Z} \setminus \{\pm 1\}$. Si ha $r \equiv 1 \pmod{c}$, dunque qualsiasi primo che divida r non appartiene a P e conduce ad una contraddizione. □

Lemma 7.20. *$\mathbb{Q}_p$ ha grado di trascendenza non numerabile su Q.*

Dimostrazione. Segue dal fatto che $\mathbb{Q}_p$ ha la cardinalità del continuo. □

Lemma 7.21. *Sia F/K estensione di campi, $\beta \subseteq F$, $h : B \to F$ tale che*

$$h(x) \in K(x) \subset K \quad \forall\, x \in B.$$

Se $F/K(B)$ è algebrica allora lo è anche $F/K(h(B))$; se B è algebricamente indipendente su K allora lo è anche $h(B)$. In particolare, se B è base di trascendenza di F su K allora lo è anche $h(B)$.

Dimostrazione. Osserviamo innanzitutto che, comunque scelti $x \in F$, $y \in K(x) \setminus K$, x è algebrico su $K(y)$. Infatti, presi $f(X), g(X) \in K[X]$, con X indeterminata, tali che $yg(x) = f(x)$, $f(X) - yg(X)$ è un polinomio in $K(y)[X]$ che si annulla in x. Segue in particolare che x è algebrico su $K(j(B))$ per ogni $x \in B$.
Supponiamo che $F/K(B)$ sia algebrica. Per quanto detto lo è anche $K(B)/K(j(B))$; dunque lo è $F/K(j(B))$.
Supponiamo ora che B sia algebricamente indipendente. Consideriamo un sottoinsieme finito $B' \subset B$. Segue dall'osservazione iniziale che h è iniettiva e che $K(B')/K(h(B'))$ è estensione algebrica. La cardinalità di $h(B')$ è uguale al grado di trascendenza di $K(B')$ su K; dunque $h(B')$ è base di trascendenza di $K(B')$ su K e in particolare è algebricamente indipendente su K. □

Lemma 7.22. *Sia $|\cdot|$ ultrametrico su K, $\mathcal{O}$ l'anello di valutazione, $\mathcal{M}$ il suo ideale massimale. Sia $f(X_1, ..., X_n) \in \mathcal{O}[X_1, ..., X_n]$; $a_1, ..., a_n \in \mathcal{O}$; $b_1, ..., b_n \in \mathcal{M}$. Valgono le implicazioni*

$$|f(a_1, ..., a_n)| = 1 \Rightarrow |f(a_1 + b_1, ..., a_n + b_n)| = 1;$$
$$|f(a_1, ..., a_n)| < 1 \Rightarrow |f(a_1 + b_1, ..., a_n + b_n)| < 1;$$

Dimostrazione. Notiamo che

$$g(X_1, ..., X_n) := f(a_1 + X_1, ..., a_n + X_n) \in \mathcal{O}[X_1, ..., X_n].$$

Allora

$$|g(b_1, ..., b_n) - g(0, ..., 0)| < 1;$$

la tesi segue dall'osservazione 1.16. □

Teorema 7.23. *Sia K estensione finitamente generata di $\mathbb{Q}$ e sia $S \subset K \setminus \{0\}$ finito. Allora per infiniti primi p esiste un'immersione $j : K \to \mathbb{Q}_p$ tale che $|j(s)|_p = 1$ per ogni $s \in S$.*

Dimostrazione. Osserviamo preliminarmente che, a meno di ingrandire S, possiamo supporre che $s^{-1} \in S$ per ogni $s \in S$; dunque basterà assicurarci che j mappi S in $\mathbb{Z}_p$.
Sia $x_1, ..., x_n$ una base di trascendenza di K su $\mathbb{Q}$. $K/\mathbb{Q}(x_1, ..., x_n)$ è finita e separabile, dunque esiste $\alpha \in K$ algebrico su $\mathbb{Q}(x_1, ..., x_n)$ tale che

$$K = \mathbb{Q}(\alpha, x_1, ..., x_n).$$

α annulla un polinomio $\mu(Y) \in \mathbb{Q}[x_1, ..., x_n][Y]$ irriducibile su $\mathbb{Q}(x_1, ..., x_n)[Y]$; dunque

$$\mu(Y) = h(Y, x_1, ..., x_n)$$

con $h(Y, X_1, ..., X_n) \in \mathbb{Z}[Y, X_1, ..., X_n]$, considerando $Y, X_1, ..., X_n$ indeterminate.
Chiamiamo $h_m(x_1, ..., x_n)$, con $h_m(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_m] \setminus \{0\}$, il coefficiente direttivo di $\mu(Y)$. Chiamiamo inoltre $\Delta(x_1, ..., x_n)$, con $\Delta(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_m] \setminus \{0\}$, il discriminante di $\mu(Y)$, che non è nullo data l'irriducibilità e separabilità di $\mu(Y)$.
Per ogni $s \in S$ esistono $f_s(Y, X_1, ..., X_n) \in \mathbb{Z}[Y, X_1, ..., X_n]$, $g_s(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$ tali che

$$s = \frac{f_s(\alpha, x_1, ..., x_n)}{g_s(x_1, ..., x_n)}.$$

per il lemma 7.18 esistono $a_1, ..., a_n \in \mathbb{Z}$ tali che

$$h_m(a_1, ..., a_n) \neq 0;$$

$$\Delta(a_1, ..., a_n) \neq 0;$$

$$g_s(a_1, ..., a_n) \neq 0 \ \ \forall\ s \in S.$$

Inoltre, per il lemma 7.19, esistono infiniti primi p tali che

$$h(b, a_1, ..., a_n) \equiv 0 \pmod{p}$$

per qualche $b \in \mathbb{Z}$. A meno di escludere un numero finito di tali primi, possiamo anche supporre che per ognuno di essi valgano

$$\Delta(a_1, ..., a_n) \not\equiv 0 \pmod{p};$$

$$g_s(a_1, ..., a_n) \not\equiv 0 \pmod{p} \ \ \forall\ s \in S.$$

Per il lemma 7.20 esistono $\theta_1, ..., \theta_n \in \mathbb{Q}_p$ algebricamente indipendenti. Alla luce del lemma 7.21 possiamo supporre, a meno di moltiplicare θ_i per un'opportuna potenza di p e sommare a_i, che valga

$$|\theta_i - a_i|_p < 1 \ \ \forall\ 1 \leq i \leq n.$$

Allora, in virtù del lemma 7.22, valgono:

$$|h(b, \theta_1, ..., \theta_n)|_p < 1$$

$$|\Delta(\theta_1, ..., \theta_n)|_p = 1$$

$$|g_s(\theta_1, ..., \theta_n)|_p = 1 \ \ \forall\ s \in S.$$

Sia $\pi : \mathbb{Z}_p \to \mathbb{F}_p$ la proiezione al quoziente e $\bar{\pi} : \mathbb{Z}_p[Y] \to \mathbb{F}_p[Y]$: la riduzione modulo $p\mathbb{Z}_p$. Sia inoltre $\tilde{\mu}(Y) = h(Y, \theta_1, ..., \theta_n) \in \mathbb{Z}_p[Y]$. $\bar{\pi}(\tilde{\mu})(Y)$ si annulla in $\pi(b)$ e ha discriminante $\pi(\Delta(\theta_1, ..., \theta_n)) \neq 0$; dunque la sua derivata non si annulla in $\pi(b)$. Ne segue che

$$|\tilde{\mu}(b)|_p < |\tilde{\mu}'(b)|_p^2 = 1.$$

Possiamo dunque applicare il lemma di Hensel (6.21), che ci assicura l'esistenza di $\xi \in \mathbb{Z}_p$ tale che

$$\tilde{\mu}(\xi) = 0.$$

Possiamo allora stabilire l'immersione $j : K \to \mathbb{Q}_p$ che mappa:

$$x_i \mapsto \theta_i \ \ \forall\ s \in S$$

$$\alpha \mapsto \xi,$$

per la quale vale

$$|j(s)| = \frac{|f_s(\theta_1,\ ...,\ \theta_n)|_p}{|g_s(\theta_1,\ ...,\ \theta_n)|_p} \leq 1 \ \ \forall\ s \in S.$$

□

Lemma 7.24. *Sia $|\cdot|$ ultrametrico su K, $\mathcal{O}$ l'anello di valutazione. Siano $f \in \mathcal{O}[X] \setminus \mathcal{O}$ monico, $a \in K$. Se $f(a) = 0$ allora $a \in \mathcal{O}$.*

Dimostrazione. Sia $n := \deg f$. Preso $a \in K \setminus \mathcal{O}$ si ha $|a|^n > |a|^{n-1} \geq |f(a) - a^n|$; segue che $|f(a)| = |a|^n$ (1.16). □

Proposizione 7.25. *Comunque presi $n > 1$ intero e $P, \tilde{P}$ insiemi finiti disgiunti di primi, esiste K campo di numeri di grado n tale che si immerga in $\mathbb{Q}_p$ per ogni $p \in P$ e non si immerga in $\mathbb{Q}_{\tilde{p}}$ per ogni $\tilde{p} \in \tilde{P}$.*

Dimostrazione. Per il teorema cinese del resto esistono $a, b \in \mathbb{Z}$ tali che:

$$-1 - a \equiv b \equiv n \pmod{p} \ \ \forall\ p \in P;$$

$$a \equiv b \equiv \tilde{p} \pmod{\tilde{p}^2} \ \ \forall\ \tilde{p} \in \tilde{P}.$$

Sia

$$f(X) = X^n + aX + b \in \mathbb{Z}[X].$$

$f(X)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein. Sia α radice di $f(X)$ nella chiusura algebrica di $\mathbb{Q}$ e sia $K := \mathbb{Q}(\alpha)$. Comunque preso $p \in P$ si ha

$$|f(1)|_p < |f'(1)|^2 = 1;$$

dunque per il lemma di Hensel (6.21) esiste $\xi \in \mathbb{Z}_p$ tale che $f(\xi) = 0$ e $j : K \to \mathbb{Q}_p : \alpha \mapsto \xi$ è immersione.
Supponiamo per assurdo che K si immerga in $Q_{\tilde{p}}$ per qualche $\tilde{p} \in \tilde{P}$. Allora l'immagine di α sarebbe radice di $f(X)$ in $\mathbb{Q}_{\tilde{p}}$ e per il lemma 7.24 sarebbe in $\mathbb{Z}_p$. Per continuità di $f(X)$ e la densità di $\mathbb{Z}$ in $(\mathbb{Z}_{\tilde{p}}, |\cdot|_{\tilde{p}})$ (5.5) esisterebbe $c \in \mathbb{Z}$ tale che $|f(c)|_{\tilde{p}} < 1/\tilde{p}$. Ma si verifica facilmente che ciò non è possibile. □