UNIVERSITÀ DEGLI STUDI DI ROMA

TOR VERGATA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica

RAZIONALITÀ FUNZIONE ZETA SU VARIETÀ ALGEBRICHE

Tesi di Laurea in Teoria dei Numeri

Relatore
Chiar.mo Prof.
Renatus Schoof

Laureando
Daniele Mastrostefano

Anno accademico 2014/2015

INTRODUZIONE

In questa tesi viene presentata la famosa congettura di Weil sulla funzione zeta di varietà algebriche e in particolare viene dimostrata la razionalità di tale funzione.
La tesi è strutturata in questo modo:
i primi 10 capitoli sono introduttori:
ho voluto inserirli in modo che, qualsiasi persona che conosca le basi della matematica (diciamo che possieda una laurea triennale in matematica), possa leggere e capire il materiale presentato senza aver bisogno di ulteriori conoscenze, e in particolar modo, possa capire la dimostrazione della razionalità della funzione zeta, usando come ausilio soltanto il materiale contenuto in questo documento.
I capitoli XI e XIII racchiudono l'anima di questa tesi.
Dopo il XIII capitolo ci sarà una sezione dedicata allo svolgimento di alcuni esercizi che di tanto in tanto proporrò al lettore; gli esercizi con svoglimento sono contrassegnati dal loro numero identificativo. Ci saranno invece alcuni esercizi (senza un tale numero accanto) che vengono lasciati come riflessione personale al lettore e che non verranno dimostrati visto che esulano un poco dalla trattazione dell'argomento principale di questa tesi.
Un'avvertimento particolare va rivolto a chi ha intenzione di leggere il capitolo XII:
esso infatti è a parte dal resto della tesi e può essere benissimo omesso,
senza alterare la lettura generale.
In particolare per affrontarlo c'è bisogno di una buona conoscenza del mondo delle curve ellittiche, che non verranno presentate in questa tesi.

INDICE

Capitolo IX
Serie formali

IX.1 L'anello delle serie formali.
IX.2 Derivata di serie.
IX.3 Il raggio di convergenza.
IX.4 Composizione di serie formali.
IX.5 La crescita del modulo.
IX.6 Zeri di serie formali.
IX.7 $\mathbb{C}_p$ versus $\mathbb{C}$.

Capitolo X
Funzioni $p-$adiche

X.1 Logaritmo ed esponenziale.
X.2 La serie esponenziale di Artin-Hasse.
X.3 La funzione θ.

Capitolo XI
La congettura di Weil

Capitolo XII
Congettura di Weil per curve ellittiche

Capitolo XIII
Razionalità della funzione zeta di una varietà algebrica

XIII.1 Costruzione del carattere additivo χ_s.
XIII.2 $\zeta(V,t)$ è una funzione $p-$adica meromorfa.
XIII.3 Generalizzazione alle serie formali.
XIII.4 Condizione per la razionalità.
XIII.5 Razionalità della funzione zeta.
XIII.6 Razionalità per varietà algebriche qualsiasi.

Soluzione esercizi

Bibliografia

Capitolo I

Varietà algebriche

I.1 **Varietà affini.**

Fissiamo una volta per tutte un campo $\mathbb{K}$ perfetto
(ogni sua estensione algebrica è separabile; un campo è perfetto se e soltanto se ha caratteristica 0 o ha caratteristica $p > 0$, ma in tal caso, ogni elemento possiede una radice $p-$esima, ovvero il morfismo di Frobenius dell'estensione è suriettivo);
denotiamo con $\bar{\mathbb{K}}$ una sua chiusura algebrica e con $Gal(\bar{\mathbb{K}}/\mathbb{K})$ il gruppo di Galois assoluto di $\mathbb{K}$.

Definizione 1.1. Uno spazio affine $n-$ dimensionale su $\mathbb{K}$ è l'insieme:
$\mathbb{A}^n = \mathbb{A}^n(\bar{\mathbb{K}}) = \{P = (x_1, ..., x_n) : x_i \in \bar{\mathbb{K}}\}$,
mentre denotiamo l'insieme delle sue coordinate razionali come:
$\mathbb{A}^n(\mathbb{K}) = \{P = (x_1, ..., x_n) \in \mathbb{A}^n,\ x_i \in \mathbb{K}\}$,

Sia $\bar{\mathbb{K}}[X] = \bar{\mathbb{K}}[X_1, ..., X_n]$ e $I \trianglelefteq \bar{\mathbb{K}}[X]$;
a tale ideale associamo l'insieme:
$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0, \forall f \in I\}$.

Definizione 1.2. Un insieme algebrico affine è un insieme della forma V_I.
Se V è un insieme algebrico, definiamo l'ideale associato a V come:
$I(V) = \{f \in \bar{\mathbb{K}}[X] \mid f(P) = 0, \forall P \in V\}$;
un insieme algebrico si dice definito su $\mathbb{K}$ se il suo ideale $I(V)$ può essere generato da polinomi in $\mathbb{K}[X]$; in tal caso denotiamo tale insieme con $V/\mathbb{K}$.

Osservazione 1.3. Per il teorema della base di Hilbert,
ogni ideale in $\bar{\mathbb{K}}[X]$ e in $\mathbb{K}[X]$ è finitamente generato.

Osservazione 1.4. Supponiamo che V è definito su $\mathbb{K}$ e supponiamo che $f_1, ..., f_m$ siano i generatori di $I(V/\mathbb{K}) := \{f \in \mathbb{K}[X] \mid f(P) = 0, \forall P \in V\}$,
allora $V/\mathbb{K} = \{P \in \mathbb{A}^n(\mathbb{K}) \mid f_1(P) = ... = f_m(P) = 0\}$.

Definizione 1.5. Un insieme algebrico affine V è chiamata varietà affine se $I(V)$ è un ideale primo di $\bar{\mathbb{K}}[X]$.

Definizione 1.6. Sia $V/\mathbb{K}$ una varietà;
l'anello delle coordinate di $V/\mathbb{K}$ è definito da:
$\mathbb{K}[V] := \mathbb{K}[X]/I(V/\mathbb{K})$.

Siccome $\mathbb{K}[V]$ è un dominio, ha senso considerare il suo campo dei quozienti:

$\mathbb{K}(V) := Frac(\mathbb{K}[V])$, chiamato campo delle funzioni di $V/\mathbb{K}$.

Definizione 1.7. Sia V una varietà;
la dimensione di V, denotata con $\dim(V)$, è il grado di trascendeza di $\bar{\mathbb{K}}(V)/\bar{\mathbb{K}}$.

Osservazione 1.8. $\dim(\mathbb{A}^n) = n$;
mentre se $V = \{P \in \mathbb{A}^n \mid f(P) = 0\}$,
con f un polinomio non costante allora $\dim(V) = n - 1$.

Definizione 1.9. Sia V una varietà, $P \in V$ e $f_1, ..., f_m \in \bar{\mathbb{K}}[X]$ generatori di $I(V)$;
allora V è non singolare o liscia in P se la matrice
$\left(\frac{\partial f_i(P)}{\partial x_j}\right)_{\substack{1\leq i\leq m \\ 1\leq j\leq n}}$, ha rango $n - \dim(V)$.

Definizione 1.10. Un polinomio $f \in \bar{\mathbb{K}}[X_0, ..., X_n]$ è omogeneo di grado d se per ogni $\lambda \in \bar{\mathbb{K}}$ vale $f(\lambda X_0, ..., \lambda X_n) = \lambda^d f(X_0, ..., X_n)$.
Un ideale $I \in \bar{\mathbb{K}}[X]$ si dice omogeneo se è generato da polinomi omogenei.

Ad ogni ideale omogeneo I associamo l'insieme
$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0$, per ogni f polinomio omogeneo in $I\}$.

Definizione 1.11. Un insieme algebrico proiettivo è un insieme della forma V_I per qualche ideale omogeneo I; se V è un insieme algebrico proiettivo, l'ideale omogeneo associato a V è l'ideale $I(V) \trianglelefteq \bar{\mathbb{K}}[X]$ generato da:

$\{f \in \bar{\mathbb{K}}[X] \mid f$ è omogeneo e $f(P) = 0, \forall P \in V\}$.
Se tale ideale omogeneo associato a V può essere generato da polinomi in $\mathbb{K}[X]$ si dice che V è definita su $\mathbb{K}$.

Definizione 1.12. Un insieme algebrico proiettivo è chiamato varietà proiettiva se il suo ideale omogeneo è primo.

Definiamo ora le mappe $\phi_i : \mathbb{A}^n \longrightarrow \mathbb{P}^n$, date da:

$\phi_i(y_1, ..., y_n) = [y_1, ..., y_{i-1}, 1, y_i, ..., y_n]$;

posto $H_i = \{X : X_i = 0\}$, iperpiano in $\mathbb{P}^n$,
e posto $U_i = \mathbb{P}^n \setminus H_i$, abbiamo una biiezione naturale:

$\phi_i^{-1} : U_i \longrightarrow \mathbb{A}^n$ data da:
$\phi_i^{-1}[x_0, ..., x_n] = \left(\frac{x_0}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\right)$.

Ora sia V un insieme algebrico proiettivo con ideale omogeneo $I(V)$,
allora $V \cap \mathbb{A}^n$, ovvero $\phi_i^{-1}(V \cap U_i)$, per qualche i,
è un insieme algebrico affine con ideale associato

$I(V \cap \mathbb{A}^n) = \{f(Y_1, ..., Y_{i-1}, 1, Y_i, ..., Y_n) \mid f(X_0, ..., X_n) \in I(V)\}$;

Osservazione 1.13. Il processo di rimpiazzare il polinomio $f(X_0, ..., X_n)$ con $f(Y_1, ..., Y_{i-1}, 1, Y_i, ..., Y_n)$ si chiama deomogenizzazione rispetto a X_i;

Osservazione 1.14. Notiamo che V è ricoperta dagli insiemi algebrici affini $V \cap U_0, ..., V \cap U_n$.

Viceversa per ogni $f(Y) \in \bar{\mathbb{K}}[Y]$ definiamo $f^*(X_0, ..., X_n) = X_i^d f\left(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right)$, l'omogenizzazione di f rispetto a X_i, con $d = deg(f)$.

Definizione 1.15. Sia $V \subset \mathbb{A}^n$ un insieme algebrico affine con ideale $I(V)$ e consideriamo V come sottoinsieme di $\mathbb{P}^n$ tramite la mappa ϕ_i;
denotiamo con $\bar{V}$ la chiusura proiettiva di V, come quell'insieme algebrico proiettivo il quale ideale omogeneo $I(\bar{V})$ è generato da: $\{f^*(X) : f(X) \in I(V)\}$.

Enunciamo ora una proposizione, senza però darne la dimostrazione, che comunque si può trovare in: [2,I.2.3].

Proposizione 1.16.
1) Sia V una varietà affine; allora $\bar{V}$ è una varietà proiettiva e $V = \bar{V} \cap \mathbb{A}^n$.
2) Sia V una varietà proiettiva; allora $V \cap \mathbb{A}^n$ è una varietà affine.

Definizione 1.17. Sia $V/\mathbb{K}$ una varietà proiettiva e scegliamo $\mathbb{A}^n \subset \mathbb{P}^n$ in modo che $V \cap \mathbb{A}^n \neq \emptyset$;
allora la dimensione di V è la dimensione di $V \cap \mathbb{A}^n$;
il campo delle funzioni di V denotato con $\mathbb{K}(V)$ è il campo delle funzioni di $V \cap \mathbb{A}^n$.

Definizione 1.18. Sia V una varietà proiettiva e $P \in V$ e scegliamo $\mathbb{A}^n \subset \mathbb{P}^n$ in modo che $P \in \mathbb{A}^n$;
allora V è non singolare in P se $V \cap \mathbb{A}^n$ non è singolare in P.

Osservazione 1.19. Il campo delle funzioni di una varietà proiettiva V può essere identificato con il campo delle funzioni razionali $\frac{f(X)}{g(X)}$, tali che:
1) f e g sono polinomi omogenei dello stesso grado.
2) $g \notin I(V)$.
3) Due funzioni $\frac{f_1}{g_1}$ e $\frac{f_2}{g_2}$ sono identificate se $f_1 g_2 - f_2 g_1 \in I(V)$.

I.2 **Mappe razionali tra varietà**.

Definizione 2.1. Siano V_1 e V_2 varietà proiettive in $\mathbb{P}^n$;
una mappa razionale da V_1 a V_2

è una mappa $\phi : V_1 \longrightarrow V_2$,
$\phi = [f_0, ..., f_n]$, ove le funzioni $f_i \in \bar{\mathbb{K}}(V_1)$ hanno la proprietà che per ogni punto $P \in V_1$ nel quale sono definite contemporaneamente, si ha $\phi = [f_0, ..., f_n] \in V_2$.

Definizione 2.2. Una mappa razionale $\phi = [f_0, ..., f_n] : V_1 \longrightarrow V_2$
è regolare in $P \in V_1$ se esiste una funzione $g \in \bar{\mathbb{K}}(V_1)$ tale che:
1) Ogni gf_i è regolare in P.
2) Esiste qualche i per cui $gf_i(P) \neq 0$.

Se una tale g esiste, poniamo:
$\phi(P) = [gf_0(P), ..., gf_n(P)]$.

Definizione 2.3. Una mappa razionale regolare in ogni punto si dice morfismo.

Definizione 2.4. Siano V_1 e V_2 varietà proiettive in $\mathbb{P}^n$;
diciamo che V_1 e V_2 sono isomorfe se esistono due morfismi
$f : V_1 \to V_2$, $g : V_2 \to V_1$ uno inverso dell'altro.

Osservazione 2.5. Per l'osservazione precedente e usando il trucchetto di moltiplicare per un polinomio omogeneo opportuno per pulire i denominatori, possiamo ridefinire una mappa razionale $\phi : V_1 \longrightarrow V_2$ come una mappa della forma
$\phi = [f_0(X), ..., f_n(X)]$, ove:
1) $f_i(X) \in \bar{\mathbb{K}}[X]$ sono polinomi omogenei, con lo stesso grado, non tutti in $I(V_1)$.
2) Per ogni $f \in I(V_2)$, $f(f_0(X), ..., f_n(X)) \in I(V_1)$.

Infine possiamo ridefinire la regolarità in questo modo:
una mappa razionale $\phi = [f_0, ..., f_n] : V_1 \longrightarrow V_2$ è regolare in $P \in V_1$,
se esistono polinomi omogenei $g_0, ..., g_n \in \bar{\mathbb{K}}[X]$ tali che:
1) $g_0, ..., g_n$ hanno lo stesso grado;
2) $f_i g_j \equiv f_j g_i \pmod{I(V_1)}$, per ogni $0 \leq i, j \leq n$.
3) $g_i(P) \neq 0$ per qualche i.

in tal caso poniamo: $\phi(P) = [g_0(P), ..., g_n(P)]$.

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [1].

Capitolo II

Gruppi topologici

Definizione 1.1. Un gruppo G equipaggiato con una topologia per cui la mappa: $(x, y) \longrightarrow xy^{-1}$ è continua, viene detto gruppo topologico.
Un sottogruppo di un gruppo topologico è un gruppo topologico per la topologia indotta.

Osservazione 1.2. Se G è un gruppo topologico allora le mappe:
$x \longrightarrow x^{-1}$ e $x \longrightarrow ax$ sono continue.

Esempi 1.3.
1) $\mathbb{R}^n$ è un gruppo topologico rispetto alla metrica euclidea.
2) Il gruppo $M_{n,m}(\mathbb{R})$, delle matrici n x m a entrate reali,
è un gruppo topologico se vediamo ogni matrice come un vettore in $\mathbb{R}^{nm}$,
e lo dotiamo della topologia euclidea.

Definizione 1.4. Uno spazio topologico si dice localmente compatto
se ogni suo elemento ha un intorno compatto.
Un gruppo topologico si dice localmente compatto
se un suo punto (ad esempio l'elemento neutro) possiede un intorno compatto
(basta la condizione su un elemento?).

Definizione 1.5. Un anello topologico A è un anello commutativo equipaggiato con una topologia per cui le mappe $(x, y) \longrightarrow x + y$ e $(x, y) \longrightarrow xy$ sono continue.

Osservazione 1.6. Si vede facilmente che combinando il secondo con il primo assioma si ottiene che la mappa $(x, y) \longrightarrow x - y$ è continua.
Quindi A è anche un gruppo topologico additivo.

Definizione 1.7. Un campo topologico $\mathbb{K}$ è un campo equipaggiato con una topologia tale che le seguenti mappe siano continue:
1)$(x, y) \longrightarrow x + y$.
2)$(x, y) \longrightarrow xy$.
3)$x \longrightarrow x^{-1}$, per ogni $x \neq 0$.

Definizione 1.8. Un campo con valutazione è un campo $\mathbb{K}$ in cui è definito un valore assoluto.

Proposizione 1.9.
Sia $(\mathbb{K}, |\cdot|)$ un campo con valutazione,
allora $\mathbb{K}$ è un campo topologico con la metrica $d(x, y) = |x - y|$.

Dim: La mappa $(x, y) \longrightarrow x - y$ è banalmente continua.
Ora occupiamoci della moltiplicazione:
abbiamo $\frac{x+h}{y+k} - \frac{x}{y} = \frac{hy-kx}{y(y+k)}$;

allora se $y \neq 0$ e $|k| < \frac{|y|}{2}$ e $c = max\{|x|, |y|\}$,

$|\frac{x+h}{y+k} - \frac{x}{y}| < 2c\frac{|h|+|k|}{|y|^2} \to 0$ $(|h|, |k| \to 0)$,
da cui la continuità della moltiplicazione. ■

Proposizione 1.10.
Sia $\mathbb{K}$ un campo con valutazione.
Allora il completamento $\hat{\mathbb{K}}$ del campo $\mathbb{K}$ è anche esso un campo con valutazione.

Dim: Il completamento $\hat{\mathbb{K}}$ è ovviamente un anello topologico,
e la mappa inversa è continua sull'insieme degli elementi invertibili.
Basta quindi mostrare che tale completamento è un campo:
sia $(x_n)_n$ una successione di Cauchy in $\mathbb{K}$ che definisce un elemento non nullo nel completamento; siccome dunque la successione $|x_n|$ non converge a 0, esiste una costante positiva $\varepsilon > 0$ e un indice $N > 0$ tali che $|x_n| > \varepsilon$, per tutti gli $n \geq N$.
La successione $\left(\frac{1}{x_n}\right)_{n \geq N}$ è anche essa di Cauchy (facile esercizio!);
la successione $\left(\frac{1}{x_n}\right)_n$, completata ponendo $x_n = 1$ per $n < N$,
è un'inversa della successione (x_n) nel completamento $\hat{\mathbb{K}}$. ■

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].
Un'altra buona referenza per studiare e approfondire
l'ambito dei gruppi topologici è [9].

Capitolo III

Gli interi $p-$adici

III.1 **Breve introduzione agli interi $p-$adici.**

Definizione 1.1. Un intero $p-$adico (con p numero primo) è una serie formale della forma $\sum_{n\geq 0} a_n p^n$, ove si possono scegliere i coefficienti a_n nell'insieme $\{0, 1, ..., p-1\}$
(attenzione: si può facilmente osservare che si otterrebbe lo stesso insieme di numeri $p-$adici se al posto dell'insieme $\{0, 1, ..., p-1\}$ si prendesse, ad esempio, l'insieme $\{-\frac{p-1}{2}, ..., 0, ..., \frac{p-1}{2}\}$, etc...);

Dando all'insieme di tutti i numeri $p-$adici una somma e una moltiplicazione naturale (somma e moltiplicazione di serie ma con l'aggiunta del riporto) si ottiene un anello denotato con $\mathbb{Z}_p$;

Definizione 1.2. L'ordine $p-$adico è la mappa $\nu : \mathbb{Z}_p \longrightarrow \mathbb{N}$
definita ponendo $v\left(\sum_{k\geq 0} a_k p^k\right) = min\{k : a_k \neq 0\}$;
essa soddisfa le seguenti proprietà:
$\nu(ab) = \nu(a)\nu(b)$
$\nu(a+b) \geq min\{\nu(a), \nu(b)\}$,
se $a, b, a+b$ non sono zero,
altrimenti si pone $\nu(0) = \infty$.

Definizione 1.3. Tale ordine induce un modulo naturale su $\mathbb{Z}_p$
definito ponendo $|a| = p^{-\nu(a)}$, detto modulo $p-$adico.

Proposizione 1.4.
$\mathbb{Z}_p$ è un dominio ad ideali principali.
In particolare tutti e soli i suoi ideali (a parte l'ideale nullo) sono della forma: $(p^n) = p^n\mathbb{Z}_p = \{x : x = \sum_{k\geq n} a_k p^k\}$;
Tali ideali soddisfano la seguente catena discendente:
$(1) \supseteq (p) \supseteq ... \supseteq (p^n) \supseteq ...$.
$\mathbb{Z}_p$ è un anello locale con ideale massimale (p),
e gruppo delle unità $\mathbb{Z}_p \setminus p\mathbb{Z}_p =: \mathbb{Z}_p^* = \{x = \sum_{k\geq 0} a_k p^k, a_0 \neq 0\}$
(dunque è ovvio osservare che $\mathbb{Z}_p$ è Noetheriano ma non Artiniano).

Dim: Dimostriamo che $\mathbb{Z}_p$ è un dominio:

l'anello commutativo $\mathbb{Z}_p$ non è 0, quindi basta mostrare che non ha 0-divisori:
siano $a = \sum_{i\geq 0} a_i p^i$ e $b = \sum_{i\geq 0} b_i p^i$, non nulli,
e poniamo $v = \nu(a)$ e $w = \nu(b)$ i loro ordini;
allora ne deriva facilmente che $p \nmid a_v b_w$,
e per definizione di moltiplicazione, il primo coefficiente non nullo del prodotto ab
è c_{v+w} che soddisfa: $0 < c_{v+w} < p$ e $c_{v+w} \equiv a_v b_w \pmod{p}$.
Dimostriamo che il gruppo delle unità di $\mathbb{Z}_p$ è proprio $\{x = \sum_{k\geq 0} a_k p^k, a_0 \neq 0\}$:
se un intero $p-$adico a è invertibile, allora anche la sua riduzione $\pmod{p}$ lo è:
questo mostra che $\mathbb{Z}_p^* \subset \{x = \sum_{k\geq 0} a_k p^k, a_0 \neq 0\}$.
Viceversa, dobbiamo dimostrare che ogni intero $p-$adico a di ordine $\nu(a) = 0$
è invertibile:
possiamo trovare un $0 < b_0 < p$ con $a_0 b_0 \equiv 1 \pmod{p}$
e scegliamo un $k \in \mathbb{Z}$ tale che $a_0 b_0 = 1 + kp$;
se scriviamo $a = a_0 + p\alpha$, allora $ab_0 = 1 + p\kappa$;
se dimostriamo che l'intero $p-$adico $1 + p\kappa$ è invertibile, deduciamo che a lo è.
Ma per fare ciò basta osservare che: $(1 + p\kappa)^{-1} = 1 - (\kappa p) + (\kappa p)^2 - ...$
$= 1 + c_1 p + c_2 p^2 + ...$, con i $c_1 \in \{0, 1, ..., p-1\}$.
Da quanto appena mostrato si deduce immediatamente che $\mathbb{Z}_p$ è un anello locale,
con unico ideale massimale: $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^*$.
Resta da dimostrare che tutti gli ideali di $\mathbb{Z}_p$ sono della forma (p^n):
sia $I \neq 0$ un ideale di $\mathbb{Z}_p$ e sia $a \neq 0$ un elemento in I con ordine minimale $k = \nu(a)$;
allora $a = p^k u$, con $u \in \mathbb{Z}_p^*$.
allora $p^k = u^{-1} a \in I$ e quindi $(p^k) \subset I$.
Viceversa, per ogni $b \in I$ sia $w = \nu(b) \geq k$
e scriviamo $b = p^w u' = p^k p^{w-k} u' \in p^k \mathbb{Z}_p$, da cui $I \subset (p^k)$. ■

Definizione 1.5. Il campo $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$ è il campo dei numeri $p-$adici.

Osservazione 1.6. Si vede facilmente che per $\mathbb{Q}_p$
valgono le seguenti rappresentazioni:
1)$\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.
2)$\mathbb{Q}_p = \bigcup_{m\geq 0} p^{-m}\mathbb{Z}_p$.
3)$\mathbb{Q}_p^* = \bigcup_{m\in\mathbb{Z}} p^m \mathbb{Z}_p^*$.

Da queste rappresentazioni ne risulta che possiamo estendere il valore assoluto $p-$adico
su tutto $\mathbb{Q}_p$ in questo modo: sia $x \in \mathbb{Q}_p^*$ allora $x = p^m u$, con $m \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^*$; poniamo
allora $\nu(x) = ord_p(x) = m$ e $|x| = p^{-m}$; infine poniamo $|0| = 0$.

III.2 **Topologia in $\mathbb{Z}_p$.**

Proposizione 2.1. Con l'addizione $\mathbb{Z}_p$ è un gruppo topologico.

Dim: Infatti se $|x-a| \leq |p^n|$ e $|y-b| \leq |p^n|$,
allora $|(x-y)-(a-b)| \leq |p^n|$,
da cui la continuità della mappa: $(x,y) \longrightarrow x-y$.
In più osserviamo che c'è un sistema fondamentale di intorni di 0 della forma:
$p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset ...$. ■

Proposizione 2.2.
$\mathbb{Z}_p^*$, con la moltiplicazione, è un gruppo topologico.

Dim: Infatti, se $a' \in a(1+p^n\mathbb{Z}_p)$ e $b' \in b(1+p^n\mathbb{Z}_p)$
allora $a'b'^{-1} \in ab^{-1}(1+p^n\mathbb{Z}_p)$,
da cui la continuità della mappa: $(x,y) \longrightarrow xy^{-1}$.
In più osserviamo che c'è un sistema fondamentale di intorni di 1 della forma:
$1+p\mathbb{Z}_p \supset 1+p^2\mathbb{Z}_p \supset ...$. ■

Proposizione 2.3.
Con la metrica $p-$adica l'anello $\mathbb{Z}_p$ è un anello topologico.
In più è uno spazio metrizzabile, compatto, completo.

Dim: Sappiamo già che $\mathbb{Z}_p$ è un gruppo topologico,
è sufficiente dimostrare la continuità della moltiplicazione:
fissiamo a e b in $\mathbb{Z}_p$, e consideriamo $x = a+h$ e $y = b+k$,
allora $|xy-ab| = |(a+h)(b+k)-ab| = |ak+bh-hk|$
$\leq max\{|a|,|b|\}(|h|+|k|)+|h||k| \to 0$, $(|h|,|k| \to 0)$,
che prova la continuità della moltiplicazione nel punto (a,b).
Il fatto che sia compatto deriva dalla rappresentazione come prodotto di insiemi equipaggiato della topologia prodotto: $\mathbb{Z}_p = \prod_{n\geq 0}\{0,1,...,p-1\}$;
da qui si vede anche che $\mathbb{Z}_p$ è totalmente sconnesso, visto che le sue componenti connesse sono solo i punti. Si vede infine facilmente che è completo, anzi che è il completamento dell'anello $\mathbb{Z}$ equipaggiato con la topologia indotta:
per vedere bene il processo di completamento, osserviamo che se $x = \sum_{n\geq 0} a_n p^n$
allora $x_m = \sum_{n=0}^{m} a_n p^n$ è una successione di Cauchy convergente a x. ■

Corollario 2.4.
L'addizione e la moltiplicazione di interi $p-$adici sono le uniche operazioni continue su $\mathbb{Z}_p$ che estendono le usuali addizioni e moltiplicazioni su $\mathbb{Z}$. ■

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].
Vedere anche [12].

Capitolo IV

Spazi ultrametrici

IV.1 **Valore assoluto ultrametrico.**

Osservazione 1.1. Il valore assoluto su $\mathbb{Q}_p$ è un valore assoluto ultrametrico, che oltre alla solite condizioni, verifica una condizione più forte della disuguaglianza triangolare, ovvero che $|x+y| \leq max\{x,y\}$.
Ovviamente la distanza indotta $d(x,y) = |x-y|$, verifica la stessa proprietà.

Osservazione 1.2. Più in generale, per induzione, osserviamo che la distanza ultrametrica verifica la seguente disuguaglianza: $d(x_1,x_n) \leq max\{d(x_1,x_2),...,d(x_{n-1},x_n)\}$;
consideriamo ora un ciclo di $n \geq 3$ punti distinti x_i, $1 \leq i \leq n$, e $x_{n+1} = x_1$;
possiamo assumere $d(x_1,x_n) = \max\limits_{i \leq n} d(x_i,x_{i+1})$
e ricordando che vale $d(x_1,x_n) \leq max\{d(x_1,x_2),...,d(x_{n-1},x_n)\}$,
allora $d(x_1,x_n) = d(x_i,x_{i+1})$, per almeno un indice $1 \leq i \leq n-1$;
quindi un ciclo ha almeno due coppie di punti consecutivi con distanza uguale e massimale; in particolare in un insieme di 3 elementi almeno due coppie hanno uguale lunghezza: in uno spazio ultrametrico, ogni triangolo è isoscele o equilatero, con al più un lato più corto.

In totale abbiamo ottenuto il seguente

Lemma 1.3.
Sia (X,d) spazio ultrametrico,
allora valgono le seguenti affermazioni:
1)Se $d(x,z) > d(z,y) \Rightarrow d(x,z) = d(x,y)$.
2)Se $d(x,z) \neq d(z,y) \Rightarrow d(x,y) = max\{d(x,z),d(z,y)\}$. ■

Lemma 1.4.
1)Una successione $(x_n)_n$, con $d(x_n,x_{n+1}) \to 0$, $(n \to \infty)$,
è una successione di Cauchy.
2)Se $x_n \to x \neq a$, allora definitivamente $d(x_n,a) = d(x,a)$.

Dim: 1)Se $d(x_n,x_{n+1}) < \varepsilon, \forall n \geq N$,
allora $d(x_n,x_{n+m}) \leq \max\limits_{0 \leq i < m} d(x_{n+i},x_{n+i+1}) < \varepsilon, \forall n \geq N, \forall m$.
2)In effetti, $d(x_n,a) = d(x,a)$ non appena $d(x_n,x) < d(x,a)$. ■

Definizione 1.5. Sia G un gruppo abeliano equipaggiato con una metrica invariante d, che soddisfi cioè, $d(x+z,y+z) = d(x,y), \forall x,y,z \in G$;
per ogni $x \in G$ definiamo $|x| = d(x,0)$;

allora $|-x| = |x|$ e $|x+y| \leq |x| + |y|$.
Questo mostra che G è un gruppo topologico.
Se poi tale metrica d soddisfa la disuguaglianza ultrametrica,
anche il modulo si comporterà allo stesso modo.
In tal caso vale la regola che il più grande vince:
se $|x| > |y| \Rightarrow |x+y| = |x|$

Osservazione 1.6. Consideriamo una successione $(a_n)_n$ in un gruppo abeliano ultrametrico completo e sia $s_n = \sum_{i<n} a_i$, supponendo che $s_n \to s$, $(n \to \infty)$;
allora $a_n = s_{n+1} - s_n \to 0$;
viceversa se $a_n \to 0$ allora la successione s_n sarà di Cauchy e quindi convergente.
Dunque in un gruppo abeliano ultrametrico completo una serie $\sum_{k\geq 0} a_k$ converge se e soltanto se $a_n \to 0$, $(n \to \infty)$.

IV.2 **Spazi vettoriali su $\mathbb{Q}_p$.**

Proposizione 2.1.
Sia V uno spazio vettoriale finito dimensionale su $\mathbb{Q}_p$.
Allora tutte le norme su V sono equivalenti.

Dim: Sia $n = \dim(V)$ e scegliamo una base $(e_i)_{1\leq i\leq n}$ di V.
Allora abbiamo una mappa $\phi(x) : \mathbb{Q}_p^n \longrightarrow V$,
definita ponendo $\phi(x) = \phi((x_1, ..., x_n)) = \sum_{k=1}^{n} x_i e_i$,
che definisce un isomorfismo algebrico.
Dotiamo lo spazio $\mathbb{Q}_p^n$ della norma dell'estremo superiore: $||x||_\infty = \sup_{1\leq i\leq n} |x_i|$;
dobbiamo dimostrare che l'isomorfismo ϕ è bicontinuo:
$||\sum_i x_i e_i|| \leq max||x_i e_i|| = max|x_i|||e_i|| \leq max|x_i| max||e_i|| = C||x||_\infty$;
allora $||\phi(x)|| \leq C||x||_\infty$, quindi ϕ è continua.
Infine dimostriamo che ϕ è una mappa aperta:
Sia $B = \{x \in \mathbb{Q}_p^n : ||x||_\infty \leq 1\}$;
mostreremo che $\phi(B)$ contiene una palla aperta di V di raggio positivo centrata in 0.
Sia $S_1 = \{x \in \mathbb{Q}_p^n : ||x||_\infty = 1\}$,
allora S_1 è un sottospazio chiuso del compatto B, quindi è compatto;
quindi $\phi(S_1)$ è compatto; in più tale immagine non contiene l'origine di V per la biettività di ϕ;
allora la distanza tra 0 e $\phi(S_1)$ è positiva ed il minimo è assunto in un valore $\phi(x_0)$;
$x \in S_1 \Rightarrow ||\phi(x)|| \geq ||\phi(x_0)|| \geq \varepsilon > 0$.
Ora se $v \in V \setminus 0$ ha norma $||v|| < \varepsilon$ allora $||\lambda v|| < \varepsilon$, $\forall \lambda : |\lambda| \leq 1$;
quindi se $||v|| < \varepsilon$ allora $\lambda \in \mathbb{K}, |\lambda| \leq 1 \Rightarrow \lambda v \notin \phi(S_1)$.

Ora possiamo scrivere $v = \sum_{k=1}^{n} v_i e_i = \phi((v_i))$
e possiamo supporre che $|v_n| = max|v_i|$;
prendiamo allora $\lambda = \frac{1}{v_n}$, allora $\lambda v = \phi((\frac{v_i}{v_n})) = \phi(w) \in \phi(S_1)$;
allora deve succedere che $|\lambda| > 1$ cosi che $||(v_i)||_\infty < 1$.
Questo mostra che $v = \phi((v_i))$, con $||v_i||_\infty < 1$
e quindi $v \in \phi(B)$ e infine $B_{<\varepsilon}(V) \subset \phi(B)$. ■

Corollario 2.2.
Siano V e W due spazi vettoriali finito dimensionali normati su $\mathbb{Q}_p$ e $\alpha : V \longrightarrow W$ una mappa lineare; allora α è continua. ■

Sia $\mathbb{K}$ estensione di $\mathbb{Q}_p$ considerato come spazio vettoriale su $\mathbb{Q}_p$;
ogni valore assoluto che estende quello $p-$adico è una norma ultrametrica su $\mathbb{K}$.

Proposizione 2.3.
C'è al più un valore assoluto su $\mathbb{K}$ che estende quello su $\mathbb{Q}_p$.

Dim: siano $|.|_1$ e $|.|_2$ due valori assoluti su $\mathbb{K}$ che estendono quello su $\mathbb{Q}_p$;
per la proposizione IV.2.1 queste due norme sono equivalenti e quindi esistono costanti $0 < c \leq C < \infty$ tali che $c|x|_1 \leq |x|_2 \leq C|x|_1$;
allo stesso modo: $c|x^n|_1 \leq |x^n|_2 \leq C|x^n|_1$ e quindi $c|x|_1^n \leq |x|_2^n \leq C|x|_1^n$
oppure $|x|_1 c^{\frac{1}{n}} \leq |x|_2 \leq |x|_1 C^{\frac{1}{n}}$
e mandando $n \to \infty$ e siccome $c^{\frac{1}{n}} \to 1$ e $C^{\frac{1}{n}} \to 1$
si ottiene $|x|_1 = |x|_2$, $x \in \mathbb{K}$. ■

Osservazione 2.4. Sia $\mathbb{K}$ un'estensione di Galois di $\mathbb{Q}_p$
e supponiamo che esista un'estensione del valore assoluto p-adico a tutto $\mathbb{K}$;
allora per ogni automorfismo σ di $\mathbb{K}/\mathbb{Q}_p$,
possiamo considerare il valore assoluto: $|x|' = |\sigma(x)|$
e per la proposizione questo valore assoluto coincide con quello iniziale;
Ora sia $G = Gal(\mathbb{K}/\mathbb{Q}_p)$ e per ogni $x \in \mathbb{K}$ consideriamo l'elemento:
$N(x) = \prod_{\sigma \in G} \sigma(x) \in \mathbb{Q}_p$;
abbiamo $|N(x)| = |x|^{\sharp G}$; dunque $|x| = |N(x)|^{\frac{1}{\sharp G}}$.

Sia $\mathbb{K}$ un'estensione finita di grado d di $\mathbb{Q}_p$,
e indichiamo con N la mappa $N : \mathbb{K}^* \longrightarrow \mathbb{Q}_p^*$
che manda x in $N(x)$;
essa può essere definita immergendo $\mathbb{K}$ in un estensione di Galois L e poi prendendo il prodotto di tutte le d distinte immersioni $\mathbb{K} \hookrightarrow L$.

Prima di procedere enunciamo il seguente

Lemma 2.5.
Sia f un valore assoluto generalizzato su un campo $\mathbb{K}$;
(cioè un valore assoluto che verifica rispetto alla somma una disuguaglianza del tipo: $f(x+y) \leq Cmax\{f(x), f(y)\}$, con $C > 0$ costante).
Se f è limitato sull'immagine dei numeri naturali,
allora è un valore assoluto ultrametrico.

Dim: supponiamo in prima istanza $n = 2^r$
allora $f(a_1 + a_2) \leq Cmax\{f(a_1), f(a_2)\}$,
$f(a_1 + a_2 + a_3 + a_4) \leq C^2 max\{f(a_1), f(a_2), f(a_3), f(a_4)\}$
e iterando per induzione
$f\left(\sum_{k=1}^{n} a_k\right) \leq C^r max\{f(a_1), ..., f(a_n)\}$;
consideriamo ora $(1+x)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^k$,
allora abbiamo $f((1+x)^{n-1}) \leq C^r \max_i \{f\left(\binom{n-1}{k}\right) f(x^i)\}$;
se f è limitato sull'immagine di $\mathbb{N}$ in $\mathbb{K}$,
abbiamo $f(k) \leq A, \forall k \in \mathbb{N}$
e quindi $f((1+x)^{n-1}) \leq C^r A\ max\{1, f(x)^{n-1}\}$;
dunque $f(1+x) \leq C^{\frac{r}{n-1}} A^{\frac{1}{n-1}} max\{1, f(x)\}$
e mandando $n \to \infty$ otteniamo $f(1+x) \leq max\{1, f(x)\}$
e poi in generale, fissati $a \neq 0$ e $b \in \mathbb{K}$, abbiamo
$f(a) \neq 0$ e $f(a+b) = f(a)f\left(1 + \frac{b}{a}\right) \leq f(a)max\{1, f\left(\frac{b}{a}\right)\} \leq max\{f(a), f(b)\}$. ■

Teorema 2.6.
Sia $\mathbb{K}$ un'estensione finita di grado d del campo $\mathbb{Q}_p$ dei numeri $p-$adici.
allora per ogni $x \in \mathbb{K}$, $f(x) = |N(x)|^{\frac{1}{d}}$
definisce l'unico valore assoluto su $\mathbb{K}$ che estende quello $p-$adico.

Dim: Se $a \in \mathbb{Q}_p$ è ovvio che $N(a) = a^d$ e quindi che $|a| = |N(a)|^{\frac{1}{d}}$ e quindi che tale formula descrive un'estensione del valore assoluto $p-$adico.
In più è ovvio che $f(xy) = f(x)f(y)$.
Resta da dimostrare la disuguaglianza ultrametrica:
scegliamo una qualsiasi norma su $\mathbb{K}$ tale che $||\mathbb{K}|| = |\mathbb{Q}_p|$, ad esempio, scegliamo una base $e_1, ..., e_d$ di $\mathbb{K}$ su $\mathbb{Q}_p$ e usiamo la norma dell'estremo superiore sulle componenti in tale base.
Ricordiamo ora che, visto che $\mathbb{Q}_p$ è localmente compatto,
(infatti $\mathbb{Z}_p$ è, dentro $\mathbb{Q}_p$, la palla unitaria centrata nell'origine;
per $x \in \mathbb{Q}_p$ abbiamo le seguenti equivalenze:
$x \in \mathbb{Z}_p \Leftrightarrow v(x) \geq 0 \Leftrightarrow |x| \leq 1 \Leftrightarrow d(x,0) \leq 1$;
similmente se $k \geq 0$, l'ideale $p^k\mathbb{Z}_p$ è la palla centrata in zero definita da $d(x,0) \leq p^{-k}$;
tali palle formano un sistema fondamentale di intorni di 0 in $\mathbb{Z}_p$ e in $\mathbb{Q}_p$;
Siccome $\mathbb{Z}_p$ contiene un intorno di 0, è aperto e chiuso, (Facile esercizio!) anzi è un

intorno compatto di 0 in $\mathbb{Q}_p$ e questo prova che $\mathbb{Q}_p$ è localmente compatto)
allora $\mathbb{K} \cong \mathbb{Q}_p^d$ è localmente compatto.
Siccome la funzione f è continua e non si annulla sull'insieme compatto $||x|| = 1$, è limitata superiormente e inferiormente su questo insieme,
ovvero: $0 < \varepsilon \leq f(x) \leq A < \infty$, per $||x|| = 1$.
Per $x \in \mathbb{K}^*$ scegliamo $\lambda \in \mathbb{Q}_p$ con $||x|| = |\lambda|$;
quindi $\frac{x}{\lambda}$ ha norma 1, per cui vale che $\varepsilon \leq f(\frac{x}{\lambda}) \leq A$, e siccome $f(\frac{x}{\lambda}) = \frac{f(x)}{|\lambda|}$, abbiamo $\varepsilon|\lambda| \leq f(x) \leq A|\lambda|$ e dunque $\varepsilon||x|| \leq f(x) \leq A||x||$;
allora se poniamo $a = \varepsilon^{-1}$ abbiamo $||x|| \leq af(x)$ e $f(x) \leq A||x||$;
supponiamo ora $f(x) \leq 1$, allora
$f(1+x) \leq A||1+x|| \leq Amax\{||1||, ||x||\} \leq Amax\{||1||, a\} = C = Cmax\{f(1), f(x)\}$.
In generale se $f(y) \geq f(x)$ applichiamo la disuguaglianza appena trovata ad $\frac{x}{y}$,
infine moltiplicando entrambi i lati per $f(y)$ otteniamo: $f(x+y) \leq Cmax\{f(x), f(y)\}$.
Questo mostra che f è un valore assoluto generalizzato e visto che estende il valore assoluto $p-$adico, lui è limitato su $\mathbb{N}$ e quindi è un valore assoluto ultrametrico. ■

Osservazione 2.7. A questo punto siamo pronti per estendere il valore assoluto $p-$adico a tutto $\bar{\mathbb{Q}}_p$:
sia $x \in \bar{\mathbb{Q}}_p$ allora esiste un'estensione finita di $\mathbb{Q}_p$ tale che $x \in \mathbb{K}$; possiamo dunque estendere il valore assoluto $p-$adico a tutto $\mathbb{K}$ e definire in modo univoco $|x|$; iterando questo ragionamento per ogni $x \in \bar{\mathbb{Q}}_p$ e sfruttando l'unicità dell'estensione del valore assoluto per estensioni finite di $\mathbb{Q}_p$, si ottiene l'estensione globale e ben definita desiderata.

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].

Capitolo V

Il campo $\mathbb{C}_p$

V.1 **Algoritmo di Newton**.

Proposizione 1.1.
Sia A un anello e $P \in A[X]$, allora esistono polinomi P_1, P_2 in $A[X,Y]$ tali che:
$P(X+h) = P(X) + h \cdot P_1(X,h) = P(X) + h \cdot P'(X) + h^2 P_2(X,h)$.

Dim: Supponiamo $P(X) = \sum a_n X^n$, una somma finita,
allora $P(X+h) = \sum a_n (X+h)^n = \sum a_n X^n + h \sum n a_n X^{n-1} + h^2 \cdot P_2(X,h)$. ■

Proposizione 1.2 (Algoritmo di Newton).
Sia $P(X) \in \mathbb{Z}_p[X]$ e $x \in \mathbb{Z}_p$ tale che $P(x) \equiv 0 \pmod{p^n}$;
se $k = \nu(P'(x)) < \frac{n}{2}$, allora $y = N_P(x) = x - \frac{P(x)}{P'(x)}$ soddisfa:
1)$P(y) \equiv 0 \pmod{p^{n+1}}$.
2)$y \equiv x \pmod{p^{n-k}}$.
3)$\nu(P'(y)) = \nu(P'(x))$.

Dim: Poniamo $P(x) = p^n z$, $z \in \mathbb{Z}_p$ e $P'(x) = p^k u$, $u \in \mathbb{Z}_p^*$;
allora è immediato che: $y - x = -\frac{P(x)}{P'(x)} = -p^{n-k} z u^{-1}$;
in più $P(y) = P(x) - \frac{P(x)}{P'(x)} P'(x) + (y-x)^2 t$ e per la proposizione V.1.1 $t \in \mathbb{Z}_p$.
Di conseguenza $P(y) = (y-x)^2 t \in p^{2n-2k}\mathbb{Z}_p \subset p^{n+1}\mathbb{Z}_p$.
Infine $P'(y) = P'(x + (y-x)) = P'(x) + (y-x)s = p^k u + p^{n-k} w s = p^k v$;
in particolare $v = u + p^{n-2k} w s \in u + p\mathbb{Z}_p \subset \mathbb{Z}_p^*$;
quindi $\nu(P'(y)) = k$. ■

V.2 **Lemma di Hensel**.

Teorema 2.1 (Lemma di Hensel).
Supponiamo che $P \in \mathbb{Z}_p[X]$ e $x \in \mathbb{Z}_p$ soddisfino $P(x) \equiv 0 \pmod{p^n}$,
allora se $k = \nu(P'(x)) < \frac{n}{2}$, esiste un'unica radice $\xi \in \mathbb{Z}_p$ di P
tale che $\xi \equiv x \pmod{p^{n-k}}$ e $\nu(P'(\xi)) = \nu(P'(x))$.

Dim: Esistenza: Sia $x_0 = x$ e definiamo una approsimazione x_1 della radice,
sfruttando l'algortimo di Newton, che soddisfi $x_1 \equiv x_0 \pmod{p^{n-k}}$
e $P(x_1) \equiv 0 \pmod{p^{n+1}}$ e $\nu(P'(x_1)) = \nu(P'(x_0))$.
Similmente possiamo trovare un'approssimazione x_2 della radice che migliori l'approssimazione x_1 e che soddisfi $x_2 \equiv x_1 \pmod{p^{n-k+1}}$
e $P(x_2) \equiv 0 \pmod{p^{n+2}}$ e $\nu(P'(x_2)) = \nu(P'(x_1))$.

Iterando il procedimento ottieniamo una successione di Cauchy $(x_n)_n$ in $\mathbb{Z}_p$ (spazio ultrametrico completo) che converge in modulo $p-$adico ad un certo ξ che verifica $P(\xi) = 0$ e $\xi \equiv x \pmod{p^{n-k}}$.

Unicità: Siano ξ, η due radici di P che soddisfano le condizioni richieste;
allora $\xi \equiv \eta \pmod{p^{n-k}}$ e siccome $n > 2k$
allora $n - k \geq k + 1$ e quindi $\xi \equiv \eta \pmod{p^{k+1}}$;
ora $P(\eta) = P(\xi) + P'(\xi)(\eta - \xi) + (\eta - \xi)^2 a$
e da qui si ricava subito $(\eta - \xi)(P'(\xi) + (\eta - \xi)a) = 0$;
ma $P'(\xi) + (\eta - \xi)a \neq 0$, visto che il suo ordine è superiore a k, dunque $\eta = \xi$. ■

Per i nostri futuri scopi, premettiamo una definizione:

Definizione 2.2. Definiamo $\mathcal{O}_{\mathbb{C}_p} = \{x \in \mathbb{C}_p : |x| \leq 1\}$,
anello locale contenuto in $\mathbb{C}_p$,
e definiamo $\mathfrak{p}_{\mathbb{C}_p} = \{x \in \mathbb{C}_p : |x| < 1\}$,
l'ideale massimale di $\mathcal{O}_{\mathbb{C}_p}$.
Infine il quoziente $\mathcal{O}_{\mathbb{C}_p}/\mathfrak{p}_{\mathbb{C}_p}$ è il campo residuo di $\mathbb{C}_p$.

Osservazione 2.3. Questa costruzione è generale:
preso un campo ultrametrico $\mathbb{K}$, si definiscono $\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{p}_{\mathbb{K}}$ esattamente come sopra e infine il campo residuo di $\mathbb{K}$ sarà il loro quoziente.

Osservazione 2.4. Il lemma di Hensel vale anche per polinomi in $\mathcal{O}_{\mathbb{K}}[X]$, con $\mathbb{K}$ estensione finita di $\mathbb{Q}_p$, e si ottiene come sopra, ovvero prendendo i risultati V.1.1., V.1.2, V.2.1 e piazzando al posto di $\mathbb{Z}_p$ l'anello $\mathcal{O}_{\mathbb{K}}$.

V.3 **Il campo** $\bar{\mathbb{Q}}_p$.

Proposizione 3.1.
Il campo $\bar{\mathbb{Q}}_p$, chiusura algebrica di $\mathbb{Q}_p$, non è completo.

Dim: Sia $\alpha = \sum_{n=1}^{\infty} \zeta_{n'} p^n$,
ove $n' = n$ se $(n, p) = 1$, altrimenti $n' = 1$.
Se per assurdo $\bar{\mathbb{Q}}_p$ è completo, allora la serie, che è certamente di Cauchy,
convergerà ad un elemento $\alpha \in \bar{\mathbb{Q}}_p$;
allora α vive in un'estensione finita $\mathbb{K}$ di $\mathbb{Q}_p$;
supponiamo che $\zeta_{n'} \in \mathbb{K}, \forall n < m$;
possiamo assumere che $p \nmid m$;
allora $\beta = p^{-m} \left(\alpha - \sum_{n=1}^{m-1} \zeta_{n'} p^n \right) \in \mathbb{K}$ e $\beta \equiv \zeta_m \pmod{p}$;
allora $X^m - 1 \equiv 0 \pmod{p}$ ha soluzioni in $\mathbb{K}$.

Per il Lemma di Hensel, (siccome $p \nmid m$) $\mathbb{K}$ contiene una soluzione di $X^m - 1 = 0$
che è congruente a $\beta \pmod{p}$, e quindi a $\zeta_m \pmod{p}$;
ora siccome le $m-$esime radici dell'unità sono distinte $\pmod{p}$,
(vedi VI.1.3) segue che $\zeta_m \in \mathbb{K}$;
in più per induzione $\zeta_m \in \mathbb{K}$ per tutti gli m non divisibili per p;
ma le radici dell'unità coprime con p sono distinte $\pmod{p}$, (vedi sempre VI.1.3)
quindi quanto appena dimostrato ci dice che abbiamo infinite classi residue distinte
$\pmod{p}$ nell'anello degli interi di $\mathbb{K}$;
ma l'estensione $\mathbb{K}/\mathbb{Q}_p$ è finita, e questo porta a una contraddizione. ■

V.4 **Il campo $\mathbb{C}_p$.**

Definizione 4.1. Poniamo $\mathbb{C}_p$ come il completamento rispetto al valore assoluto $p-$adico di $\bar{\mathbb{Q}}_p$.

Proposizione 4.2.
Il campo $\mathbb{C}_p$ è algebricamente chiuso.

Dim: Per prima cosa dimostriamo il seguente

Lemma 4.3 (Krasner).
Supponiamo $\mathbb{K}$ un campo completo rispetto ad un valore assoluto non-Archimedeo,
(ad esempio quello $p-$adico);
siano $\alpha, \beta \in \bar{\mathbb{K}}$, con α separabile su $\mathbb{K}(\beta)$.
Infine supponiamo che per tutti i coniugati, $\alpha_i \neq \alpha$,
di α valgano le seguenti disuguaglianze:
$|\beta - \alpha| < |\alpha - \alpha_i|$,
(ove $|\cdot|$ indica l'unica estensione del valore assoluto $p-$adico a tutto $\mathbb{K}$)
allora $\mathbb{K}(\alpha) \subset \mathbb{K}(\beta)$.

Dim: Consideriamo l'estensione $\mathbb{K}(\alpha, \beta)/\mathbb{K}(\beta)$ e sia $L/\mathbb{K}(\beta)$ la chiusura di Galois;
sia $\sigma \in Gal(L/\mathbb{K}(\beta))$, allora $\sigma(\beta - \alpha) = \beta - \sigma(\alpha)$;
per l'unicità dell'estensione del valore assoluto, abbiamo che:
$|\beta - \sigma(\alpha)| = |\beta - \alpha| < |\alpha_i - \alpha|$, per tutti gli $\alpha_i \neq \alpha$;
di conseguenza $|\alpha - \sigma(\alpha)| \leq max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\} < |\alpha_i - \alpha|$;
da qui segue che $\sigma(\alpha) = \alpha$ e che quindi $\alpha \in \mathbb{K}(\beta)$. ■

Ritorniamo ora alla dimostrazione della proposizione:
supponiamo che α sia algebrico su $\mathbb{C}_p$ e sia $f(X)$ il suo polinomio monico irriducibile;
siccome $\bar{\mathbb{Q}}_p$ è denso in $\mathbb{C}_p$, possiamo scegliere un polinomio monico $g(X) \in \bar{\mathbb{Q}}_p[X]$
i quali coefficienti siano molto vicini a quelli di $f(X)$;
allora $g(\alpha) = g(\alpha) - f(\alpha)$ è molto vicino a 0;
scrivendo $g(X) = \prod_j (X - \beta_j)$, osserviamo che per qualche radice β di $g(X)$ deve
accadere che $|\alpha - \beta|$ è piccolo;

in particolare possiamo scegliere $g(X)$ e poi β in modo che $|\alpha - \beta| < |\alpha - \alpha_i|$,
per tutti i coniugati α_i di α (e distinti da α)
allora per il lemma di Krasner $\alpha \in \mathbb{C}_p(\beta) = \mathbb{C}_p$. ■

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3],
per quanto riguarda l'algoritmo di Newton e il lemma di Hensel;
mentre la dimostrazione della non completezza di $\bar{\mathbb{Q}}_p$ e del fatto che $\mathbb{C}_p$ è algebricamente chiuso, provengono da [4].
Per approfondire meglio tutti i concetti appena accennati nella definizione V.2.2, vedere sempre [3] o [5], il primo capitolo, o ancora meglio [6].

Capitolo VI

Radici dell'unità

Definizione 1.1. Con la scrittura $\mu_{p^\infty}(\mathbb{K})$, intendiamo l'insieme di tutte le radici dell'unità in $\mathbb{K}$ di ordine una potenza del primo p ; con la scrittura $\mu_{(p)}(\mathbb{K})$ intendiamo l'insieme delle radici dell'unita in $\mathbb{K}$ di ordine coprimo con p; infine con la scrittura $\mu(\mathbb{K})$ intendiamo l'insieme di tutte le radici dell'unità in $\mathbb{K}$.

Proposizione 1.2.
Sia $\mathbb{K}$ un'estensione ultrametrica di $\mathbb{Q}_p$;
allora $\mu_{p^\infty}(\mathbb{K}) = \mu(\mathbb{K}) \cap (1 + \mathfrak{p}_\mathbb{K})$.

Dim: Per prima cosa, se $\zeta \in \mu(\mathbb{K})$ ha come ordine una potenza del primo p,
denotata con $\bar{\zeta}$ la riduzione di ζ modulo $\mathfrak{p}_\mathbb{K}$,
allora $\zeta^{p^f} = 1 \Rightarrow \bar{\zeta}^{p^f} = \bar{1} \Rightarrow \zeta \in 1 + \mathfrak{p}_\mathbb{K}$,
siccome il campo residuo di $\mathbb{K}$ ha caratteristica p.
Viceversa, se $\zeta \in 1 + \mathfrak{p}_\mathbb{K}$ ha ordine $n > 1$, scriviamo $\zeta = 1 + \xi$, con $0 < |\xi| < 1$;
allora $1 = (1 + \xi)^n = 1 + \xi(n + \xi\alpha)$,
che implica $n + \xi\alpha = 0$ e che $|n| = |\xi\alpha| \leq |\xi| < 1$, che implica $p|n$;
ora se $n \neq p$ ripetiamo questi ragionamenti con ζ^p al posto di ζ, che ha ordine $\frac{n}{p} > 1$;
alla fine troviamo che n è una potenza di p.

Corollario 1.3.
Se indichiamo con $\varepsilon : \mathcal{O}_\mathbb{K} \longrightarrow \mathcal{O}_\mathbb{K}/\mathfrak{p}_\mathbb{K}$,
la riduzione modulo $\mathfrak{p}_\mathbb{K}$, allora:
la restrizione di ε a $\mu(\mathbb{K})$ ha kernel $\mu_{p^\infty}(\mathbb{K})$;
è iniettiva su $\mu_{(p)}(\mathbb{K})$: la distanza tra due distinte radici dell'unità
di ordine coprimo con p è 1. Questo implica che tali radici hanno una riduzione modulo $\mathfrak{p}_\mathbb{K}$ distinta. ■

Proposizione 1.4.
La distanza tra due radici p-esime dell'unità, con $p \neq 2$ primo, è $|p|^{\frac{1}{p-1}}$.

Dim: Basta dimostrare che, presa ζ radice p-esima dell'unità,
vale $|1 - \zeta| = |1 - \zeta^i| = |p|^{\frac{1}{p-1}}$, per ogni indice $i = 1, ..., p-1$:
a tal proposito, fissata una radice primitiva ζ,
consideriamo il polinomio ciclotomico $\phi_p(X) = \prod_{i=1}^{p-1}(X - \zeta^i)$.
Allora $\phi_p(1) = p = \prod_{i=1}^{p-1}(1 - \zeta^i)$;

ora ricordandoci dell'unicità dell'estensione del valore assoluto $p-$adico per le estensione finite di $\mathbb{Q}_p$ e osservando che tutti i termini $(1-\zeta^i)$ sono coniugati tra loro, otteniamo: $|1-\zeta|^{p-1} = |1-\zeta^i|^{p-1} = |p|$, da cui la tesi. ■

Tutto ciò si può generalizzare nella seguente

Proposizione 1.5.
Sia ζ radice dell'unità di ordine p^t, $t \geq 1$;
Allora $|\zeta - 1| = |p|^{\frac{1}{\varphi(p^t)}}$, con $\varphi(n)$ la funzione totiente di Eulero.

Dim: La lasciamo come esercizio al lettore. ■

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].

Capitolo VII

Gruppo di Galois assoluto di $\mathbb{F}_p$

VII.1 **Limite proiettivo**.

Definizione 1.1. Un sistema inverso di gruppo topologici su I è un oggetto della forma (I, G_i, π_{ji}) tali che:
1) $(I, \geq)$ è un sistema diretto,
ovvero un insieme parzialmente ordinato con un ordinamento $\geq$ in cui per ogni coppia a, b di elementi in I esiste un elemento $c \in I$ tale che $a \leq c$ e $b \leq c$.
2) G_i è un gruppo topologico,$\forall i$
(osserviamo che tale costruzione non vale solo per gruppi, ma si può estendere facilmente ad anelli, moduli oppure si può dare tale definizione solo per insiemi).
3) Per ogni $i \leq j$ in I, π_{ji} è un morfismo di gruppi topologici da G_j ad G_i,
tale che per ogni $i \in I$ π_{ii} è l'identità, e per ogni $i \leq j \leq k$ in I si ha $\pi_{ji} \circ \pi_{kj} = \pi_{ki}$.

Definizione 1.2. Sia $(G_i)_i$ un sistema inverso di gruppi;
definiamo $L = \{(x_i) \in \prod G_i \mid i \leq j \Rightarrow \pi_{ji}(x_j) = x_i\}$;
infine dotiamo tutti i gruppi G_i di una struttura topologica (al limite quella discreta) e diamo a $\prod G_i$ la topologia prodotto e ad L la topologia di sottospazio;
allora L è detto limite inverso dei G_i e viene indicato con $L = \varprojlim_i G_i$.

Osservazione 1.3. È possibile dare anche un'altra definizione,
utile in alcune occasioni, di limite inverso:
una successione $(E_n, \phi_n)_n$ di insiemi e di mappe $\phi_n : E_{n+1} \longrightarrow E_n$ è chiamata sistema proiettivo.
Un insieme E con delle mappe $\psi_n : E \longrightarrow E_n$ tali che $\psi_n = \phi_n \circ \psi_{n+1}$, è chiamato un limite proiettivo della successione $(E_n, \phi_n)_n$ se per ogni altro insieme X e per ogni successione di mappe $f_n : X \longrightarrow E_n$ con $f_n = \phi_n \circ f_{n+1}$, esiste un unica mappa $f : X \longrightarrow E$ tale che $f_n = \psi_n \circ f$.

Le due definizioni sono collegate dal seguente

Teorema 1.4.
Per ogni sistema proiettivo $(E_n, \phi_n)_{n \geq 0}$ (secondo la definizione dell'osservazione VII.1.3) c'è un limite proiettivo $E = \varprojlim_n E_n \subset \prod_{n \geq 0} E_n$,
con mappe ψ_n fornite dalle (restrizioni delle) proiezioni.
In più se $(E', \psi'_n)_n$ è un altro limite proiettivo della stessa successione,
allora esiste un' unica biezione $f : E' \longrightarrow E$ tale che $\psi'_n = \psi_n \circ f$.

Dim: Proviamo in primis l'esistenza:
definiamo $E = \{(x_n) : \phi_n(x_{n+1}) = x_n, \forall n \geq 0\}$;
se $x \in E$ allora $\phi_n(p_{n+1}(x)) = p_n(x)$,
quindi per le restrizioni ψ_n delle proiezioni p_n varrà:
$\phi_n \circ \psi_{n+1} = \psi_n$.
Dimostriamo ora che E verifica insieme alle sue mappe associate la proprietà universale:
sia E' un altro insieme con delle mappe $\psi'_n : E' \longrightarrow E_n$
che soddisfano $\phi_n \circ \psi'_{n+1} = \psi'_n$;
tali ψ'_n definiscono una mappa vettoriale:
$(\psi'_n) : E' \longrightarrow \prod E_n$;
la relazione $\phi_n(\psi'_{n+1}(y)) = \psi'_n(y)$,
mostra che l'immagine di (ψ'_n) è contenuta in E;
allora esiste un'unica mappa $f : E' \longrightarrow E$ tale che $\psi'_n = \psi_n \circ f$,
e questa non è nient'altro che la mappa (ψ'_n).

Rimane dunque da provare l'unicità:
se (E, ψ_n) e (E', ψ'_n) hanno la proprietà universale di fattorizzazione,
esiste un'unica mappa $f' : E \longrightarrow E'$ con $\psi_n = \psi'_n \circ f'$.
Insieme a quanto scritto sopra si trova che $\psi'_n = \psi'_n \circ f' \circ f$,
ovvero che $f' \circ f$ è una fattorizzazione della mappa identità $id : E' \longrightarrow E'$.
Siccome però abbiamo assunto l'unicità di una tale fattorizzazione per la successione (E'_n, ϕ'_n) otteniamo che $f' \circ f = id$;
similmente si prova che $f \circ f' = id$ (stavolta su E). ■

Corollario 1.5.
Quando tutte le mappe di transizione ϕ_n in un sistema proiettivo $(E_n, \phi_n)_{n\geq 0}$ sono suriettive, il limite proiettivo $(E, (\psi_n))$ di questo sistema ha mappe di proiezione ψ_n suriettive ed in particolare E non è vuoto.

Dim: Per la costruzione di E come sottoinsieme del prodotto $\prod E_n$,
è sufficiente dimostrare che se fissiamo una componente $x_n \in E_n$, troviamo in realtà un successione in E che ha come componente $n-$esima proprio x_n;
basta scegliere un $x_{n+1} \in E_{n+1}$ con $\phi_n(x_{n+1}) = x_n$
(ed è possibile trovarlo grazie alla suriettività di ϕ_n).
A questo punto si itera tale procedimento e si conclude utilizzando l'assioma numerabile della scelta. ■

Osservazione 1.6. Quando il sistema proiettivo $(E_n, \phi_n)_{n\geq 0}$ è formato da spazi topologici e da mappe di transizione continue, allora la costruzione appena fatta mostra immediatamente che anche il limite proiettivo sarà uno spazio topologico con mappe di proiezione continue con la proprietà universale di fattorizzazione attraverso una mappa continua.
Quando tutti gli E_n sono di Hausdorff, il sottospazio $\varprojlim_n E_n$ è di Hausdorff (perché sottospazio del prodotto cartesiano degli E_n che sarà di Hausdorff) ed è chiuso:

è l'intersezione di tutti gli insiemi chiusi definiti dall' uguaglianza delle mappe continue p_n con le mappe continue $\phi_n \circ p_{n+1}$.

Proposizione 1.7.
Un limite proiettivo di spazi non vuoti e compatti è non vuoto e compatto.

Dim: Sia (K_n, ϕ_n) un sistema proiettivo composto da spazi compatti.
Il prodotto $\prod K_n$ è un compatto e siccome il loro limite proiettivo è un suo sottospazio chiuso è anche esso compatto.
Definiamo ora gli insiemi:
$K'_n = \phi_n(K_{n+1}) \supset K''_n = \phi_n(K'_{n+1}) \supset ...$
e sia L_n la loro intersezione.
Siccome tali spazi sono compatti e non vuoti, anche L_n sarà non vuoto.
In più $\phi_n(L_{n+1}) = L_n$, e le restrizioni delle mappe ϕ_n agli insiemi L_n formano un sistema proiettivo con mappe di transizione suriettive:
tale sistema ha un limite non vuoto.
Ma siccome $\varprojlim_n L_n \subset \varprojlim_n K_n$, la proposizione è dimostrata. ■

Corollario 1.8.
Un limite proiettivo di insieme non vuoti finiti è non vuoto. ■

Proposizione 1.9.
In un limite proiettivo $E = \varprojlim_n E_n$ di spazi topologici,
una base per la topologia è costituita dagli insiemi $\psi_n^{-1}(U_n)$, per $n \geq 0$,
ove U_n è un aperto arbitrario di E_n.

Dim: Prendiamo una famiglia $x = (x_i)$ nel limite proiettivo,
e dimostriamo che gli insieme aperti sopra menzionati che contengono x
formano una base di intorni aperti per questo punto:
se prendiamo due insiemi aperti $V_n \subset E_n$ e $V_{n-1} \subset E_{n-1}$
le condizioni $x_n \in V_n$ e $x_{n-1} \in V_{n-1}$,
portano a $\psi_n(x) = x_n \in V_n \cap \phi_{n-1}^{-1}(V_{n-1})$.
Chiamiamo $U_n = V_n \cap \phi_{n-1}^{-1}(V_{n-1})$, insieme aperto di E_n.
Allora la condizione precedente è equivalente a $x \in \psi_n^{-1}(U_n)$.
Per induzione, si può dimostrare che un base di insiemi aperti nel prodotto
$\left(\prod_{n \leq N} V_n \times \prod_{n > N} E_n\right)$ ha un' intersezione con il limite proiettivo della forma $\psi_N^{-1}(U_N)$,
per qualche insieme aperto $U_N \subset E_N$. ■

Osservazione 1.10. Supponiamo che il sistema proiettivo $(G_n, \phi_n)_n$ è formato da gruppi G_n e omomorfismi ϕ_n, allora il limite proiettivo $G = \varprojlim_n G_n$ è un gruppo non vuoto (contiene la stringa elemento neutro $(e, e, ...)$) e le proiezioni $\psi_n : G \longrightarrow G_n$ sono omomorfismi.

Esempi 1.11.
1) Il limite proiettivo di $E_n = \prod_{0 \leq i \leq n} X_i$, con X_i spazi topologici,
è omeomorfo al prodotto $\prod_{i \geq 0} X_i$.
Infatti le proiezioni canoniche $\prod_{i \geq 0} X_i \longrightarrow E_n$ forniscono una fattorizzazione continua
e biettiva $\prod_{i \geq 0} X_i \longrightarrow \varprojlim_n E_n$,
che è una mappa aperta vista la definizione di insiemi aperti nei due spazi.

2) La mappa $\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$,
che prende $x = \sum_{i \geq 0} a_i p^i$ e lo manda in (x_n), con $x_n = \sum_{i<n} a_i p^i \pmod{p^n}$,
definisce un isomorfismo di anelli topologici:
Infatti le mappe di transizione ϕ_n sono date da:
$\sum_{i<n+1} a_i p^i \pmod{p^{n+1}} \longrightarrow \sum_{i<n} a_i p^i \pmod{p^n}$;
questo mostra che nella costruzione del limite proiettivo la successione (x_n) è esattamente la successione delle classi delle somme parziali di x.
le relazioni:
$x_1 = a_0$, $x_2 = a_0 + a_1 p, ...$
e $a_0 = x_1$, $a_1 = \frac{x_2 - x_1}{p}, ...$
mostrano che la fattorizzazione $\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ è biettiva e quindi definisce un isomorfismo algebrico.
Infine siccome essa è una mappa continua tra uno spazio topologico compatto a uno di Hausdorff, è anche un omeomorfismo.

Definizione 1.12. Un gruppo profinito è un gruppo $G \cong \varprojlim_i G_i$,
per un certo sistema inverso di gruppi topologici G_i.

Osservazione 1.13. Dalla definizione VII.1.12 e dal secondo esempio VII.1.11, si deduce che $\mathbb{Z}_p$ è un gruppo profinito.

Lascio come riflessione personale le seguenti proposizioni:

Proposizione 1.14.
Un gruppo è profinito se e soltanto se esiste una base di intorni del suo elemento neutro composta da sottogruppi normali di indice finito.

Proposizione 1.15.
Un gruppo è profinito se e soltanto se è compatto e totalmente sconnesso.

VII.2 **Il gruppo di Galois assoluto di un'estensione di Galois**.

Sia $\mathbb{E}/\mathbb{F}$ un'estensione di Galois di campi, e sia $G = Gal(\mathbb{E}/\mathbb{F})$.
Sia poi $(\mathbb{K}_i, i \in I)$ la famiglia di tutte le estensioni di Galois finite di $\mathbb{F}$ contenute in $\mathbb{E}$. Allora $\mathbb{E} = \bigcup_i \mathbb{K}_i$:
Infatti $\bigcup_i \mathbb{K}_i \subset \mathbb{E}$.
Inoltre se $x \in \mathbb{E}$, allora la chiusura normale $\mathbb{F}^N(x)$ di $\mathbb{F}(x)$ è un'estensione finita perché è ottenuta aggiungendo a $\mathbb{F}$ tutti i coniugati di x, che sono algebrici su $\mathbb{F}$ è stanno in $\mathbb{E}$.
Inoltre $\mathbb{F}^N(x)/\mathbb{F}$ è separabile perché è una sottoestensione di $\mathbb{E}$.
Quindi $x \in \mathbb{F}^N(x) \subset \mathbb{E}$ che è dunque di Galois finita, e questo ci dà l'altra inclusione.
Poniamo ora $G_i = Gal(\mathbb{K}_i/\mathbb{F})$;
Vogliamo dimostare che i G_i, insieme ad un'opportuna famiglia di omomorfismi, formano un sistema inverso di gruppi, di cui è possibile calcolare il limite inverso.
Osserviamo quindi:
1) Se $\mathbb{K}_i \subset \mathbb{K}_j$, allora abbiamo un naturale omomorfismo tra gruppi di Galois
$\pi_{ji} : G_j \longrightarrow G_i$.
2) Se $i_1, i_2 \in I$, allora $\mathbb{K}_{i_1}\mathbb{K}_{i_2} = \mathbb{K}_j$, per un certo $j \in I$, e quindi $\mathbb{K}_{i_1}, \mathbb{K}_{i_2} \subset \mathbb{K}_j$.
A questo punto per ottenere un sistema inverso basta prendere la terna (I, G_i, π_{ji}), dove su I consideriamo la relazione $i \leq j \Leftrightarrow \mathbb{K}_i \subset \mathbb{K}_j$.
Con queste notazioni abbiamo la seguente:

Proposizione 2.1.
$G = Gal(\mathbb{E}/\mathbb{F}) \cong \varprojlim_i G_i$,
dove l'isomorfismo è un isomorfismo di gruppi.

Dim: Per ogni $i \in I$, abbiamo un omomorfismo di gruppi $\theta_i : G \longrightarrow G_i$.
Questi inducono un omomorfismo di gruppi $\theta : G \longrightarrow \prod_i G_i$
definito ponendo $\theta(x) = (\theta_i(x))_i$;
Ovviamente $\theta(G) \subset L = \varprojlim_i G_i$.
Facciamo vedere ora che θ definisce un isomorfismo di G con L.
Sia quindi $g \neq 1$ in G.
Allora esiste $x \in \mathbb{E}$ tale che $g(x) \neq x$, e supponiamo $x \in \mathbb{K}_i$ per un certo i.
Pertanto $(\theta(g))_i \in G_i$ manda x in $g(x)$, quindi $\theta(g)$ non è l'identità in $\prod G_i$.
Dunque θ è iniettiva.
Sia ora $(g_i) \in L$. Se $x \in \mathbb{E}$ e $x \in \mathbb{K}_i$, poniamo $g(x) = g_i(x)$.
Questa è una buona definizione: (g_i) sta in L,
quindi se $\mathbb{K}_i \cap \mathbb{K}_j \neq \emptyset$ allora g_i e g_j coincidono sull'intersezione.
Quindi abbiamo ben definito una mappa da $\mathbb{E} \longrightarrow \mathbb{E}$ che lascia fisso $\mathbb{F}$.
Ma chiaramente $\theta(g) = (g_i)$, quindi θ è anche surgettiva. ■

Usiamo l'isomorfismo θ utilizzato nella dimostrazione della proposizione precedente

per mettere una topologia su G.
In questo modo $G = Gal(\mathbb{E}/\mathbb{F})$ è un gruppo profinito, e se poniamo $U_i = Gal(\mathbb{E}/\mathbb{K}_i)$, (U_i) definisce un sistema fondamentale di intorni aperti di 1: sappiamo come sono costruiti gli intorni aperti di 1 nel $\prod_i G_i$.
Consideriamo quindi l'applicazione composta $G \longrightarrow \varprojlim_i G_i \longrightarrow G_i$
(la prima tramite θ, la seconda tramite proiezione).
Allora un sistema fondamentale di intorni aperti di 1 sarà dato dai nuclei di queste applicazioni al variare di i.
Ma, dato i, il nucleo di questa applicazione non è altro che l'insieme degli elementi di G che sono l'identità sul campo fissato da G_i, cioè $\mathbb{K}_i$, da cui si ottiene quello che volevamo.

VII.3 **Il gruppo di Galois assoluto di $\mathbb{F}_p$.**

Osservazione 3.1. Per quanto detto sopra deriva facilmente che:
$Gal(\mathbb{F}_{q^\infty}/\mathbb{F}_q) \cong \varprojlim_i Gal(\mathbb{F}_{q^i}/\mathbb{F}_q)$, con $q = p^n$, p primo e $n \in \mathbb{N}$.

Prendiamo ora il morfismo di Frobenius:
$\sigma : \mathbb{F}_{q^\infty} \longrightarrow \mathbb{F}_{q^\infty}$,
definito come $\sigma(a) = a^q$, con $q = p^n$, p primo e $n \in \mathbb{N}$.
Allora $Gal(\mathbb{F}_{q^i}/\mathbb{F}_q)$ è ciclico di ordine i generato dalla restrizione del morfismo di Frobenius a $\mathbb{F}_{q^i}$, che indichiamo con σ_i;
In più osserviamo che $\mathbb{F}_{q^j} \supset \mathbb{F}_{q^i} \Leftrightarrow i|j$
e in tal caso il morfismo di restrizione manda $\sigma_j \longrightarrow \sigma_i$.

Allora abbiamo ottenuto che:

Proposizione 3.2.
$Gal(\mathbb{F}_{q^\infty}/\mathbb{F}_q) \cong \varprojlim_i \mathbb{Z}/i\mathbb{Z}$,
ove si prende come ordinamento su $\mathbb{N} \setminus \{0\}$ la divisibilità.

Per concludere, dimostriamo il seguente

Teorema 3.3
$\varprojlim_i \mathbb{Z}/i\mathbb{Z} \cong \prod_p \mathbb{Z}_p$, al variare dei primi p.

Dim: Sia $P = \prod_p \mathbb{Z}_p$ e consideriamo le mappe $f_i : P \longrightarrow \mathbb{Z}/i\mathbb{Z}$ da definire;
mostriamo che (P, f_i) è un limite proiettivo del sistema $(\mathbb{Z}/i\mathbb{Z})_i$:
sia $i \in \mathbb{N}^+$; allora possiamo scrivere $i = \prod_p p^{\nu_p(i)}$,
con gli $\nu_p(i)$, interi positivi, quasi tutti nulli;
sappiamo poi che $\mathbb{Z}/i\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{\nu_p(i)}\mathbb{Z}$;

quindi poniamo: $f_i : P \longrightarrow \prod_p \mathbb{Z}/p^{\nu_p(i)}\mathbb{Z} \cong \mathbb{Z}/i\mathbb{Z}$ (ove la prima mappa è la proiezione).
Tali f_i sono compatibili con le proiezioni $f_{ji} : \mathbb{Z}/j\mathbb{Z} \longrightarrow \mathbb{Z}/i\mathbb{Z}$, quando $i|j$.
Per definizione degli f_i, la topologia di P è proprio la meno fine tra le topologie per cui tutti gli f_i sono continui.
Per concludere basta mostrare che (P, f_i) è un limite proiettivo del sistema $(\mathbb{Z}/i\mathbb{Z})_i$ nel senso degli anelli:
sia R un anello e $h_i : R \longrightarrow \mathbb{Z}/i\mathbb{Z}$, un morfismo, compatibile con gli f_{ji};
allora usando degli isomorfismi come prima si ottengo delle mappe
$h_{ip} : R \longrightarrow \mathbb{Z}/p^{\nu_p(i)}\mathbb{Z}$,
compatibili con gli omomorfismi di restrizione del sistema proiettivo $(\mathbb{Z}/p^\nu\mathbb{Z})_{\nu\in\mathbb{N}}$.
Al variare degli indici i gli h_{ip} definiscono un morfismo di anelli:
$h_p : R \longrightarrow \varprojlim_\nu \mathbb{Z}/p^\nu\mathbb{Z} = \mathbb{Z}_p$;
infine al variare di p si ottiene un morfismo di anelli: $h : R \longrightarrow P$.
Tale h soddisfa $h_i = f_i \circ h$.
Siccome poi gli h_{ip} sono univocamente determinati dagli h_i, anche h lo sarà. ■

Da qui deduciamo il seguente

Toerema 3.4.
Sia $\mathbb{F}$ un campo finito;
allora $Gal(\bar{\mathbb{F}}/\mathbb{F}) \cong \prod_p \mathbb{Z}_p$, come gruppi topologici;
in più tramite questo isomorfismo, σ corrisponde a $(1, 1, ...)$,
che è una copia di $\mathbb{Z}$ nel prodotto;
dunque il morfismo di Frobenius non genera tutto il gruppo di Galois assoluto di un campo finito ma genera solo un sottogruppo denso in esso. ■

VII.4 $\mathbb{F}_{p^\infty}$ è il campo residuo di $\mathbb{C}_p$.

Vale il seguente

Teorema 4.1.
$\mathcal{O}_{\mathbb{C}_p}/\mathfrak{p}_{\mathbb{C}_p} = \mathbb{F}_{p^\infty}$

Dim: Iniziamo con la seguente

Proposizione 4.2.
Il campo residuo di $\bar{\mathbb{Q}}_p$ è una chiusura algebrica di $\mathbb{F}_p$.

Dim: Siccome ogni elemento $x \in \bar{\mathbb{Q}}_p$ genera un'estensione finita $\mathbb{K}/\mathbb{Q}_p$,
allora il campo residuo di $\mathbb{K}$ è un'estensione finita di $\mathbb{F}_p$;
questo prova che il campo residuo di $\bar{\mathbb{Q}}_p$ è un'estensione algebrica di $\mathbb{F}_p$.
Viceversa, se $\xi \neq 0$ è algebrico su $\mathbb{F}_p$, appartiene al gruppo ciclico $\mathbb{F}_p(\xi)^*$

e di conseguenza è una radice dell'unità di un ordine m coprimo con p;
consideriamo allora l'estensione ciclotomica $\mathbb{Q}_p(\mu_m)$;
se $\zeta \neq \eta$ sono due radici $m-$esime dell'unità,
allora $|\zeta - \eta| = 1$ e le riduzioni di ζ e di η sono distinte (vedi VI.1.3);
quindi il campo residuo di $\mathbb{Q}_p(\mu_m)$ contiene m distinte radici $m-$esime dell'unità e quindi contiene anche ξ. ■

ora concludiamo la dimostrazione del teorema:
sicuramente vale $\mathcal{O}_{\mathbb{Q}_p}/\mathfrak{p}_{\mathbb{Q}_p} \subseteq \mathcal{O}_{\mathbb{C}_p}/\mathfrak{p}_{\mathbb{C}_p}$;
per dimostrare che sono effettivamente uguali basta usare la densità:
infatti preso un elemento $[x] \in \mathcal{O}_{\mathbb{C}_p}/\mathfrak{p}_{\mathbb{C}_p}$, con $x \in \mathcal{O}_{\mathbb{C}_p}$, per la densità di $\mathcal{O}_{\mathbb{Q}_p}$ in $\mathcal{O}_{\mathbb{C}_p}$ posso trovare un $x' \in \mathcal{O}_{\mathbb{Q}_p}$ tale che $|x - x'| < 1$ in $\mathbb{C}_p$, ovvero $x - x' \in \mathfrak{p}_{\mathbb{C}_p}$ e dunque $[x] = [x']$. ■

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].
Per quanto riguarda il gruppo di Galois assoluto di un estensione di Galois, e per quanto riguarda il gruppo di Galois assoluto del campo $\mathbb{F}_p$, vedere [7].

Capitolo VIII

Caratteri additivi

Definizione 1.1. Sia $\mathbb{K}$ un campo e $\psi : \mathbb{F}_q \longrightarrow \mathbb{K}^*$ un omomorfismo di gruppi; allora ψ si dice carattere additivo.

Proposizione 1.2.
Sia G un gruppo e $\mathbb{K}$ un campo;
ogni insieme di morfismi distinti da G in $\mathbb{K}$, è linearmente indipendente nel $\mathbb{K}$-spazio vettoriale di tutte le funzioni $G \longrightarrow \mathbb{K}$.

Dim: Siccome l'indipendenza lineare di una qualsiasi famiglia riguarda solo i suoi sottoinsiemi finiti,
possiamo direttamente lavorare con un insieme finito di morfismi distinti:
lavoriamo allora per induzione sul numero di morfismi ψ_i;
certamente la relazione di indipendenza è vera per un solo morfismo;
supponiamo che sia vera per ogni $n-1$ distinti morfismi e consideriamo n distinti morfismi ψ_i;
partiamo dalla relazione di dipendenza: $\sum_{k=1}^{n} \alpha_k \psi_k(x) = 0$, con $x \in G$ e $\alpha_i \in \mathbb{K}$;
moltiplichiamo per $\psi_1(a), a \in G$ e otteniamo:
$\sum_{k=1}^{n} \alpha_k \psi_1(a)\psi_k(x) = 0.$
D'altra parte, rimpiazzando x con ax nella relazione di dipendenza, otteniamo:
$\sum_{k=1}^{n} \alpha_k \psi_k(a)\psi_k(x) = 0;$
ora sottraiamo queste due equazioni:
$\sum_{k=2}^{n} \alpha_k (\psi_1(a) - \psi_k(a))\psi_k(x) = 0.$
Per induzione tutti i coefficienti di questa combinazione devono annullarsi e siccome possiamo sempre trovare un $a \in G$ tale che $\psi_1(a) \neq \psi_n(a)$, troviamo che $\alpha_n = 0$ e usando di nuovo l'induzione si ottiene che $\alpha_i = 0, \forall 1 \leq i \leq n$. ■

Proposizione 1.3.
Sia $\mathbb{F}$ un campo finito e $\tau : \mathbb{F} \longrightarrow \mathbb{K}^*$
un carattere additivo non banale; allora ogni altro carattere additivo ψ è della forma:
$\psi(x) = \tau(ax)$, per qualche $a \in \mathbb{F}$.

Dim: L'identità $\tau(a(x+y)) = \tau(ax) + \tau(ay)$,
mostra che $x \longrightarrow \tau(ax)$ è un carattere additivo;
in più la mappa $a \longrightarrow \tau_a$,

con $\tau_a(x) = \tau(ax)$,
è un morfismo: $\tau_{a+b}(x) = \tau(ax + bx) = \tau(ax)\tau(bx) = \tau_a(x)\tau_b(x)$;
è anche iniettivo: τ è un carattere non banale,
dunque $\tau_a(x) = 1 \Rightarrow a = 0$.
L'insieme dei caratteri $(\tau_a)_a$ costituiscono una base dello $\mathbb{K}-$spazio vettoriale delle funzioni $\mathbb{F} \longrightarrow \mathbb{K}^*$;
ogni carattere additivo deve stare in questa famiglia,
a causa della proposizione precedente. ■

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].

Capitolo IX

Serie formali

IX.1 **L'anello delle serie formali**.

Definizione 1.1. Sia A un anello commutativo unitario non nullo,
e sia $f(X) = \sum_{n\geq 0} a_n X^n$ una serie di potenze formale;
definiamo l'ordine della serie come il numero intero positivo:
$\omega = \omega(f) = min\{n \in \mathbb{N} : a_n \neq 0\}$, con la convenzione $\omega(0) = \infty$.
tale ω verifica la relazione $\omega(f+g) \geq min\{\omega(f), \omega(g)\}$,
con uguaglianza se gli ordini di f e g sono diversi.
In più $\omega(x^n f) = n + \omega(f)$, che mostra che:
$\{f : \omega(f) \geq n\} = X^n A[[X]]$.
In più siccome $A[[X]]/X^n A[[X]] = A[X]/(X^n)$,
abbiamo anche $A[[X]] = \varprojlim_n A[X]/(X^n)$,
e l'anello $A[[X]]$ appare come completamento di $A[X]$ per la topologia in cui gli ideali (X^n) formano un sistema fondamentale di intorni di 0.
Infine se A non ha zero divisori, vale anche $\omega(fg) = \omega(f) + \omega(g)$.

Lemma 1.2.
Se A è un dominio, allora $A[[X_1, ..., X_n]]$ è un dominio.

Dim: Infatti se $\omega(f) \neq \infty$ e $\omega(g) \neq \infty$
allora $\omega(fg) \neq \infty$, quindi $A[[X]]$ è un dominio;
a questo punto si itera la costruzione. ■

IX.2 **Derivata di serie**.

Definizione 2.1. L'operatore di derivata formale è definito ponendo:
$D(\sum_{k\geq 0} a_k X^k) = \sum_{k\geq 1} k a_k X^{k-1}$,
e soddisfa $D(fg) = D(f)g + fD(g)$.

Osservazione 2.2. Siccome $\omega(D(f)) \geq \omega(f) - 1$, si ha che tale operatore è anche continuo rispetto alla topologia in $A[[X]]$ definita precedentemente.
In più osserviamo che, siccome $\frac{D^k(X^n)}{k!} = \binom{n}{k} X^{n-k}$,
se indichiamo con $f(0)$ il termine costante della serie di potenze formali $f(X) = \sum_{k\geq 0} a_k X^k$, allora vale: $\frac{D^k(f(0))}{k!} = a_k$.

Osservazione 2.3. Supponiamo di avere un campo $\mathbb{K}$ completo rispetto ad un valore assoluto ultrametrico, allora una serie $f(X) = \sum_{k\geq 0} a_k X^k$ con $a_k \in \mathbb{K}$, converge precisamente quando il suo termine generale converge a 0 (vedi IV.1.6).
Ora se $r \geq 0$ è tale che $|a_n|r^n \to 0$, allora la serie converge almeno per $|x| \leq r$ e in tal caso otteniamo una funzione da $B_{\leq r}(0)$ in $\mathbb{K}$.

IX.3 **Il raggio di convergenza**.

Definizione 3.1. Il raggio di convergenza di una serie di potenze $f = \sum_{n\geq 0} a_n X^n$, avente coefficienti in un campo $\mathbb{K}$, è quel numero $0 \leq r_f \leq \infty$
definito da $r_f = sup\{r \geq 0 : |a_n|r^n \to 0\}$;
si vede facilmente che $r_f = sup\{r \geq 0 : (|a_n|r^n)_n$ è limitata $\}$.

Proposizione 3.2 (Hadamard).
Il raggio di convergenza di $f = \sum_{n\geq 0} a_n X^n$ è:

$$r_f = \frac{1}{\limsup_{n\to\infty} |a_n|^{\frac{1}{n}}}.$$

Dim: Sia r_f definito come nella formula di Hadamard;
se $|x| > r_f$ abbiamo $\lim_{n\to\infty} \sup_{k\geq n} |x||a_k|^{\frac{1}{k}} = |x| \cdot \frac{1}{r_f} > 1$;
quindi la successione decrescente $\sup_{k\geq n} |x||a_k|^{\frac{1}{k}}$ è più grande di 1 e per infiniti valori di k abbiamo $|a_k||x|^k > 1$, ovvero il termine generale di f non tende a 0 e la serie che definisce f diverge.
Se $|x| < r_f$, scegliamo un $r : |x| < r < r_f$ e siccome: $\lim_{n\to\infty} \sup_{k\geq n} r|a_k|^{\frac{1}{k}} < 1$, possiamo scegliere un N opportuno in modo che $\sup_{k\geq n} r|a_k|^{\frac{1}{k}} < 1$.
Di conseguenza $|a_k|r^k < 1$ per tutti i $k \geq N$
e $|a_k x^k| = |a_k|r^k \left(\frac{|x|^k}{r^k}\right) < \frac{|x|^k}{r^k} \to 0$, $(k \to \infty)$;
quindi il termine generale della serie di f tende a 0 e la serie converge. ■

Esempi 3.3.
1) Il raggio di convergenza di $\sum_{n\geq 0} X^n$ è $r_f = 1$
tale serie diverge per $|x| = 1$, siccome il termine generale non tende a 0.
2) Ogni serie della forma: $f = \sum_{n\geq 0} a_n X^n \in \mathbb{Z}_p[[X]]$, ha raggio di convergenza $r_f \geq 1$;
ad esempio $(1+X)^a = \sum_{n\geq 0} \binom{a}{n} X^n$, con $a \in \mathbb{Z}_p$.

3) Invece la serie $\sum_{n\geq 0} \frac{X^{p^n}}{p^n}$ ha i coefficienti che tendono all'infinito (in modulo) ma ha raggio di convergenza uguale a 1
(in particolare converge se e soltanto se $|x| < 1$).

Proposizione 3.4.
Siano f e g due serie di potenze formali convergenti, a coefficienti in un campo $\mathbb{K}$, estensione completa di $\mathbb{Q}_p$;
allora il loro prodotto fg è una serie convergente;
più precisamente $r_{fg} \geq min\{r_f, r_g\}$;
in più vale $(fg)(x) = f(x)g(x)$, per $|x| < min\{r_f, r_g\}$.

Dim: è una diretta conseguenza del seguente

Teorema 3.5.
Siano $f(X) = \sum_{n\geq 0} a_n X^n$ e $g(X) = \sum_{n\geq 0} b_n X^n$
due serie di potenze tali che $a_n, b_n \to 0$ $(n \to \infty)$;
allora $(fg)(X) = \sum_{n\geq 0} c_n X^n$, ove $c_n = \sum_{k=0}^{n} a_k b_{n-k} \to 0$.
In più vale $(fg)(x) = f(x)g(x)$ per $|x| \leq 1$.

Dim: Rimpiazzando $a_n x^n$ con a_n e similmente $b_n x^n$ con b_n,
si vede che è sufficiente considerare il caso $x = 1$;
sia c_n come sopra, allora dobbiamo provare la seguente affermazione:
se $\sum_{n\geq 0} a_n$ e la $\sum_{n\geq 0} b_n$ convergono,
allora anche la $\sum_{n\geq 0} c_n$ converge e vale:
$\sum_{n\geq 0} c_n = \sum_{n\geq 0} a_n \cdot \sum_{n\geq 0} b_n$:
siccome in $\mathbb{K}$ la moltiplicazione è continua,
allora $\sum_{i\geq 0} a_i \cdot \sum_{j\geq 0} b_j - \sum_{i\leq N} a_i \cdot \sum_{j\leq N} b_j \to 0$ $(N \to \infty)$;
Ora mostriamo che
$\sum_{i\geq 0} a_i \cdot \sum_{j\geq 0} b_j - \sum_{k\leq N} c_k \to 0$:
scegliamo un N_ε sufficiente grande in modo che $|a_i| \leq \varepsilon, |b_i| \leq \varepsilon$ per $i \geq N_\varepsilon$;
la differenza $\sum_{i\leq N} a_i \cdot \sum_{j\leq N} b_j - \sum_{k\leq N} c_k$ è la somma di vari termini $a_i b_j$ con $i + j > N$;
il contributo di questi termini è minore o uguale a $C\varepsilon$, se C è una costante opportuna che maggiora i moduli dei coefficienti delle serie e se $N > 2N_\varepsilon$ in modo che almeno un indice tra i e j sia maggiore di N_ε. ■

Corollario 3.6.
Sia $r > 0$, l'insieme delle serie di potenze formali $f(X) = \sum_{n\geq 0} a_n X^n$,
tali che $|a_n| r^n \to 0$, è un anello;
in più per ogni $x \in B_{\leq r}$ la mappa valutazione $f \longrightarrow f(x)$ è un omomorfismo da questo anello al campo base $\mathbb{K}$. ■

Esercizio 1. Per ogni polinomio f il raggio di convergenza della composizione $f \circ g$ è $\geq r_g$ e vale $(f \circ g)(x) = f(g(x))$ per $|x| < r_g$.

Proposizione 3.7
Il raggio di convergenza di $f(X) = \sum_{n\geq 0} a_n X^n$ e della sua derivata formale
$D(f)(X) = \sum_{n\geq 1} n a_n X^{n-1}$ è lo stesso: $r_f = r_{D(f)}$.

Dim: Proviamo questa proposizione quando il campo è un'estensione di $\mathbb{Q}_p$ o di $\mathbb{R}$ con un valore assoluto normalizzato:
sappiamo che $\frac{1}{n} \leq |n| \leq n$ per $n \in \mathbb{N}$ e anche che $n^{\pm\frac{1}{n}} \to 1$, $(n \to \infty)$.
Questo prova che $\limsup_{n\to\infty} |na_n|^{\frac{1}{n-1}} = \limsup_{n\to\infty} |na_n|^{\frac{1}{n}} = \limsup_{n\to\infty} |a_n|^{\frac{1}{n}}$. ■

Osservazione 3.8. Anche se il raggio di convergenza di f e di Df è lo stesso, diciamo r, il comportamento delle due serie sulla sfera $S_r = \{x : |x| = r\}$ può essere diverso: ad esempio, la serie $f(X) = \sum_{n\geq 0} X^{p^n}$ ha raggio di convergenza $r_f = 1$ e diverge su $|x| = 1$; mentre la sua derivata $D(f)(X) = \sum_{n\geq 0} p^n X^{p^n - 1}$ converge in $|x| = 1$.

IX.4 **Composizione di serie formali**.

Osservazione 4.1. Supponiamo ora di avere $f, g \in \mathbb{K}[[x]]$, con $g(X) \in X\mathbb{K}[[X]]$;
allora $\omega(g^n) \geq n$ e se $f(X) = \sum_{n\geq 0} a_n X^n$,
allora $f(g(Y)) = \sum_{n\geq 0} a_n (g(Y))^n = \sum_{n\geq 0} c_n Y^n$,
è ben definita siccome la famiglia $(a_n(g(Y))^n)_n$ è sommabile: la determinazione dei coefficienti c_n coinvolge solo un numero finito di termini.

Osservazione 4.2. La sostituzione $X = g(Y)$ fornisce un omomorfismo:
$f(X) \longrightarrow (f \circ g)(Y)$, che manda 1 in 1 e che è continuo rispetto alla topologia metrizzabile che vede gli ideali $X^k\mathbb{K}[[X]]$ come sistema fondamentale di intorni di 0,
siccome $\omega(f) \geq k \Rightarrow \omega(f \circ g) \geq k$.

Osservazione 4.3. è facile verificare la seguente identità:
$(f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)$,
se g è una serie formale con $\omega(g) \geq 1$.

Di conseguenza si trova (per induzione) che $f^n \circ g = (f \circ g)^n, n \geq 1$.

Proposizione 4.4.
Siano g e h due serie di potenze formali con ordine strettamente positivo;
allora per ogni altra serie di potenze formali f abbiamo:
$(f \circ g) \circ h = f \circ (g \circ h)$.

Dim: Entrambi i lati sono ben definiti e sono uguali se $f(x) = x^n$,
siccome in tal caso $f \circ g = g^n$;
di conseguenza la proposizione è vera per ogni polinomio f (per linearità);
infine il caso generale $f(X) = \sum_{n\geq 0} a_n X^n$ segue da:
$(f \circ g) \circ h = (\sum_{n\geq 0} a_n g^n) \circ h = \sum_{n\geq 0} a_n (g^n \circ h) = \sum_{n\geq 0} a_n (g \circ h)^n = f \circ (g \circ h)$. ■

Teorema 4.5.
Sia $f(X) = \sum_{n\geq 0} a_n X^n$, allora le seguenti sono equivalenti:

1)$\exists g \in \mathbb{K}[[X]]$ con $g(0) = 0$ e $(f \circ g)(X) = X$.
2)$a_0 = f(0) = 0$ e $a_1 = f'(0) \neq 0$.

Quando loro sono soddisfatte allora c'è un'unica serie formale g che soddisfa la proprietà 1) e che in aggiunta soddisfa anche $(g \circ f)(X) = X$.

Dim: 1) $\Rightarrow$ 2): Se $g(X) = \sum_{m\geq 1} b_m X^m$,
allora l'identità $(f \circ g)(X) = X$ può essere riscritta più esplicitamente come:
$\sum_{n\geq 0} a_n g(X)^n = a_0 + a_1 b_1 X + X^2(...) = X$,
che implica $a_0 = 0, a_1 \neq 0$.
2) $\Rightarrow$ 1): l'uguaglianza $(f \circ g)(X) = X$ richiede che $a_1 b_1 = 1$ e che il coefficiente di X^n in $\sum_{k=1}^{n} a_k (g(X))^k$ si annulli (per $n \geq 2$).
Il coefficiente di X^n è della forma $a_1 b_n + P_n(a_2, ..., a_n, b_1, ..., b_{n-1})$,
con P_n polinomio con coefficienti interi;
siccome $a_1 \neq 0$ si può dividere per esso nella relazione scritta sopra e ricavare b_n.
In questo modo riusciamo a costruire l'inversa g desiderata.
Infine se f soddisfa 2) e g è scelta come in 1),
allora $b_0 = 0$ e $b_1 = \frac{1}{a_1}$, allora applicando il teorema a g,
possiamo scegliere una serie h tale che $(g \circ h)(X) = X$;
allora $h(X) = (f \circ g) \circ h(X) = f \circ (g \circ h)(X) = f(X)$,
che implica $g \circ f(x) = g \circ h(X) = X$. ■

Osservazione 4.6. è facile verificare la seguente identità:
$D(fg) = D(f)g + fD(g)$, per $f, g \in \mathbb{K}[[X]]$;

da qui si ricava che (se $f = g$):
$D(g^2) = 2gD(g)$ e per induzione $D(g^n) = ng^{n-1}D(g)$
e per linearità $D(f \circ g)(Y) = D(f(g(Y)))D(g(Y))$,
per tutte le serie $g \in Y\mathbb{K}[[Y]]$ e i polinomi $f \in \mathbb{K}[X]$.

Teorema 4.7 (Regola della catena).
Siano f e g due serie di potenze formali con $g(0) = 0$;
allora vale $D(f \circ g)(Y) = D(f(g(Y)))D(g(Y))$.

Dim: Fissiamo g e facciamo variare f in $\mathbb{K}[[X]]$;

allora $\omega(f) \geq k \Rightarrow \omega(f \circ g) \geq k \Rightarrow \omega(D(f \circ g)) \geq k - 1$,
e $\omega(f) \geq k \Rightarrow \omega(D(f)) \geq k-1 \Rightarrow \omega(D(f \circ g)(Y)) = \omega\left(D(f(g(Y)))D(g(Y))\right)) \geq k-1$;

tutto ciò implica che l'identità $D(f \circ g)(Y) = D(f(g(Y)))D(g(Y))$, valida nel sottospazio denso dei polinomi, si estende per continuità a tutto $\mathbb{K}[[X]]$. ■

IX.5 **La crescita del modulo**.

Definizione 5.1.
1) Poniamo $M_r(f) = \max_{n \geq 0}\{|a_n|r^n\}$.
2) Diciamo che $r \in [0, r_f)$ è un raggio regolare se $M_r(f) = |a_n|r^n$
per esattamente un indice n;
(in tal caso il monomio $a_n r^n$ è detto dominante).
3) r si dice raggio critico se per almeno due indici distinti n
vale l'uguaglianza $M_r(f) = |a_n|r^n$.

Osservazione 5.2. Per definizione $|f(x)| \leq M_r(f)$, se $|x| = r < r_f$,
con l'uguaglianza per tutti i raggi regolari r.

Lemma 5.3.
Sia $c_n \geq 0$ una successione di numeri reali positivi e $0 < R \leq \infty$
tale che per ogni $r < R$, $c_n r^n \to 0$.
Allora la mappa $r \longrightarrow M(r) = \sup_{n \geq 0} c_n r^n$
è continua e convessa nell'intervallo $I = [0, R)$,
liscia eccetto su un insieme discreto $\Delta = \{r_1 < r_2 < ...\} \subset I$.
In più tra due valori consecuti di Δ,
M coincide con un singolo monomio $c_m r^m$.

Dim: Sia $0 < r < R$;
dimostrare che la mappa $r \longrightarrow M(r)$ è continua e convessa nell'intervallo $I = [0, R)$,
è un facile esercizio che lasciamo al lettore.
Ora siccome $c_n r^n \to 0$, c'è un intero $m \geq 0$
tale che $c_m r^m = \max_{n \geq 0} c_n r^n = M(r)$.

Se $N > m$ e $0 < s < r$, allora:
$c_N r^N \leq c_m r^m \Rightarrow \frac{c_N}{c_m} r^{N-m} \leq 1 \Rightarrow \frac{c_N}{c_m} s^{N-m} < 1 \Rightarrow c_N s^N < c_m s^m$.
Di conseguenza, solo un numero finito di monomi,
quelli per cui $N < m$, possono competere con $c_m s^m$, per $s < r$;
i raggi critici $s < r$ sono particolari soluzioni di $s^{j-i} = \frac{c_i}{c_j}$, $(0 \leq i < j \leq m)$.
L'insieme Δ è finito o consiste di una successione crescente convergente a R. ■

Corollario 5.4.
Ogni serie di potenze convergente e non nulla f ha solo un numero finito di raggi critici minori di un qualsiasi $r < r_f$, mentre i raggi regolari formano un insieme denso in $[0, r_f)$. ■

Corollario 5.5 (Teorema di Liouville).
Sia $f(X) \in \mathbb{K}[[X]]$ con raggio di convergenza infinito.
Se la funzione $|f|$ è limitata su $\mathbb{K}$ e $|\mathbb{K}^*|$ è denso in $\mathbb{R}_{\geq 0}$, allora f è costante.
Più precisamente, se esiste una costante $C > 0$ e un numero naturale $N \in \mathbb{N}$ tali che:
$|f(x)| \leq C|x|^N$, per ogni $x \in \mathbb{K}$ con $|x| \geq c$, allora f è un polinomio con $deg(f) \leq N$.

Dim: Scriviamo $f(x) = \sum_{n \geq 0} a_n x^n$;
abbiamo $|a_n| r^n \leq M_r(f) = |f(x)|_{|x|=r} \leq C r^N$,
se $r \geq c$ è un raggio regolare;
ma dal lemma e dal fatto che $|\mathbb{K}^*|$ è denso in $\mathbb{R}_{\geq 0}$,
questo accade almeno per una successione di valori $r_j = |x_j| \to \infty$, $x_j \in \mathbb{K}$;
per tale successione accade che $|a_n| \leq C r_j^{N-n}$.
Mandando $j \to \infty$, troviamo $a_n = 0, \forall n > N$;
questo prova che f è un polinomio di grado al più N. ■

Teorema 5.6.
Siano f e g due serie di potenze con $g(0) = 0$;
se $|x| < r_g$ e $M_{|x|}(g) < r_f$,
allora $r_{f \circ g} > |x|$ e vale $(f \circ g)(x) = f(g(x))$.

Dim: Supponiamo che $x \in \mathbb{K}$ soddisfi la condizione $|x| = r$;
ricordiamo che se $f(X) = \sum_{n \geq 0} a_n X^n$ e $g(Y) = \sum_{n \geq 0} b_n Y^n$,
la serie $(f \circ g)(Y) = \sum_{n \geq 0} c_n Y^n$
è ottenuta raggruppando potenze uguali nello sviluppo di $\sum_{n \geq 0} a_n (g(Y))^n$.

Definiamo i polinomi $f_N(X) = \sum_{0 \leq n \leq N} a_n X^n$,
allora la formula $(f_N \circ g)(x) = f_N(g(x))$,
è valida se $|x| < r_g$, per l'esercizio 1.
Sia $y = g(x)$;

siccome $|y| = |g(x)| \leq M_r(g) < r_f$, abbiamo $f_N(y) \to f(y)$ $(N \to \infty)$;
resta da dimostrare che $(f_N \circ g)(x) \to (f \circ g)(x)$.

Scriviamo $(f_N \circ g)(Y) = \sum_{k \geq 0} c'_k(N) Y^k$,
allora $((f - f_N) \circ g)(Y) = \sum_{k > N} c''_k(N) Y^k$, con i coefficienti c_k che verificano:
$c_k = c'_k(N) + c''_k(N)$ e $c_k = c'_k(N)$ per $k \leq N$.

Ricordiamo che $(f \circ g)(Y) - (f_N \circ g)(Y) = \sum_{n > N} a_n (g(Y))^n = \sum_{k > N} c''_k(N) Y^k$,
è ottenuta raggruppando i monomi dello stesso grado.
Ogni monomio in $(g(Y))^n$ è una somma di prodotti di n monomi in $g(Y)$,
quando lo valutiamo in un punto y con $\rho = M_{|y|}(g)$,
il suo valore assoluto è minore o uguale a ρ^n.
Scegliamo ora un $y \in \mathbb{C}_p$, con:

1) $|x| = r < |y| < r_g$, in modo che $g(y)$ sia ben definito.
(Infatti possiamo trovare in $\mathbb{C}_p$ un elemento y tra r e r_f perché $|\mathbb{C}_p^*|$ è denso in $R_{>0}$:
infatti basta mostrare che $|\bar{\mathbb{Q}}_p^*|$ è denso in $R_{>0}$:
sia $x \in \bar{\mathbb{Q}}_p \setminus \mathbb{Q}_p$, allora x soddisfa un'equazione polinomiale
della forma $\sum_{i=0}^{n} a_i x^i = 0$, con $a_i \in \mathbb{Q}_p$ e $n \geq 2$;
per il principio di competizione devono esistere due indici $i \neq j$
tali che $|a_i x^i| = |a_j x^j| \neq 0$ e quindi $|x|^{i-j} = \frac{|a_j|}{|a_i|} \in p^{\mathbb{Z}}$, da cui $|x| \in p^{\frac{1}{i-j}\mathbb{Z}}$;
questo significa che $|\bar{\mathbb{Q}}_p^*| \subseteq p^{\mathbb{Q}}$;
viceversa, siccome il polinomio $X^e = p$, con radice $\pi_e = p^{\frac{1}{e}}$, è di Eisenstein,
il campo $\mathbb{Q}_p(\pi_e)$ definisce un'estensione algebrica di grado e su $\mathbb{Q}_p$;
di conseguenza possiamo scrivere $\bar{\mathbb{Q}}_p = \bigcup_{e \geq 1} \mathbb{Q}_p(\pi_e)$ e trovare che $|\bar{\mathbb{Q}}_p^*| \supseteq \bigcup_{e \geq 1} p^{\frac{1}{e}\mathbb{Z}} = p^{\mathbb{Q}}$.
Osserviamo che $\bar{\mathbb{Q}}_p^*$ è denso in $\mathbb{C}_p^*$
e quindi possiamo concludere che $|\mathbb{C}_p^*| = p^{\mathbb{Q}}$).

2) $|g(y)| \leq M_{|y|}(g) = \rho < r_f$, in modo che $f(g(y))$ è ben definito.
(Questo è possibile dalla continuità della mappa $t \longrightarrow M_t(g)$
e dal fatto che $M_r(g) < r_f$).
Allora abbiamo $|c''_k(N) y^k| \leq \sup_{n > N} |a_n| \rho^n \to 0$, $(N \to \infty)$;
questo mostra che la successione $(c_k y^k)_k$ vive nella chiusura dell'insieme costituito dalla successione $(c'_k(N) y^k)_k$;
ma per ogni N, la successione $c'_k(N) y^k \to 0$, $(k \to \infty)$
e lo spazio delle successioni che tendono a 0 è completo;
quindi anche $c_k y^k \to 0$, $r_{f \circ g} \geq |y| > |x|$,
e anche $(f \circ g)(y) - (f_N \circ g)(y) \to 0$. ■

IX.6 **Zeri di serie formali**.

Sia $\mathbb{K}$ estensione completa di $\mathbb{Q}_p$, e sia $\mathcal{O} = B_{\leq 1}(\mathbb{K})$;
sia $f(X) = \sum_{n\geq 0} a_n X^n \in \mathbb{K}[[X]]$ tale che $r_f > 0$.

Proposizione 6.1
Sia $f = \sum_{n\geq 0} a_n X^n \in \mathcal{O}[[X]]$ una serie di potenze con $a_n \to 0$, $(n \to \infty)$;
sia $a \in \mathcal{O}$; allora esiste una serie di potenze formali g tale che:
$f(X) = f(a) + (X - a)g(X)$;
in più $g(X) = \sum_{n\geq 0} b_n X^n$ con $b_n \to 0$, $(n \to \infty)$ e $r_g \geq r_f$.

Dim: Rimpiazzando f con $f_1(X) = f(aX)$,
siccome anche il coefficiente $n-$esimo di f_1 tenderà a zero,
possiamo supporre direttamente $a = 1$:
l'equazione $f(X) = f(1) + (X - 1)g(X)$ ci porta alle seguenti identità:
$a_0 = f(1) - b_0$, $a_n = b_{n-1} - b_n$;
da qui ricaviamo $b_0 = f(1) - a_0 = \sum_{i>0} a_i$ e $b_n = b_{n-1} - a_n$
e per induzione $b_n = \sum_{i>n} a_i$.
Di conseguenza $|b_n| \to 0$.
Se $r_f = 1$ abbiamo concluso;
altrimenti se $r_f > 1$ prendiamo un qualsiasi $r > 1$ con $r < r_f$, cosi che $|a_n| r^n \to 0$;
quindi esiste una costante $c > 0$ tale che: $|a_n| r^n \leq c$;
allora il $|b_n| \leq \sup_{i>n} |a_i| \leq c \sup_{i>n} \frac{1}{r^i} = \frac{c}{r^{n+1}}$;
da qui ricaviamo che la successione $(|b_n| r^n)_n$ è limitata, e quindi $r_g \geq r$.
Facendo crescere r verso r_f, troviamo che $r_g \geq r_f$. ■

Teorema 6.2 (Strassman).
Una serie di potenze $f(X) = \sum_{n\geq 0} a_n X^n \in \mathcal{O}[[X]]$,
con $a_n \to 0$ ha solo un numero finito di zeri in $\mathcal{O}$.

Dim: Occupiamoci in primis degli zeri sulla sfera unitaria:
definiamo $\mu := min\{n : |a_n| = \sup_i |a_i|\} \leq \nu := sup\{n : |a_n| = \sup_i |a_i|\}$.
Se $\mu = \nu$ allora f non ha zeri sulla sfera unitaria.
(Se ci fossero zeri x con $|x| = 1$ allora $\sum_{n\geq 0} a_n x^n = 0$
ma allora $|a_\mu| = |\sum_{n\geq 0, n\neq\mu} a_n x^n|$ e questo è assurdo).
Mostreremo più precisamente che f ha $\nu - \mu$ zeri (contati con la loro molteplicità) sulla sfera unitaria.

Supponiamo $\nu \geq 1$ e $f(a) = 0$ per qualche $a : |a| = 1$.
scriviamo $f(X) = (X - a)g(X)$ con $g \in \mathcal{O}[[X]]$ tale che il suo coefficiente $n-$esimo tende a 0 (tale fattorizzazione deriva dalla proposizione IX.6.1);
riduciamo modulo $\mathfrak{p} = B_{<1}(\mathbb{K})$ e otteniamo:
$\bar{f}(X) = (X - \bar{a})\bar{g}(X)$, nel campo residuo.
Allora $deg(\bar{f}) = 1 + deg(\bar{g})$, $\omega(\bar{f}) = \omega(\bar{g})$, $\nu = 1 + \nu_g$, $\mu = \mu_g$.
Quindi $\nu - \mu > \nu_g - \mu_g$;
Osserviamo che ogni altro zero $b \neq a$ di f è anche zero di g;
ora se $\nu = \mu + 1$ abbiamo $\nu_g = \mu_g$ e quindi g non si annulla su $\mathcal{O}^*$;
in questo caso f ha solo uno zero in $\mathcal{O}^*$ e $\nu = \mu + 1$.
Se invece $\nu > \mu + 1$ possiamo ripetere la procedura per g:
in questo modo dopo al più $\nu - \mu$ passi,
l'ultima serie $h \in \mathcal{O}[[X]]$ ottenuta, con coefficiente $n-$esimo infinitesimo,
soddisferà $\nu_h = \mu_h$ e quindi non si annullerà sulla sfera unitaria.
Questo processo porta ad una fattorizzazione della forma:
$f = P \cdot h$, con P un polinomio e $h \in \mathcal{O}[[X]]$, con coefficiente $n-$esimo infinitesimo.
Infine occupiamoci degli zeri in $\mathfrak{p}$:
se $f(a) = 0$ per qualche $a \in \mathfrak{p}$, consideriamo $f_a(X) = f(aX)$,
per la quale vale $r_{f_a} = \frac{r_f}{|a|} > r_f \geq 1$.
Grazie al primo passo otteniamo che f_a ha un numero finito di zeri nella sfera unitaria;
quindi f ha un numero finito di zeri sulla sfera critica di raggio $r = |a|$.
(Infatti se $f(a) = 0$, $r = |a|$ deve essere un raggio critico e per vederlo si usa il principio di competizione del modulo).
Ma siccome f ha un numero finito di raggi critici $r < 1$
(vedi corollario IX.5.4), la conclusione segue immediatamente. ■

Osservazione 6.3. Per una serie della forma $f(X) = \sum_{n \geq 0} a_n X^n \in \mathcal{O}[[X]]$,
con $a_n \to 0$, abbiamo ottenuto una fattorizzazione della forma:
$f = P \cdot h$, con P un polinomio e $h \in \mathcal{O}[[X]]$, con coefficiente $n-$esimo infinitesimo.
Se supponiamo che $f \in \mathcal{O}[[X]]$ è una funzione $p-$adica intera, cioè una serie di potenze con raggio di convergenza infinito, allora esiste una fattorizzazione della forma $f = P \cdot h$, con $P \in \mathcal{O}[X]$ un polinomio e $h \in \mathcal{O}[[X]]$,
funzione $p-$adica intera.

Corollario 6.4.
Sia $f(X) = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[[X]]$, una serie di potenze convergente,
e supponiamo che $r < r_f$ sia un raggio critico per f;
siano anche $\mu := min\{n : |a_n| r^n = M_r(f)\} < \nu := sup\{n : |a_n| r^n = M_r(f)\}$.
Allora contando la molteplicità abbiamo:
f ha al più $\nu - \mu$ zeri nella sfera $S_r(\mathbb{K})$.
f ha al più ν zeri nella palla chiusa $B_{\leq r}(\mathbb{K})$.
f ha al più μ zeri nella palla aperta $B_{<r}(\mathbb{K})$.

Infine osserviamo che siccome i raggi critici di una tale serie formano un insieme discreto, e siccome gli zeri di ogni serie di potenze convergente hanno come modulo un raggio critico (grazie al principio di competizione), e su ogni sfera critica ci sono un numero finito di zeri, si ha che gli zeri di una serie di potenze convergente con raggio di convergenza R formano un insieme discreto con i rispettivi moduli nell'intervallo $[0, R)$. ■

Enunciamo ora un importantissimo teorema senza darne la dimostrazione
(che comunque si può trovare in [3,VI.2.2])

Teorema 6.5.
Sia $\mathbb{K}$ un campo completo e algebricamente chiuso, estensione di $\mathbb{Q}_p$
e sia $f(X) = \sum_{n\geq 0} a_n X^n \in \mathbb{K}[[X]]$ una serie di potenze convergente non nulla.
Se f ha un raggio critico $r < r_f$,
allora f ha uno zero sulla sfera critica di raggio r in $\mathbb{K}$.
Più precisamente , se $\mu < \nu$, sono definiti come nel corollario IX.6.4,
allora f ha esattamente $\nu - \mu$ zeri, contati con molteplicità,
sulla sfera critica $|x| = r$ di $\mathbb{K}$: esiste un polinomio $P \in \mathbb{K}[X]$ di grado $\nu - \mu$ e una serie di potenze convergente $g \in \mathbb{K}[[X]]$, con $f = P \cdot g$ e $r_g \geq r_f$
(con g che non si annulla sulla sfera $S_r(\mathbb{K})$).
In particolare, se f è una funzione $p-$adica intera in $\mathbb{K}[[X]]$, allora si ha la stessa fattorizzazione con g funzione $p-$adica intera.

Corollario 6.7.
Sia $f \in \mathbb{K}[[X]]$ una serie di potenze convergente che non ha zeri in una qualche palla chiusa $|x| \leq r < r_f$ in $\bar{\mathbb{K}}$;
allora $\frac{1}{f}$ è data da una serie di potenze convergente con $r_{\frac{1}{f}} \geq r$.
Se f non ha zeri nella palla aperta $|x| < r' \leq r_f$ in $\bar{\mathbb{K}}$,
allora $\frac{1}{f}$ è data da una serie di potenze convergente con $r_{\frac{1}{f}} \geq r'$.

Dim: Sia $f(X) = \sum_{n\geq 0} a_n X^n$;
siccome $a_0 = f(0) \neq 0$ possiamo rimpiazzare f con $\frac{f}{f(0)}$ in modo da assumere $a_0 = 1$.
Definiamo $g(X) = \sum_{n\geq 1} a_n X^n$, cosi che $f = 1 + g$ e $r_f = r_g$.
La serie formale di potenze $\frac{1}{f}$ è la composizione:
$\frac{1}{f(X)} = \frac{1}{1+Y} \circ g(X)$;
per stimare il suo raggio di convergenza rimpiazziamo $\mathbb{K}$ con $\bar{\mathbb{K}}$,
e quindi assumiamo $\mathbb{K}$ algebricamente chiuso;
dal teorema IX.6.5, f non ha raggi critici minori o uguali a r e $|a_0| > |a_n| r^n$ per $n \geq 1$.
Questo mostra che $M_r(g) = \max_{n\geq 1} |a_n| r^n < |a_0| = 1$;
allora, dal teorema IX.5.6, è valida la valutazione numerica della composizione non appena $|x| < r_g = r_f$ e $M_{|x|}(g) < r_{\frac{1}{1+Y}} = 1$,

che accade quando $|x| \leq r$, siccome $M_{|x|}(g) \leq M_r(g) < 1$;
il teorema IX.5.6 prova anche che $r_{\frac{1}{f}} \geq r$;
la seconda parte del corollario si ottiene per $r \nearrow r'$. ■

Definizione 6.7. Una funzione si dice intera se è una serie di potenze con raggio di convergenza infinito.

IX.7 $\mathbb{C}_p$ versus $\mathbb{C}$.

Osservazione 7.1. Abbiamo osservato in questo capitolo che campi $\mathbb{K}$, estensioni ultrametriche di $\mathbb{Q}_p$, con l'aggiunta di particolari proprietà, quali:

1) Completezza.
2) Chiusura algebrica.
3) Densità del valore assoluto in $\mathbb{R}_{\geq 0}$.

Si comportano come il campo dei numeri complessi (almeno per quanto riguarda il loro rapporto con l'anello delle serie di potenze).

Ma possiamo osservare che il campo $\mathbb{C}_p$ incarna tutte e tre le proprietà,
e per questo si avvicina maggiormente al campo $\mathbb{C}$.
Per spiegare meglio a cosa è dovuta questa somiglianza possiamo enunciare il seguente

Teorema 7.2. $\mathbb{C}_p \cong \mathbb{C}$ (almeno algebricamente).

Dim: Ricordiamo inizialmente i seguenti teoremi di Steinitz:

1) Due chiusure algebriche di uno stesso campo sono isomorfe.
2) Ogni estensione di campi ha una base di trascendenza.
3) Due basi di trascendenza hanno la stessa cardinalità.

Ora siano $\mathbb{Q}^a$ e $\mathbb{Q}^b$ le chiusure algebriche di $\mathbb{Q}$ rispettivamente in $\mathbb{C}_p$ e in $\mathbb{C}$.
Allora abbiamo un isomorfismo $\mathbb{Q}^a \cong \mathbb{Q}^b$.
Ora questi due campi sono numerabili, ma i campi $\mathbb{C}_p$ e $\mathbb{C}$ hanno la potenza del continuo, di conseguenza hanno lo stesso grado di trascendenza su $\mathbb{Q}$.
In più ogni estensione di $\mathbb{Q}$ che abbia la potenza del continuo ha una base di trascendenza proprio con questa cardinalità;
da quanto detto sopra allora possiamo prendere basi di trascendenza $(X_i)_{i\in I}$ e $(Y_i)_{i\in I}$ rispettivamente in $\mathbb{C}_p$ e in $\mathbb{C}$;
ora però $\mathbb{C}_p$ è una chiusura algebrica di $\mathbb{Q}(X_i)_{i\in I}$ e $\mathbb{C}$ è una chiusura algebrica di $\mathbb{Q}(Y_i)_{i\in I}$, quindi abbiamo $\mathbb{C}_p \cong \mathbb{C}$. ■

Infine osserviamo che topologicamente non ci può essere un isomorfismo

(visto che uno ha un valore assoluto Archimedeo, l'altro ne ha uno non Archimedeo), però ricordiamo che l'immagine del valore assoluto di $\mathbb{C}_p$ è densa nell'immagine del valore assoluto di $\mathbb{C}$.

Bibliografia:
Il materiale di questo capitolo proviene principalmente da: [3].

Capitolo X

Funzioni $p-$adiche

X.1 **Logaritmo ed esponenziale**.

Lemma 1.1.
Sia $n \geq 1$ un intero e sia $S_p(n)$ la somme delle cifre di n in base p;
allora $ord_p(n!) = \frac{n-S_p(n)}{p-1}$.

Dim: Il numero degli interi k con un fissato ordine $ord_p(k) = \nu$,
che compaiono in $n!$ corrispondono a multipli di p^ν che non sono multipli di $p^{\nu+1}$
(e sono minori o uguali a n): sono $\left\lfloor \frac{n}{p^\nu} \right\rfloor - \left\lfloor \frac{n}{p^{\nu+1}} \right\rfloor$;
quindi $ord_p(n!) = \sum_{\nu \geq 1} \nu \left(\left\lfloor \frac{n}{p^\nu} \right\rfloor - \left\lfloor \frac{n}{p^{\nu+1}} \right\rfloor \right) = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor$;
se scriviamo n in base p come $n = n_0 + n_1 p + ...$(somma finita),
allora $\left\lfloor \frac{n}{p} \right\rfloor = n_1 + n_2 p + ...$,
$\left\lfloor \frac{n}{p^2} \right\rfloor = n_2 + n_3 p + ...$,
etc...
quindi $n = n_0 + p \left\lfloor \frac{n}{p} \right\rfloor$,
$\left\lfloor \frac{n}{p} \right\rfloor = n_1 + p \left\lfloor \frac{n}{p^2} \right\rfloor$,
etc...
quindi sommando tutte queste equazioni si ottiene che:
$n + ord_p(n!) = S_p(n) + p\ ord_p(n!)$, da cui la tesi. ■

Definizione 1.2. Poniamo $exp(x) = \sum_{k \geq 0} \frac{x^k}{k!}$,
e $log(1+x) = \sum_{k \geq 1} \frac{x^k (-1)^{k+1}}{k}$.

Esercizio 2.
Le serie che definisco il logaritmo e l'esponenziale $p-$adico convergono rispettivamente per $|x| < 1$ e $|x| < r_p := |p|^{\frac{1}{p-1}}$.

Osservazione 1.3. L'esponenziale $p-$adico, a differenza di quello complesso, non è una funzione intera.

Esercizio 3.
Per $|x| < r_p$ abbiamo:
$|log(1+x)| = |x|$.

$|exp(x)| = 1$.
$|1 - exp(x)| = |x|$.

Corollario 1.4.
L'unico zero di $log(1+x)$ nella palla $|x| < r_p$ è $x = 0$.

Proposizione 1.5.
Per due indeterminate X, Y valgono le seguenti identità formali:
$exp(X+Y) = exp(X)exp(Y)$.
$log(exp(X)) = X$.
$exp(log(1+X)) = 1+X$.

Dim: Per la prima identità osserviamo che:
$\frac{X^i}{i!} \cdot \frac{Y^j}{j!} = \frac{X^i Y^j}{i!j!} = \binom{i+j}{i} \frac{X^i Y^j}{(i+j)!}$.
Raggrupando i termini con $i+j = n$ otteniamo la somma $\frac{(X+Y)^n}{n!}$.
Occupiamoci della seconda identità:
nella serie $log(1+X) = \sum_{n\geq 1} a_n X^n$,
vorremo sostiutire $X = e^Y - 1 = b_1 Y + b_2 Y^2 + ...$ $(b_1 = 1)$;
Se espandiamo la seguente espressione, raggruppando le potenze di Y, otteniamo:
$\sum_{n\geq 1} a_n (b_1 Y + b_2 Y^2 + ...)^n = \sum_{n\geq 1} c_n Y^n$,
con $c_n = a_1 b_n + a_2(...) + ... + a_{n-1}(...) + a_n b_1^n$.
Per $2 \leq j \leq n-1$ il coefficiente di a_j è un polinomio in termini dei $b_1, ..., b_{n-1}$ con coefficienti interi; il problema è calcolare c_n nei valori razionali $a_n = \frac{(-1)^{n-1}}{n}$, $b_n = \frac{1}{n!}$.
Il risultato di questo calcolo è ben noto: lo stesso identico calcolo si ottiene nel caso della sostituzione della serie di potenze a valori reali $x = e^y - 1$ nella serie di potenze a valori reali $log(1+x)$; ma in tal caso sappiamo che il risultato è $log(e^y) = y$;
di conseguenza tutti i $c_n = 0, n \geq 2$ e $c_1 = 1$.
La terza identità si ottiene allo stesso modo. ■

Proposizione 1.6.
Per $|x| < r_p$ e $|y| < r_p$ abbiamo:
$exp(x+y) = exp(x)exp(y)$.
$log(exp(x)) = x$.
$exp(log(1+x)) = 1+x$.

Dim: Osserviamo che se $a_n \to 0$ e $b_n \to 0$,
allora la famiglia $(a_n b_m)_{n,m\geq 0}$ è sommabile;
quindi la sua somma è indipendente da come si sommano i termini;
quindi la prima identità vale non appena entrambe le variabili sono nel dominio di convergenza dell'esponenziale $p-$adico.
Lavoriamo sulla seconda identità: dobbiamo dimostrare che è legittimo sostituire un valore $x \in \mathbb{C}_p, |x| < r_p$ nell'identità formale:

$X = log(e^X) = log(1 + e(X))$, ove $e(X) = \sum_{n\geq 1} \frac{X^n}{n!} = e^X - 1$;
la sostituzione nella somma può essere ottenuta come somma di due contributi:
$x = \sum_{n\leq N} \frac{(-1)^{n+1} e(X)^n}{n}_{|X=x} + \sum_{m>N} \frac{(-1)^{m+1} e(X)^m}{m}_{|X=x}$.
Nella prima somma finita la sostituzione si può fare in ogni termine in accordo con la formula:
$e(X)^n \mid_{X=x} = (x + \frac{x^2}{2!} + ...)^n = e(x)^n$, per $|x| < r_p$.
Siccome $|e(x)| = |x| < r_p < 1$,
abbiamo $\sum_{n\leq N} \frac{(-1)^{n+1} e(x)^n}{n} \longrightarrow log(1 + e(x)) = log(e^x)$, $(N \to \infty)$.
La dimostrazione della seconda indentità sarà completata non appena mostriamo che la seconda somma è arbitrariamente vicina a 0, $(N \to \infty)$:
quando $|x| < r_p$ ogni monomio che compare nello sviluppo di $e(x)$ soddisfa $|\frac{x^i}{i!}| < r_p$ e ogni monomio che compare nello sviluppo di $e(x)^m$ ha valore assoluto minore di r_p^m;
quindi tutti i monomi che appaiono nella valutazione del secondo contributo hanno un valore assoluto minore di $\sup_{m>N} |\frac{(-1)^{m+1}}{m}| r_p^m$.
Siccome la serie del logaritmo converge, è possibile scegliere un N opportuno in modo che tutti i termini $|\frac{1}{m}| r_p^m$, per $m > N$, siano, insieme alla loro somma,
piccoli a piacere.
La verifica della terza identità è simile. ■

Osservazione 1.7. La derivata del logaritmo $log(1 + X)$ è $\frac{1}{1+X} = \sum_{n\geq 0} (-1)^n X^n$,
che ovviamente ha raggio di convergenza $r = 1$; quindi per IX.3.7 anche il logaritmo ha raggio di convergenza uguale a 1. In particolare si può osservare che per $|x| = 1$ il logaritmo $p-$adico diverge (anche l'esponenziale $p-$adico diverge per $|x| = r_p$).

Osservazione 1.8. Sappiamo che e^X ha ordine 0 e $log(1 + X)$ ha ordine 1;
definiamo $e(X) = e^X - 1$, di ordine 1;
allora $log(e^X) = log(1 + e(X)) = X + \sum_{k\geq 2} c_k X^k$, è ben definita,
e $D(log(e^X)) = \begin{cases} \frac{1}{1+e(X)} \cdot e^X = 1 \\ 1 + \sum_{k\geq 2} k c_k X^{k-1} \end{cases}$
Confrontando queste due espressioni si trova:
$0 = k c_k \in \mathbb{Q}$, da cui $c_k = 0$, per $k \geq 2$;
questo prova che $log(e^X) = log(1 + e(X)) = X$;
ma da X.1.5 si ha che $e(X) \circ log(1 + X) = X$,
ovvero $exp \circ log(1 + X) - 1 = X$, da cui $e^{log(1+X)} = 1 + X$.

Osservazione 1.9. Consideriamo $f(X) = \sum_{n\geq 0} X^n = \frac{1}{1-X} \in \mathbb{Q}_p[[X]]$
e $g(Y) = Y - Y^p \in \mathbb{Q}_p[[Y]]$;

presa una radice $\zeta \in \mu_{p-1}$ di g, osserviamo che vale $f(g(\zeta)) = f(0) = 1$;
ma $r_{f\circ g} = 1$ e la serie $f \circ g$ non converge nella sfera unitaria,
cosi che $(f \circ g)(\zeta)$ non è ben definito.
Osserviamo anche che $r = |\zeta| = 1$ e $M_r(g) = 1$, quindi $M_r(g)$ non è minore stretto di r_f, e la sostituzione non è giustificata da IX.5.6.

Osservazione 1.10. Da IX.5.6 abbiamo $log(e^x) = x$, quando $|x| < r_p$,
siccome $M_{|x|}(e(\cdot)) = |x|$ e $|x| = r < r_p < r_{log} = 1$;
similmente $exp(log(1 + x)) = 1 + x$, quando $|x| < r_p$,
siccome $M_{|x|}(log(1 + \cdot)) = |x|$, per $|x| = r < r_p$.
Questo ci dimostra che l'esponenziale e il logaritmo $p-$adico sono isometrie inverse nella palla aperta $B_{<r_p}(\mathbb{K})$.

X.2 **La serie esponenziale di Artin-Hasse**.

Definizione 2.1 (Serie esponenziale di Artin-Hasse).
$E(X) = exp(\sum_{k\geq 0} \frac{X^{p^k}}{p^k})$.

Osservazione 2.2. Si vede facilmente che $E(X) = \sum_{n\geq 0} a_n X^n$,
con $a_n \in \mathbb{Q} \cap \mathbb{Z}_p$; quindi si deduce che $r_E \geq 1$.

Definizione 2.3 (Funzione di Moebius).
La funzione di Moebius è la funzione arimtetica $\mu(n)$ definita in questo modo:
$\mu(1) = 1$; e se n è libero da quadrati, della forma $n = p_1 \cdots p_k$, con $p_1, ..., p_k$ primi distinti, allora $\mu(n) = (-1)^k$; altrimenti, se n non è libero da quadrati allora $\mu(n) = 0$.

Definizione 2.4.
La funzione $v(n)$ è la funzione aritmetica definita in questo modo:
$v(1) = 0$, e per $n > 1$, $v(n) =$ numero primi distinti che dividono n.

Esercizio 4.
Valgono le seguenti identità:
1) $\sum_{d|n} \mu(d) = \lfloor \frac{1}{n} \rfloor$;
2) $\sum_{d|n} |\mu(d)| = 2^{v(n)}$.

Esercizio 5.
Valgono le seguenti identità di serie formali:
1) $\sum_{n\geq 1} \frac{-\mu(n)}{n} log(1 - x^n) = x$;

2) Per ogni primo p, $\displaystyle\sum_{n\geq 1, p\nmid n} \frac{-\mu(n)}{n} log(1-x^n) = x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + ...$.

Corollario 2.5.
Abbiamo le seguenti identità di serie formali:
$exp(x) = \displaystyle\prod_{n\geq 1} (1-x^n)^{\frac{-\mu(n)}{n}}$,
$E(x) = \displaystyle\prod_{n\geq 1, p\nmid n} (1-x^n)^{\frac{-\mu(n)}{n}}$. ■

Osservazione 2.6. La serie di potenze $e^{\frac{x^p}{p}} = 1 + \frac{x^p}{p} + ...$
converge almeno per $|x| < r_p$, siccome $|\frac{x^p}{p}| \leq |x|$, per $|x| \leq r_p$.
In più vale la seguente identità:
$E(x) = \displaystyle\prod_{k\geq 0} exp\left(\frac{x^{p^k}}{p^k}\right)$, per $|x| < r_p$
(per dimostrarla basta usare il seguente lemma 2.8; lasciamo i dettagli al lettore che a questo punto dovrebbe essere in grado di cavarsela da solo).

Infine il raggio di convergenza di $h(x) = \displaystyle\sum_{k\geq 0} \frac{x^{p^k}}{p^k}$ è: $r_h = 1$,
e quindi si vede facilmente che risulta ben definita la composizione
$exp(h(x)) = E(x)$, per $|x| < r_p$.

Teorema 2.7.
$E(X) \in 1 + X\mathbb{Z}_p[[X]]$.
$r_E = 1$ e valgono le seguenti uguaglianze:
$|E(x)| = 1$, $|E(x) - 1| = |x|$, se $|x| < 1$.

Dim: Quando $p \nmid n$, la serie $(1-x^n)^{\frac{-\mu(n)}{n}}$ ha coefficienti in $\mathbb{Z}_p$ (per vederlo si usi IX.3.3 esempio 2)) e quindi converge almeno per $|x| < 1$;
il prodotto infinito ha anch'esso coefficienti in $\mathbb{Z}_p$;
anche lui quindi converge per $|x| < 1$ grazie al seguente

Lemma 2.8.
Per ogni successione $(a_n)_n$ in un campo ultrametrico completo $\mathbb{K}$,
con $a_n \to 1$, il prodotto $p_N = \displaystyle\prod_{n<N} a_n$ converge ad un limite denotato con $\displaystyle\prod_{n\geq 0} a_n$.
Più in generale se $(a_n)_n$ è una successione di funzioni a valori in $\mathbb{K}$ definita su un insieme S, e se $a_n \to 1$ unifromemente in S,
allora p_N convergente uniformemente in S al $\displaystyle\prod_{n\geq 0} a_n$.

Dim: Per ipotesi, definitivamente si ha $|a_n| = 1$ (vedere IV.1.4 2)).
Allora $|p_N| \leq C$, per ogni $N \geq 0$.
Ora $p_{N+1} - p_N = (a_N - 1)p_N$, quindi $|p_{N+1} - p_N| \leq C|a_N - 1| \to 0$;
questo prova che la successione p_N è di Cauchy e siccome $\mathbb{K}$ è completo, converge.

La seconda parte del lemma segue dalla prima. ■

Tutto ciò prova che $E(x) \in 1 + x\mathbb{Z}_p[[x]]$ e che $r = r_E \geq 1$.
Dimostriamo ora che tale raggio di convergenza è esattamente 1;
proviamo in primis la seguente identità:
$E(x^p) = \prod_{k=0}^{p-1} E(x\zeta^k)$, ove ζ è una radice $p-$esima dell'unità diversa da 1:
l'esponente nel prodotto è $(1 + \zeta + ... + \zeta^{p-1})x + p(\frac{x^p}{p} + \frac{x^{p^2}}{p^2} + ...)$
e siccome la prima parentesi è nulla, si ottiene l'identità.
Ora ogni serie di potenze $E(\zeta^k x)$ ha lo stesso raggio di convergenza $r = r_E$;
d'altra parte il raggio di convergenza di $E(x^p)$ è $r^{\frac{1}{p}}$,
quindi da IX.3.4 otteniamo che $r^{\frac{1}{p}} \geq min\{r, r, ..., r\} = r$.
Dunque $r \geq r^p$ che implica $r \leq 1$.
Per dimostrare le identità con il valore assoluto, basta applicare la regola che afferma che in un campo ultrametrico il numero con valore assoluto più grande predomina in una somma (rimandiamo al capitolo IV). ■

Un altro modo per dimostrare che $E(X) \in 1 + X\mathbb{Z}_p[[X]]$
è usare il seguente teorema:

Teorema 2.10 (Dieudonnè-Dwork).
Sia $f(x) \in 1 + x\mathbb{Q}_p[[x]]$, allora le seguenti sono equivalenti:
1) $f(x) \in 1 + x\mathbb{Z}_p[[x]]$.
2) $\frac{f(x)^p}{f(x^p)} \in 1 + px\mathbb{Z}_p[[x]]$.

Dim: 1) $\Rightarrow$ 2): se $f(x) \in 1 + x\mathbb{Z}_p[[x]]$ allora $f(x)^p \equiv f(x^p) \pmod p$;
da questo e dal fatto che $f(x^p) \in 1 + x\mathbb{Z}_p[[x]]$ e quindi è invertibile in esso,
si ottiene facilmente 2).
2) $\Rightarrow$ 1): scriviamo $f(x) = \sum_{i\geq 0} a_i x^i$, $a_0 = 1, a_i \in \mathbb{Q}_p$
e supponiamo che $\left(\sum_{i\geq 0} a_i x^i\right)^p = \left(\sum_{i\geq 0} a_i x^{pi}\right)\left(1 + p\sum_{j\geq 0} b_j x^j\right)$, con $b_j \in \mathbb{Z}_p$;
ora confrontando i coefficienti si ottiene
$a_1 = b_1$ e per trovare il coefficiente di x^n basta analizzare la seguente equazione
$\left(\sum_{i\leq n} a_i x^i\right)^p = \sum_{i\leq n} a_i^p x^{pi} + p(...)$;
a questo punto facciamo induzione sugli a_i, $i < n$, ricordando che $a_0 = 1, a_1 = b_1$,
supponendo che questi siano in $\mathbb{Z}_p$;
ne risulta che è conveniente lavorare $\pmod{p\mathbb{Z}_p}$;
il coefficiente di x^n al lato sinistro dell'equazione è
$a_i^p + pa_n + \alpha$, se $ip = n$, e con la convenzione che $a_{\frac{n}{p}} = 0$, se $\frac{n}{p}$ non è intero, e $\alpha \in p\mathbb{Z}_p$;
il coefficiente di x^n al lato destro dell'equazione è $a_{\frac{n}{p}} + \beta$, con $\beta \in p\mathbb{Z}_p$;
siccome $\frac{n}{p} < n$, l'ipotesi induttiva mostra che

$a_{\frac{n}{p}} \in \mathbb{Z}_p$ e quindi che vale $a_{\frac{n}{p}}^p \equiv a_{\frac{n}{p}} \pmod{p\mathbb{Z}_p}$;
comparando i termini si ottiene $pa_n \in p\mathbb{Z}_p \Rightarrow a_n \in \mathbb{Z}_p$. ■

Corollario 2.11. $E(X) \in 1 + X\mathbb{Z}_p[[X]]$.

Dim: Chiaramente $E(X) \in 1 + X\mathbb{Q}_p[[X]]$;
quindi basta mostrare che $\dfrac{E(X)^p}{E(X^p)} = exp(pX) = \displaystyle\sum_{n=0}^{\infty} \frac{(pX)^n}{n!} \in 1 + pX\mathbb{Z}_p[[X]]$;
allora è sufficiente mostrare che $ord_p(\frac{p^n}{n!}) > 0$:
$ord_p(\frac{p^n}{n!}) = n - \frac{n-S_n}{p-1} > 0$, siccome $S_n > 0$ e $n\left(1 - \frac{1}{p-1}\right) \geq 0$, $\forall n \geq 1$, e $\forall p$. ■

X.3 **La funzione** θ.

Definizione 3.1. $\theta(X) = exp(\pi(X - X^p))$, con π radice di $X^{p-1} + p = 0$.

Proposizione 3.2.
1) La serie $\theta(X)$ è convergente se $|x| \leq 1 + \varepsilon$, per un opportuno $\varepsilon > 0$.
2) $\theta(1)$ è una radice primitiva p-esima dell'unità.
3) Se $x \in \mathbb{C}_p$ è tale che $x^{p^s} = x$,
allora $\theta(1)^{\sum_{k=0}^{s-1} x^{p^k}} = \displaystyle\prod_{k=0}^{s-1} \theta(x^{p^k}) = exp(\pi(x - x^{p^s}))$.

Dim: 1) Per dimostrare il primo punto faremo vedere che il raggio di convergenza di $\theta(X)$ è esattamente $p^{\frac{p-1}{p^2}}$; per tale scopo usiamo la seguente

Proposizione 3.3.
Il raggio di convergenza della serie $f(x) = e^{x + \frac{x^p}{p}}$ è $r_f = r_p^{\frac{2p-1}{p^2}}$.
Quindi $r_p < r_f < 1$; in più vale $|f(x)| = 1$, per $|x| < r_f$.

Dim: Come serie di potenze formali abbiamo:
$E(x) = e^{x + \frac{x^p}{p}} \cdot exp\left(\displaystyle\sum_{j \geq 2} \frac{x^{p^j}}{p^j}\right)$,
e viceversa $e^{x + \frac{x^p}{p}} = E(x) \cdot exp\left(-\displaystyle\sum_{j \geq 2} \frac{x^{p^j}}{p^j}\right)$.
Ora osserviamo che $M_r\left(\displaystyle\sum_{j \geq 2} \frac{x^{p^j}}{p^j}\right) = |\frac{1}{p^2}| r^{p^2}$, per $0 \leq r \leq r_p^{\frac{1}{p^2}}$;
la sostituzione numerica di $g(x) = \displaystyle\sum_{j \geq 2} \frac{x^{p^j}}{p^j}$ in $exp(x)$ è possibile quando

$|x| < r_g = 1$ e $M_r(g) < r_p$.
La seconda condizione è valida quando
$\frac{|x|^{p^2}}{|p^2|} < |p|^{\frac{1}{p-1}}$, ovvero $|x| < r_p^{\frac{2p-1}{p^2}}$.
Siccome $\frac{1}{p} < \frac{1}{p}(2 - \frac{1}{p}) = \frac{2p-1}{p^2} < 1$,
osserviamo che $r_p < r_p^{\frac{2p-1}{p^2}} < 1$.
Questo ci dice che la valutazione numerica è valida nella regione considerata sopra e dunque $r_f \geq r_p^{\frac{2p-1}{p^2}}$.
Osserviamo anche che nella sua palla di convergenza, tutti i fattori in
$e^{x+\frac{x^p}{p}} = E(x) \cdot exp\left(-\sum_{j\geq 2} \frac{x^{p^j}}{p^j}\right)$
hanno valore assoluto uguale a 1, quindi
$|e^{x+\frac{x^p}{p}}| = 1$, per $|x| < r_p^{\frac{2p-1}{p^2}}$.
Ora consideriamo le tre serie $\frac{1}{E(x)}$, $g(x) = exp\left(-\frac{x^{p^2}}{p^2}\right)$ e $h(x) = exp\left(\sum_{j\geq 3} \frac{x^{p^j}}{p^j}\right)$ con i rispettivi raggi di convergenza che denotiamo con ρ_1, ρ_2, ρ_3.
Siccome $|E(x)| = 1$ per $|x| < 1 = r_E$, allora la serie $E(x)$ non ha zeri nella palla aperta di raggio 1 e applicando il corollario IX.6.7 si ha che la funzione $\frac{1}{E(x)}$ descrive una serie di potenze convergente con raggio di convergenza $\rho_1 \geq 1$;
in più si ha che $g(x) = \frac{1}{E(x)} \cdot f(x) \cdot h(x)$ e dal teorema IX.3.4 si ottiene
$\rho_2 \geq min\{\rho_1, r_f, \rho_3\}$; ma siccome $\rho_2 < \rho_3 < 1 \leq \rho_1$ si trova che $\rho_2 \geq r_f$.
Ora rimane da osservare (usando la formula di Hadamard) che $\rho_2 = r_p^{\frac{2p-1}{p^2}}$. ■

A questo punto deduciamo facilmente il punto 1) della proposizione tramite questa sostituzione: $x = \pi y \Rightarrow exp(x + \frac{x^p}{p}) = exp(\pi(y - y^p))$,
da cui si ottiene immediatamente $r_{\theta(x)} = r_p^{-\frac{(p-1)^2}{p^2}}$.

2) **Proposizione 3.4 (Dwork)**.
Sia $\zeta = e^{x+\frac{x^p}{p}} \mid_{x=\pi}$;
allora $\zeta \in \mu_p$ ed è tale che $\zeta \equiv 1 + \pi \pmod{\pi^2}$.

Dim: $e^{x+\frac{x^p}{p}} \equiv 1 + x \pmod{x^2}$ dunque basta dimostrare che ha senso la composizione e la valutazione numerica in $x = \pi$; se poniamo $e^{x+\frac{x^p}{p}} = \sum_{n\geq 0} a_n x^n$,
è sufficiente dimostrare che $|a_n \pi^n| < |\pi| = r_p$, per $n \geq 2$:
sappiamo da X.3.3 che il raggio di convergenza di $e^{x+\frac{x^p}{p}}$ è $r_p^{\frac{2p-1}{p^2}}$
quindi certamente abbiamo: $|a_n| r_p^{\frac{n(2p-1)}{p^2}} \leq 1$ e quindi $|a_n \pi^n| \leq r_p^{n - \frac{n(2p-1)}{p^2}} = r_p^{\frac{n(p-1)^2}{p^2}}$;
quindi se $p \geq 5$, $\forall n \geq 2$, abbiamo finito, visto che $\frac{n(p-1)^2}{p^2} \geq \frac{16n}{25} > 1$;
se $p = 3$ abbiamo $\frac{n(p-1)^2}{p^2} = \frac{4n}{9} > 1, \forall n \geq 3$, e siccome il coefficiente a_2 è lo stesso di quello di $E(X)$, e quindi è 3-intero, abbiamo concluso anche in questo caso;

infine se $p = 2$ vale che $\frac{n(p-1)^2}{p^2} = \frac{n}{4} > 1, \forall n \geq 5$, e nei casi $n \leq 4$, siccome vale che $e^{x+\frac{x^2}{2}} \mid_{x=\pi=-2} = 1 + \pi + \pi^2 + \frac{2\pi^3}{3} + \frac{5\pi^4}{12} + ...$, (esercizio!) e dall'analisi dei termini $\frac{2\pi^3}{3}$ e $\frac{5\pi^4}{12} \equiv 0 \pmod{\pi^2}$ si conclude anche in questo ultimo caso;

infine sia $\phi(x) = x^p$ e $h(x) = x + \frac{x^p}{p}$ allora vale:
$(exp(x + \frac{x^p}{p}))^p = \phi \circ exp(x + \frac{x^p}{p}) = \phi \circ (exp \circ h)(x) = (\phi \circ exp) \circ h(x) = exp(ph(x)) = e^{px}e^{x^p}$, e siccome ϕ e h sono polinomi, non abbiamo bisogno di nessuna condizione di convergenza per applicare queste composizioni (vedi IX esercizio 1);
di conseguenza possiamo scrivere:
$\zeta^p = (exp(x + \frac{x^p}{p}) \mid_{x=\pi})^p = e^{p\pi}e^{\pi^p} = e^{p\pi}e^{-p\pi} = 1.$ ■
Anche in questo caso deduciamo il punto 2) della proposizione ricorrendo alla sostituzione: $x = \pi y \Rightarrow exp(x + \frac{x^p}{p}) = exp(\pi(y - y^p)$.

3) Ora sia $x \in \mathbb{C}_p$ tale che $x^{p^s} = x$ e definiamo $H(T) = \prod_{k=0}^{s-1} \theta(Tx^{p^k})$
che converge per $|t| < 1 + \varepsilon$; in più se $|t| < 1$ vale anche
$\theta(tx^{p^k}) = exp(\pi(tx^{p^k} - t^p x^{p^{k+1}})) \Rightarrow H(t) = exp\left(\pi(t - t^p)\left(\sum_{k=0}^{s-1} x^{p^k}\right)\right)$
$= exp(\pi(t - t^p))^{\sum_{k=0}^{s-1} x^{p^k}}$ e quest'ultima uguaglianza deriva dal fatto che $\sum_{k=0}^{s-1} x^{p^k}$ è uguale alla traccia su $\mathbb{Q}_p$ di x e quindi è in realtà un elemento di $\mathbb{Z}_p$;
in definitiva abbiamo $H(T) = \theta(T)^{\sum_{k=0}^{s-1} x^{p^k}}$,
e siccome entrambe le serie convergono per $|t| < 1 + \varepsilon$,
tale uguaglianza vale in particolare per $T = 1$. ■

Teorema 3.5 (Dwork).
Sia π soluzione di $X^{p-1} + p = 0$;
allora $\mathbb{K} = \mathbb{Q}_p(\pi)$ è un'estensione di Galois di $\mathbb{Q}_p$;
è totalmente e moderatamente ramificata di grado $p - 1$ e $\mathbb{K} = \mathbb{Q}_p(\mu_p)$.
Più precisamente:
1) Il campo $\mathbb{K}$ contiene un'unica $p-$esima radice dell'unità $\zeta \in \mu_p$
tale che $\zeta \equiv 1 + \pi \pmod{\pi^2}$.
2) La serie $\theta(X)$ ha raggio di convergenza $p^{\frac{p-1}{p^2}}$.
3) Per ogni $a \in \mathbb{Q}_p$ con $a^p = a$,
abbiamo $\theta(a) \in \mu_p$ e $\theta(a) \equiv 1 + a\pi \pmod{\pi^2}$, cosi chè $\theta(1) = \zeta$.

Dim: Abbiamo già dimostrato quasi tutto.
Osserviamo in più che $X^{p-1} + p$ è un polinomio di Eisenstein rispetto a p. Questo prova che $\mathbb{K}$ è totalmente ramificato sopra $\mathbb{Q}_p$ (ogni estensione di $\mathbb{Q}_p$ con l'aggiunta

di una radice di un polinomio di Eisenstein è totalmente ramificata) e di grado $p-1$, quindi è anche moderatamente ramificato.
Se π, π' sono due radici di questo polinomio, allora:
$\left(\frac{\pi'}{\pi}\right)^{p-1} = 1$, quindi tutte le radici di $X^{p-1}+p$ sono ottenute come una radice particolare π per tutti gli elementi $\zeta \in \mu_{p-1}$.
Quindi l'estensione $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ è separabile (perché in caratteristica 0) e normale (e dunque di Galois) perché valgono le seguenti identità (che non dimostrerò)
$\mu(\mathbb{Q}_p) = \mu_{p-1}$, se p è dispari, altrimenti $\mu(\mathbb{Q}_2) = \{\pm 1\}$.
L'unicità di una radice $p-$esima dell'unita $\zeta \equiv 1+\pi \pmod{\pi^2}$,
segue dall'osservazione che due radici $p-$esime dell'unità distano r_p (vedere VI.1.3):
due distinte radici $p-$esime di 1 non sono congruenti $\pmod{\pi^2}$.
Le altre parti del teorema seguono facilmente dalle considerazioni precedenti.

Osservazione 3.6. Sia $\zeta \neq 1$ radice dell'unità di ordine p;
allora sappiamo che $\xi = \zeta - 1$ è radice di un polinomio della forma:
$x^{p-1} + px(...) + p = 0$, e quindi $|\xi| = r_p$.
Sia ora π soluzione di $x^{p-1}+p=0$;
siccome π e ξ hanno lo stesso valore assoluto,
deve accadere che $\xi = \pi u$, per qualche unità u;
allora $\zeta = 1 + \pi u$.
Se $a^{p-1} = 1$, diciamo $a \equiv k \pmod{p}$ con $1 \leq k < p$,
allora entrambi $\theta(a)$ e $\theta(1)^k$ sono radici $p-$esime dell'unità
congruenti a $1 + k\pi \pmod{\pi^2}$ e il teorema X.3.5 implica $\theta(a) = \theta(1)^k$.

Osservazione 3.7. Sia $f \geq 1$ e $\theta^f(x) = exp(\pi(x - x^{p^f})) = \theta(x)\theta(x^p)\cdots\theta(x^{p^{f-1}})$,
converge almeno quando ogni fattore converge;
la condizione più restrittiva è data dall'ultimo termine:
la convergenza di $\theta(x^{p^{f-1}})$ avviene se:
$|x^{p^{f-1}}| < p^{\frac{p-1}{p^2}}$,
che se poniamo $q = p^f$ equivale a dire che: $|x| < p^{\frac{p-1}{pq}}$.
In particolare il raggio di convergenza di $\theta^f(x)$ è $p^{\frac{p-1}{pq}} > 1$.

Osservazione 3.8. Siccome $\frac{\pi^p}{p} = -\pi$, possiamo scrivere

$$E(\pi X) = exp\left(\sum_{k=0}^{\infty} \frac{(\pi X)^{p^k}}{p^k}\right) = \theta(X) \prod_{k=2}^{\infty} exp\left(\frac{(\pi X)^{p^k}}{p^k}\right)$$

$$\Rightarrow \theta(X) = E(\pi X) \prod_{k=2}^{\infty} exp\left(-\frac{(\pi X)^{p^k}}{p^k}\right).$$

Se definiamo l'insieme:
$G(b) = \{f(X) \mid f(X) \in 1 + X\mathbb{C}_p[[X]]$, f converge per $ord(x) > -b$, $|f(X) - 1| < 1\}$

(qui per ord si intende l'estensione dell'ordine $p-$adico a tutto $\mathbb{C}_p$;
ad esempio si può estendere il valore assoluto $p-$adico nel modo consueto
e poi definire $ord(x) = log_p(|x|)$), da quanto trovato precedentemente deduciamo che

$\theta(X) \in G(\frac{p-1}{p^2})$. Infine osserviamo che se $f(X) = 1 + \sum_{k=1}^{\infty} a_k X^k \in \mathbb{C}_p[[X]]$ allora $f(X) \in G(b) \Leftrightarrow ord(a_k) \geq kb, \forall k \geq 1$.

Bibliografia:
Il materiale di questo capitolo proviene principalmente da [3] e da [5].
Vedere anche [12].

Capitolo XI

La congettura di Weil

Congettura di Weil 1.1.

Sia V una varietà algebrica proiettiva n-dimensionale
non singolare sopra un campo finito $\mathbb{F}_q$,
e sia: $\zeta(V,T) = exp\left(\sum_{k\geq 1} \frac{T^k N_k}{k}\right)$,
la funzione zeta associata a V, con $N_k = \sharp V(\mathbb{F}_{q^k})$,
allora valgono le seguenti affermazioni:

1) **Razionalità**: $\zeta_V(s) = \zeta(V, q^{-s})$ è una funzione razionale di $T = q^{-s}$;
più precisamente, esistono polinomi $P_1(T), ..., P_{2n}(T)$ tali che:
$\zeta_V(s) = \prod_{k=0}^{2n} P_k(T)^{(-1)^{k+1}}$,
con ogni $P_k(T) \in \mathbb{Z}[T]$ e in più: $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^n T$.

2) **Equazione funzionale**:
$\zeta_V(n-s) = \pm q^{\frac{n\chi}{2} - \chi s}\zeta_V(s)$,
ove: χ = caratteristica di Eulero-Poincarè di V.

3) **Ipotesi di Riemann**:
Ogni polinomio ha una fattorizzazione della forma:
$P_k(T) = \prod_j (1 - \alpha_{kj} T)$
e vale: $|\alpha_{kj}| = q^{\frac{k}{2}}$, $\forall 1 \leq k \leq 2n-1$, $\forall j$.

Osservazione 1.2. Deligne nel seminario Bourbaky ha dimostrato che tale congettura, in particolare il terzo punto, implica la famosa congettura di Ramanujan-Petersson, che afferma che data una forma modulare di peso $2k$, definta dalla sua serie di Fourier $f = \sum_{n\geq 1} c_n q^n$, con $c_1 = 1$, che sia un'autofunzione normalizzata per tutti gli operatori di Hecke, il polinomio $1 - c_p T + p^{2k-1}T^2$, per p primo, ammette una fattorizzazione della forma $(1 - \alpha_p T)(1 - \alpha'_p T)$, con: $\alpha_p + \alpha'_p = c_p$, $\alpha_p \alpha'_p = p^{2k-1}$, tale che le radici α_p, α'_p siano complesse e coniugate;
ciò si può riesprimere dicendo che: $|\alpha_p| = |\alpha'_p| = p^{k-\frac{1}{2}}$ oppure $|c_p| \leq 2p^{k-\frac{1}{2}}$ oppure $|c_n| \leq n^{k-\frac{1}{2}}\sigma_0(n)$, con $\sigma_0(n)$ la funzione numero divisori di n.

Osservazione 1.3. Questa congettura è stata proposta da Weil nel 1949 e provata da lui stesso per curve e varietà abeliane; nel 1960 Dwork provò la razionalità in generale; l'equazione funzionale fu dimostrata da Artin, Grothendieck e altri intorno al 1965, usando la coomologia l-adica; infine nel 1973/1974 Deligne provò l'ipotesi di Riemann.

Esercizio 6. Conoscendo la funzione zeta di una certa varietà V,
come posso calcolare i numeri N_k ?

Esercizio 7. Calcolare $\zeta(\mathbb{P}^N, T)$.

Bibliografia: Si può trovare una buona introduzione a tale congettura sulla pagina Wikipedia: *Weil conjectures*. Per il teorema di Deligne vedere [10];
Per una buona introduzione alle forme modulari vedere [11];

Capitolo XII

Congettura di Weil per curve ellittiche

Cerchiamo ora di risolvere un caso particolare di questa congettura:
supponiamo per ora che $V = \mathbb{E}$, una curva ellittica su $\mathbb{F}_q$;
sia l un primo diverso da $p = char(\mathbb{F}_q)$
e ricordiamo che abbiamo una mappa:
$End(\mathbb{E}) \longrightarrow End(T_l(\mathbb{E}))$,
$\Psi \longrightarrow \Psi_l$, (ove $T_l(\mathbb{E})$ indica il Tate modulo di $\mathbb{E}$ relativo al primo l,
che si costruisce come $T_l(\mathbb{E}) = \varprojlim_i \mathbb{E}[l^i]$).

Ricordiamo ora, senza darne la dimostrazione (che comunque si può trovare in [1] e che usa esclusivamente il Weil-pairing), la seguente

Proposizione 1.1. Sia $\Psi \in End(\mathbb{E})$, allora $det(\Psi_l) = deg(\Psi)$
e $Tr(\Psi_l) = 1 + deg(\Psi) - deg(1 - \Psi)$.

Teorema 1.2. Sia $\mathbb{E}/\mathbb{F}_q$ una curva ellittica,
e sia: $\phi : \mathbb{E} \longrightarrow \mathbb{E}$,
$(x, y) \longrightarrow (x^q, y^q)$,
il q-esimo morfismo di Frobenius, e sia: $a = q + 1 - \sharp\mathbb{E}(\mathbb{F}_q)$.

1) Siano $\alpha, \beta \in \mathbb{C}$ le radici del polinomio $T^2 - aT + q$.
Allora α e β sono complessi e coniugati e soddisfano $|\alpha| = |\beta| = \sqrt{q}$
e per ogni $n \geq 1$, $\sharp\mathbb{E}(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$.

2) Il morfismo di Frobenius verifica:
$\phi^2 - a\phi + q = 0$, in $End(\mathbb{E})$.

Dim: Come già sappiamo: $\sharp\mathbb{E}(\mathbb{F}_q) = deg(1 - \phi)$.
Ora $det(\phi_l) = deg(\phi) = q$,
$Tr(\phi_l) = 1 + deg(\phi) - deg(1 - \phi) = 1 + q - \sharp\mathbb{E}(\mathbb{F}_q) = a$
quindi il polinomio caratteristico di ϕ_l è:
$det(T - \phi_l) = T^2 - Tr(\phi_l)T + det(\phi_l) = T^2 - aT + q$.

1) Siccome il polinomio caratteristico di ϕ_l ha coefficienti in $\mathbb{Z}$
allora possiamo fattorizzarlo in $\mathbb{C}$ come $(T - \alpha)(T - \beta)$.
In più per ogni frazione $\frac{m}{n} \in \mathbb{Q}$ vale:
$det(\frac{m}{n} - \phi_l) = \frac{det(m - n\phi_l)}{n^2} = \frac{deg(m - n\phi_l)}{n^2} \geq 0$.
Siccome dunque il polinomio quadratico $T^2 - aT + q$ è non negativo su tutto $\mathbb{Q}$,
allora è negativo su tutto $\mathbb{R}$
(per continuità del polinomio e per la densità di $\mathbb{Q}$ in $\mathbb{R}$).

Da qui deduciamo che le radici sono complesse e coniugate, ma non reali, o reali, ma coincidenti, (quindi in totale possiamo dire che sono complesse e coniugate) e che $|\alpha| = |\beta|$ e siccome $\alpha\beta = q$ abbiamo anche che $|\alpha| = |\beta| = \sqrt{q}$.

Ora occupiamoci della seconda parte del primo punto:
per ogni intero $n \geq 0$ il q^n-esimo morfismo di Frobenius ϕ^n verifica:
$\sharp\mathbb{E}(\mathbb{F}_{q^n}) = deg(1 - \phi^n)$.
Segue che il polinomio caratteristico di ϕ_l^n è dato da:
$det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n)$
(per vederlo basta inserire ϕ_l nella sua forma canonica di Jordan, che sarà triangolare superiore con α, β sulla diagonale e poi elevare alla n).
In particolare: $\sharp\mathbb{E}(\mathbb{F}_{q^n}) = deg(1 - \phi^n) = det(1 - \phi_l^n) = 1 - \alpha^n - \beta^n + q^n$.

2) Per il teorema di Hamilton-Cayley $\phi_l^2 - a\phi_l + q = 0$, allora deduciamo come al solito che: $deg(\phi^2 - a\phi + q) = det(\phi_l^2 - a\phi_l + q) = 0$,
e quindi per definizione: $\phi^2 - a\phi + q = 0$ in $End(\mathbb{E})$. ■

Siamo pronti ora per la dimostrazione della congettura di Weil:

Teorema 1.3. Sia $V = \mathbb{E}/\mathbb{F}_q$ una curva ellittica.
Allora esiste un intero a tale che: $\zeta(V, T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$;
in più $\zeta(V, \frac{T}{q}) = \zeta(V, T)$,
e $1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$,
con $|\alpha| = |\beta| = \sqrt{q}$.

Dim: $log(\zeta(V, T)) = \sum_{n=1}^{\infty} \frac{\sharp\mathbb{E}(\mathbb{F}_{q^n})T^n}{n} = \sum_{n=1}^{\infty} \frac{(1 - \alpha^n - \beta^n + q^n)T^n}{n}$
$= -log(1 - T) + log(1 - \alpha T) + log(1 - \beta T) - log(1 - qT)$

da cui si deduce $\zeta(V, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$.

Infine grazie alla proposizione abbiamo che α e β sono complessi coniugati con valore assoluto $\sqrt{q}$ e soddisfano $\alpha + \beta = a \in \mathbb{Z}$.
L'equazione funzionale segue immediatamente. ■

Osservazione 1.4. Se operiamo il cambio di variabili $T = q^{-s}$ allora abbiamo:
$\zeta_V(s) = \zeta(V, q^{-s}) = \frac{(1-aq^{-s}+q^{1-2s})}{(1-q^{-s})(1-q^{1-s})}$.

L'equazione funzionale ci dice che:
$\zeta_V(s) = \zeta_V(1 - s)$, che coincide come struttura all'equazione funzionale della famosa funzione zeta di Riemann (sui complessi);
questo ci dice (lavorando per analogia) che $\zeta_V(s) = 0 \Leftrightarrow |q^s| = \sqrt{q} \Leftrightarrow Re(s) = \frac{1}{2}$.

Bibliografia: Il materiale di questo capitolo proviene principalmente da: [1].

Capitolo XIII

Razionalità della funzione zeta di una varietà algebrica

Per dimostrare la razionalità della funzione zeta supponiamo inizialmente di lavorare su un varietà algebrica particolare della forma:
$V = \{x = (x_1, ..., x_n) \in \mathbb{F}_{q^\infty} : f(x) = 0, x_1 \cdots x_n \neq 0\}$, con $f \in \mathbb{F}_q[X_1, ..., X_n]$.
In seguito svolgeremo il caso generale.

XIII.1 **Costruzione del carattere additivo** χ_s.

Definizione 1.1 (Rappresentante o sollevamento di Teichmuller).
Per ogni elemento $\bar{x} \in \mathbb{F}_q$ c'è un unico elemento $x = Teich(\bar{x}) \in \mathcal{O}_{\mathbb{C}_p}$ la quale riduzione modulo $\mathfrak{p}_{\mathbb{C}_p}$ è proprio $\bar{x}$ e tale che $x^q = x$.

Scriviamo qui sotto alcune proprietà di $Teich$ facili da verificare:
1) $Teich(\bar{x}\bar{y}) = Teich(\bar{x})Teich(\bar{y})$.
2) Se $\bar{x} \in \mathbb{F}_p \Rightarrow Teich(\bar{x}) \in \mathbb{Z}_p$
(in generale se T è estensione massimale non ramificata di $\mathbb{Q}_p$ in $\mathbb{C}_p$, oppure si può prendere T come il completamento di $\mathbb{Q}_p(\zeta_{p-1}, \zeta_{p^2-1}, \zeta_{p^3-1}, ...)$, allora $Teich(\bar{x}) \in T$).
3) $Teich(\bar{x} + \bar{y}) \equiv Teich(\bar{x}) + Teich(\bar{y}) \pmod{p\mathcal{O}_T}$.
4) Sia σ l'automorfismo di Frobenius di $T/\mathbb{Q}_p$, definito dalla proprietà:
$\sigma(\alpha) \equiv \alpha^p \pmod{p\mathcal{O}_T}$, $\forall \alpha \in T$, con $|\alpha| \leq 1$; ricordiamo che vale $\sigma(\zeta_{p^s-1}) = \zeta_{p^s-1}^p$;
allora vale anche che: $\sigma(Teich(\bar{x})) = (Teich(\bar{x}))^p$.

Definizione 1.2. Definiamo $\chi : \mathbb{F}_p \longrightarrow \mathbb{C}_p^*$
ponendo: $\chi(\bar{x}) = \zeta_p^{Teich(\bar{x})}$.

Osservazione 1.3. Si verifica immediatamente che in questo modo abbiamo ottenuto un carattere additivo (ricordiamo inoltre che ζ_p è una radice p-esima primitiva dell'unità, e che visto che $\zeta_p = 1 + \lambda$, $|\lambda| < 1$ e $Teich(\bar{x}) \in \mathbb{Z}_p$, $\chi(\bar{x})$ è un elemento ben definito in $\mathbb{C}_p$);
infine osserviamo che χ non è banale visto che $Teich(\bar{x}) \notin p\mathbb{Z}_p$, per $\bar{x} \neq 0$.

Ora generaliziamo la costruzione:

Definizione 1.4. Definiamo $\chi_s : \mathbb{F}_q \longrightarrow \mathbb{C}_p^*$
ponendo $\chi_s(\bar{x}) = \chi(Tr_{\mathbb{F}_q/\mathbb{F}_p}(\bar{x}))$,
ove la traccia è definita al solito modo: $Tr_{\mathbb{F}_q/\mathbb{F}_p}(y) = \sum_{k=0}^{s-1} y^{p^k}$ e $q = p^s$.

Osservazione 1.5. Siccome la mappa traccia per campi finiti è suriettiva,

ne deriva che il carattere appena costruito non è banale.
In più osserviamo che dalle proprietà di $Teich$ segue facilmente che:
$\chi_s(\bar{x}) = \zeta_p^{\sum_{k=0}^{s-1}(Teich(\bar{x}))^{p^k}}$, ma non vale la formula $\zeta_p^{\sum_{k=0}^{s-1}(Teich(\bar{x}))^{p^k}} = \prod_{k=0}^{s-1} \zeta_p^{(Teich(\bar{x}))^{p^k}}$,
perché in generale $Teich(\bar{x}) \notin \mathbb{Z}_p$.

Siamo pronti ora a generalizzare la costruzione del nostro carattere additivo:

Definizione 1.6. Sia $q = p^l$ e poniamo $\theta_l(X) = exp(\pi(X - X^q)) = \prod_{k=0}^{l-1} \theta(X^{p^k})$;
da X.3.7 sappiamo che $\theta_l \in G\left(\frac{p-1}{pq}\right)$;
definiamo allora $\chi_s : \mathbb{F}_{q^s} \longrightarrow \mathbb{C}_p^*$
ponendo $\chi_s(\bar{z}) = \prod_{k=0}^{s-1} \theta_l(z^{q^k})$, $z = Teich(\bar{z})$.

XIII.2 $\zeta(V,t)$ **è una funzione** $p-$**adica meromorfa**.

Siano $q = p^l$ e V una varietà algebrica definita come sopra;

Proposizione 2.1 $\zeta(V,t) \in \mathbb{Z}[[t]]$.

Dim: Sia σ l'automorfismo di Frobenius di $\mathbb{F}_{q^\infty}/\mathbb{F}_q$.
Tale σ agisce in modo naturale su V:
se $x = (x_1, ..., x_n) \in V$ allora $\sigma(x) = x^q := (x_1^q, ..., x_n^q) \in V$ (abbiamo già analizzato il gruppo di Galois di $\mathbb{F}_{q^\infty}/\mathbb{F}_q$ per una sua maggiore comprensione);
siccome i vari $x_i \in \mathbb{F}_{q^\infty} = \bigcup_{i=1}^{\infty} \mathbb{F}_{q^i}$,
allora esisterà una oppurtuna potenza di q che li elimina tutti contemporaneamente, ovvero l'orbita di un punto x tramite questa azione è finita e sarà della forma:
$\{x, x^q, ..., x^{q^{l-1}}\}$ e definiamo l la lunghezza di tale orbita;
allora abbiamo: $\mathbb{F}_q(x_1, ..., x_n) = \mathbb{F}_{q^l}$ (ovvio);
infine: $x \in V_s = V(\mathbb{F}_{q^s}) \Leftrightarrow l \mid s$ (anche questo è abbastanza ovvio);
dunque se noi poniamo D_l come il numero delle orbite di lunghezza l, allora
$N_s = \sharp V_s = \sum_{l|s} lD_l$ (ovvio per quanto detto sopra);
quindi $\sum_{s=1}^{\infty} \frac{t^s}{s} N_s = \sum_{s=1}^{\infty} \frac{t^s}{s} \sum_{l|s} lD_l = \sum_{l=1}^{\infty} D_l \sum_{j=1}^{\infty} \frac{lt^{lj}}{lj}$
$= \sum_{l=1}^{\infty} D_l(-log(1-t^l)) = log\left(\prod_{l=1}^{\infty} \left(\frac{1}{1-t^l}\right)^{D_l}\right)$

$\Rightarrow \zeta(V,t) = \prod_{l=1}^{\infty} \left(\frac{1}{1-t^l}\right)^{D_l}$; sviluppando tale prodotto
verrà certamente una serie di potenze a coefficienti in $\mathbb{Z}$. ■

Esercizio 8.
Se noi riscriviamo $\prod_{l=1}^{\infty} \left(\frac{1}{1-t^l}\right)^{D_l} = 1 + \sum_{k=1}^{\infty} a_k t^k$,
allora abbiamo appena dimostrato che $a_k \in \mathbb{N}$;
dare una stima molto banale sulla crescita di tali coefficienti
(in particolare la stima dovrebbe essere della forma: $a_k \leq q^{kn}$).

Esercizio 9. Nel caso di una curva ellittica $\mathbb{E}/\mathbb{F}_q$, $q = p^l$,
qual è la stima banale che si può dare sui vari N_s?
e qual è invece la stima non banale e a quali serie maggioranti e minoranti conduce?
(in questo caso è difficile dare una stima sui coefficienti della funzione zeta,
ma si possono trovare delle serie o meglio delle funzioni che maggiorano o minorano
la funzione zeta).

Da qui in poi il nostro scopo sarà quello di trovare una buona formula per tali N_s e riuscire poi a dimostrare che la funzione zeta è una funzione p-adica meromorfa.

Sia χ_s il carattere definito prima;
$$\sum_{x_0 \in \mathbb{F}_{q^s}} \chi_s(x_0 f(x_1,...,x_n)) = \begin{cases} 0, & \text{se } f(x_1,...,x_n) \neq 0 \\ q^s, & \text{se } f(x_1,...,x_n) = 0 \end{cases}$$
allora è ovvio che: $q^s N_s = \sum_{x_0 \in \mathbb{F}_{q^s}, (x_1,...,x_n) \in (\mathbb{F}_{q^s}^*)^n} \chi_s(x_0 f(x_1,...,x_n))$
$= (q^s-1)^n + \sum_{(x_0,x_1,...,x_n) \in (\mathbb{F}_{q^s}^*)^{n+1}} \chi_s(x_0 f(x_1,...,x_n))$
ricordandoci che se $x_0 = 0$, la prima somma vale $\sharp(\mathbb{F}_{q^s}^*)^n = (q^s-1)^n$.

Supponiamo ora che f abbia grado d e sia $X_0 f(X_1,...,X_n) = \sum_u \bar{a}_u X^u$,

$\bar{a}_u \in \mathbb{F}_q$, $u = (u_0,...,u_n)$, $u_0 = 1$, $d \geq \sum_{k=1}^{n} u_k$, $X^u := X_0^{u_0} \cdots X_n^{u_n}$.

Ora se $\bar{x} = (\bar{x}_0, \bar{x}_1, ..., \bar{x}_n) \in (\mathbb{F}_{q^s}^*)^{n+1} \Rightarrow \chi_s(\bar{x}_0 f(\bar{x})) = \chi_s\left(\sum_u \bar{a}_u \bar{x}^u\right) = \prod_u \chi_s(\bar{a}_u \bar{x}^u)$;
se noi poniamo $a_u = Teich(\bar{a}_u)$, $x = (x_0,...,x_n) = Teich(\bar{x}) = (Teich(\bar{x}_0),...,Teich(\bar{x}_n)), \Rightarrow$
$\chi_s(\bar{x}_0 f(\bar{x})) = \prod_u \theta_l(a_u x^u)\theta_l(a_u^q x^{qu}) \cdots \theta_l(a_u^{q^{s-1}} x^{q^{s-1}u}) =$
$\prod_u \theta_l(a_u x^u) \prod_u \theta_l(a_u x^{qu}) \cdots \prod_u \theta_l(a_u x^{q^{s-1}u})$, (osserviamo che $a_u^q = a_u$);

definiamo allora $F(X) = \prod_u \theta_l(a_u X^u) = \sum_{v=(v_0,...,v_n), dv_0 \geq v_1+...+v_n} A_v X^v$.

Analizzando meglio tali coefficienti A_v, siccome $\theta_l \in G(k)$, (con $k = \frac{p-1}{pq}$), quando $v_1 + ... + v_n \leq dv_0$ si trova che $ord(A_v) \geq v_0 k$, (lo lascio come esercizio, visto che non c'è nulla di geniale ed è più facile pensarci da soli che leggerne una dimostrazione).

Allora $F(X)$ e quindi anche $F(X)F(X^q)\cdots F(X^{q^{s-1}})$
converge per $|x| := \sup\{|x_1|, ..., |x_n|\} < 1 + \varepsilon$, per un opportuno $\varepsilon > 0$.

In totale abbiamo il seguente:

Lemma 2.2. $\chi_s(\bar{x}_0 f(\bar{x})) = F(x)F(x^q)\cdots F(x^{q^{s-1}}) \Rightarrow$
$q^s N_s = (q^s - 1)^n + \sum_{x^{q^s-1}=1} F(x)F(x^q)\cdots F(x^{q^{s-1}})$.

Consideriamo ora un campo T e il $T-$spazio vettoriale $W = T[X_0, ..., X_n]$.
Sia $H \in W$, allora abbiamo un endomorfismo naturale che indichiamo ancora con H dato da $H : W \longrightarrow W,\ \xi \longrightarrow H\xi$, ovvero la moltiplicazione per H.
In più definiamo $\psi_q : W \longrightarrow W$ come quell'unica mappa $T-$lineare tale che:
$\psi_q(X^v) = \begin{cases} 0, & \text{se } q \nmid v \\ X^{\frac{v}{q}}, & \text{altrimenti} \end{cases}$
ove $v = (v_0, ..., v_n)$ e $q \mid v \Leftrightarrow q \mid v_i, \forall i$;
(ne deriva facilmente che $(\psi_q \xi)(x) = \frac{1}{q^{n+1}} \sum_{y^q = x} \xi(y)$).

Sia $R \in \mathbb{R}_{>0}$ e definiamo $W'_R = \{\xi \in W \mid \xi = \sum_{u_0 \leq R, du_0 \geq u_1+...+u_n} A_u X^u\}$,
e fissato un intero positivo N supponiamo che $H \in W'_N$;
allora è facile verificare che la composizione $\psi_q \circ H : W'_R \longrightarrow W'_{R+N} \longrightarrow W'_{\frac{R+N}{q}}$
è un endomorfismo di W'_R, se R è sufficientemente grande (basta prendere $R > \frac{N}{q-1}$).

Lemma 2.3.
$(q-1)^{n+1} Tr(\psi_q \circ H) \mid_{W'_R} = \sum_{x^{q-1}=1} H(x)$.

Dim: Siccome entrambi i membri dell'equazione sono lineari in H possiamo supporre che H sia un monomio, diciamo $H = X^u$, $u = (u_0, ..., u_n)$, $u_0 \leq R$, $du_0 \geq u_1 + ... + u_n$;
allora $\sum_{x^{q-1}=1} x^u = \begin{cases} 0, & \text{se } (q-1) \nmid u \\ (q-1)^{n+1}, & \text{altrimenti} \end{cases}$
visto che $x \longrightarrow x^u$ è un carattere moltiplicativo non banale su $(\mathbb{F}_q^*)^{n+1}$, se $(q-1) \nmid u$;
d'altra parte, fissato u, abbiamo: $(\psi_q \circ X^u)(X^v) = \psi_q(X^{u+v})$ è 0 o un monomio per ogni v; quindi per calcolare $Tr(\psi_q \circ X^u)$ dobbiamo solo chiederci per quali v accade che $(\psi_q \circ X^u)(X^v) = X^v$, e questo accade per $u + v = qv$;

da qui segue che: $Tr(\psi_q \circ X^u) = \begin{cases} 0, & \text{se } (q-1) \nmid u \\ 1, & \text{altrimenti} \end{cases}$

da cui la tesi. ■

Ora sia s un intero positivo;
è facile verificare che $H(X)H(X^q)\cdots H(X^{q^{s-1}})$ è un elemento di $W'_{N(\sum_{k=0}^{s-1} q^k)}$ e che $\frac{R+N\left(\sum_{k=0}^{s-1} q^k\right)}{q^s} < R$, se $R > \frac{N}{q-1}$;
quindi la mappa $\psi_q \circ H(X)H(X^q)\cdots H(X^{q^{s-1}})$ è un endomorfismo di W'_R quando R è sufficientemente grande;
siccome $\psi_q \circ H(X^q) = H(X) \circ \psi_q$ (ovvio),
allora è immediato verificare che: $\psi_{q^2} \circ H(X)H(X^q) = (\psi_q \circ H(X))^2$
e per induzione su $s > 2$ che: $\psi_{q^s} \circ H(X)H(X^q)\cdots H(X^{q^{s-1}}) = (\psi_q \circ H(X))^s$.

Osservazione 2.4. Per il lemma XIII.2.3, troviamo che:
$(q^s-1)^{n+1} Tr(\psi_q \circ H(X))^s \mid_{W'_R} = \sum_{x^{q^s-1}=1} H(x)H(x^q)\cdots H(x^{q^{s-1}})$.

Definizione 2.5. Poniamo ora $Z(t) = exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s} \sum_{x^{q^s-1}=1} F(x)F(x^q)\cdots F(x^{q^{s-1}})\right)$
e poniamo $F_N(X) = \sum_{v_0 \le N, dv_0 \ge v_1+\ldots+v_n} A_v X^v$.

Osservazione 2.6. Siccome $F(x)F(x^q)\cdots F(x^{q^{s-1}})$
converge per $|x| < 1+\varepsilon$ otteniamo che
$\sum_{x^{q^s-1}=1} F(x)F(x^q)\cdots F(x^{q^{s-1}}) = \lim_{N\to\infty} \sum_{x^{q^s-1}=1} F_N(x)F_N(x^q)\cdots F_N(x^{q^{s-1}})$
$= \lim_{N\to\infty} (q^s-1)^{n+1} Tr(\psi_q \circ F_N)^s \Rightarrow Z(t) = exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s}(q^s-1)^{n+1} Tr(\psi_q \circ F_N)^s\right)$.

Definizione 2.7. Definiamo ora l'operatore ϕ che agisce sugli elementi $h \in \mathbb{C}_p[[T]]$ in questo modo: $h^\phi(t) = h(qt)$.
Consideriamo poi $h_N(t) = exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s} Tr(\psi_q \circ F_N)^s\right)$.
Lasciamo per facile esercizio le due seguenti identità:
1) $exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s}(q^s-1) Tr(\psi_q \circ F_N)^s\right) = \frac{h_N(qt)}{h_N(t)} = h_N^{\phi-1}(t)$.
2) $exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s}(q^s-1)^{n+1} Tr(\psi_q \circ F_N)^s\right) = h_N^{(\phi-1)^{n+1}}(t)$
(che seguono facilmente usando lo sviluppo di Newton del binomio
e la definizione di ϕ).

Esercizio 10. Sia f un endomorfismo di uno spazio vettoriale finito dimensionale su un campo di caratteristica 0, allora vale:
$exp\left(\sum_{s=1}^{\infty}\frac{t^s}{s}Tr(f^s)\right) = (det(I-tf))^{-1}$, con I = mappa identità.

Osservazione 2.8. A questo punto è evidente che:
$h_N(t) = exp\left(\sum_{s=1}^{\infty}\frac{t^s}{s}Tr(\psi_q \circ F_N)^s\right) = (det(I - t(\psi_q \circ F_N)))^{-1}$
$\Rightarrow Z(t) = \left(\lim_{N\to\infty} det(I - t(\psi_q \circ F_N))\right)^{-(\phi-1)^{n+1}}$.

Osservazione 2.9 Dimostrando che $Z(t)$ è una funzione $p-$adica meromorfa seguirà che $\zeta(V,t)$ è una funzione p-adica meromorfa,
infatti: $\zeta(V,qt) = exp\left(\sum_{s=1}^{\infty}\frac{q^s t^s}{s}N_s\right)$
$= exp\left(\sum_{s=1}^{\infty}\frac{t^s}{s}(q^s-1)^n\right)\lim_{N\to\infty} exp\left(\sum_{s=1}^{\infty}\frac{t^s}{s}(q^s-1)^{n+1}Tr(\psi_q \circ F_N)^s\right)$
$= exp\left(\sum_{s=1}^{\infty}\frac{t^s}{s}(q^s-1)^n\right)Z(t) = \left(exp\left(\sum_{s=1}^{\infty}\frac{t^s}{s}\right)\right)^{(\phi-1)^n} Z(t) = \frac{1}{(1-t)^{(\phi-1)^n}}Z(t)$.

Resta da dimostrare per i nostri scopi la seguente

Proposizione 2.10.
$Z(t)$ è una funzione p-adica meromorfa.

XIII.3 **Generalizzazione alle serie formali**.

Tutto quello che abbiamo fatto in XIII.2 riguardava i polinomi;
cerchiamone una generalizzazione alle serie formali:

Definizione 3.1. Sia $R = \mathbb{C}_p[[x_0,...,x_n]]$, e sia $\mathfrak{m} \trianglelefteq R$,
il suo unico ideale massimale (teorema di Hilbert);
per ogni $h \in R$ definiamo $ord(h) = r \Leftrightarrow r = min\{k : h^k \in \mathfrak{m}\}$
e inseriamo su R la topologia $\mathfrak{m}-$adica;
una base per tale topologia è: $\{\mathfrak{m}^r : r \geq 0\}$
e vale che $h_m \longrightarrow h \Leftrightarrow ord(h_m - h) \longrightarrow \infty$, $(m \longrightarrow \infty)$;
consideriamo ora delle mappe $\mathbb{C}_p$-lineari su R che indichiamo con A,
continue rispetto alla topologia $\mathfrak{m}-$adica;

Osservazione 3.2. Tali mappe verificano $A\left(\sum_{\alpha} c_\alpha x^\alpha\right) = \sum_{\alpha} c_\alpha A(x^\alpha)$

e $\lim_{|\alpha|\longrightarrow\infty} A(x^\alpha) = 0$, ricordando che se $\alpha = (\alpha_0, ..., \alpha_n) \Rightarrow |\alpha| = \sum_{k=0}^{n} \alpha_k$.

Definizione 3.3. Se noi scriviamo $A(x^\beta) = \sum_{\alpha} a_{\alpha\beta} x^\alpha$ allora diciamo che la matrice associata ad A è $(a_{\alpha\beta})_{\alpha,\beta\in\mathbb{Z}_{\geq 0}^{(n+1)}}$ e che A ha supporto finito se la sua matrice associata ha un numero finito di entrate non nulle;
in questo caso A può essere identificato con un endomorfismo di $\mathbb{C}_p[x_0, ..., x_n]$.

Osservazione 3.4. Valgono le seguenti formule:
1) Se A è descritta dalla matrice $(a_{\alpha\beta})$,
allora $A\left(\sum_{\beta} c_\beta x^\beta\right) = \sum_{\alpha}\left(\sum_{\beta} a_{\alpha\beta} c_\beta\right) x^\alpha$.
2) Se A e B sono due tali mappe continue e lineari descritte da matrici $(a_{\alpha\beta}), (b_{\alpha\beta})$ allora $A \circ B$ è descritta dalla matrice $(c_{\alpha\beta}), c_{\alpha\beta} = \sum_{\gamma} a_{\alpha\gamma} b_{\gamma\beta}$.

Osservazione 3.5. Riconsideriamo l'applicazione (lineare e continua) $H : R \longrightarrow R$ data dalla moltiplicazione per H e osserviamo che se $H = \sum_{\alpha} h_\alpha x^\alpha$ allora la matrice associata ad H è della forma: $(h_{\alpha-\beta})$ con $h_{\alpha-\beta} = 0$ se $\alpha - \beta \notin \mathbb{Z}_{\geq 0}^{n+1}$
(osserviamo che tale H generalizza l'omonima definita precedentemente).
Un'altra utile generalizzazione è quella di ψ_q, ottenuta ponendo:
$\psi_q\left(\sum_{\alpha} a_\alpha x^\alpha\right) = \sum_{\alpha} a_{q\alpha} x^\alpha$;
è chiaro che anche lei è lineare e continua.

Osservazione 3.6. Se $H = \sum_{\alpha} h_\alpha x^\alpha \Rightarrow (\psi_q \circ H)(x^\beta) = \sum_{\alpha} h_{q\alpha-\beta} x^\alpha$;
di conseguenza si trova che $\psi_q \circ H$ è rappresentata dalla matrice $(h_{q\alpha-\beta})_{\alpha,\beta}$.

Esercizio 11. $H \circ \psi_q = \psi_q \circ H_q$, se $H_q(x_0, ..., x_n) = H(x_0^q, ..., x_n^q)$.

Definizione 3.7. Ora, presa una mappa lineare e continua $A : R \longrightarrow R$ con matrice $(a_{\alpha,\beta})$ denotiamo con $Tr(A)$ la serie $\sum_{\alpha} a_{\alpha\alpha}$ (se essa converge); notiamo che se A ha supporto finito allora tale traccia coincide proprio con la traccia di un endomorfismo dello spazio vettoriale dei polinomi, di dimensione finita.

Definizione 3.8. Definiamo $R_0 := \{H = \sum_{\alpha} h_\alpha x^\alpha \in R \mid \exists M > 0 :$

$|h_\alpha|_p \leq \left(\frac{1}{p}\right)^{M|\alpha|}, \forall \alpha \in \mathbb{Z}_{\geq 0}^{n+1}\}$.

Osservazione 3.9. Se $H \in R_0$, allora esiste un $\rho > 1$, ad esempio se M è definito come sopra, possiamo prendere $\rho = p^a$, $0 < a < M$, tale che $H(u_0, ..., u_n)$ converge quando $|u_i| \leq \rho$, infatti: $|h_\alpha u_0^{\alpha_0} \cdots u_n^{\alpha_n}| \leq |h_\alpha| \rho^{|\alpha|} \leq \left(\frac{1}{p}\right)^{(M-a)|\alpha|}$
(che converge a zero quando $|\alpha| \to \infty$) .

Lasciamo come esercizio i due seguenti lemmi:

Lemma 3.10.
R_0 è un sottoanello di R, e se $j_0, ..., j_n$ sono interi positivi e $H \in R_0$,
allora $H(x_0^{j_0}, ..., x_n^{j_n}) \in R_0$. ■

Lemma 3.11.
Sia $H \in R_0$ e $\psi = \psi_q \circ H$, $q \geq 2$;
per ogni $s \geq 1$ vale la seguente formula:
$(q^s - 1)^{n+1} Tr(\psi^s) = \sum_{u^{q^s-1}=1} H(u)H(u^q) \cdots H(u^{q^{s-1}})$.
(è soltanto una generalizzazione dell'analoga formula scritta precedentemente;
si dimostra per il caso $s = 1$ in modo simile a prima, usando anche XIII.3.9 per verificare che certi oggetti siano ben definiti e poi si usa l'esercizio 11, facendo composizioni e lavorando induttivamente, per arrivare al caso $s \geq 1$ generico). ■

Definizione 3.12. Sia come al solito $A : R \longrightarrow R$ descritta dalla matrice $(a_{\alpha,\beta})$;
definiamo la serie di potenze caratteristica di A come:
$det(I - tA) := \sum_{m \geq 0} (-1)^m \left(\sum_\sigma \varepsilon_\sigma a_{\alpha_1 \sigma(\alpha_1)} \cdots a_{\alpha_m \sigma(\alpha_m)} \right) t^m$, dove la seconda somma è su tutti i sottoinsiemi di m elementi $\{\alpha_1, ..., \alpha_m\} \in \mathbb{Z}_{\geq 0}^m$ e su tutte le permutazioni σ di questi insiemi.
Osserviamo che se A ha supporto finito allora $det(I - tA)$ si riduce al polinomio caratteristico di un endomorfismo dello spazio vettoriale finito dimensionale dei polinomi.

Lemma 3.13.
Se $H \in R_0$ allora per ogni $q \geq 2$ intero positivo, la serie caratteristica di $\psi = \psi_q \circ H$ è ben definita e ha raggio di convergenza infinito (ovvero descrive una funzione p-adica intera).

Dim: Sia $H = \sum_\alpha h_\alpha x^\alpha$ e sia $M > 0$ tale che $|h_\alpha| \leq |p|^{M|\alpha|}$, $\forall \alpha$;
sappiamo che ψ ha matrice associata $(a_{\alpha\beta} = h_{q\alpha-\beta})$;
ora sia $\{u_0, ..., u_m\} \subset \mathbb{Z}_{\geq 0}^{n+1}$ e sia σ una permutazione di questo insieme;
allora abbiamo: $|a_{\alpha_1 \sigma(\alpha_1)} \cdots a_{\alpha_m \sigma(\alpha_m)}| \leq \left(\frac{1}{p}\right)^{M \sum_{i=1}^m |q\alpha_i - \sigma(\alpha_i)|}$;
Ora osserviamo che $|q\alpha_i - \sigma(\alpha_i)| = q|\alpha_i| - |\sigma(\alpha_i)|$
se $q\alpha_i - \sigma(\alpha_i) \in \mathbb{Z}_{\geq 0}^{n+1}$ ed è 0 altrimenti;

nell'ultimo caso però abbiamo $a_{\alpha_i\sigma(\alpha_i)} = 0$;
di conseguenza abbiamo $|a_{\alpha_1\sigma(\alpha_1)} \cdots a_{\alpha_m\sigma(\alpha_m)}| \leq \left(\frac{1}{p}\right)^{M(q-1)\sum_{i=1}^{m}|\alpha_i|}$;
è evidente che il lato destro di questa equazione tende a zero quando $max\{|\alpha_i|\} \to \infty$ e quindi $det(I - tA)$ è ben definita come serie.

In più da quanto scritto sopra otteniamo anche che:
$det(I - tA) = \sum_{m\geq 0} b_m t^m$ con $|b_m|^{\frac{1}{m}} \leq \max_{\alpha_1,\ldots,\alpha_m} |p|^{\frac{M(q-1)\sum_{i=1}^{m}|\alpha_i|}{m}}$,
dove il massimo è sopra distinti $\alpha_1, ..., \alpha_m \in \mathbb{Z}_{\geq 0}^{n+1}$;

$$\text{ma quando } m \to \infty \text{ il } \min_{\alpha_1,\ldots,\alpha_m} \frac{M(q-1)\sum_{i=1}^{m}|\alpha_i|}{m} \to \infty$$

che implica $\lim_{m\to\infty} |b_m|^{\frac{1}{m}} = 0$
ovvero che il raggio di convergenza di $det(I - tA)$ è infinito. ■

Lemma 3.14.
Se $A : R \longrightarrow R$ è una mappa lineare continua per cui $det(I - tA)$ e $Tr(A^s)$ sono ben definiti, per ogni $s \geq 1$, allora:
$$det(I - tA) = exp\left(-\sum_{s=1}^{\infty} \frac{Tr(A^s)}{s} t^s\right).$$

Dim: Se A ha supporto finito, allora l'asserto segue dall'esercizio 10.
Consideriamo ora una successione $(A^{(m)})_{m\geq 1}$ di mappe con supporto finito,
ognuna descritta da una matrice $(a_{\alpha\beta}^{(m)})_{\alpha,\beta\in\mathbb{Z}_{\geq 0}^{n+1}}$, che soddisfano la seguente condizione:
per ogni α e β abbiamo $a_{\alpha\beta}^{(m)} = a_{\alpha\beta}$ o $a_{\alpha\beta}^{(m)} = 0$, per ogni $m >> 0$;
Sicuramente possiamo trovare una successione $(A^{(m)})_{m\geq 1}$ con questa proprietà.

Usiamo ora in $\mathbb{C}_p[[t]]$ la topologia prodotto (se lo identifichiamo come un prodotto numerabile di copie di $\mathbb{C}_p$, in ognuna delle quali c'è la solita topologia $p-$adica).
Più esplicitamente una successione di serie formali $(f_m)_{m\geq 1}$,
con $f_m = \sum_{i\geq 0} b_{mi} t^i$, converge a $f = \sum_{i\geq 0} b_i t^i$, se e soltanto se $\lim_{m\to\infty} b_{mi} = b_i$, $\forall i$.
Osserviamo che se in aggiunta si suppone che $f_m(0) = 0$, $\forall m$,
allora $exp(f_m)$ convergerà ad $exp(f)$.

Ora siccome ogni $A^{(m)}$ soddisfa la proposizione,
per concludere basta mostrare i due seguenti fatti:

1) $\lim_{m\to\infty} det(I - tA^{(m)}) = det(I - tA)$.
2) $\lim_{m\to\infty} Tr((A^{(m)})^s) = Tr(A^s)$, $\forall s \geq 1$.

Dimostriamo il punto 1):

Consideriamo i coefficienti $b_l^{(m)}$ e b_l di t^l in $det(I - tA^{(m)})$ e in $det(I - tA)$, rispettivamente. Per definizione si ha:
$b_l^{(m)} := (-1)^l \sum_{\sigma} \varepsilon(\sigma) a^{(m)}_{\alpha_1\sigma(\alpha_1)} \cdots a^{(m)}_{\alpha_l\sigma(\alpha_l)}$,
ma per la nostra scelta degli $A^{(m)}$ ogni prodotto nella somma sarà 0
oppure sarà un termine nella corrispondente somma che definisce b_l.
Ma presa un qualsiasi insieme $\{\alpha_1, ..., \alpha_l\}$ e presa una qualsiasi permutazione σ di questo insieme, il prodotto $\varepsilon(\sigma) a_{\alpha_1\sigma(\alpha_1)} \cdots a_{\alpha_l\sigma(\alpha_l)}$ apparirà nella somma che definisce $b_l^{(m)}$ per $m >> 0$.
Siccome noi sappiamo però che $det(I - tA)$ esiste,
la tesi del punto 1) segue immediatamente.

Dimostriamo ora il punto 2):
Per definizione abbiamo:
$Tr((A^{(m)})^s) = \sum_{\alpha_1,...,\alpha_s} a^{(m)}_{\alpha_1\alpha_2} \cdots a^{(m)}_{\alpha_{s-1}\alpha_s} a^{(m)}_{\alpha_s\alpha_1}$.
Per ipotesi ogni prodotto $a^{(m)}_{\alpha_1\alpha_2} \cdots a^{(m)}_{\alpha_{s-1}\alpha_s} a^{(m)}_{\alpha_s\alpha_1}$ è 0 o un termine della corrispondente somma che definisce $Tr(A^s)$.
Ma ogni prodotto $a_{\alpha_1\alpha_2} \cdots a_{\alpha_{s-1}\alpha_s} a_{\alpha_s\alpha_1}$ appare nella somma che definisce $Tr((A^{(m)})^s)$ per $m >> 0$. Siccome sappiamo che $Tr(A^s)$ esiste, deduciamo il punto 2). ■

Ritorniamo ora sui nostri passi:

Dimostrazione proposizione XIII.2.10:
Ricordiamo che abbiamo posto $F(X) = \prod_u \theta_l(a_u X^u) = \sum_{v, dv_0 \geq v_1 + ... + v_n} A_v X^v$
e $Z(t) = exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s} \sum_{x^{q^s - 1} = 1} F(x) F(x^q) \cdots F(x^{q^{s-1}}) \right)$;
ma se dimostriamo che $F(X) \in R_0$ allora possiamo applicare il lemma XIII.3.14
e riscrivere $Z(t)$ come:
$Z(t) = exp\left(\sum_{s=1}^{\infty} \frac{t^s}{s} (q^s - 1)^{n+1} Tr(\psi_q \circ F)^s \right) = (det(I - t(\psi_q \circ F)))^{-(\phi-1)^{n+1}}$;
infine (sempre sotto l'ipotesi $F(X) \in R_0$) dal lemma XIII.3.13 otteniamo che $Z(t)$ è una funzione p-adica meromorfa, che conclude la proposizione;

resta quindi da dimostrare che $F(X) \in R_0$:
ricordiamo che abbiamo già dimostrato che: $ord(A_v) \geq v_0 k$, $k = \frac{p-1}{pq}$,
allora siccome $|v| \leq v_0 + v_1 + ... + v_n \leq (d+1) v_0$,
si ha che se prendiamo come costante $M = \frac{k}{d-1}$
vale che $|A_v| = p^{-ord(A_v)} \leq p^{-M|v|}$, $\forall v$. ■

XIII.4 **Condizione per la razionalità**.

Teorema 4.1.
Sia $f(t) = \sum_j A_j t^j$
serie di potenze con coefficienti in un campo arbitrario Ω; sia:

$$\Lambda_{s,k} = det \begin{bmatrix} A_s & A_{s+1} \ ... & A_{s+k} \\ A_{s+1} & A_{s+2} \ ... & A_{s+k+1} \\ \vdots & \vdots & \vdots \\ A_{s+k} & A_{s+k+1} \ ... & A_{s+2k} \end{bmatrix}$$

allora la serie rappresenta una funzione razionale se $\exists k > 0 : \Lambda_{s,k} = 0, \forall s \geq s_0$.

Dim: iniziamo con un facile

Esercizio 12. Siano U e V spazi vettoriali su un campo $\mathbb{K}$
e siano $v_1, ..., v_n$ vettori linearmente indipendenti di V;
supponiamo che ϕ, ψ siano due mappe lineari da V in U
tali che $\psi(v_{i-1}) = \phi(v_i), i = 2, 3, ..., n$;
se $\phi(v_1), ..., \phi(v_{n-1})$ sono linearmenti dipendenti,
allora $\phi(v_2), ..., \phi(v_n)$ sono linearmente dipendenti.

A questo punto scegliamo k minimale rispetto alla condizione che esista un s_0 tale che $\Lambda_{s,k} = 0, \forall s \geq s_0$;
per $s \geq 0$ siano $v_s^{(k)} = (A_s, ..., A_{s+k}) \in \Omega^{k+1}$,
$W_s =< v_s^{(k)}, ..., v_{s+k}^{(k)} >$,
$U_s =< v_s^{(k)}, ..., v_{s+k-1}^{(k)} >$,
cosi che $U_s \subset W_s \subset \Omega^{k+1}, U_{s+1} \subset W_s$.
Per ipotesi $\dim W_s \leq k, \forall s \geq s_0$ e k è minimale nell'insieme dei numeri naturali positivi per cui vale questa relazione di dipendenza lineare per tutti gli s sufficientemente grandi; il nostro obiettivo ora è quello di dimostrare che $\dim U_s = k$, per $s \geq s_0$:
sia $s' \geq s_0$; dimostreremo che $\dim U_s < k \Rightarrow \lambda_{s,k-1} = 0, \forall s \geq s'$,
contraddicendo la minimalità di k;
infatti siano: $\phi(v_s^{(k)}) = v_s^{(k-1)}, \psi(v_s^{(k)}) = v_{s+1}^{(k-1)}, \forall s \geq 0$;
se $\dim U_{s'} < k$ allora $\{v_{s'}^{(k)}, ..., v_{s'+k-1}^{(k)}\}$ è linearmente dipendente;
di conseguenza $\{\phi(v_{s'}^{(k)}), ..., \phi(v_{s'+k-1}^{(k)})\}$ è linearmente dipendente
e per l'esercizio 12 anche $\{\phi(v_{s'+1}^{(k)}), ..., \phi(v_{s'+k}^{(k)})\}$ lo è;
da qui iterando si trova che $\{\phi(v_s^{(k)}), ..., \phi(v_{s+k-1}^{(k)})\}$ è linearmente dipendente $\forall s \geq s'$,
ovvero che $\{v_s^{(k-1)}, ..., v_{s+k-1}^{(k-1)}\}$ è linearmente dipendente $\forall s \geq s'$,
contraddicendo la minimalità di k.

Da quanto appena dimostrato si deduce facilmente che U_s è indipendente da s per $s \geq s_0$ (infatti U_s e U_{s+1} sono sottospazi k-dimensionali di W_s, il quale ha dimensione

limitata da k; se ne deduce che $U_s = W_s = U_{s+1}$).

Infine da quest'ultima affermazione riusciamo a ricavare la razionalità di f:
infatti, la $(k+1)$-tupla $z = (z_k, ..., z_0) \in \Omega^{k+1}$
agisce su Ω^{k+1} tramite il prodotto scalare $(x_0, ..., x_k) \longrightarrow \sum_{j=0}^{k} x_j z_{k-j}$;
quindi visto che U_s ha dimensione k per tutti gli $s \geq s_0$, riusciamo a trovare un vettore ortogonale ad esso in Ω^{k+1}, ovvero un elemento z tale che $z.U_s = 0$,
che implica $z.v_s^{(k)} = z_k A_s + ... + z_0 A_{s+k} = 0$, $\forall s \geq s_0$,
che mostra che $f(t)(z_0 + z_1 t + ... + z_k t^k)$ è un polinomio. ■

XIII.5 **Razionalità della funzione zeta**.

Riassiumiamo quanto abbiamo già visto:

1) Se $\zeta(t) = \sum_j A_j t^j$,
allora $|A_j|_\infty \leq q^{\alpha j}$, per un opportuno α.
2) $A_j \in \mathbb{Z}$, $\forall j$.
3) $\zeta(t) = \frac{h(t)}{g(t)}$, ove $h(t)$ e $g(t)$ sono funzioni p-adiche intere e $g(0) \neq 0$.

Per dimostrare la razionalità di $\zeta(t)$ per XIII.4.1
è sufficiente dimostrare che $\exists s_0$ e $\exists k$ tale che $\Lambda_{s,k} = 0$, $\forall s \geq s_0$
allora basta provare che $|\Lambda_{s,k}|_\infty |\Lambda_{s,k}|_p < 1$
che, poichè $\Lambda_{s,k} \in \mathbb{Z}$ e poichè $\forall n \in \mathbb{Z} \setminus \{0\}$ $|n|_p \geq \frac{1}{|n|_\infty}$, implicherebbe $\Lambda_{s,k} = 0$.

Osserviamo che $|\Lambda_{s,k}|_\infty \leq (k+1)! q^{\alpha(s+2k)(k+1)}$
(infatti

$$\Lambda_{s,k} = det \begin{bmatrix} A_s & A_{s+1} & ... & A_{s+k} \\ A_{s+1} & A_{s+2} & ... & A_{s+k+1} \\ \vdots & \vdots & & \vdots \\ A_{s+k} & A_{s+k+1} & ... & A_{s+2k} \end{bmatrix}$$

$$=: det \begin{bmatrix} B_{0,0} & B_{0,1} & ... & B_{0,k} \\ B_{1,0} & B_{1,1} & ... & B_{1,k} \\ \vdots & \vdots & & \vdots \\ B_{k,0} & B_{k,1} & ... & B_{k,k} \end{bmatrix} = (\text{ per definizione }) \sum_{\sigma \in S_{k+1}} \varepsilon_\sigma \prod_{i=0}^{k} B_{i,\sigma(i)}$$

si ottiene che $|\Lambda_{s,k}|_\infty \leq \sum_{\sigma \in S_{k+1}} \prod_{i=0}^{k} |B_{i,\sigma(i)}|_\infty$,
ma da 1) si ha che $|B_{i,\sigma(i)}|_\infty \leq q^{\alpha(s+2k)}$

e quindi si ottiene che $|\Lambda_{s,k}|_\infty \leq \sum_{\sigma \in S_{k+1}} \prod_{i=0}^{k} |B_{i,\sigma(i)}|_\infty \leq (k+1)! q^{\alpha(s+2k)(k+1)}$,
come preannunciato);

dunque resta da stimare $|\Lambda_{s,k}|_p$.
Sia $R > 1$ numero reale, e sia $t_0 \in \mathbb{C}_p$ tale che $|t_0| = s \leq \frac{1}{R}$ (questo è possibile grazie a quanto detto nella dimostrazione del teorema IX.5.6).
Sia $g'(t) = g(\frac{t}{t_0})$, allora $g'(t)$ è anche essa una funzione $p-$adica intera.
Sia $M = M_1(g')$, allora ponendo $g''(t) = \frac{g'(t)}{M}$ abbiamo ottenuto ancora una funzione $p-$adica intera ma che stavolta appartiene all'anello $\mathcal{O}[[t]]$;
per il teorema IX.6.2 g'' ha un numero finito di zeri in $\mathcal{O}$ e usando più volte la proposizione IX.6.1 lavorando su tali zeri si ottiene una fattorizzazione del tipo
$g''(t) = P(t)k(t)$, con $P(t)$ polinomio che ha come zeri tutti gli zeri di g'' contenuti in $\mathcal{O}$ e $k(t)$ una funzione $p-$adica intera con zeri ω tali che $|\omega| > 1$;
operando la sostituzione $s = \frac{t}{t_0}$ e moltiplicando entrambi i membri per M si ottiene $g(s) = f(s)g_R(s)$, con $f(t) = 1 + b_1 t + ... + b_l t^l$, polinomio e g_R funzione $p-$adica intera con tutti i suoi zeri ω che verificano la condizione $|\omega| > \frac{1}{s} > R$.

Esercizio 13. Se $h(t) = \sum_{j \geq 0} A_j t^j \in \mathbb{C}_p[[t]]$, converge per $|t| \leq R$,
allora esiste una costante $M > 0$, tale che $|A_j| \leq \frac{M}{R^j}$, per tutti gli j.

Allora $\zeta(t)f(t) = \frac{h(t)}{g_R(t)} = \sum_j C_j t^j$ è limitata nel disco $|t|_p \leq R$
(infatti per IX.6.7 $\frac{1}{g_R(t)}$ è limitata in tale disco),
allora abbiamo $|C_j|_p \leq \frac{M}{R^j}$,
per un opportuna costante M dipendente solo da R;
sia $k > l$, allora abbiamo $C_{s+l} = A_s b_l + ... + A_{s+l} b_0$
cosi che $\Lambda_{s,k} = det \begin{bmatrix} A_s & A_{s+1} \ ... & A_{s+l-1} & C_{s+l} \ ... & C_{s+k} \\ A_{s+1} & A_{s+2} \ ... & A_{s+l} & C_{s+l+1} \ ... & C_{s+k+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{s+k} & A_{s+k+1} \ ... & A_{s+k+l-1} & C_{s+k+l} \ ... & C_{s+2k} \end{bmatrix}$
ora sfruttando il fatto che $A_j \in \mathbb{Z}$ e quindi che $|A_j|_p \leq 1$ e la disuguaglianza sui C_j scritta sopra, si ottiene facilmente:

$|\Lambda_{s,k}|_p \leq M^{k-l+1} \frac{1}{R^{(k-l+1)s+(k-l+1)\frac{l+k}{2}}}$,
cosi che $|\Lambda_{s,k}|_\infty |\Lambda_{s,k}|_p \leq M^{k-l+1} \frac{1}{R^{(k-l+1)s} R^{(k-l+1)\frac{l+k}{2}}} (k+1)! q^{\alpha(k+1)s} q^{2\alpha k(k+1)} = \frac{\xi_{k,l}}{\left(\frac{R^{k-l+1}}{q^{\alpha(k+1)}}\right)^s}$;
fissiamo ora R in modo che $\frac{R}{q^\alpha} > 1$;
fissato R determiniamo anche l;
scegliamo poi k in modo che

$\theta = \left(\frac{R}{q^\alpha}\right)^{k+1} R^{1-l} > 1$;
infine possiamo trovare un s_0 tale che $\frac{\xi_{k,l}}{\theta^s} < 1, \forall s \geq s_0$. ■

XIII.6 **Razionalità per varietà algebriche qualsiasi**.

Teorema 6.1.
Se V è una varietà su un campo finito $\mathbb{F}_q$,
la funzione $\zeta(V,t)$ è razionale.

Dim: enunciamo in primis il seguente

Lemma 6.2.
Se V è una varietà su $\mathbb{F}_q$ e W è una sottovarietà chiusa in V e $U = V \setminus W$,
allora $\zeta(V,t) = \zeta(W,t)\zeta(U,t)$.

Dim: $\forall m \geq 1,\ |V(\mathbb{F}_{q^m})| = |W(\mathbb{F}_{q^m})| + |U(\mathbb{F}_{q^m})|$;
siccome $exp(u+v) = exp(u)exp(v)$, la tesi segue immediatamente. ■

Mostriamo ora che se la funzione zeta è razionale su una varietà della forma:
$V = \{x = (x_1, ..., x_n) \in \mathbb{F}_{q^\infty}^n \mid f(x) = 0, x_1 \cdots x_n \neq 0\}$, che chiameremo di prima specie, allora è razionale su una ipersuperficie in $\mathbb{A}^n_{\mathbb{F}_q}$ definita da un polinomio non nullo $f \in \mathbb{F}_q[x_1, ..., x_n]$, che chiameremo varietà di seconda specie.

Infatti sia V varietà di seconda specie e denotiamo con $H_i = \{x : x_i = 0\}$,$1 \leq i \leq n$;
per ogni $I \subset \{1, ..., n\}$ poniamo:
$V_I = V \cap \left(\bigcap_{i \in I} H_i\right)$ e $V_I^0 = V_I \setminus \bigcup_{i \notin I} H_i$;
riflettendo un secondo su quanto appena scritto si trova che in V_I^0 un elemento x ha in corrispondenza degli indici $i \in I$, $x_i = 0$, e in corrispondenza degli indici $i \notin I$, $x_i \neq 0$; quindi possiamo concludere che:
V_I^0 è isomorfo ad un'ipersuperficie in $\mathbb{A}^{n-\sharp I}_{\mathbb{F}_q}$, di prima specie,
per la quale sappiamo che la sua funzione zeta è razionale,
e che vale la fattorizzazione $V = \amalg_I V_I^0$
che porta a $\zeta(V,t) = \prod_I \zeta(V_I^0, t)$,
che ci dice che anche $\zeta(V,t)$ è razionale.

A questo punto siamo pronti per concludere il nostro teorema:

Sia $V = \{x = (x_1, ..., x_n) \mid f_1(x) = ... = f_m(x) = 0\}$
con $f_i(x) \in \mathbb{F}_q[x_1, ..., x_n],\ \forall 1 \leq i \leq m$;

allora $V = \bigcap_{i=1}^{m} V_i$, con V_i un' ipersuperficie
(ad esempio prendo $V_i = \{x \mid f_i(x) = 0\}$);

ora per ogni $B \subset \{1, ..., m\}$ definiamo $W_B = \bigcup_{i \in B} V_i$
e tramite tutti questi vogliamo riscrivere V;
facciamo un esempio: nel caso $m = 3$ posso riscrivere V come

$V = W_{\{1,2,3\}} \setminus (W_{\{1,2\}} \setminus W_{\{1\}} \cup W_{\{2,3\}} \setminus W_{\{2\}} \cup W_{\{1,3\}} \setminus W_{\{3\}})$;
da qui grazie al lemma ricaviamo che

$\zeta(V,t) = \frac{\zeta(W_{\{1,2,3\}},t)\zeta(W_{\{1\}},t)\zeta(W_{\{2\}},t)\zeta(W_{\{3\}},t)}{\zeta(W_{\{1,2\}},t)\zeta(W_{\{1,3\}},t)\zeta(W_{\{2,3\}},t)}$;

generalizzando questo ragionamento combinatorico al caso m qualsiasi, si ottiene:
$\zeta(V,t) = \prod_{B \subset \{1,...,m\}} \zeta(W_B,t)^{-(-1)^{\sharp B}}$.

Siccome W_B è ancora una ipersuperficie, questo mostra come il passo precedente (cioè la razionalità per ipersuperfici) ci porti a dimostrare la razionalità della funzione zeta su una varietà affine qualsiasi.

Infine se vale per ogni varietà affine, allora vale anche per quelle proiettive, visto che per esse abbiamo una partizione della forma I.1.14 . ■

Bibliografia: Il materiale di questo capitolo proviene da [5] e da [8].
Vedere anche [12].

SOLUZIONI ESERCIZI.

Esercizio 1: Se $|x| < r_g$, prendiamo $f = g$ in IX.3.4 e otteniamo
$g^2(x) = g(x)^2$ e per induzione $g^n(x) = g(x)^n$ per ogni $n \in \mathbb{N}$;
da qui prendendo combinazioni lineari di queste equazioni, si ottiene:
$(f \circ g)(x) = f(g(x))$ per $|x| < r_g$, per ogni polinomio f.

Esercizio 2: Siccome $|k| = 1$ per tutti gli interi k coprimi con p,
allora per avere la convergenza della prima serie
deve succedere che $|\frac{x^k}{k}| \to 0$, $(k \to \infty)$, che implica $|x| < 1$.
Viceversa, quando $|x| < 1$, $|\frac{x^k}{k}| \leq k|x|^k \to 0$, $(k \longrightarrow \infty)$.
Per quanto riguarda la seconda serie: $|\frac{x^k}{k!}| = |x|^k|p|^{-ord_p(k!)} = |p|^{kord_p(x)-ord_p(k!)}$
e ora usando X.1.1, si ha che l'esponente è uguale a $k(ord_p(x) - \frac{1}{p-1}) + \frac{S_p(k)}{p-1}$.
Siccome $S_p(k) = 1$ quando $k = p^j$, con $j \geq 0$,
abbiamo che $|\frac{x^k}{k!}| \to 0 \Leftrightarrow k(ord_p(x) - \frac{1}{p-1}) \to \infty$,
e questo succede precisamente quando $ord_p(x) > \frac{1}{p-1} \Leftrightarrow |x| < |p|^{\frac{1}{p-1}}$.

Esercizio 3: Per $k \geq 1$ abbiamo $S_p(k) \geq 1$ e quindi $ord_p(k!) \leq \frac{(k-1)}{p-1}$;
di conseguenza $|k| \geq |k!| \geq r_p^{k-1}$;
$|\frac{x^k}{k}| \leq |\frac{x^k}{k!}| \leq \left(\frac{|x|}{r_p}\right)^{k-1} \cdot |x| < |x| < 1$,
per $k \geq 2$ e $0 < |x| < r_p$;
di conseguenza il valore assoluto di tutti i termini delle serie che definiscono l'esponenziale
e il logaritmo $p-$adico è strettamente più piccolo del valore assoluto del primo termine: ricordiamo che $exp(x) = 1 + \sum_{k \geq 1} \frac{x^k}{k!}$ e che il termine con il valore assoluto più grande vince, quindi $|exp(x)| = 1$;
mentre $|exp(x) - 1| = |x|$;
e similmente si lavora con il logaritmo $|log(1 + x)| = |x|$, per $|x| < r_p$.

Esercizio 4: 1) Se $n > 1$ e $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e d è un divisore di n con $\mu(d) \neq 0$,
allora d è il prodotto dei primi in un sottoinsieme dei p_i;

$\sum_{d|n} \mu(d) = 1 + \sum_i \mu(p_i) + \sum_{i,j} \mu(p_i p_j) + ...$
$= 1 - k + \binom{k}{2} - .... + (-1)^k = (1-1)^k = 0.$
Se $n = 1$, $\sum_{d|1} \mu(d) = \mu(1) = 1.$
Quindi in totale $\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor$.

2) Similmente $\sum_{d|n} |\mu(d)| = (1+1)^k = 2^k = 2^{v(n)}$.

Esercizio 5: 1) $\sum_{n\geq 1} \frac{\mu(n)}{n} log(1-x^n) = \sum_{n\geq 1} \mu(n) \sum_{m\geq 1} \frac{x^{nm}}{nm}$

$= \sum_{N\geq 1} \frac{x^N}{N} \sum_{n|N} \mu(n) = x$ (usando l'esercizio 4);

2) $\sum_{n\geq 1, p\nmid n} \frac{\mu(n)}{n} log(1-x^n) = \sum_{n\geq 1, p\nmid n} \mu(n) \sum_{m\geq 1} \frac{x^{nm}}{nm}$

$= \sum_{N\geq 1} \frac{x^N}{N} \sum_{n|N, p\nmid n} \mu(n)$;

la condizione $n|N$ e n coprimo con p implica che $n|Np^{-\nu}$, ove $\nu = ord_p(N)$;
la corrispondente somma si annulla, sempre usando l'esercizio 4, eccetto se $N = p^\nu$,
e in tal caso $\sum_{n\geq 1, p\nmid n} \frac{\mu(n)}{n} log(1-x^n) = \sum_{N=p^\nu} \frac{x^N}{N}$.

Esercizio 6: $N_n = \frac{1}{(n-1)!} \frac{d^n}{dT^n} log(\zeta(V,T)) \mid_{T=0}$.

Esercizio 7: Sia $V = \mathbb{P}^N$ allora $\sharp V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^{N} q^{ni}$;

allora: $log\zeta(V,T) = \sum_{n=1}^{\infty} \sum_{i=0}^{N} \frac{q^{ni}T^n}{n} = \sum_{i=0}^{N} -log(1-q^iT)$;

di conseguenza $\zeta(V,T) = \prod_{i=0}^{N} \frac{1}{(1-q^iT)}$.

Esercizio 8: La stima più banale che si può dare sugli N_s è:
$N_s \leq q^{sn} = \sharp \mathbb{F}_{q^s}^n$; allora otteniamo:
$\zeta(V,t) \leq exp\left(\sum_{s=1}^{\infty} \frac{(q^nt)^s}{s}\right) = exp(log\frac{1}{1-q^nt}) = \frac{1}{1-q^nt} = \sum_{k=0}^{\infty} q^{nk}t^k$;
da qui si ottiene $a_k \leq q^{kn}$.

Esercizio 9: In questo caso la stima più banale
(visto che una curva ellittica è descritta da equazioni di Weierstrass) è $N_s \leq 2p^{ls}+1$;
la stima non banale ci è fornita dal Teorema di Hasse: $|\sharp\mathbb{E}(\mathbb{F}_{p^{ls}}) - p^{ls} - 1| \leq 2\sqrt{p^{ls}}$,
quindi abbiamo: $p^{ls} + 1 - 2\sqrt{p^{ls}} \leq \sharp\mathbb{E}(\mathbb{F}_{p^{ls}}) \leq p^{ls} + 1 + 2\sqrt{p^{ls}}$
che facendo i conti ci porta a:
$\frac{1}{1-p^lt} \frac{1}{1-t} (1 - p^{\frac{l}{2}}t)^2 \leq \zeta(\mathbb{E}, t) \leq \frac{1}{1-p^lt} \frac{1}{1-t} \frac{1}{(1-p^{\frac{l}{2}}t)^2}$.

Esercizio 10: L'esercizio segue usando la forma canonica di Jordan:
se supponiamo che f abbia una matrice associata A in forma di Jordan con blocchi

$A_1, ..., A_l$ di dimensioni $n_1, ..., n_l$ e autovalori $\lambda_1, ..., \lambda_l$, allora:
$Tr(f^s) = \sum_{k=1}^{l} n_k \lambda_k^s$, mentre $det(I - tf) = \prod_{k=1}^{l} (1 - t\lambda_k)^{n_k}$;
a questo punto inserendo queste informazione nell'equazione si ottiene un' identità.

Esercizio 11: Supponiamo che $H = \sum_{\alpha} h_\alpha x^\alpha$;

allora: $H \circ \psi_q \left(\sum_{\beta} b_\beta x^\beta \right) = H \left(\sum_{\beta} b_{q\beta} x^\beta \right) = \sum_{\gamma} \left(\sum_{\alpha+\beta=\gamma} h_\alpha b_{q\beta} \right) x^\gamma$;

d'altra parte si ha che: $\psi_q \circ H_q \left(\sum_{\beta} b_\beta x^\beta \right) = \psi_q \left(\sum_{\gamma} \left(\sum_{q\alpha+\beta=\gamma} h_\alpha b_\beta \right) x^\gamma \right) = \sum_{\gamma} \left(\sum_{q\alpha+\beta=q\gamma} h_\alpha b_\beta \right) x^\gamma$;
ma in quest'ultima espressione si ha che β deve essere divisibile per q,
da cui riscrivendo quest'ultima serie si ottiene la serie scritta in precedenza:
le due espressioni coincidono.

Esercizio 12: Supponiamo che $\phi(v_2), ..., \phi(v_n)$ sono linearmente indipendenti,
allora $\phi(v_2), ..., \phi(v_{n-1})$ sono indipendenti e quindi dall'ipotesi si ottiene che
$\phi(v_1)$ sta nello span di $\phi(v_2), ..., \phi(v_{n-1})$;
allora se $\sum_{k=1}^{n} a_k v_k = 0$ è una relazione di dipendenza non banale,
troviamo che $\sum_{k=1}^{n-1} a_k \phi(v_k) = -a_n \phi(v_n)$;

allora per quanto detto sopra dobbiamo avere $a_n = 0$ e dunque $\sum_{k=1}^{n-1} a_k v_k = 0$;

a questo punto applichiamo ψ e ricordiamoci della relazione $\psi(v_i) = \phi(v_{i+1})$
per trovare $\sum_{k=2}^{n} a_k \phi(v_k) = 0$, che è una contraddizione.

Esercizio 13: La serie $h(t)$ converge per $|t| \leq R$ se soltanto se $\lim_{j\to\infty} |A_j| R^j = 0$;
allora $M := \max_{0\leq j<\infty} |A_j| R^j$ esiste,
e pertanto $|A_j| \leq \frac{M}{R^j}$, per tutti gli j.

BIBLIOGRAFIA:

1)Joseph H. Silverman.*The Arithmetic of Elliptic Curves.*Springer Dordrecht Heidelberg London New York. GraduateTexts in Mathematics.Second Edition.

2) R.Hartshorne.*Algebraic geometry.* Springer-Verlag,NewYork,1977. GraduateTexts in Mathematics, No. 52.

3)Alain M. Robert.*A Course in p-adic Analysis.*Springer-Verlag New York,2000.Graduate Texts in Mathematics.

4)Lawrence C. Washington.*Introduction to Cyclotomic Fields.*Second Edition.Springer.Graduate Texts in Mathematics.

5)Bernard Dwork, Giovanni Gerotto, and Francis J. Sullivan.*An Introduction to G-Functions* .Princeton university press, Princeton, New Jersey,1994.

6)P. Stevenhagen. *Voortgezette Getaltheorie.*Thomas Stieltjes Instituut,2002.

7)S.Bosch.*Algebra.*Springer.

8)Mircea Mustatà.*Zeta functions in algebraic geometry.*

9)Dikran Dikranjan.*Introduction to Topological Groups.*

10)Pierre Deligne.*Formes modulaires et représentations $l-$adiques.*Séminaire N.Bourbaki, 1968/1969, p-139-172.

11)J.P.Serre.*A course in arithmetic.*Springer-Verlag New York, Graduate Texts in Mathematics.

12)Neal Koblitz.*p-adic Numbers, p -adic Analysis, and Zeta -Functions* .Second Edition.