

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

Integrazione p -adica
e
Teorema di Igusa

Tesi di Laurea in Matematica

Relatore:
Chiar.mo Prof.
Luca Migliorini

Presentata da:
Nicolas Vercheval

II Sessione
Anno Accademico 2012/2013

Introduzione

Come è noto il campo dei numeri reali si ottiene come completamento metrico del campo \mathbb{Q} dei numeri razionali rispetto alla distanza definita dal valore assoluto. Per ogni primo p esiste una valutazione, la *valutazione p -adica*, che dà luogo a metriche diverse sui numeri razionali, che misurano la divisibilità di un numero razionale per il primo dato. Un numero razionale è piccolo in senso p -adico se è divisibile per una grande potenza del primo p . Il Teorema di Ostrovski afferma che ogni valore assoluto non banale sui numeri razionali è equivalente al valore assoluto standard o a un valore assoluto p -adico. Inoltre le distanze p -adiche godono di una proprietà particolare, detta ultrametricità: la disuguaglianza triangolare vale in una forma assai più forte. Completando il campo razionale rispetto alla distanza indotta da un valore assoluto p -adico si ottiene un campo, il campo dei numeri p -adici, metricamente completo, che risulta localmente compatto e totalmente sconnesso. Tale campo contiene un anello, l'anello degli interi p -adici, compatto. Risulta da teoremi generali l'esistenza, unica a meno di normalizzazione moltiplicativa, di una misura invariante per traslazione, la misura di Haar. Questo permette di sviluppare una teoria dell'integrazione per funzioni definite su sottoinsiemi di spazi vettoriali sui numeri p -adici, che ha molte applicazioni importanti in teoria dei numeri e teoria delle rappresentazioni. Nozioni simili legate all'ultrametricità appaiono anche in fisica matematica. Infine la teoria dell'integrazione p -adica è stata una notevole fonte di ispirazione per la teoria dell'integrazione motivica, uno degli sviluppi recenti più importanti della geometria algebrica, le cui idee fondamentali sono dovute a M. Kontsevich. In

questa tesi si studiano le idee fondamentali alla base della teoria, per concludere con una dimostrazione, che si appoggia sul teorema della risoluzione delle singolarità di H. Hironaka, del teorema di razionalità di Igusa, che mostra peraltro lo stretto legame tra integrazione p -adica e proprietà aritmetiche. I primi capitoli di carattere introduttivo discutono la costruzione degli interi p -adici e le loro proprietà topologiche, e la costruzione della misura di Haar nel caso particolare dei p -adici. Si discutono alcuni esempi di integrazione p -adica. Il terzo capitolo descrive il processo di scoppimento (blow-up) di un punto o in generale di una sottovarietà, e il teorema di risoluzione delle singolarità, discutendo la sua utilità nel ricondurre l'integrazione di una funzione e all'integrazione di una funzione monomiale. Infine l'ultimo capitolo sfrutta in modo sistematico questa idea per dare una dimostrazione del teorema di Igusa.

Indice

Introduzione	i
1 I numeri p-adici	1
1.1 Definizione e prime proprietà	1
1.2 Introduzione grafica	4
2 Integrazione p-adica	11
2.1 Misura di Haar	11
2.2 Integrazione ed esempi	16
2.3 Integrazione in varietà p -adiche	19
3 Risoluzione delle singolarità	23
3.1 Il Blow up	23
3.2 Risoluzione delle singolarità	26
4 Teorema di Igusa	29
4.1 La funzione zeta	29
4.2 Teorema di Igusa	31
Bibliografia	33

Capitolo 1

I numeri p -adici

In questo testo p denoterà un primo e dato $n \in \mathbb{N}$, $A_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$.

1.1 Definizione e prime proprietà

Al fine di definire i numeri p -adici, introduciamo innanzitutto gli interi p -adici, tramite la nozione di *limite inverso*, seguendo [1].

Sia $\phi_n : A_{p^n} \rightarrow A_{p^{n-1}}$ la funzione che proietta le classi di equivalenza nelle classi in cui sono contenute. L'insieme delle coppie (A_{p^n}, ϕ_n) forma un sistema inverso, indicizzato dagli interi positivi.

Definizione 1.1. L'anello degli interi p -adici \mathbb{Z}_p è il limite inverso del sistema (A_{p^n}, ϕ_n) appena definito.

L'addizione e la moltiplicazione sono definite coordinata per coordinata, rendendo così \mathbb{Z}_p un sottoanello di $\prod_{n \geq 1} A_{p^n}$.

Diamo a A_{p^n} la topologia discreta, e a \mathbb{Z}_p la topologia prodotto.

Sia $\varepsilon_n : \mathbb{Z} \rightarrow A_{p^n}$ la funzione che associa ad un intero p -adico la sua n -esima componente.

Osservazione 1. L'elemento neutro è composto dal prodotto degli elementi neutri di A_{p^n} . Identifichiamo \mathbb{Z} con la propria immagine tramite l'omomorfismo (iniettivo) diagonale $\mathbb{Z} \rightarrow \prod A_{p^n}$.

Proposizione 1.1.1. *La successione di gruppi abeliani $0 \rightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_{p^n} \rightarrow 0$ è esatta.*

In particolare $A_{p^n} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$.

Dimostrazione. La moltiplicazione per p (e quindi per p^n) è iniettiva in \mathbb{Z}_p ; infatti se $x = (\varepsilon_n(x)) = (x_n)$ è un intero p -adico tale che $px = 0$ abbiamo che $px_{n+1} = 0$ per ogni n e x_{n+1} è della forma $p^n y_{n+1}$ con $y_{n+1} \in A_{p^{n+1}}$; poiché $x_n = \phi_{n+1}(x_{n+1})$ allora anche x_n è divisibile per p^n e quindi è zero.

È chiaro che il nucleo di ε_n contiene $p^n\mathbb{Z}_p$; inoltre, se $x = (x_n)$ appartiene al nucleo, si ha che $x_m \equiv 0 \pmod{[p^n]}$ per ogni $m \geq n$. Ciò implica che esiste un elemento $y_{m-n} \in A_{p^{m-n}}$ tale che la sua identificazione tramite l'isomorfismo $A_{p^{m-n}} \rightarrow p^n\mathbb{Z}_p/p^m\mathbb{Z}_p \subset A_{p^m}$ soddisfi $x_m = p^n y_{m-n}$. Consideriamo $y = (y_i)$ e verifichiamo immediatamente che $x = p^n y$, provando la proposizione. \square

Proposizione 1.1.2.

a) *Un elemento di \mathbb{Z}_p è invertibile sse non è divisibile per p .*

b) *Sia \mathbb{U} il gruppo delle unità di \mathbb{Z}_p : ogni elemento non nullo di \mathbb{Z}_p può essere scritto in maniera unica come $p^n u$ dove $u \in \mathbb{U}$ e $n \geq 0$.*

Dimostrazione. Proviamo a): Sia $x = (x_n) \in \mathbb{Z}_p$, esso non è divisibile per p se e solo se la proiezione x_1 in A_p è non nulla, quindi invertibile. Per ogni m esistono allora (non univocamente definite) $y_m, z_m \in A_{p^m}$, dove y_m ha come proiezione l'inversa di x_1 , tali che $x_m y_m = 1 - pz_m = 1 - p^m z_m^m$. In particolare:

$$x_m y_m (1 + pz_m + \dots + p^{m-1} z_m^{m-1}) = 1$$

il che prova l'invertibilità di x_m ; inoltre poiché la proiezione dell'inversa coincide con l'inversa della classe precedente, possiamo costruire classe per classe anche quella di x .

D'altra parte, dato $x = (x_n) \in \mathbb{Z}_p$ non nullo, sia m il più grande intero per cui $x_m = 0$; possiamo pertanto scrivere $x = p^m u$ dove u ha proiezione non nulla in A_p ed è quindi invertibile per a). La scomposizione è chiaramente unica. \square

Definizione 1.2. Sia $x \in \mathbb{Z}_p$ non nullo. Sia n tale che $x = p^n u$ con $u \in \mathbb{U}$; La funzione $v_p : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ definita da $v_p(x) := n$ è allora detta valutazione p -adica di x .

Se poniamo $v_p(0) = \infty$ abbiamo che

$$v_p(xy) = v_p(x) + v_p(y), \quad v_p(x + y) \geq \inf(v_p(x), v_p(y)).$$

Con questa valutazione \mathbb{Z}_p diventa un *anello euclideo*.

Proposizione 1.1.3. *La topologia di \mathbb{Z}_p può essere definita dalla distanza non archimedea (anche detta ultramettrica)*

$$d(x, y) = p^{-v_p(x-y)}, \quad d(x, y) \leq \max\{d(x, z), d(z, y)\} \quad \forall z \in \mathbb{Z}_p.$$

L'anello \mathbb{Z}_p è uno spazio metrico completo, dove \mathbb{Z} è denso.

Intanto osserviamo che le traslazioni $x \rightarrow x + a$ sono omeomorfismi di \mathbb{Z}_p e sono isometrie per la distanza non archimedea, quindi basta considerare gli intorno dell'origine. Gli ideali $p^n \mathbb{Z}_p$ formano un sistema fondamentale di intorno di 0; poiché $x \in p^n \mathbb{Z}_p$ esattamente quando $v_p(x) \geq n$, questi intorno non sono altro che le palle centrate nell'origine di raggio p^{-n} , la topologia su \mathbb{Z}_p è definita dalla distanza $d(x, y) = p^{-v_p(x-y)}$.

Le proprietà topologiche degli interi p -adici verranno discusse nella prossima sezione. Intanto definiamo i numeri p -adici.

Definizione 1.3. Il campo dei numeri p -adici, scritto come \mathbb{Q}_p è il campo delle frazioni di \mathbb{Z}_p .

Si vede facilmente che ogni elemento (non nullo) può essere scritto unicamente come $p^n u$ dove $n \in \mathbb{Z}$ e $u \in \mathbb{U}$. Si può così estendere la valutazione p -adica, la quale diventa maggiore di zero solo per gli elementi di \mathbb{Z}_p .

Proposizione 1.1.4. *Attribuendo a \mathbb{Q}_p la norma non archimedea*

$$|x| = p^{-v_p(x)},$$

otteniamo un campo completo, localmente compatto, che contiene \mathbb{Z}_p come sottoanello aperto e chiuso, e \mathbb{Q} come sottoinsieme denso. In particolare \mathbb{Q}_p è il completamento di \mathbb{Q} rispetto alla distanza p -adica.

1.2 Introduzione grafica

Nel capitolo precedente abbiamo visto come i numeri p -adici siano il completamento dei numeri razionali rispetto ad un'opportuna norma. Si potrebbe dire di più: data un'arbitraria norma non banale, su \mathbb{Q} , il suo completamento è o un campo p -adico oppure quello reale [2, pag. 46].

L'intenzione ora, è quella di trovare un modello grafico che abbia le stesse proprietà topologiche dei numeri p -adici.

Per rappresentarlo graficamente, definiamo innanzitutto le ellissi a p foglie.

Definizione 1.4. Presi p punti $\{a_1, \dots, a_p\}$ equidistanziati sulla retta reale nel piano definiamo una p -ellisse passante per quei punti come l'unione di $p-1$ semicirconferenze di uguale raggio, di estremi $\{a_i, a_{i+1}\} \forall i < p$ e giacenti nello stesso semipiano, con una semiellisse, giacente nel semipiano opposto, di estremi $\{a_1, a_p\}$.

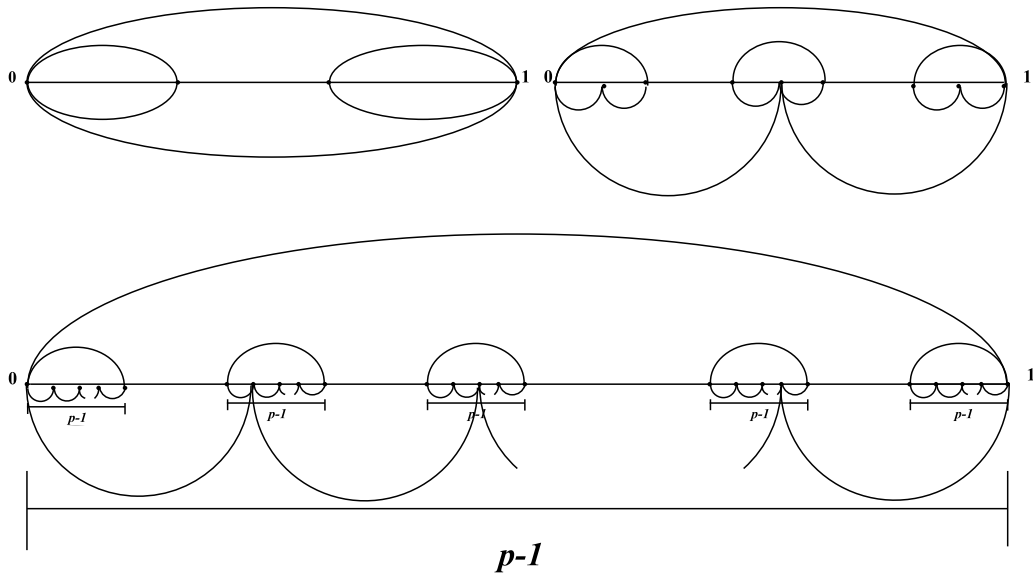
Considerando ora una p -ellisse dove $a_1 = 0$ e $a_p = 1$, vogliamo disegnare p altre ellissi simili, $2p-1$ volte più piccole, passanti per i punti $\{b_1^j, \dots, b_p^j\}$ in modo tale che $a_j = b_j^j \quad \forall j < p$.

Chiamiamo la prima p -ellisse, ellisse di livello zero e le p -ellissi interne, p -ellissi di primo livello. Iterando per ogni p -ellisse interna n volte otterremo p -ellissi di ennesimo livello.

Osservazione 2. La distanza tra due p -ellissi vicine di pari livello è costante. Infatti, se consideriamo una p -ellisse passante per $\{a_1, \dots, a_p\}$, contenente p p -ellissi passanti per $\{b_1^j, \dots, b_p^j\}$ abbiamo che

$$|b_1^{j+1} - b_p^j| = |b_{j+1}^{j+1} - b_j^j| - \sum_{0 < i < j+1} |b_{i+1}^{j+1} - b_i^{j+1}| - \sum_{j < k < p} |b_{k+1}^j - b_k^j|;$$

poiché $|b_{j+1}^{j+1} - b_j^j| = |a_{j+1} - a_j|$ e la distanza $|b_{i+1}^j - b_i^j| = c \quad \forall j, i < p$ è costante, $|b_1^{j+1} - b_p^j|$ non dipende da j .



Definizione 1.5. Fissato un primo p , chiamiamo insieme di Cantor generalizzato il sottoinsieme di \mathbb{R} definito da

$$\mathbf{Cantor}_p := \bigcap_{n \in \mathbb{N}} p(\mathbf{E}_p^n),$$

dove $p(\mathbf{E}_p^n)$ sono le proiezioni sulla ascissa delle p -ellissi di livello n .

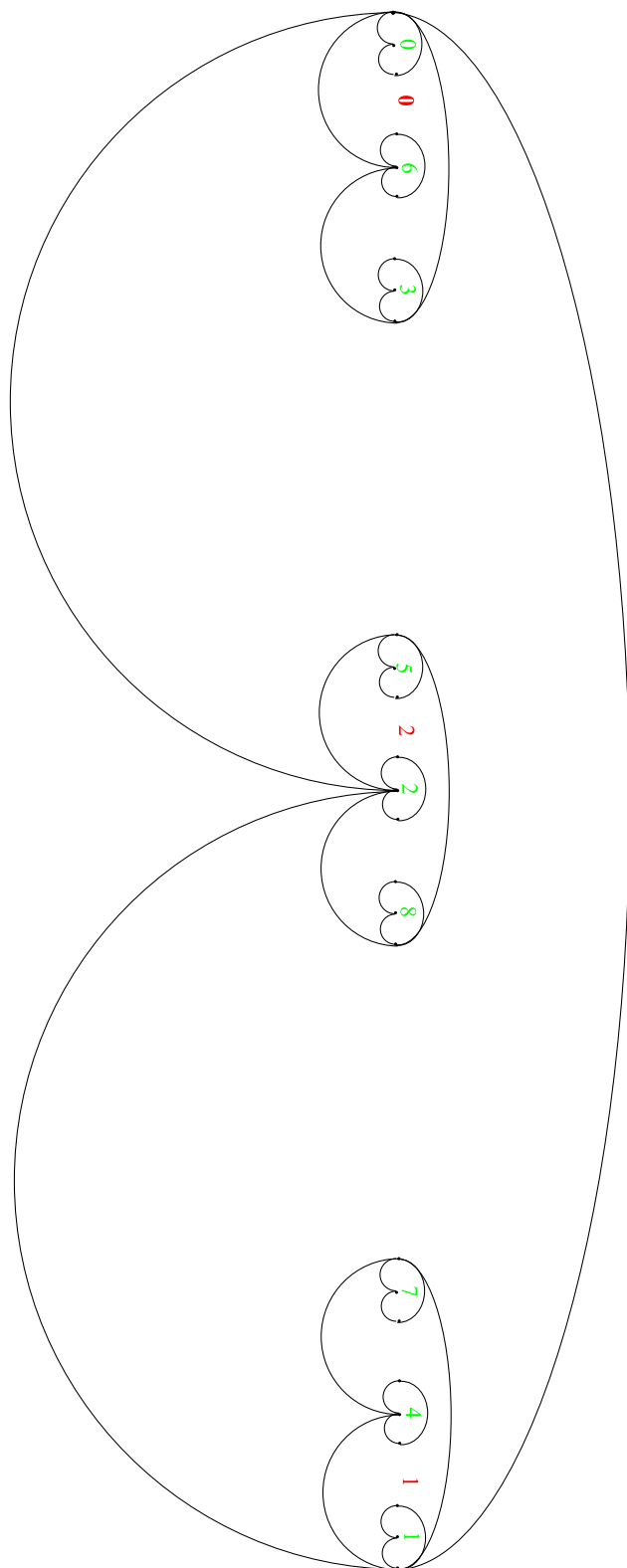
La metrica è quella indotta da \mathbb{R}^2 .

Osservazione 3. 0 e 1 appartengono all'insieme di Cantor generalizzato, inoltre se $p = 2$ quest'ultimo coincide con l'insieme di Cantor.

Osservazione 4. Dato $\xi \in \mathbf{Cantor}_p$ e dato $n \in \mathbb{N}$, esiste un'unica ellisse di ennesimo livello che lo contiene. In particolare, variando n , esse formano una famiglia di intorno del punto. Poiché esse contengono sottoinsiemi non connessi, \mathbf{Cantor}_p è localmente (oltre che globalmente) sconnesso. Più precisamente è totalmente sconnesso, ovvero le sue componenti connesse sono i punti.

Osservazione 5. \mathbf{Cantor}_p è compatto in quanto chiuso (è intersezione di chiusi) e limitato.

Ora vogliamo dare un ordine alle p -ellissi dello stesso livello. Per senso antiorario intendo contare le p -ellissi attribuendo 0 ad una p -ellisse data

Figura 1.1: Esempio con $p = 3$ e $n = 1, 2$

e spostandosi verso l'origine, ripartendo dalla p -ellisse più lontana quando esse sono finite. Le p -ellissi di primo livello le ordiniamo in senso antiorario partendo da quella che contiene l'origine. Le p -ellissi di n -esimo livello, contenute nella stessa p -ellissi di livello $n - 1$, le ordiniamo in senso antiorario partendo dall'unica p -ellissi che ha intersezione con la p -ellisse di livello $n - 2$. Ora le ordiniamo globalmente contando le p -ellissi dello stesso ordine relativo secondo l'ordine delle p -ellissi di livello $n - 1$ nelle quali sono contenute. Costruiamo per ogni n $\psi_n: \mathbf{Cantor}_p \rightarrow A_{p^n}$ in maniera tale che ogni punto contenuto in una delle p^n p -ellissi di livello n abbia come immagine la classe di equivalenza che contiene il numero corrispondente. La funzione è chiaramente suriettiva.

Proposizione 1.2.1. *La funzione ψ definita nel modo seguente*

$$\begin{aligned} \psi: \mathbf{Cantor}_p &\longrightarrow \mathbb{Z}_p \\ \xi &\longrightarrow (\dots, \psi_n(\xi), \dots, \psi_1(\xi)) \end{aligned}$$

è un omeomorfismo.

Dimostrazione. Innanzitutto è biunivoca: ad ogni infinita intersezione delle proiezioni delle p -ellissi corrisponde l'elemento formato dalle classi dell'ordine di quest'ultime. Una base di aperti di \mathbb{Z}_p è formata dagli insiemi di elementi in cui i primi n componenti sono fissati e gli altri sono variabili. Una famiglia di intorni aperti di $\psi(\xi)$ è data da questa base e corrisponde ai sottoinsiemi di \mathbf{Cantor}_p i cui elementi sono contenuti dentro la p -ellisse di livello n che contengono anche ξ . Sono pertanto una famiglia di intorni di ξ . \square

Osservazione 6. In tal modo possiamo attribuire a \mathbb{Z}_p le proprietà di compattezza, locale e globale sconnessione che possiede \mathbf{Cantor}_p .

Osservazione 7. Dal grafico si nota come, identificando \mathbb{N} come sottoinsieme di \mathbb{Z}_p , $\psi^{-1}(\mathbb{N})$ sia l'insieme corrispondente alle intersezioni finite delle p -ellissi ed è denso.

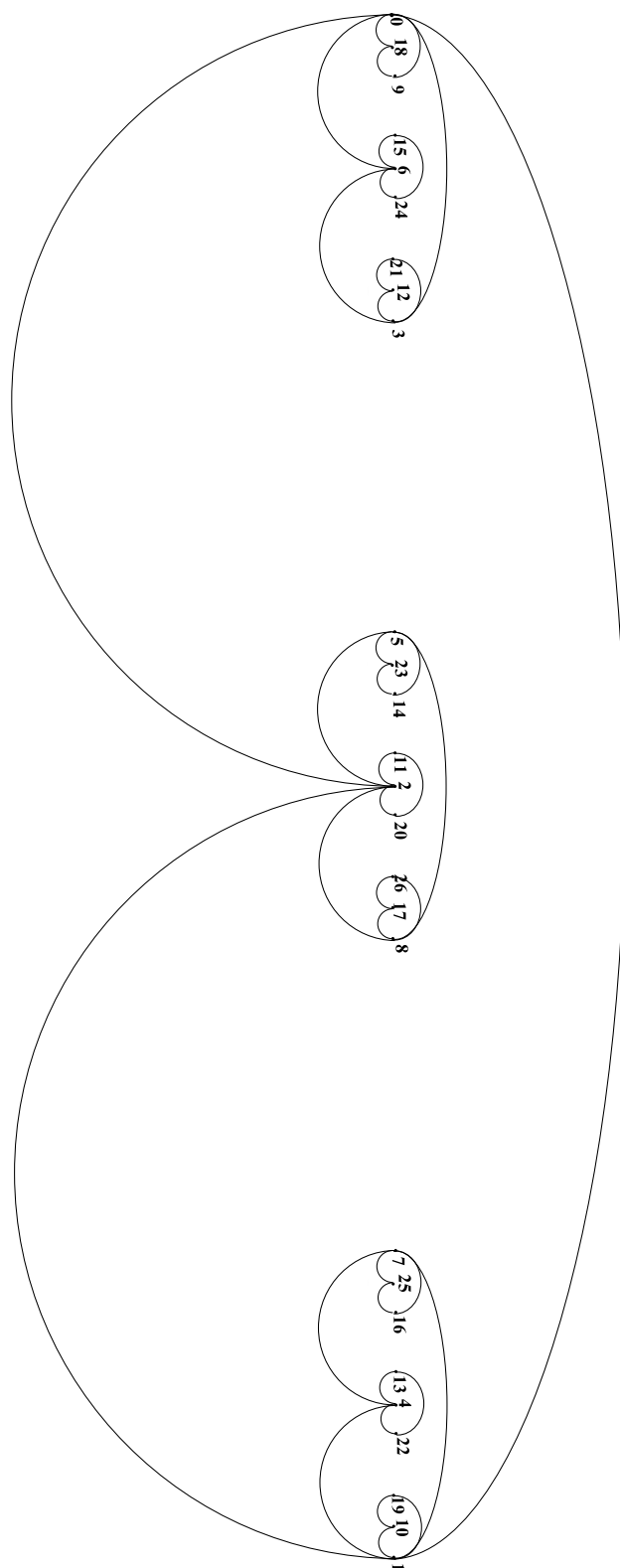


Figura 1.2: Identificazione dei numeri minori di 27 con $p = 3$

Per rappresentare \mathbb{Q}_p basta considerare altre infinite p -ellissi a cui attribuiremo un livello negativo in maniera speculare, che contengono la p -ellisse di primo livello, in maniera tale da rispettare la natura frattale.

Proposizione 1.2.2. *La distanza indotta dalla norma su \mathbb{Q}_p induce una distanza in \mathbf{Cantor}_p esprimibile così: la distanza tra due elementi ξ e χ appartenenti a \mathbf{Cantor}_p è uguale a p^{-m} dove $m \in \mathbb{Z}$ è il livello della più piccola p -ellisse che contiene entrambi.*

Questa rappresentazione è utile per illustrare le proprietà della distanza non euclidea.

Sia a un numero p -adico, i dischi di raggio p^{-m} di a (per la natura della distanza basta considerare le potenze di p), sono gli elementi contenuti nella stessa p -ellisse di livello m che contiene a . Quindi ogni elemento del disco è centro di esso. Se due circonferenze si intersecano, allora qualunque punto che giace nell'intersezione è il centro dei due dischi, i quali dovranno essere o contenuti l'un l'altro oppure coincidenti. Questo è bene evidente dal grafico. La nonarchimediteà può essere osservata dal fatto che la somma di due elementi a e b di norma rispettivamente p^{-n} e p^{-m} , con $m \geq n$, è contenuta nella p -ellisse centrata in a di livello m , la quale è contenuta nella più piccola p -ellisse che contiene lo zero e a . In particolare se $m > n$ la p -ellisse di livello m centrata in b non ha punti in comune con le p -ellissi di livello k , $m \geq k > n$ centrate in a e quindi anche nello 0, (se ne avesse b , che è distante m , sarebbe anch'esso ivi contenuto). Perciò, in tal caso, la norma della somma è uguale al massimo della norma degli addendi.

Tale proprietà si riassume con la suggestiva frase: tutti i triangoli sono isosceli.

Osservazione 8. Poiché ogni disco è omeomorfo a \mathbb{Z}_p , notiamo che \mathbb{Q}_p è completo, totalmente sconnesso e localmente compatto.

Capitolo 2

Integrazione p -adica

2.1 Misura di Haar

Introduciamo ora una misura positiva definita sui sottoinsiemi boreliani di \mathbb{Q}_p , invariante per traslazione. Essa si chiama misura di Haar, e la sua esistenza ed unicità è provata per ogni gruppo topologico localmente compatto e T1, ovvero dove gli insiemi contenenti i singoli punti sono chiusi [3]. Noi la costruiremo esplicitamente sul campo dei numeri p -adici.

Definizione 2.1. Chiamiamo ricoprimento essenziale di un sottoinsieme compatto $K \in \mathbb{Q}_p$ un ricoprimento aperto finito di K , nel quale ogni aperto figura una sola volta, ed ha intersezione non nulla con K :

$$\mathfrak{U} = \{U_i\}_{i=1}^N, U_i \neq U_j \text{ per } i \neq j, U_i \cap K \neq \emptyset \text{ per ogni } i.$$

Proposizione 2.1.1. *Dato un sottoinsieme compatto $K \subset \mathbb{Q}_p$ e un intero n , esiste un unico ricoprimento essenziale con dischi di raggio p^{-n} . Definiamo $\alpha(K)_n$ il numero di dischi del ricoprimento essenziale.*

Dimostrazione. Poiché due dischi con lo stesso raggio sono coincidenti o disgiunti, ogni punto è contenuto in un unico disco con raggio fissato. \square

Proposizione 2.1.2. *La successione $p^{-n}\alpha(K)_n$ ha limite.*

Dimostrazione. Basta far vedere che è positiva e decrescente. Chiaramente è positiva. Poiché ogni disco di raggio p^{-n} è unione disgiunta di p dischi di raggio $p^{-(n+1)}$, essi formeranno un ricoprimento di K . Pertanto:

$$p^{-n}\alpha(K)_n = p^{-(n+1)}p\alpha(K)_n \geq p^{-(n+1)}\alpha(K)_{n+1}.$$

□

Definizione 2.2. Poniamo

1. $\mu^*(K) := \lim_{n \rightarrow \infty} p^{-n}\alpha(K)_n$ per $K \subseteq \mathbb{Q}_p$ compatto.
2. $\mu^*(A) := \sup\{\mu^*(K) \mid K \subseteq A, K \text{ compatto}\}$ per $A \subseteq \mathbb{Q}_p$ aperto.
3. $\mu^*(U) := \inf\{\mu^*(A) \mid A \supseteq U, A \text{ aperto}\}$ per $U \subseteq \mathbb{Q}_p$ qualsiasi.

Proposizione 2.1.3. *La definizione è ben posta.*

Dimostrazione. Siano K, K' compatti di \mathbb{Q}_p con $K \subseteq K'$. Poiché ogni ricoprimento essenziale di K' ricopre anche K , $p^{-n}\alpha(K')_n \geq p^{-n}\alpha(K)_n$ e $\mu^*(K') \geq \mu^*(K)$. In particolare dato un compatto aperto non vi è ambiguità. Gli altri casi sono analoghi. □

Osservazione 9. Dato $U \subseteq \mathbb{Q}_p$, $\mu^*(U)$ è non negativa, e non sempre nulla. Ad esempio $\mu^*(D)$ dove D è un qualunque disco, è uguale al raggio.

Lemma 2.1.4. *Dato X , spazio topologico T_2 , sia $K \subseteq X$ compatto e $U_1, U_2 \subseteq X$ aperti tale che $K \subseteq U_1 \cup U_2$. Allora esistono $K_1, K_2 \subseteq X$ compatti tale che $K_1 \subseteq U_1$, $K_2 \subseteq U_2$ e $K = K_1 \cup K_2$.*

Dimostrazione. Definiamo $L_1 = K \setminus U_1$ e $L_2 = K \setminus U_2$. K è chiuso perché X è Hausdorff quindi ogni L_i è chiuso. Poiché ogni L_i è un sottospazio chiuso di K , segue che ogni L_i è compatto. Inoltre, poiché $K \subseteq U_1 \cup U_2$, $L_1 \cap L_2 = \emptyset$. Poiché sono compatti e disgiunti possiamo separare L_1 e L_2 con due aperti disgiunti rispettivamente V_1 e V_2 .

Definiamo $K_1 = K \setminus V_1$ e $K_2 = K \setminus V_2$. Per la stessa ragione di prima K_1 e K_2 sono compatti.

$$K_1 = K \setminus V_1 \subseteq K \setminus L_1 = K \setminus (K \setminus U_1) = K \cap (K \cap U_1^c)^c = K \cap (K^c \cup U_1) \subseteq U_1$$

. Allo stesso modo $K_2 \subseteq U_2$. Inoltre $K_1 \cup K_2 = K - (V_1 \cap V_2) = K$. \square

Ricordiamo che una misura esterna su X è una funzione reale φ^* positiva definita nell'insieme delle parti 2^X di X , tale che, dati due sottoinsiemi $A, B \in X$, ed una famiglia di sottoinsiemi $A_i \in X \quad \forall i \in \mathbb{N}$:

a) $\varphi^*(\emptyset) = 0$

b) $A \subset B \longrightarrow \varphi^*(A) \leq \varphi^*(B)$

c) $\varphi^*\left(\bigcup_{i \in \mathbb{N}} A_i\right) \leq \sum_{i \in \mathbb{N}} \varphi^*(A_i)$.

Osservazione 10. L'ultima proprietà è meno restrittiva di quanto richiesto ad una misura. Tieniamo presente però che la misura esterna è definita per ogni sottoinsieme di X .

Proposizione 2.1.5. *La funzione $\mu^* : 2^{\mathbb{Q}_p} \longrightarrow \mathbb{R}^+ \cup \{0\} \cup \{\infty\}$ è una misura esterna.*

Dimostrazione. Chiaramente $\mu^*(\emptyset) = 0$.

La monotonia viene direttamente dalla monotonia sui compatti.

Dimostriamo la subaddittività numerabile dapprima sugli aperti.

Innanzitutto dati K, K' compatti $\mu^*(K \cup K') \leq \mu^*(K) + \mu^*(K')$, infatti l'unione dei ricoprimenti essenziale dei due insiemi è ricoprimento dell'unione dei due insiemi.

Sia $\{A_n \mid n \in \mathbb{N}\}$ una collezione numerabile di aperti. Consideriamo un insieme compatto $K \subseteq \bigcup_{n \in \mathbb{N}} A_n \Rightarrow K \subseteq \bigcup_{k=1}^n A_n$.

Usiamo induttivamente il lemma 2.1.4 per trovare K_1, \dots, K_n compatti tali che $K = \bigcup_{k=1}^n K_n$ e $K_k \subseteq A_k$ per $1 \leq k \leq n$. Per quanto abbiamo detto prima:

$$\mu^*(K) \leq \sum_{k=1}^n \mu^*(K_k) \leq \sum_{k=1}^n \mu^*(A_k) \leq \sum_{n \in \mathbb{N}} \mu^*(A_n).$$

Quindi:

$$\mu^*\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \sup\{\mu^*(K) \mid K \subseteq \bigcup_{n \in \mathbb{N}} A_n\} \leq \sum_{n \in \mathbb{N}} \mu^*(A_n).$$

Sia $\{U_n \mid n \in \mathbb{N}\}$ famiglia di insiemi numerabile. Supponiamo $\sum_{n \in \mathbb{N}} \mu^*(U_n) < \infty$.

Sia $\epsilon > 0$ e chiamiamo $A_n \supseteq U_n$ un aperto tale che $\mu^*(A_n) \leq \mu^*(U_n) + \frac{\epsilon}{2^n}$.

Allora:

$$\mu^*\left(\bigcup_{n \in \mathbb{N}} U_n\right) \leq \mu^*\left(\bigcup_{n \in \mathbb{N}} A_n\right) \leq \sum_{n \in \mathbb{N}} \mu^*(A_n) \leq \sum_{n \in \mathbb{N}} \mu^*(U_n) + \frac{\epsilon}{2}.$$

Data l'arbitrarietà di ϵ

$$\mu^*\left(\bigcup_{n \in \mathbb{N}} U_n\right) \leq \sum_{n \in \mathbb{N}} \mu^*(U_n).$$

□

Vogliamo ora dimostrare che μ^* ristretta ai sottoinsiemi boreliani è effettivamente una misura.

Viene spontaneo quindi usare il teorema di Carathèodory [4, pag.182].

Definizione 2.3. Data φ^* misura esterna su X , diciamo che un insieme $A \in X$ è Carathèodory misurabile mediante φ^* se:

$$\varphi^*(E) = \varphi^*(E \cap A) + \varphi^*(E \cap A^c) \quad \forall E \subseteq X$$

dove A^c è il complementare di A .

Teorema 2.1.6 (Teorema di Carathèodory). *Sia φ^* una misura esterna su X spazio topologico, allora gli insiemi Carathèodory misurabili formano una σ -algebra ristretta alla quale φ^* diventa una misura φ completa.* □

Proposizione 2.1.7. *Gli aperti di \mathbb{Q}_p sono Carathèodory misurabili mediante μ^* .*

Dimostrazione. Mostriamo innanzitutto che dati $K_1, K_2 \subseteq \mathbb{Q}_p$, disgiunti allora $\mu^*(K_1 \cup K_2) = \mu^*(K_1) + \mu^*(K_2)$. Infatti dati due ricoprimenti essenziali

di K_1 e K_2 con dischi di raggio abbastanza piccolo (in modo che non abbiano dischi in comune) essi formano un ricoprimento essenziale di $K_1 \cup K_2$; e quindi $\alpha(K_1)_n + \alpha(K_2)_n = \alpha(K_1 \cup K_2)$.

Sia ora $A \subseteq \mathbb{Q}_p$ aperto tale che $\mu^*(A) < \infty$ e sia $U \in \mathbb{Q}_p$. Prendiamo ora V tale che $U \subseteq V \subseteq \mathbb{Q}_p$ e tale che $\mu^*(V) \leq \mu^*(U) + \epsilon$. Sia ora $K_1 \subseteq V \cap A$, compatto tale che $\mu^*(V \cap A) - \epsilon \leq \mu^*(K_1)$ e sia $K_2 \subseteq V \cap A^C$ tale che $\mu^*(V \cap A^C) - \epsilon \leq \mu^*(K_2)$. Poiché $K_1 \subseteq A$, $V \cap A^C \subseteq V \cap K_1^C$ quindi:

$$\mu^*(V \cap A^C) - \epsilon \leq \mu^*(V \cap K_1^C) \leq \mu^*(K_2).$$

Per quanto abbiamo detto prima:

$$\begin{aligned} \mu^*(U \cap A) + \mu^*(U \cap A^C) - 2\epsilon &\leq \mu^*(V \cap A) + \mu^*(V \cap A^C) - 2\epsilon \leq \mu^*(K_1) + \mu^*(K_2) \\ &= \mu^*(K_1 \cup K_2) \leq \mu^*((V \cap A) \cup (V \cap K_1^C)) \\ &\leq \mu^*(V) \leq \mu^*(U) + \epsilon. \end{aligned}$$

Ne segue che:

$$\mu^*(U \cap A) + \mu^*(U \cap A^C) \leq \mu^*(U) + 3\epsilon$$

e quindi:

$$\mu^*(U \cap A) + \mu^*(U \cap A^C) \leq \mu^*(U).$$

□

Definizione 2.4. Una misura φ definita sui boreliani di uno spazio topologico X si dice internamente regolare se, per qualunque $E \subset X$ misurabile:

$$\varphi(E) = \sup \{ \varphi(K) : K \subseteq E, K \text{ compatto} \}.$$

Definizione 2.5. Una misura φ definita sui boreliani di uno spazio topologico X si dice esternamente regolare se, per qualunque $E \subset X$ misurabile:

$$\varphi(E) = \inf \{ \varphi(A) : X \subseteq A \subset X, A \text{ aperto} \}.$$

Definizione 2.6. Una misura definita sui boreliani di uno spazio topologico X si dice regolare se è internamente ed esternamente regolare e i compatti hanno misura finita.

Teorema 2.1.8. *Definendo μ , la misura di Haar come la restrizione di μ^* ai sottoinsiemi boreliani, si ha una misura regolare e completa, invariante per traslazioni.*

Dimostrazione. Il teorema di Carathéodory ci dice che gli insiemi Carathéodory misurabili mediante μ^* formano una sigma algebra nella quale la restrizione di μ^* è una misura completa. Poiché vi appartengono gli aperti, vi appartengono anche i boreliani.

È chiaramente regolare per costruzione, e basta dimostrare che è invariante per traslazione sui compatti. Questo segue direttamente dal fatto che una traslazione di vettore a porta un ricoprimento essenziale del compatto K in un ricoprimento essenziale del compatto traslato $a + K$. \square

2.2 Integrazione ed esempi

Utilizzando la teoria dell'integrazione, sono definite le funzioni a valori reali misurabili che possiamo integrare.

Le funzioni che ci interessano sono norme di polinomi a n variabili, della forma $|\sum_{\{j_1, \dots, j_n\} \in \mathbb{N}^n} a_{j_1 \dots j_n} X_1^{j_1} \dots X_n^{j_n}|$ dove $a_{j_1 \dots j_n} \in \mathbb{Q}_p$ è non nullo solo per un numero finito di indici. Queste funzioni hanno immagine numerabile perché la norma di un numero p -adico prende valori nell'insieme numerabile $\{p^n\}_{n \in \mathbb{Z}}$.

Per tali funzioni possiamo tradurre l'integrale in una serie. Infatti sia $A \in \mathbb{Z}_p$ misurabile e sia $f : A \rightarrow \mathbb{R}$ come sopra; se $A_f(c) := \{x \in A | f(x) = c\}$ allora per la numerabilità dell'immagine

$$\int_A f(x) d\mu = \sum_{c \in \text{Im}(f)} \int_{A_f(c)} f(x) d\mu = \sum_{c \in \text{Im}(f)} \int_{A_f(c)} c \cdot d\mu = \sum_{c \in \text{Im}(f)} c \cdot \mu(A_f(c)).$$

Esempio 2.1. Sia $s \geq 0$ un numero reale, e sia $d \geq 0$ intero. Allora

$$\int_{\mathbb{Z}_p} |x^d|^s d\mu = \frac{p-1}{p-p^{-ds}}.$$

Dimostrazione. Sappiamo che $|x^d|^s = \frac{1}{p^{nds}}$ se

$$x \in p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p.$$

Dato che $\mathbb{Z}_p = \bigcup_{n \in \mathbb{N}} (p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p)$ abbiamo che

$$\int_{\mathbb{Z}_p} |x^d|^s = \sum_{n=0}^{\infty} \frac{1}{p^{nds}} (p^{-n} - p^{-n-1}) = \left(1 - \frac{1}{p}\right) \frac{1}{1 - p^{-ds-1}} = \frac{p-1}{p - p^{-ds}}.$$

□

Possiamo naturalmente estendere la misura e l'integrale agli spazi vettoriali r -dimensionali su \mathbb{Q}_p , come \mathbb{Q}_p^r . Generalizziamo l'utile formula precedente.

Esempio 2.2. Sia $s \geq 0$ un numero reale, e sia $d_1, \dots, d_r \geq 0$ interi. Allora

$$\int_{\mathbb{Z}_p^r} |x_1^{d_1}, \dots, x_r^{d_r}|^s d\mu = \prod_{i=1}^r \frac{p-1}{p - p^{-d_i s}}.$$

Dimostrazione. Possiamo usare Fubini e ricondurci all'esempio precedente. □

Esempio 2.3. Una semplice formula che ci tornerà utile è

$$\int_{|x| \leq \frac{1}{p^m}} |x|^c |dx| = \frac{p^{-m(c+1)}}{1 - p^{-m(c+1)}} \cdot \frac{p-1}{p}.$$

Purtroppo quando non si tratta di monomi i conti ed i risultati sono più complessi. Propongo un esempio meno banale.

Esempio 2.4. Sia $r \geq 0$ un numero reale, allora

$$\int_{\mathbb{Z}_p^2} |xy(x+y)|^r d\mu = \frac{p-1}{p(1 - p^{-(3r+2)})} \left(\frac{3(p-1)}{p(1 - p^{r+1})} + \frac{p-2}{p} \right).$$

Dimostrazione. Spezzando l'integrale otteniamo per simmetria

$$\int_{\mathbb{Z}_p^2} |xy(x+y)|^r d\mu = 2 \int_{|x| > |y|} |xy(x+y)|^r d\mu + \int_{|x|=|y|} |xy(x+y)|^r d\mu.$$

Ora applicando Fubini e per la nonarchimedèità otteniamo:

$$\sum_{i=0}^{\infty} \left(2 \sum_{j=i+1}^{\infty} \int_{p^i \mathbb{Z} \setminus p^{i+1} \mathbb{Z}} |x|^{2r} \int_{p^j \mathbb{Z} \setminus p^{j+1} \mathbb{Z}} |y|^r dy dx \right) + \int_{p^i \mathbb{Z} \setminus p^{i+1} \mathbb{Z}} |x|^{2r} \int_{p^i \mathbb{Z} \setminus p^{i+1} \mathbb{Z}} |(x+y)|^r |dy| |dx| \quad (2.1)$$

Sappiamo anche che se $|x| = |y|$ allora $|y+x| \leq |x|$ e che se $|y+x| < |x|$ allora $|x| = |y|$. Spezziamo l'integrale

$$\int_{p^i \mathbb{Z} \setminus p^{i+1} \mathbb{Z}} |x+y|^r |dy| |dx| = \sum_{j=i+1}^{\infty} \int_{|x+y| \in p^j \mathbb{Z} \setminus p^{j+1} \mathbb{Z}} |x+y|^r |dy| |dx| + \int_{|y|=|x|=|x+y|} |x|^r |dy| |dx|$$

Il primo integrale è su dei dischi bucati attorno a $-x$. L'ultimo integrale è su un disco dove vengono tolti altri due dischi di dimensione appena inferiore (se $p = 2$ questo insieme è vuoto). Utilizziamo l'invarianza per traslazione

$$\int_{p^i \mathbb{Z} \setminus p^{i+1} \mathbb{Z}} |x+y|^r |dy| |dx| = \sum_{j=i+1}^{\infty} \int_{p^j \mathbb{Z} \setminus p^{j+1} \mathbb{Z}} |x+y|^r |dy| |dx| + \int_{|y|=|x|=|x+y|} |x|^r |dy| |dx|.$$

Sostituiamo in (2.1):

$$\sum_{i=0}^{\infty} \left(3 \sum_{j=i+1}^{\infty} \int_{p^i \mathbb{Z} \setminus p^{i+1} \mathbb{Z}} |x|^{2r} \int_{p^j \mathbb{Z} \setminus p^{j+1} \mathbb{Z}} |y|^r |dy| |dx| \right) + \int_{|x|=|y|=|x+y|=p^{-i}} |x|^{3r} |dy| |dx|.$$

Estraiamo le costanti e calcoliamo la misura degli insiemi.

$$\begin{aligned} & 3 \sum_{i=0}^{\infty} \sum_{j=i+1}^{\infty} p^{-2ri} (p^{-i} - p^{-i-1}) p^{-jr} (p^{-j} - p^{-j-1}) + \sum_{i=0}^{\infty} p^{-3ir} (p^{-i} - 2p^{-i-1}) (p^{-i} - p^{-i-1}) = \\ & = 3 \left(\frac{p-1}{p} \right)^2 \cdot \sum_{i=0}^{\infty} \sum_{j=i+1}^{\infty} p^{-i(2r+1)} p^{-j(r+1)} + \left(1 - \frac{2}{p} \right) \cdot \left(1 - \frac{1}{p} \right) \cdot \sum_{i=0}^{\infty} p^{-i(3r+2)} = \\ & = 3 \left(\frac{p-1}{p} \right)^2 \cdot \sum_{k=0}^{\infty} \sum_{i-j=k}^{\infty} p^{-i(2r+1) + (k-i)(r+1)} + \frac{p-2}{p} \cdot \frac{p-1}{p(1-p^{-(3r+2)})} = \\ & = 3 \left(\frac{p-1}{p} \right)^2 \cdot \sum_{k=0}^{\infty} p^{k(r+1)} \sum_{i=0}^{\infty} p^{-i(3r+2)} + \frac{p-2}{p} \cdot \frac{p-1}{p(1-p^{-(3r+2)})} = \\ & = 3 \left(\frac{p-1}{p} \right)^2 \cdot \frac{1}{(1-p^{(r+1)})(1-p^{-(3r+2)})} + \frac{p-2}{p} \cdot \frac{p-1}{p(1-p^{-(3r+2)})} = \\ & = \frac{p-1}{p(1-p^{-(3r+2)})} \left(\frac{3(p-1)}{p(1-p^{r+1})} + \frac{p-2}{p} \right). \end{aligned}$$

□

2.3 Integrazione in varietà p -adiche

Le funzioni analitiche (su \mathbb{Q}_p) sono le corrispettive di quelle su \mathbb{R} e sono definite come le funzioni convergenti in serie di potenze intorno ad ogni punto. Le derivate sono a loro volta funzioni analitiche, e le regole di derivazione di esse sono analoghe a quelle reali.

Una mappa analitica f è data da $(f_1, \dots, f_m) : U \longrightarrow \mathbb{Q}_p^m$, dove le f_i sono funzioni analitiche.

Definizione 2.7. Sia X spazio topologico di Hausdorff e sia $n \geq 0$ un intero. Una carta di X è una coppia (U, φ_U) composta da un aperto di X e da un omeomorfismo $\varphi_U : U \rightarrow V \subset \mathbb{Q}_p^n$. Un atlante è una famiglia di carte $\{(U, \varphi_U)\}$ tale che per ogni U_1, U_2 con $U_1 \cap U_2 \neq \emptyset$ la composizione

$$\varphi_{U_1} \circ \varphi_{U_2}^{-1} : \varphi_{U_2}(U_1 \cap U_2) \longrightarrow \varphi_{U_1}(U_1 \cap U_2)$$

è bianaalitica. Due atlanti sono equivalenti se la loro unione è anch'essa un atlante. Infine, X con una classe di equivalenza degli atlanti (tramite la sopra citata relazione), è detta varietà p -adica di dimensione n .

Se (U, φ_U) è una carta e $p_o \in U$, allora $\varphi_U(x) = (x_1, \dots, x_n)$ è detto sistema di coordinate intorno a p_o . Le mappe analitiche tra varietà sono definite nella maniera naturale.

Lemma 2.3.1. *Una varietà p -adica è uno spazio topologico localmente compatto e totalmente sconnesso.*

Esempio 2.5. Consideriamo la retta proiettiva \mathbb{P}^1 su \mathbb{Q}_p , avente come coordinate omogenee $[x, y]$. Può essere ricoperto dai due aperti coordinati *disgiunti e compatti*

$$U := \{[x, y] \mid |\frac{x}{y}| \leq 1\} \quad \text{e} \quad V := \{(x : y) \mid |\frac{y}{x}| < 1\}.$$

Abbiamo le mappe bianaalitiche

$$U \longrightarrow \mathbb{Z}_p, \quad [x, y] \rightarrow \frac{x}{y} \quad \text{e} \quad V \longrightarrow p\mathbb{Z}_p \quad [x, y] \rightarrow \frac{y}{x}.$$

Definizione 2.8. Sia X una varietà p -adica, possiamo definire le forme differenziali analitiche nel solito modo. Dato un aperto U con coordinate (x_1, \dots, x_n) una forma di grado k può essere scritta come

$$\nu = \sum_{i_1 < \dots < i_k} f_{i_1, \dots, i_k} dx_{i_1} \wedge \dots \wedge dx_{i_k}$$

con $f_{i_1, \dots, i_k}(x_1, \dots, x_n)$ funzioni analitiche a valori in \mathbb{Q}_p .

Ora utilizziamo il linguaggio delle forme differenziali per esporre senza dimostrazione alcuni teoremi, riportati in [5].

Definizione 2.9. Sia ω una forma differenziale analitica in X e sia X localmente omeomorfo a $p^{i_1}\mathbb{Z}_p \times \dots \times p^{i_n}\mathbb{Z}_p$. Per ogni

$$A \simeq (x_1 + p^{k_1}\mathbb{Z}_p \times \dots \times p^{k_n}\mathbb{Z}_p) \subset X$$

definiamo la misura associata a ω

$$\mu_\omega(A) := \int_A |f(x)| d\mu.$$

Questa è una misura definita sui boreliani.

Teorema 2.3.2 (Prima formula di cambiamento delle variabili). *Sia $\varphi = (\varphi_1, \dots, \varphi_n) : \mathbb{Q}_p^n \rightarrow \mathbb{Q}_p^n$ una mappa analitica. Supponiamo che per $q \in \mathbb{Q}_p^n$ si abbia $\det \left(\frac{\partial \varphi_i}{\partial x_j}(q) \right) \neq 0$. Allora φ induce un omeomorfismo bianalitico*

$$\varphi : U \subset \mathbb{Q}_p^n \longrightarrow V \subset \mathbb{Q}_p^n,$$

dove U è un intorno di x e V è un intorno di $\varphi(x)$;
inoltre dato A sottoinsieme misurabile di U si ha che

$$\int_{\varphi(A)} d\mu = \int_A |\det(\text{Jac}(\varphi))| d\mu.$$

□

Corollario 2.3.3. *Sia X una varietà compatta, e sia ω una n -forma analitica su X . Allora esiste, globalmente definita, una misura μ_ω su X . In particolare, per ogni funzione continua $f : X \rightarrow \mathbb{R}$, l'integrale $\int_X f(x) \mu_\omega$ è ben definito.*

Dimostrazione. Ricopriamo una n -varietà compatta, con aperti bianaliticamente isomorfi a \mathbb{Z}_p^n ; dal ricoprimento si possono estrarre un numero finito di dischi n -dimensionali disgiunti (li possiamo prendere disgiunti perché localmente godono di proprietà topologiche analoghe a \mathbb{Z}_p^n).

Consideriamo un aperto di questo sottoricoprimento U , dove $\omega = f(x)dx_1 \wedge \dots \wedge dx_n := f(x)dx$. Per il precedente teorema, μ_ω non dipende dalla particolare scelta delle coordinate, e fornisce una misura globalmente definita. \square

Generalizziamo ora leggermente il teorema (2.3.2).

Teorema 2.3.4 (Seconda formula di cambio di variabili). *Sia $\varphi : Y \rightarrow X$ una mappa analitica di una varietà compatta. Assumiamo che φ sia bianalitica fuori da un sottospazio chiuso $Z \subset Y$ tale che $\varphi(Z) \subset X$ abbia misura nulla. Se ω è una n -forma analitica e f è una funzione analitica abbiamo che*

$$\int_X |f|^s d\mu_\omega = \int_Y |f \circ \varphi|^s |\det(\text{Jac}(\varphi))| d\mu_\omega.$$

\square

Capitolo 3

Risoluzione delle singolarità

3.1 Il Blow up

Definizione 3.1. Sia \mathbb{V} uno spazio affine e sia considerato lo spazio $\mathbb{V} \times \mathbb{P}^{n-1}(\mathbb{V})$, di coordinate $(x_1, \dots, x_n, [\xi_1, \dots, \xi_n])$. Definiamo il blow-up di \mathbb{V} in 0 come la coppia $(\text{bl}_0(\mathbb{V}), \pi)$ dove

$$\text{bl}_0(\mathbb{V}) := \{(x_1, \dots, x_n, [\xi_1, \dots, \xi_n]) \in \mathbb{V} \times \mathbb{P}^{n-1}(\mathbb{V}) \mid x_i \xi_j = x_j \xi_i \ \forall i, j \leq n\}$$

e $\pi: \text{bl}_0(\mathbb{V}) \rightarrow \mathbb{V}$ è la proiezione sulle coordinate dello spazio affine.

In generale $\text{bl}_{x_0}(\mathbb{V}) := \text{bl}_0(\mathbb{V} - \{x_0\})$ e π viene composta con una traslazione.

Osservazione 11. Fuori da $\pi^{-1}(0)$, π è un isomorfismo bianalitico, infatti in tal caso le coordinate sul proiettivizzato di \mathbb{V} , sono univocamente determinate. Lo vediamo nell'esempio seguente.

Esempio 3.1. Consideriamo il $\text{bl}_0(\mathbb{V})$ dove \mathbb{V} è uno spazio vettoriale di dimensione 2, con coordinate $x = (x_1, x_2, [\xi_1, \xi_2])$. Esso lo possiamo vedere come l'unione di $U := \{x \in \text{bl}_0(\mathbb{V}) \mid \xi_1 \neq 0\}$ e $V := \{x \in \text{bl}_0(\mathbb{K}) \mid \xi_2 \neq 0\}$. Dato $x \in U$ si ha che $x_2 = \xi_2/\xi_1 \cdot x_1 := y_1 \cdot x_1$, e U è esprimibile tramite le coordinate $(x_1, y_1) = (x_1, x_1 y_1, [1, y_1])$ e risulta essere una semplice copia di \mathbb{V} . Lo stesso ragionamento vale per V . Inoltre notiamo che tramite tali coordinate si ha che

$$\pi|_U: (x_1, y_1) \rightarrow (x_1, x_1 y_1),$$

$$\pi|_V: (x_2, y_2) \rightarrow (x_2 y_2, x_2).$$

Il blow up è uno strumento utilissimo per regolarizzare le proprietà locali di una funzione. Nel prossimo esempio vedremo un esempio sul campo complesso dove potremo analizzare il problema in maniera più geometrica.

Esempio 3.2. Sia $f = x^2 - y^3$, polinomio di $\mathbb{C}[X, Y]$ e consideriamo la *curva algebrica* $X = (f^{-1}(0))$. Essa ha una singolarità in 0 data dall'annullarsi di $\nabla f(0)$. Sia π la proiezione di $\text{bl}_0(\mathbb{C}^2)$ su \mathbb{C}^2 , chiamiamo trasformata stretta di X la $Y := \overline{\pi^{-1}(X \setminus \{0\})}$. X e Y sono *birazionali*, in quanto π^{-1} è un isomorfismo bianalitico fuori dallo 0 (ricordiamo che due curve sono birazionali se esistono funzioni razionali le cui composizioni coincidono con l'identità della prima e della seconda curva). Inoltre i punti in cui non π non è bianalitico sono finiti, e non danno problemi [6, pag. 10].

Prendiamo U e V come nell'esempio precedente.

In U $f \circ \pi = f(u_1, u_1 v_1) = u_1^2 \cdot (v_1^2 - u_1)$; la trasformata stretta di f in U è il luogo degli zeri di $v_1^2 - u_1$ ed è non singolare.

In V abbiamo $f(u_2 v_2, u_2) = u_2^2(1 - u_2 v_2^3)$, ed anche qui la trasformata stretta non ha punti singolari. Abbiamo così trovato una curva birazionale a X , senza punti singolari. Ma possiamo ottenere di più.

Eseguiamo quindi ad esempio il blow up di $U \simeq \mathbb{C}^2$ in 0 con proiezione π' .

Di nuovo esso lo possiamo vedere nell'unione di U' e V' definiti in maniera analoga a quelli precedenti. Prendendo la trasformata stretta Z di $Y \cap U$ otteniamo ancora una curva birazionale a X .

In V' abbiamo $f \circ \pi \circ \pi' = u_3^2 v(v_3 - u_3)$. Con un terzo blow up in 0 su V' con proiezione $\hat{\pi}$, definendo \hat{U}, \hat{V} nel solito modo, possiamo notare come sia in \hat{U} che in \hat{V} $f \circ \pi \circ \pi' \circ \hat{\pi}$, rispettivamente $u_3^3 v_3(v_3 - 1)$ e $u_4^2 v_4^2(1 - u_4)$ siano monomi moltiplicati per una funzione che non si annulla in 0.

Questo fatto si ripete non solo per le carte che non abbiamo considerato, ma come vedremo, per ogni polinomio. Il risultato che otteniamo in questo caso è quindi che X è birazionale ad una curva algebrica localmente definita da una funzione monomiale.

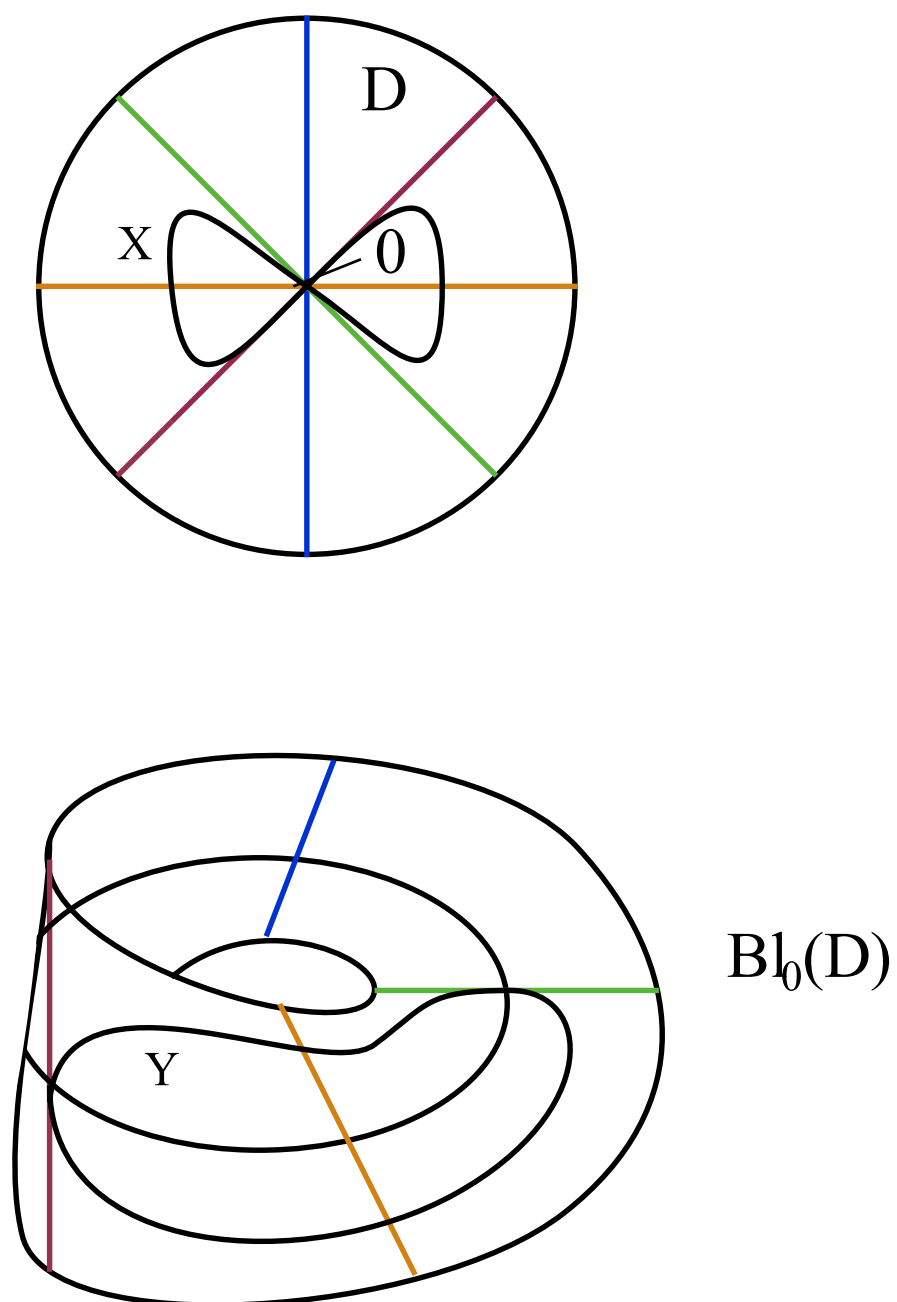


Figura 3.1: Esempio di risoluzione di singolarità tramite blowing up nello 0 , visto in un disco di centro l'origine.

Esempio 3.3. Consideriamo $\pi : \text{Bl}_0(\mathbb{Q}_p^2) \rightarrow \mathbb{Q}_p^2$, sia $X = \mathbb{Z}_p^2$ e sia $Y = \pi^{-1}(X)$. Ricopriamo $\text{Bl}_0(\mathbb{Q}_p^2)$ con due copie di \mathbb{Q}_p^2 come nell'esempio (3.1). Possiamo vedere Y come unione disgiunta di

$$A = \{(s, t) \mid |y| \leq 1, |x| \leq 1\} \quad \text{e} \quad B = \{(u, v) \mid |u| < 1, |v| \leq 1\},$$

infatti se $(s, st, [1, t])$ e $(vu, v, [v, 1])$ coincidono v e t hanno norma uguale ad uno, per la coordinata proiettiva.

$$\pi(U) = \{(x, y) \mid |y| \leq |x| \leq 1\} \quad \text{e} \quad \pi(V) = \{(x, y) \mid |x| < |y| \leq 1\}.$$

In A avremo quindi

$$\det \text{Jac}(\pi) = \det \begin{pmatrix} 1 & t \\ 0 & s \end{pmatrix} = s.$$

Mentre in B

$$\det \text{Jac}(\pi) = \det \begin{pmatrix} v & 0 \\ u & 1 \end{pmatrix} = v.$$

3.2 Risoluzione delle singolarità

Vediamo ora un esercizio di integrazione sul blow-up.

Esempio 3.4. Riprendiamo l'Esempio (2.4) e lo calcoliamo attraverso il blow-up.

Dimostrazione. Tenendo la notazione e le conclusioni dell'esempio (3.3) per il teorema del cambio di variabili otteniamo :

$$\int_{\mathbb{Z}_p^2} |xy(x+y)|^r d\mu = \int_{|s| \leq 1, |t| \leq 1} |s|^{3r+1} |t(1+t)|^r |ds \wedge dt| + \int_{|u| < 1, |v| \leq 1} |v|^{3r+1} |u(1+u)|^s |du \wedge dv| =$$

Utilizziamo il Teorema di Fubini:

$$= \int_{|s| \leq 1} |s|^{3r+1} |ds| \int_{|t| \leq 1} |t(1+t)|^r |dt| + \int_{|v| \leq 1} |v|^{3r+1} |dv| \int_{|u| < 1} |u(1+u)|^r |du| =$$

Ci ricordiamo della nonarchimedietà della norma, e dividiamo gli interi p -adici nell'unione di p dischi di raggio $1/p$.

$$\begin{aligned}
&= \frac{p-1}{p(1-p^{-(3r+2)})} \left(\sum_{1 < i < p} \int_{|t-i| < 1} d|t| + \int_{|t-1| < 1} |t-1|^r |dt| + \int_{|t| < 1} |t|^r |dt| + \int_{|u| < 1} |u|^r |dt| \right) = \\
&= \frac{p-1}{p(1-p^{-(3r+2)})} \left(\frac{p-2}{p} + \frac{p-1}{p} \cdot \frac{3p^{-r-1}}{1-p^{-r-1}} \right) = \\
&= \frac{p-1}{p(1-p^{-(3r+2)})} \left(\frac{3(p-1)}{p(1-p^{r+1})} + \frac{p-2}{p} \right)
\end{aligned}$$

□

Osservazione 12. Nell'esercizio precedente, abbiamo messo in evidenza come sia relativamente facile integrare una funzione monomiale moltiplicata per una funzione che non si annulla nell'origine. Non scordiamoci che questo è vero grazie al fondamentale uso della proprietà nonarchimedea della norma.

Il blow-up è uno strumento efficace per il calcolo degli integrali; la domanda che sorge spontanea è: attraverso di esso possiamo sempre ricondurci ad una somma di integrali facilmente computabili?

La risposta (affermativa, fortunatamente) ce la fornisce il Teorema di Hironaka sulle risoluzione delle singolarità. Esso vale per ogni campo a caratteristica 0 e dice che con un'opportuna composizione di blow up otteniamo una funzione localmente monomiale.

Definizione 3.2. Dati due spazi topologici X e Y ed una mappa $f: X \rightarrow Y$, f si dice propria se la controimmagine di un qualunque sottoinsieme compatto di Y è un compatto di X .

Teorema 3.2.1 (Risoluzione delle singolarità). *Sia $f \in \mathbb{Q}_p[X_1, \dots, X_n]$ un polinomio non costante. Esiste una varietà n -dimensionale analitica su \mathbb{Q}_p Y e una mappa propria $\pi: Y \rightarrow \mathbb{Q}_p^n$, isomorfa su $Y \setminus O$, con O sottoinsieme di misura nulla, tale che, tramite una scelta opportuna di coordinate $y_1 \dots y_n$,*

$$f \circ \pi = \lambda(y) \cdot y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$$

e

$$\text{Jac}(\pi) = \nu(y) \cdot y_1^{b_1} \cdot \dots \cdot y_n^{b_n},$$

dove $\lambda(0) \neq 0$ e $\nu(0) \neq 0$, e a_i, b_i sono interi non negativi chiamati discrepanze.

Osservazione 13. Le discrepanze possono anche essere nulle e in generale l'insieme delle discrepanze globali $(a_1, b_1), \dots, (a_k, b_k)$ con $k \in \mathbb{N}$ comprende tutte quelle locali. In particolare $k > n$.

Capitolo 4

Teorema di Igusa

In questo capitolo finale applicheremo i risultati dei capitoli precedenti, per dimostrare un risultato interessante di geometria algebrica.

4.1 La funzione zeta

Definizione 4.1. Sia f una funzione analitica $f: \mathbb{Q}_p^n \rightarrow \mathbb{Q}_p$ e sia $s \in \mathbb{R}$, la funzione zeta (locale) di f è

$$\int_{\mathbb{Z}_p^n} |f(x)|^s d\mu.$$

Teorema 4.1.1. Sia $f \in \mathbb{Z}[X_1, \dots, X_n]$. Allora la funzione zeta di f è una funzione razionale nella variabile p^{-s} . Inoltre, siano $(a_1, b_1), \dots, (a_k, b_k)$ le discrepanze associate alla risoluzione delle singolarità di f . Allora

$$Z(f, s) = \frac{P(p^{-s})}{(1 - p^{-a_1 s - b_1 - 1}) \cdots (1 - p^{-a_k s - b_k - 1})},$$

dove $P \in \mathbb{Z}[1/p][X]$. Notiamo che i poli della funzione sono $-\frac{b_1+1}{a_1}, \dots, -\frac{b_k+1}{a_k}$.

Dimostrazione. Sia $\pi: V \rightarrow \mathbb{Q}_p^n$ una risoluzione delle singolarità di f , e siano $X = \mathbb{Z}_p^n$ e $Y = \pi^{-1}(X)$ (d'ora in poi identificheremo π con la sua restrizione su Y). Y è un varietà p -adica compatta, coperta da carte disgiunte U_i sulle cui coordinate abbiamo

$$f \circ \pi = \lambda(y) \cdot y_1^{a_1} \cdots y_n^{a_n}$$

e

$$\text{Jac}(\pi) = \nu(y) \cdot y_1^{b_1} \cdot \dots \cdot y_n^{b_n}$$

dove $\lambda(y)$ e $\nu(y)$ non si annullano mai in U_i . Utilizzando la formula del cambiamento di variabile otteniamo:

$$Z(f, s) = \sum_i \int_{U_i} |\lambda(y)|^s |\nu(y)| |y_1|^{a_1 s + b_1} \cdot \dots \cdot |y_n|^{a_n s + b_n} |dy_1 \wedge \dots \wedge dy_n|.$$

Le funzioni $|\lambda(y)|$ e $|\nu(y)|$ sono localmente costanti, infatti per ogni elemento non nullo di \mathbb{Q} esiste un intorno in cui la norma è costante. Possiamo quindi assumere direttamente che siano costanti in U_i , per esempio sia $|\lambda| = p^{-d}$ e $\nu = p^{-c}$. Identificando U_i con l'immagine, riduciamo l'integrale su dei dischi polidimensionali dati da $|y_i| \leq p^{-k_i} \quad \forall i$ otteniamo $Z(f, s)$ dalla somma di termini della forma

$$\begin{aligned} & p^{-cs-d} \cdot \int_{P_i} |y|^{a_1 s + b_1} \cdot \dots \cdot |y_n|^{a_n s + b_n} |dy_1 \wedge \dots \wedge dy_n| = \\ & = p^{-cs-d} \cdot \int_{|y_1| \leq p^{k_1} |y|^{a_1 s + b_1}} |dy_1| \cdot \dots \cdot \int_{|y_n| \leq p^{k_n} |y|^{a_n s + b_n}} |dy_n| = \\ & p^{-cs-d} \cdot \left(\frac{p-1}{p} \right)^n \cdot \frac{p-k_1(a_1 s + b_1 + 1)}{1 - p - (a_1 s + b_1 + 1)} \cdot \dots \cdot \frac{p-k_n(a_n s + b_n + 1)}{1 - p - (a_n s + b_n + 1)}, \quad (4.1) \end{aligned}$$

dove abbiamo usato la formula dell'Esercizio (2.3).

La proposizione è quindi quasi dimostrata: vogliamo giusto mostrare che il numeratore nell'equazione (4.1) non ha ulteriori poli. Per fare questo, notiamo che $(f \circ \pi)(P_i) \subset \mathbb{Z}_p$. Infatti f ha coefficienti in \mathbb{Z}_p , manda quindi per la nonarchimedietà $\mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_p$. Dunque per ogni P_i

$$|\lambda(y)| \cdot |y_1|^{a_1} \cdot \dots \cdot |y_n|^{a_n} \leq 1.$$

Da ciò viene che

$$p^{-c-k_1 a_1 - \dots - k_n} \leq 1$$

e il numeratore è limitato. □

4.2 Teorema di Igusa

Per finire dimostriamo un notevole risultato che mostra un legame inaspettato tra l'integrazione p -adica e il computo delle soluzioni di una equazione algebrica in $\mathbb{Z}/p^n\mathbb{Z} := A_{p^n}$.

Definizione 4.2. Sia $f \in \mathbb{Z}_1[X_1, \dots, X_n]$, per ogni intero positivo m definiamo

$$N_m := |\{x \in (A_{p^m})^n \mid f(\text{mod } p^m)(x) = 0\}|,$$

con la convenzione che $N_0 = 1$. La serie di Poincaré di f è

$$Q(f, t) := \sum_{m=0}^{\infty} N_m \cdot t^m.$$

Esempio 4.1. Prendiamo $f(x, y) = y - x^2$. Fissato x , la congruenza $y \equiv x^2 \pmod{p^m}$ determina y , otteniamo quindi che $N_m = p^m$ per ogni m . La serie di Poincaré è quindi la seguente:

$$Q(f, t) = 1 + pt + p^2t^2 + \dots = \frac{1+t}{1-pt^2}.$$

Proposizione 4.2.1.

$$Z(f, s) = Q\left(f, \frac{1}{p^{n+s}}\right) (1 - p^s) + p^s.$$

Dimostrazione. Per ogni $m \leq 0$, consideriamo $V_m \subset \mathbb{Z}_p^n$ definito come segue:

$$V_m := \{x \in \mathbb{Z}_p^n \mid |f(x)| \leq \frac{1}{p^m}\}.$$

In maniera tale che $V_m \setminus V_{m+1}$ siano gli insiemi di livello della f . Nel Lemma seguente mostreremo che

$$\mu(V_m) = N_m \cdot \frac{1}{p^{mn}}.$$

Assumendo questo per vero, decomponiamo il dominio nelle unioni disgiunte degli insiemi di livello.

$$Z(f, s) = \int_{\mathbb{Z}_p^n} |f(x)|^s d\mu =$$

$$\begin{aligned}
&= \mu(V_0) - \mu(V_1) + \frac{1}{p^s} (\mu(V_1) - \mu(V_2)) + \frac{1}{p^{2s}} (\mu(V_2) - \mu(V_3)) + \dots = \\
&= 1 - N_1 \cdot \frac{1}{p^n} + \frac{1}{p^s} \left(N_1 \cdot \frac{1}{p^n} - N_2 \cdot \frac{1}{p^{2n}} \right) + \frac{1}{p^{2s}} \left(N_2 \cdot \frac{1}{p^{2n}} - N_3 \cdot \frac{1}{p^{3n}} \right) + \dots = \\
&= \left(1 + N_1 \cdot \frac{1}{p^{n+s}} + N_2 \cdot \frac{1}{p^{2(n+s)}} + \dots \right) - p^s \left(N_1 \cdot \frac{1}{p^{n+s}} + N_2 \cdot \frac{1}{p^{2(n+s)}} + \dots \right) = \\
&= Q \left(f, \frac{1}{p^{n+s}} \right) - p^s \cdot Q \left(f, \frac{1}{p^{n+s}} - 1 \right).
\end{aligned}$$

□

Lemma 4.2.2. *Usando la notazione della proposizione precedente (4.2.1), si ha che $\mu(V_m) = N_m \cdot \frac{1}{p^{mn}}$.*

Dimostrazione. V_m è la controimmagine in \mathbb{Z}_p^n nel sottoinsieme

$$\{x \mid f(\text{mod } p^m)(x) = 0\} \subset (A_{p^m})^n.$$

Questa si può vedere come l'unione disgiunta di N_m traslazioni del nucleo della proiezione $\mathbb{Z}_p^n \rightarrow (A_{p^m})^n$, ovvero l'unione disgiunta delle traslazioni di $p^m \mathbb{Z}_p^n$. □

Teorema 4.2.3 (Teorema di Igusa). *Definite Q ed f come sopra,*

$Q(f, t)$ è una funzione razionale.

Dimostrazione. Con un semplice cambio di variabile $t = p^{-s}$ possiamo riscrivere il risultato della proposizione (4.2.1) come

$$Q(f, p^{-nt}) = \frac{tZ(f, s) - 1}{t - 1}.$$

Il teorema (4.1.1) ci dice che funzione zeta di f è una funzione razionale e il teorema è così dimostrato. □

Bibliografia

- [1] J.P. Serre (1996), *A Course in Arithmetic* (Springer).
- [2] Fernando Q.Gouvêa (1997), *p-adic Numbers: An Introduction* (Springer).
- [3] Jonathan Gleason, *Existence and uniqueness of Haar measure*.
- [4] Terence Tao, *An introduction to measure theory*.
- [5] Mihnea Popa, *Modern aspects of the cohomological study of varieties, Chapter 3: p-adic integration*.
- [6] I.R. Shafarevich (1974), *Basic Algebraic Geometry* (Springer-Verlag).